Osnove sigurnosti operacijskog sustava na poslužitelju

Debian

L301

OBRAZOVNI PROGRAMI srca

priručnik za polaznike

srce
Sveučilište u Zagrebu
Sveučilišni računski centar

Ovu su inačicu priručnika izradili:

Autor: Ante Jurjević

Recenzent: Darko Culej

Urednik: Dominik Kenđel

Lektor: dr. sc. Jasna Novak Milić

Sveučilište u Zagrebu

Sveučilišni računski centar

Josipa Marohnića 5, 10000 Zagreb

edu@srce.hr

ISBN 978-953-382-003-3 (meki uvez)

ISBN 978-953-382-004-0 (PDF)

Verzija priručnika L301-20221117

Sadržaj

Uvod

Trajanje poglavlja:
10 min

Ovaj tečaj uvodi polaznike u osnove sigurnosti operacijskog sustava Debian. Tečaj služi kao za proširenje stečenih znanja iz svih prethodnih tečajeva (L101, L102, L201 i L202) te zajedno s njima predstavlja osnovu za napredno korištenje operacijskog sustava Linux. Operacijski sustav koji se koristi je Debian, konkretno Debian 11 za koji su izrađene vježbe.

Po završetku ovoga tečaja moći ćete:

- ograničiti pristup poslužitelju
- prilagoditi sigurnosne postavke servisa
- uspostaviti mehanizme zaštite od napada
- osigurati autentikacijske servise, mail, web i servise za dijeljenje datoteka
- uspostaviti nadzor sigurnosti poslužitelja
- uspostaviti sigurnosnu pohranu poslužitelja.

1. Osnove sigurnosti

Trajanje poglavlja:
25 min

Po završetku ove cjeline moći ćete:

- opisati što obuhvaća pojam računalna sigurnost
- imenovati najčešće prijetnje sigurnosti računala i načine prevencije

Cjelina obrađuje osnove sigurnosti, najčešće mogućnosti zlouporabe računalnih sustava i najčešće sigurnosne propuste administratora.

1.1. Osnove sigurnosti

1.1.1. Što je računalna sigurnost?

Mogućnost zlouporabe računalnih sustava je višestruka i višeslojna. Podaci koji putuju Internetom mogu se presresti ili izmijeniti. Legitimni korisnici mogu zlonamjerno iskoristiti računalni sustav ili neovlaštena osoba može zaobići zaštite sustava kroz postojeće sigurnosne propuste u softveru ili iskorištavanjem loše administracije. Računalna sigurnost bavi se prevencijom i pravovremenom detekcijom nedozvoljenoga korištenja računalnih resursa.

1.1.2. Prijetnje sigurnosti računala

Nekorišteni servisi i otvoreni portovi

Jednostavne poslužitelje je jednostavnije zaštiti od kompleksnijih. Puna instalacija operacijskog sustava *Debian 11* (u nastavku *Debian*) sadrži više od 500 instaliranih paketa i biblioteka što potencijalno može biti problem jer neki servisi ili portovi su po zadanim postavkama uključeni. Neželjeni servisi mogu uzrokovati nepotrebni promet ili korištenje resursa poslužitelja, te se isti mogu koristiti kao sredstvo zloupotrebe. Pri instalaciji preporučeno je odabrati minimalnu opciju instaliranih paketa i ovisno o svrsi poslužitelja instalirati dodatne pakete. Potrebno je skenirati mrežna sučelja za otkrivanje portova i isključiti one koji se ne koriste.

Ranjivosti u kôdu i konfiguraciji

Napadač može kroz ranjivost u servisu kompromitirati cijeli sustav i sve podatke koji su na njemu, i potencijalno može provaliti na ostale poslužitelje na istoj podmreži. Ranjivosti unutar servisa mogu proći nezapaženo tijekom razvoja i testiranja, a te ranjivosti mogu potencijalno dati napadaču administratorske ovlasti. Većina instaliranih paketa i biblioteka koji se instaliraju operacijskim sustavom *Debian* su stabilni i temeljito testirani. Ne postoji potpuno siguran softver, ali kod većine servisa koji se koriste u produkciji i javno su dostupni, bugovi su pronađeni i popravljeni, a kôd je promijenjen da bi odgovarao sigurnosnim politikama.

*Web-s*tranice http://www.cert.org i https://www.securityfocus.com/ objavljuju greške u kôdu i/ili načine na kojih ih se može iskoristiti. Administratori moraju aktivno pratiti i pravovremeno krpati sporne greške u kôdu kako njihovi sustavi ne bi bili ugroženi.

Inherentno nesigurni servisi

Postoje servisi koji su napravljeni da se koriste samo unutar sigurnih mreža, što ih čini inherentno nesigurnima kad se koriste na Internetu. Primjer takvih servisa su telnet i *File Transfer Protocol* (ftp) koji koriste nekriptirani promet u kojem se mogu pronaći korisnička imena i lozinke za autentikaciju. Ako netko prati mrežni promet između dvaju poslužitelja, može doći do tih osjetljivih podataka.

Još jedan primjer nesigurnih servisa su NFS i NIS. NFS po zadanim postavkama nema autentikaciju ili sigurnosni mehanizam koji bi spriječio da se NFS *share* montira na drugi operacijski sustav i da se pregledavaju podaci na njemu. NIS, također, posjeduje osjetljive informacije koje mora znati svako računalo na mreži uključujući lozinke, prava nad datotekama ili baze podataka.

Preporučene preventivne mjere su korištenje razmjene kriptografskih ključeva, jednokratne lozinke, kriptirana autentikacija i kriptirana komunikacija.

Primjeri ne sigurnih protokola i njihove sigurne alternative:

- http > https
- ftp > sftp (paket openssh)
- telnet > ssh (paket openssh)
- pop3 > imap/imaps.

Nesigurne lozinke i ključevi

Lozinke su primarni način autentikacije korisnika, a jedan od lakših načina kompromitiranja sustava je koristeći nesigurne i zadane lozinke.

Zadane lozinke je potrebno promijeniti odmah nakon instalacije operacijskog sustava. Sigurni servisi ponekad u svojim paketima imaju zadane sigurne ključeve za razvoj ili testiranje. Ako ti ključevi ostanu nepromijenjeni i koriste se u produkciji, svi korisnici s istim zadanim ključevima mogu imati pristup tom resursu i svim osjetljivim informacijama koje sadrži.

Neke od sigurnosnih metoda upravljanja lozinkama automatski provjeravaju kvalitetu lozinke i ne dopuštaju nesigurne lozinke, te nakon određenog vremenskog razdoblja zahtijeva od korisnika da promijeni lozinku.

Napadi *Denial of Service* (DoS)

Napade DoS izvršava jedan ili više napadača šaljući veliku količinu mrežnih paketa prema operacijskom sustavu. Na ovaj način legitimni korisnici nisu u mogućnosti doći do servisa ili resursa koji nalaze na tom operacijskom sustavu. Napadi DoS mogu se spriječiti sustavima za otkrivanje i sprječavanje napada NIDS (*network intrusion detection system*) ili HIDS (*host intrusion detection system*).

1.1.3. Najveće sigurnosne pogreške

Osim ranjivosti servisa i operacijskoga sustava, najčešće provale u informacijske sisteme događaju se i zbog administratorskih grešaka. Ovo su najčešći administratorski propusti prema SANS-u (*SysAdmin, Audit, Network, Security Institute*):

1) Povezivanje poslužitelja na Internet prije sigurnosnog očvršćivanja.
2) Povezivanje testnih i razvojnih operacijskih sustava na Internet sa zadanim korisničkim računima i lozinkama.
3) Neažuriranje operacijskoga sustava nakon otkrivanja sigurnosnih ranjivosti.
4) Korištenje protokola *telnet* i drugih protokola za upravljanje operacijskim sustavima, usmjerivačima i vatrozidima čiji mrežni promet nije kriptiran.
5) Dodavanje ili promjena korisničkih lozinki korisnicima koji nisu autenticirani, tj. nije im se potvrdio identitet.
6) Nepostavljeno, krivo podešavanje ili neodržavanje testiranja sigurnosnih kopija.
7) Instalacija, pokretanje i održavanje nepotrebnih servisa, posebno servisa *ftpd, telnetd, finger, rpc, mail i rservices*.
8) Implementiranje vatrozida s pravilima koji ne zaustavljaju zlućudan mrežni promet.
9) Ne implementiranje ili ažuriranje softvera za detekciju virusa ili napada.
10) Nedovoljno educiranje korisnika o tome na što je potrebno obratiti pozornost i što napraviti ako primijete potencijalni sigurnosti problem.
11) Dozvoljavanje neiskusnih i necertificiranim osobama da vode brigu o sigurnosti važnih sustava.

1.1.4. Zanimljivi izvori

Poveznice:

- http://www.tldp.org/HOWTO/Security-HOWTO/x82.html
- https://dkorunic.net/pdf/Linux-sigurnost.pdf
- https://www.sans.org/security-resources/mistakes

2. Ograničavanje pristupa

Trajanje poglavlja:
280 min

Po završetku ove cjeline moći ćete:

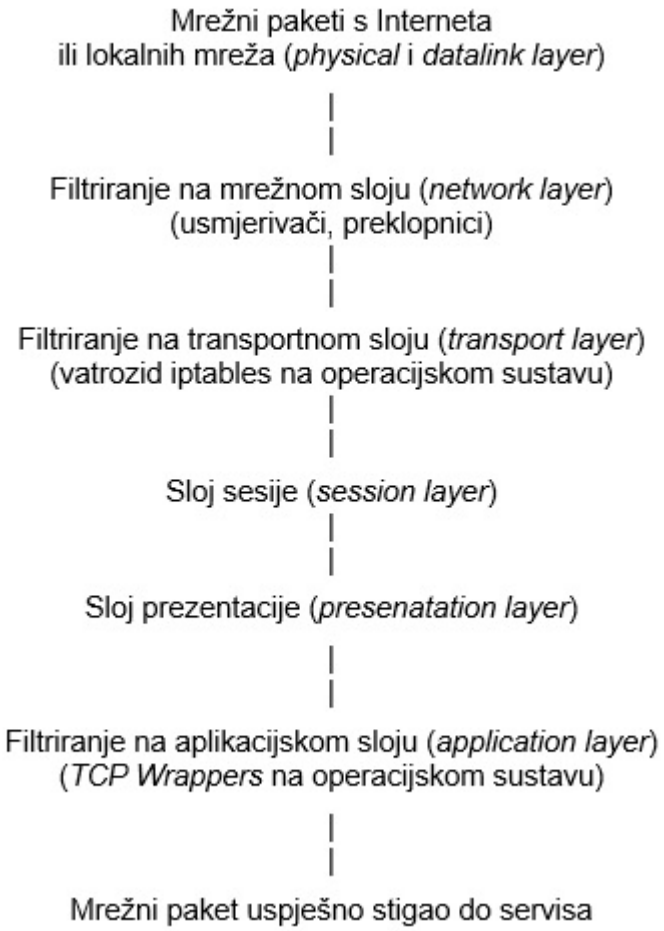
- opisati mogućnosti filtriranja po OSI (Open Systems Interconnection) slojevima
- primijeniti mogućnosti servisa iptables kako bi se mrežni promet filtrirao po IP adresi, portu, mrežnom sučelju i zabilježio u dnevničkom zapisu sav onemogućeni mrežni promet
- koristiti servis TCP Wrappers za filtriranje na osnovi servisnoga procesa (daemona)
- razlikovati pojmove autentikacija i autorizacija
- omogućiti ili onemogućiti spajanje pojedinih korisnika protokolom SSH
- ograničiti pristup DNS servisu bind9 ili njegovim funkcijama koristeći liste za kontrolu pristupa
- ograničiti pristup servisu postfix za svaki korak SMTP komunikacije
- omogućiti ili onemogućiti pristup direktorijima, datotekama ili lokaciji koristeći apache2 modul mod_access potpuno ili djelomično onemogućiti spajanje na bazu podatka
- primijeniti pravila za translatiranje izvorišnih i odredišnih IP adresa koristeći mehanizam NAT
- omogućiti ili onemogućiti pristup resursima na Internetu lokalnim računalima koristeći servis proxy.

Ova cjelina obrađuje načine ograničavanja pristupa koristeći servis *iptables* kao osnovni alat za upravljanje vatrozidom i *TCP Wrapper* za detaljniju kontrolu pristupa prema *Linux* servisima. Ograničavanje može biti definirano i na svakom pojedinom servisu kao što je *bind, apache2, postfix i mysql* te njihovim mogućnostima. Na kraju cjeline obrađuje se filtriranje izravnog pristupa koji omogućuje ili onemogućuje pristup lokalnih mreža Internetu i njegovim resursima.

2.1. Načini ograničavanja pristupa

2.1.1. Filtriranje mrežnog prometa prema OSI slojevima

Mrežni promet koji primaju operacijski sustav i njegovi servisi može se filtrirati (pristup se omogućuje ili onemogućuje) na nekoliko razina.



Tijekom rješavanja problema na operacijskom sustavu koji se tiču pristupa mreži potrebno je obratiti pozornost na sve gore navedene slojeve.

2.1.2. Pristupne liste na mrežnom sloju

Ograničavanje pristupa može se napraviti na mrežnom sloju, tj. prije nego što promet dođe do operacijskog sustava i njegovih servisa.

Na usmjerivaču (*router*) i preklopniku (*switch*), pored opcija usmjeravanja i prosljeđivanja dolaznog i odlaznog podatkovnog prometa, mogu se izraditi pristupne liste (*Access Control List, ACL*). Pristupnim listama omogućuje se ili onemogućuje pristup resursima na mreži, prema tome ista pravila se odnose i na operacijske sustave koji su spojeni na tu mrežu.

U pristupnim listama kreiraju se pravila koja mogu sadržavati izvorišnu IP adresu, odredišnu IP adresu, protokol, MAC adrese, port itd.

Dolazni promet:

Protokol	Port	Izvorišna IP adresa	Dopusti/ zabrani	Opis
TCP	80	0.0.0.0/0	Dopusti	Dopusti sav dolazni HTTP promet sa svih IPv4 adresa
TCP	443	0.0.0.0/0	Dopusti	Dopusti sav dolazni HTTPS promet svih IPv4 adresa
TCP	22	192.0.2.0/24	Dopusti	Dopusti dolazni SSH (Secure Shell) promet samo iz privatne mreže raspona 192.168.0.0 – 192.168.255.255
TCP	3389	192.0.2.0/24	Dopusti	Dopusti dolazni RDP promet samo iz privatne mreže raspona 192.168.0.0 – 192.168.255.255
All	All	0.0.0.0/0	Zabrani	Zabrani sav dolazeći IPv4 promet koji nije definiran prethodnim pravilima

Odlazni promet:

Protokol	Port	Izvorišna IP adresa	Dopusti/ zabrani	Opis
TCP	80	0.0.0.0/0	Dopusti	Dopusti sav odlazni HTTP promet sa svih IPv4 adresa
TCP	443	0.0.0.0/0	Dopusti	Dopusti sav odlazni HTTPS promet sa svih IPv4 adresa
TCP	32768-65535	0.0.0.0/0	Dopusti	Dopusti sav odlazni IPv4 promet prema prema rasponu TCP portova od 32768 do 65535
All	All	0.0.0.0/0	Zabrani	Zabrani sav odlazeći IPv4 promet koji nije definiran prethodnim pravilima

2.1.3. Vatrozid (servis iptables)

Vatrozid je najčešće prva linija obrane od napada na poslužitelj, njegove servise i resurse. Uz sprječavanja napada, vatrozid se može koristiti i kao sustav upozoravanja na napade.

Vatrozid se koristi na tri načina:

1) odbijanje neželjenog i zlućudnog dolaznog prometa
2) sprječavanje neželjenog i zlućudnog odlaznog prometa
3) zapis u dnevničkom zapisu neželjenog, sumnjivog i zlućudnog prometa.

Iptables

Na distribuciji *Debian GNU/Linux* vatrozid *iptables* donosi istoimeni paket i dio je standardne instalacije. *Iptables* imaju tri standardne tablice – Filter, Nat i Mangle.

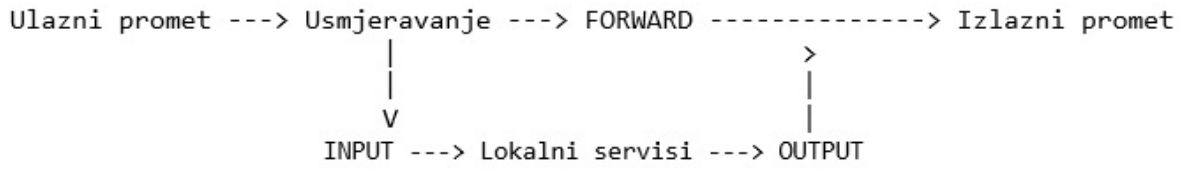
Napomena

Tablica NAT (*Network Address Translation*) koristi se za translaciju izvorišnih i/ili odredišnih IP adresa paketa koji prolazi kroz usmjerivač ili vatrozid, a tablica Mangle za modificiranje IP paketa. Tablica NAT je obrađena u poglavlju „Onemogućavanje izravnoga pristupa", a tablica Mangle se ne koristi za vatrozid pa nije obrađena u ovom tečaju.

Filter tablica ima tri lanca:

- INPUT – svi paketi koje poslužitelj prima.
- OUTPUT – svi paketi koje poslužitelj šalje.
- FORWARD – svi paketi koji nisu namijenjeni niti su podrijetlom iz operacijskog sustava, ali se preusmjeravaju kroz njega. Ovaj se lanac koristi kada koristimo poslužitelj kao usmjerivač.

Slikom je prikazan tipični promet kroz sustav. Kao što se vidi na slici, svi paketi prolaze kroz jedan od triju lanaca (ulaz, izlaz ili prosljeđivanje) te je vatrozidom moguće filtrirati sve pakete korištenjem jednog od tih triju lanaca.



`Iptables` – osnovna naredba za dodavanje i brisanje pravila vatrozida. Osnovna sintaksa je:

```
iptables [-t tablica] naredba lanac akcija
```

`Iptables` pravilo kombinira tablicu, lanac, akciju, izvorišnu ili odredišnu IP adresu, port ili neki drugi atribut za određeni paket.

Najčešće naredbe su:

Naredba	Opis
`-a, --append`	Dodavanje pravila na kraj lanca.
`-C, --check`	Provjeravanje postojanja pravila.
`-D, --delete`	Brisanje pravila iz lanca.
`-I, --insert`	Ubacivanje pravila u lanac (na određeno mjesto u lancu ili na početak).
`-L, --list`	Ispis pravila.
`-F, --flush`	Brisanje svih pravila (u lancu, ako je on naveden ili ako su sva pravila ista u svim lancima).

Najčešće akcije koje se koriste u tablici filter:

Akcija	Opis
DROP	Odbijanje paketa.
ACCEPT	Prihvaćanje paketa.
QUEUE	Prosljeđivanje paketa u prostor korisničkih procesa.
RETURN	Povratak paketa u prethodni lanac (kad se rabi gniježđenje lanaca).
REJECT	Slično kao DROP, ali pošiljatelj paketa dobiva povratnu informaciju da je paket odbijen. Rijeđe se koristi od opcije DROP jer generira dodatni promet koji može zakrčiti mrežni promet u slučaju napada DoS.

Politika lanca

Mrežni paket se uspoređuje s pravilima unutar lanca i primjenjuje se prvo pravilo s kojim se paket podudara. Kad u lancu nema pravila s kojim se paket podudara, primjenjuje se politika lanca. Ako je ta politika ACCEPT svi paketi će biti propušteni. Da bi vatrozid obavljao svoju funkciju, potrebno je promijeniti politike na DROP. Na ovaj način se svi paketi odbacuju, osim ako nisu eksplicitno propušteni u spomenutim tablicama.

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
COMMIT
```

Drugi način blokiranja prometa, a bez upotrebe korištenja politike lanca DROP, je stvaranje pravila koje će zabraniti sav promet i staviti ga na kraj lanca INPUT:

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
--append INPUT --jump DROP
COMMIT
```

Kod gornjih dvaju primjera onemogućen je sav promet prema i od poslužitelja.

Dozvoljavanje i onemogućavanje prometa

Sljedeća pravila propustit će promet elektronske pošte, bio on *sendmail* ili *postfix,* tj. promet će biti propušten za port 25.

```
--append INPUT --protocol tcp --dport 25 --match state --state NEW,ESTABLISHED --jump ACCEPT
--append OUTPUT --protocol tcp --sport 25 --match state --state ESTABLISHED --jump ACCEPT
```

Za promet *web*-stranica potrebno je propustiti port 80 i 443:

```
--append INPUT --protocol tcp --dport 80 --match state --state NEW,ESTABLISHED --jump ACCEPT
--append INPUT --protocol tcp --dport443 --match state --state NEW,ESTABLISHED --jump ACCEPT
--append OUTPUT --protocol tcp --sport 80 --match state --state NEW,ESTABLISHED --jump ACCEPT
--append OUTPUT --protocol tcp --sport 443 --match state --state NEW,ESTABLISHED --jump ACCEPT
```

Za udaljenu administraciju poslužitelja potrebno je omogućiti i SSH promet:

```
--append INPUT --protocol tcp --dport 22 --match state --state NEW,ESTABLISHED --jump ACCEPT
--append OUTPUT --protocol tcp --sport 22--match state --state ESTABLISHED --jump ACCEPT
```

Blokiranje prometa prema dolaznoj IP adresi:

```
--append INPUT --source 192.168.100.0 --jump DROP
```

Kako bi se samo određene IP adrese ili podmreže mogle spojiti na SSH, potrebno je navesti izvor.

```
   --append INPUT --protocol tcp --source 192.168.100.0/24 --dport 22 --match state --state
NEW,ESTABLISHED --jump ACCEPT
   --append OUTPUT --protocol tcp --sport 22 --match state --state ESTABLISHED --jump ACCEPT
```

Sljedeće pravilo omogućava SSH spajanje samo prema podmreži 192.168.100.0/24.

```
--append OUTPUT--protocol tcp --destination 192.168.100.0/24 --dport 22 --match state --state
NEW,ESTABLISHED --jump ACCEPT
--append INPUT--protocol tcp --sport 22 --match state --state ESTABLISHED -j ACCEPT
```

Dozvoljavanje i onemogućavanje prometa prema mrežnim sučeljima:

```
--append INPUT --in-interface eth1 --source 192.168.100.0/24 --jump DROP
--append INPUT--in-interface eth0 --protocol tcp --dport 22 --match state --state
NEW,ESTABLISHED --jump ACCEPT
--append INPUT--in-interface eth1 --destination 192.168.100.0/24 --jump DROP
--append OUTPUT --out-interface eth0 --protocol tcp --sport 22 --match state --state
ESTABLISHED --jump ACCEPT
```

`Iptables` pravila primjenjuju se po njihovom redoslijedu od početka prema kraju. Ako se prvo pravilo primjeni na određeni paket, tada se taj paket neće provjeravati prema ostalim pravilima. Pravilo DROP nalazi se na kraju kako bi blokiralo sav promet koji nije obuhvatilo niti jedno pravilo prije.

Ispis i brisanje pravila vatrozida

Naredba `Iptables` koristi se `-nL` opcijom `-nL` za prikaz važećih aktualnih pravila vatrozida.

```
$ sudo iptables -nL
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:80
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:443

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

Naredbom `iptables -F` ili `iptables --flush` brišu se sva aktivna pravila iz vatrozida. Potreban je oprez pri korištenju te naredbe, jer se tada koriste samo politike nad lancima, a ako su te politike DROP, tada računalo postaje nedostupno s mreže.

Spremanje i testiranje pravila vatrozida

`iptables-save` - naredba za spremanje trenutačnih pravila vatrozida. Unaprijed je definirano da ta naredba šalje *output* na *stdout* pa treba napraviti preusmjeravanje u datoteku:

```
$ sudo iptables-save > /etc/iptables/rules.v4

$ cat /etc/iptables/rules.v4
# Generated by iptables-save v1.6.0 on Mon Jul 16 06:43:47 2018
*filter
:INPUT ACCEPT [365:21460]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [196:17000]
--append INPUT -p tcp -m state --state NEW -m tcp --dport 443 --jump ACCEPT
```

```
--append INPUT -p tcp -m state --state NEW -m tcp --dport 80 --jump ACCEPT
COMMIT
```

Nakon spremanja `iptables` pravila u datoteku `/etc/iptables/rules.v4`, tekstualnim uređivačem naprave se potrebne izmjene.

`iptables-apply` je naredba za primjenu pravila sa zaštitom od prekidanja vlastite SSH veze. Naredba primijeni željeni skup pravila i čeka potvrdu korisnika.

```
$ sudo iptables-apply /etc/iptables/rules.v4
Applying new iptables rules from '/etc/iptables/rules.v4'... done.
Can you establish NEW connections to the machine? (y/N)
```

Ako lošom konfiguracijom korisnik prekine vlastitu vezu, tada naredba neće dobiti korisnikovu potvrdu. U tom će slučaju po isteku vremena za odgovor naredba vratiti konfiguraciju vatrozida na prijašnju verziju:

```
Timeout! Something happened (or did not). Better play it safe...
Reverting to old iptables rules... done.
```

Kako bi `iptables` pravila bila aktivna i nakon ponovnog pokretanja operacijskoga sustava, potrebno je instalirati alat *iptables-persistent* i pokrenuti naredbe za spremanje *iptables* pravila:

```
$ sudo apt-get install iptables-persistent
$ sudo iptables-save > /etc/iptables/rules.v4
$ sudo ip6tables-save > /etc/iptables/rules.v6
```

Loopback, ICMP i uspostavljeni promet

Pri stvaranju pravila vatrozida, preporučuje se postaviti nekoliko pravila kako bi se omogućio legitimni mrežni promet. Sljedeća pravila omogućavaju *loopback*, ICMP (ping) i bilo koji uspostavljeni promet.

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]

--append INPUT --in-interface lo --jump ACCEPT
--append INPUT --protocol icmp --jump ACCEPT
--append INPUT --match state --state ESTABLISHED,RELATED --jump ACCEPT
```

```
--append OUTPUT --out-interface lo --jump ACCEPT
--append OUTPUT --protocol icmp --jump ACCEPT
--append OUTPUT --match state --state ESTABLISHED,RELATED --jump ACCEPT

COMMIT
```

Bilježenje dnevničkih zapisa

Za bilježenje prometa u dnevničkom zapisu LOG pravilo se postavlja na kraj lanca. LOG se može staviti prije bilo kojeg drugog pravila koji omogućava mrežni promet, ali se ne preporučuje jer takvo pravilo generira velik broj dnevničkih zapisa.

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]

--append INPUT --in-interface lo --jump ACCEPT
--append INPUT --protocol icmp --jump ACCEPT
--append INPUT --match state --state ESTABLISHED,RELATED --jump ACCEPT
--append INPUT --jump LOG --log-prefix "iptables-input-drop "

--append OUTPUT --out-interface lo --jump ACCEPT
--append OUTPUT --protocol icmp --jump ACCEPT
--append OUTPUT --out-interface state --state ESTABLISHED,RELATED --jump
ACCEPT
--append OUTPUT --jump LOG --log-prefix "iptables-output-drop "

COMMIT
```

Primjer dnevničkoga zapisa za DROP pravilo:

```
$ tail -f /var/log/messages
Jan 31 13:36:15 node2 kernel: [ 1178.411004] iptables-drop IN=enp0s3
OUT= MAC=08:00:27:00:6d:7d:0a:00:27:00:00:0d:08:00 SRC=192.168.56.1
DST=192.168.56.202 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=12010 DF
PROTO=TCP SPT=54302 DPT=23 WINDOW=64240 RES=0x00 SYN URGP=0

Jan 31 13:36:18 node2 kernel: [ 1181.411434] iptables-drop IN=enp0s3
OUT= MAC=08:00:27:00:6d:7d:0a:00:27:00:00:0d:08:00 SRC=192.168.56.1
DST=192.168.56.202 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=12012 DF
PROTO=TCP SPT=54302 DPT=23 WINDOW=64240 RES=0x00 SYN URGP=0

Jan 31 13:36:24 node2 kernel: [ 1187.411676] iptables-drop IN=enp0s3
OUT= MAC=08:00:27:00:6d:7d:0a:00:27:00:00:0d:08:00 SRC=192.168.56.1
```

```
DST=192.168.56.202 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=12014 DF
PROTO=TCP SPT=54302 DPT=23 WINDOW=64240 RES=0x00 SYN URGP=0
```

2.1.4. Servis TCP Wrappers

Servis *TCP Wrappers* koristi se za kontrolu pristupa na aplikacijskom sloju za podržane servise kojima se pristupa preko mreže. *TCP Wrapper* može kontrolirati koji vanjski sustavi (prema imenu računala, IP adresi, podmreži) i korisnici mogu koristiti definirane servise. Na primjer, sprečava korisnike s nepoznate IP adrese da koriste servis FTP ili se spajaju na servisni proces *sshd*.

Većina servisa već dolazi s uključenom podrškom za *TCP Wrappers*, kao što su pop3, ftp, sshd, telnet itd. Naredbom `ldd` provjerava se ima li servisni proces ovisnost o biblioteci libwrap.so.

```
$ whereis sshd
sshd: /usr/sbin/sshd /usr/share/man/man8/sshd.8.gz
$ ldd /usr/sbin/sshd | grep libwrap.so
libwrap.so.0 => /lib/x86_64-linux-gnu/libwrap.so.0 (0x00007f51800e6000)
```

Za konfiguraciju se koriste dvije datoteke, `/etc/hosts.allow` za omogućavanje pristupa određenom servisu i `/etc/hosts.deny` za onemogućavanje pristupa. Kada *TCP Wrapper* primi zahtjev prema određenom servisu, prvo u datoteci `/etc/hosts.allow` provjeri podudara li se zahtjev s nekim pravilom. Ako pronađe pravilo koje se podudara, povezivanje se omogućuje. Ako se ne pronađe pravilo u datoteci `hosts.allow` provjera pravila se vrši u datoteci `hosts.allow`. Ako u datoteci `hosts.deny` postoji pravilo koje se podudara, promet se odbija. Ako ne pronađe odgovarajuće pravilo, dozvoljava se pristup servisu.

Kod uređivanja `hosts.allow` i `hosts.deny` svako pravilo mora biti u svom redu. Prazni redovi i redovi koji počinju komentarom (#) se ignoriraju.

Sintaksa konfiguracije za obje datoteke je ista:

```
<lista_servisnih_procesa> : <lista_klijenata> [: <naredba_ljuske_1> :
<naredba_ljuske_2> : …]
```

Opcije konfiguracije su:

Mogućnost	Objašnjenje
Lista servisnih procesa	Popis naziva procesa (ne ime servisa) koji se odvajaju zarezom ili zamjenskoga znaka ALL (wildcard).
Lista klijenata	Popis imena računala, IP adresa, podmreža ili zamjenskih znakova koji se odvajaju zarezom.
Opcija	Jedna ili popis akcija (odvojenih dvotočkom) koje se izvode pri aktivaciji pravila. Akcije dopuštaju ili zabranjuju pristup, pokreću naredbe ljuske itd.

Mogućnosti zamjenskih znakova:

Mogućnost	Objašnjenje
ALL	Podudara se sa svime. Koristi se za klijente ili servisne procese.
LOCAL	Podudara se lokalnim imenom računala bez točke u njegovu FQDN-u. Na primjer, localhost.
KNOWN	Podudara se s bilo kojim poznatim korisnikom ili bilo kojim imenom računala čije su ime i IP adresa poznati, tj. provjerava se imena računala na DNS poslužitelju, a korisnici protokolom identd.
UNKNOWN	Obratno od KNOWN.
PARANOID	Podudara se ako reverse DNS lookup (prvo po IP adresi traži ime računala, zatim obratno) vrati drugačiju IP adresu.

Napomena

Zamjenske znakove KNOWN, UNKNOWN i PARANOID preporučuje se koristiti s oprezom jer za ispravan rad oslanjaju se na dostupnost DNS poslužitelja.

U sljedećem primjeru dozvoljeno je samo spajanje na servisne procese *sshd* i *vsftpd* s *localhosta* ili s IP adrese 192.168.0.100. Linija ALL:ALL na kraju datoteke hosts.deny zabranit će sav ostali mrežni promet prema servisnim procesima.

```
$ sudo vim /etc/hosts.allow
sshd, vsftpd : 192.168.0.100,LOCAL

$ sudo vim /etc/hosts.deny
ALL : ALL
```

Sljedeće pravilo ograničava pristup do servisnih procesa sshd i vsftpd ako se nalazi u **hosts.deny** ili omogućava pristup ako se nalazi u `hosts.allow`, ako upit dolazi s domene .srce.hr

```
sshd, vsftpd : .srce.hr
```

Sljedeći primjer ima dvije opcije, naredbu ljuske koja zabilježava u dnevničkom zapisu pokušaje SSH spajanja i `deny`. Kosa crta (`\`) sprječava greške koje bi se mogle dogoditi zbog duljine pravila.

```
sshd : .srce.hr  \
       : spawn /bin/echo `/bin/date` access denied>>/var/log/sshd.log \
       : deny
```

Napomena

Servisni proces `vsftpd :` kako bi se kontrolirao pristup preko *TCP Wrapper*a potrebno je dodati konfiguraciju `tcp_wrappers=yes` u datoteku `./etc/vsftpd.conf` i ponovno pokrenuti servisni proces `vsftpd` naredbom `systemctl status vsftpd`.

2.1.5. Autentikacija i autorizacija

Autentikacija je proces potvrđivanja identiteta korisnika koji pokušava pristupiti sustavu ili potvrda autentičnosti mrežnoga prometa.

Autentikacija može biti bazirana na nečemu što osoba zna, npr. korisničko ime i lozinka. Dozvoljavanje pristupa nekom sustavu može se bazirati i na nečemu što osoba ili poslužitelj posjeduju, kao što je IP adresa ili digitalni potpis. Operacijski sustav uspoređuje primljene vjerodajnice s onima koje posjeduje. Ako su vjerodajnice važeće i korisnički račun je aktivan, korisnik je autenticiran i može pristupiti sustavu.

U slučaju autentikacije ključevima koriste se javni i privatni ključ. Korisnik na svom lokalnom računalu ima privatni ključ, a na udaljenom računalu javni ključ. Udaljeno računalo koristeći javni ključ izrađuje nasumični podatak, kriptira ga s javnim ključem i šalje korisniku. Ako korisnik posjeduje privatni ključ, pročita taj nasumični podatak i vrati ga udaljenom računalu, potvrđuje svoj identitet. Pri izradi ključa moguće je kriptirati privatni ključ s kvalitetnom lozinkom kako bi ga učinili još sigurnijim.

Autentikacija ključevima je sigurnija alternativa autentikacije lozinkom jer privatni ključ nikad ne napušta računalo, dok se lozinke, iako kriptirane, šalju nesigurnim mrežama. U scenariju gdje netko presretne SSL/TLS (*Secure Sockets Layer* / *Transport Layer Security*) promet i uspije ga dekriptirati (koristeći privatni ključ računala ili ako korisnik prihvati krivi javni ključ kad se spaja na udaljeno računalo) ili ima pristup računalu, kriptirana lozinka će biti poznata (kriptiranu lozinku moguće je pokušati otkriti alatima kao što je *John the Ripper*). U slučaju autentikacije ključevima, gdje je privatni ključ zaštićen kvalitetnom lozinkom, podaci korisnika neće biti kompromitirani. Čak i ako je jedno računalo kompromitirano, druga računala s istim javnim ključem neće biti.

Dakle, korištenje ključeva je znatno sigurnije od korištenja lozinki koje možda mogu biti dekriptirane ako je kompromitirano računalo, poslužitelj ili njihova sesija.

Autorizacija

Nakon što se korisnik, program ili poslužitelj uspješno autenticira, postupak autorizacije određuje prava pristupa resursima operacijskoga sustava. Ta prava mogu se odnositi na upravljanje određenim servisom, prava pisanja, čitanja ili izvršavanja datoteka, spajanje na određene mrežne portove itd.

2.1.6. Zanimljivi izvori

Poveznice:

- https://www.cyberciti.biz/tips/linux-iptables-examples.html
- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-tcp_wrappers_and_xinetd-tcp_wrappers_configuration_files

2.1.7. Vježba 1: Podešavanje vatrozida

1. Prije početka rada odaberite sliku stanja virtualnoga računala (*Snapshot*) **slika_jedan** za početak vježbe.

2. Prijavite se na računalo kao korisnik **linux1**. U GUI-ju pokrenite **Terminal** (*Activities* → **Terminal**). Izvršite **su** - naredbu da postanete administrator (lozinka: linux1).

3. Provjerite zadana *iptables* pravila sljedećom naredbom:

   ```
   # iptables -nL
   ```

4. Kakva je politika lanaca na zadanim pravilima? Je li mrežni promet omogućen ili onemogućen?

   _____

   _____

5. Spremite trenutačna pravila vatrozida u **/etc/iptables/rules.v4**

   ```
   # iptables-save > /etc/iptables/rules.v4
   ```

6. Otvorite datoteku koristeći **vim** tekstualni uređivač, promijenite politiku svih lanaca na DROP i dodajte preporučene postavke za vatrozid.

```
# vim /etc/iptables/rules.v4
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]

--append INPUT --in-interface lo --jump ACCEPT
--append INPUT --protocol icmp --jump ACCEPT
--append INPUT --match state --state ESTABLISHED,RELATED --jump ACCEPT

--append OUTPUT --out-interface lo --jump ACCEPT
--append OUTPUT --protocol icmp --jump ACCEPT
--append OUTPUT --match state --state ESTABLISHED,RELATED --jump ACCEPT
COMMIT
```

7. Za što se koriste gore upisne postavke za INPUT i OUTPUT lance?

8. Otvorite *web*-preglednik u Windows okruženju i upišite URL http://localhost.

9. Možete li pristupiti testnoj stranici *web*-servisa?

   _____

10. Provjerite *iptables* pravila.

11. Za što je omogućen pristup ako je definirano DROP pravilo u **/etc/iptables/rules.v4**? Što je potrebno napraviti za ažuriranje pravila servisa *iptables*?

12. Ažurirajte potrebna pravila sljedećom naredbom:

```
# iptables-apply /etc/iptables/rules.v4
```

13. Potvrdite pomoću znaka 'y' primjenu pravila.

```
Can you establish NEW connections to the machine? (y/N)
```

14. Ispišite na ekranu pravila servisa *iptables* sljedećom naredbom i provjerite ispravnost konfiguracije.

15. Otvorite *web*-preglednik u Windows okruženju i upišite URL http://localhost.

16. Možete li sada pristupiti testnoj stranici web-servisa? _____

17. U GUI-ju pokrenite **Terminal** (*Activities* → **Terminal**) i kao administrator dodajte konfiguraciju za bilježenje dnevničkoga zapisa DROP pravila:

```
# vim /etc/iptables/rules.v4
*filter
...
--append INPUT --jump LOG --log-prefix "iptables-input-drop "
--append OUTPUT --jump LOG --log-prefix "iptables-output-drop "
COMMIT
```

18. Pokrenite terminal i primijenite pravila iz datoteke **/etc/iptables/rules.v4**

```
# iptables-apply /etc/iptables/rules.v4
```

19. Potvrdite pomoću znaka 'y' primjenu pravila.

```
Can you establish NEW connections to the machine? (y/N)
```

20. Provjerite *iptables* pravila.

21. Naredbom *tail -f* pratite dnevničke zapise za pravilo DROP:

```
# tail -f /var/log/messages
```

22. Otvorite novi prozor *web*-preglednika u *Windows* okruženju i upišite URL http://localhost. Prikazuje li se *web*-stranica?

_____

23. Koje informacije možete saznati iz dnevničkog zapisa vezanoga za pravilo DROP?

_____

24. Dodajte pravila za omogućavanje mrežnoga prometa za port 80 i primijenite pravila naredbom **iptables-apply**:

```
# vim /etc/iptables/rules.v4
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
--append INPUT --protocol tcp --dport 80 --match state \n
--state NEW,ESTABLISHED --jump ACCEPT
--append INPUT --jump LOG --log-prefix "iptables-input-drop "

--append OUTPUT --protocol tcp --sport 80 --match state \n
--state NEW,ESTABLISHED --jump ACCEPT
--append OUTPUT --jump LOG --log-prefix "iptables-output-drop "
COMMIT

# iptables-apply /etc/iptables/rules.v4
```

25. Otvorite *web*-preglednik u *Windows* okruženju i upišite URL http://localhost. Možete li pristupiti testnoj stranici *web*-servisa?

26. Uklonite sva pravila iz vatrozida i promijenite politiku svih lanaca na ACCEPT.

2.1.8. Vježba 2: Podešavanje servisa TCP Wrappers

1. Prije početka rada odaberite sliku stanja virtualnoga računala (*Snapshot*) **slika_jedan** za početak vježbe.

2. Prijavite se na računalo kao korisnik **linux1**. U GUI-ju pokrenite **Terminal** (*Activities* → **Terminal**). Izvršite **su** - naredbu da postanete administrator (lozinka: linux1).

3. Provjerite stanje vatrozida naredbom `iptables -nL`.

4. Ako je politika lanaca postavljena na DROP, promijenite ih na ACCEPT:

```
# vim /etc/iptables/rules.v4
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
COMMIT

# iptables-apply /etc/iptables/rules.v4
```

5. Provjerite postoji li servisni proces *sshd* i ima li podršku za biblioteku *libwrap.so*.

```
# whereis sshd
sshd: /usr/sbin/sshd
/usr/share/man/man8/sshd.8.gz

# ldd /usr/sbin/sshd | grep libwrap.so
libwrap.so.0 => /lib/x86_64-linux-gnu/libwrap.so.0 (0x00007f51800e6000)
```

6. Izradite datoteku **/var/log/sshd.log** koja će se koristiti za bilježenje u dnevnički zapis pokušaja prijave s onemogućenih domena.

7. U datoteku **/etc/hosts.allow** dodajte sljedeću konfiguraciju:

```
sshd : LOCALHOST : spawn /bin/echo `/bin/date` access denied >>
/var/log/sshd.log : deny
```

8. Instalirajte paket tcpd i provjerite *TCP Wrapper* konfiguracije naredbom:

```
# tcpdchk -v
```

9. Što se prikazuje u izlazu naredbe?

_____

_____

10. Pratite unos dnevničkoga zapisa u datoteci **/var/log/sshd.log**:

```
# tail -f /var/log/sshd.log
```

11. Pokrenite novi **Terminal** (*Activities* → **Terminal**). Pokušajte se spojiti na lokalno računalo ssh naredbom.

```
# ssh root@localhost
```

12. Možete li se spojiti? Vidite li nove dnevničke zapise u logove u datoteci **/var/log/sshd.log**?

13. Zašto se ne možete spojiti ako ste dodali konfiguraciju u **/etc/hosts.allow**?

14. Instalirajte paket *vsftpd* i provjerite postoji li servisni proces *vsftpd* i ima li podršku za biblioteku *libwrap.so*.

```
# whereis vsftpd
vsftpd: /usr/sbin/vsftpd /etc/vsftpd.conf /usr/share/man/man8/vsftpd.8.gz

# ldd /usr/sbin/vsftpd | grep libwrap.so
libwrap.so.0 => /lib/x86_64-linux-gnu/libwrap.so.0 (0x00007fa1ed65a000))
```

15. Kako bi se kontrolirao pristup preko *TCP Wrappera* dodajte konfiguraciju **tcp_wrappers=YES** u datoteku **/etc/vsftpd.conf** i ponovno pokrenite servisni proces *vsftpd* naredbom

```
systemctl restart vsftpd
```

16. U datoteku **/etc/hosts.deny** dodajte sljedeću konfiguraciju:

```
vsftpd: ALL
```

17. Provjerite *TCP Wrapper* konfiguracije naredbom:

```
# tcpdchk -v
```

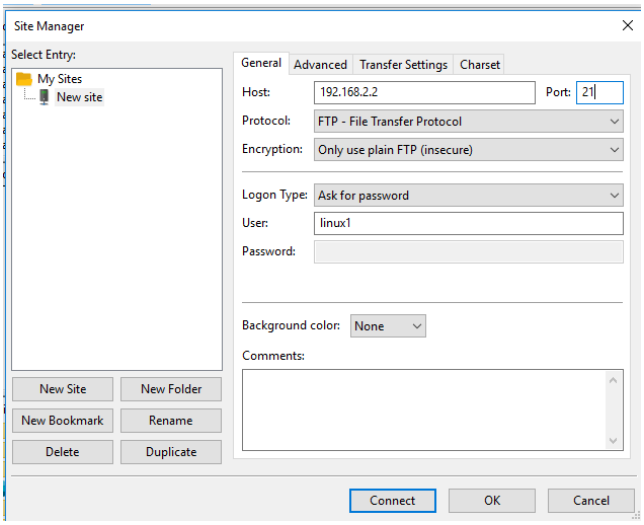
18. Što se prikazuje u izlazu naredbe?

19. U čemu je sve razlika između prijašnje konfiguracije za servisni proces *sshd* i trenutne za *vsftpd*?

20. Stvorite datoteku **/var/log/vsftpd.log** i pratite unos dnevničkog zapisa u datoteci **/var/log/vsftpd.log**:

```
# touch /var/log/vsftpd.log
# tail -f /var/log/vsftpd.log
```

21. Otvorite program *Fillezilla* u *Windows* okruženju i pokušajte se spojiti na IP adresu 192.168.2.1. i port 21:



22. Možete li se spojiti i zašto?

23. Gledajući dnevnički zapis, s koje IP adrese stiže zahtjev za spajanje?

24. Dodajte IP adresu računala s kojeg se pokušavate spojiti u datoteku **/etc/hosts.allow**:

```
vsftpd: 192.168.2.1
```

Otvorite program *Fillezilla* u *Windows* okruženju i pokušajte se spojiti na IP adresu 192.168.2.1. i port 21. Možete li se sada spojiti?

2.2. Servis za udaljeni rad

2.2.1. Servis za udaljeni rad

SSH (*Secure Shell*) omogućava korisnicima pristup naredbenom sučelju na udaljenom računalu. SSH omogućava i uspostavljanje sigurnosnoga komunikacijskog kanala preko nesigurne mreže (poput Interneta).

Konfiguracija i ponovno pokretanje servisa

Sve konfiguracije koji su vezane za servis SSH nalaze se u datoteci `/etc/ssh/sshd_config`. Nakon promjene konfiguracije potrebno je ponovno pokrenuti servis sshd:
`systemctl restart sshd`

Onemogućavanje SSH povezivanje s korisnikom root

Jedan od većih sigurnosnih propusta jest omogućavanje spajanje protokolom SSH kao korisnik `root`, jer je to poznati administratorski korisnik. Ako je lozinka slaba, moguće je provaliti na poslužitelj koristeći napad grubom silom. Preporučeno je koristiti odvojeni korisnički račun, a za administratorske ovlasti koristiti `sudo` naredbu. Prije nego se onemogući SSH spajanje s korisnikom `root`, potrebno je napraviti korisnički račun s administratorskim ovlastima.

`echo 'maja ALL=(ALL) ALL' >> /etc/sudoers`

Za onemogućavanje spajanja kao korisnik `root` potrebno je u datoteci `/etc/ssh/sshd_config` dodati: `PermitRootLogin no`

Onemogućavanje SSH povezivanja pojedinih korisnika

Prema zadanim postavkama svi sistemski korisnici mogu se povezati s protokolom SSH koristeći lozinku ili javni ključ. Nekim korisnicima potrebno je samo spajanje protokolom FTP ili provjeravanje elektroničke pošte, a samo povezivanje SSH-om predstavljalo bi nepotrebni sigurnosni rizik.

Definiranoj listi korisnika bit će odobreno SSH povezivanje, a svim ostalima zabranjeno:

```
$ sudo vim /etc/ssh/sshd_config
AllowUsers maja marko mario
```

Alternativa je dopustiti svim korisnicima SSH povezivanje, ali ga onemogućiti samo nekima:

```
$ sudo vim /etc/ssh/sshd_config
DenyUsers root ana anita ante
```

Maksimalan broj pokušaja povezivanja

S konfiguracijom `MaxAutTries` može se definirati maksimalan pokušaj autentikacije kako bi se spriječio napad grubom silom:

```
$ sudo vim /etc/ssh/sshd_config
MaxAuthTries 3
```

Autentikacija servisa SSH

Autentikacija poslužitelja i servisa događa se prije autentikacije korisnika. Poslužitelj se autenticira pomoću kriptografskih ključeva, koristeći RSA ili DSA kriptiranje. Tijekom instalacije *OpenSSH* paketa, izradit će se set privatnih i javnih ključeva za sve raspoložive tipove kriptiranja: RSA1, RSA i DSA i oni se nalaze u direktoriju `/etc/ssh`. Oni su javni ključevi poslužitelja i nemaju lozinku. Kada korisnik pri prvom spajanju prihvati nastavak uspostavljanja veze, javni se ključ poslužitelja pohranjuje u datoteku `$HOME/.ssh/known_hosts`. Taj javni ključ koristi se za izgradnju sigurnoga SSH kanala omogućavajući pregovaranje simetričnoga ključa koji se koristi za zaštitu kasnijih sesija, omogućava povjerljivi kanal, zaštitu integriteta i autentikaciju servera.

Servisni proces se naziva sshd i pokreće se na portu 22. Klijent se spaja na taj port pomoću naredbe `ssh`. U primjeru je prikazano inicijalno spajanje s klijentom SSH na udaljeno računalo:

```
$ ssh iprezime@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ECDSA key fingerprint is c9:b4:b6:8a:d7:37:8a:9b:4a:75:8d:90:0b:49:bf:35.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.15' (ECDSA) to the list of known hosts.
```

Vrste autentikacije korisnika

Nakon što je SSH kanal uspostavljen i osiguran, može se krenuti s autentikacijom korisnika. Korisnik može potvrditi svoj identitet koristeći autentikaciju lozinkom ili pomoću ključeva.

Prilikom autentikacije lozinkom koriste se autentikacijskii podaci koji su pohranjeni u datotekama `/etc/passwd` i `/etc/shadow` na računalu na kojem je pokrenut servisni proces *sshd*. U datoteci `passwd` nalazi se korisničko ime, a u datoteci `shadow` kriptirana lozinka. Tijekom SSH spajanja upisuju se korisničko ime i lozinka koja se uspoređuje s kriptiranom lozinkom na udaljenom računalu i tako potvrđuje svoj identitet:

```
iprezime@10.0.2.15's password:*********
Linux debian-1 3.2.0-4-486 #1 Debian 3.2.68-1+deb7u2 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jul  1 10:34:57 2015
$
```

2.2.2. Zanimljivi izvori

Poveznice:

- https://linux-audit.com/audit-and-harden-your-ssh-configuration/

2.2.3. Vježba 3: Ograničavanje servisa za udaljeni rad

1. Prije početka rada odaberite sliku stanja virtualnoga računala (Snapshot) **slika_jedan** za početak vježbe.
2. Prijavite se na računalo kao korisnik **linux1**. U GUI-ju pokrenite **Terminal** (*Activities* → **Terminal**). Izvršite **su** - naredbu da postanete administrator (lozinka: linux1).
3. Promijenite sljedeće konfiguracije u **/etc/ssh/sshd_config** i ponovno pokrenite servis SSH:

```
# vim /etc/ssh/sshd_config
PermitRootLogin no
DenyUsers ana
MaxAuthTries 3

# systemctl restart ssh
```

4. Kreirajte korisnika ana i marko s lozinkom *linux1*:

```
adduser ana
adduser marko
```

5. Pokrenite novi **Terminal** (*Activities* → **Terminal**). Pokušajte se spojiti na lokalno računalo **ssh** naredbom s korisnicima ana i marko.

```
# ssh ana@localhost
# ssh marko@localhost
```

6. Uspijevate li se spojiti s obama korisnicima?

_____

_____

7. Pokušajte se spojiti na lokalno računalo ssh naredbom s korisnikom marko i napišite krivu lozinku 3 puta. Kakva se obavijest prikazuje?

_____

2.3. Mrežni servisi

2.3.1. DNS

Za ograničavanje pristupa DNS servisu *bind9* ili njegovim funkcijama koriste se liste za kontrolu pristupa (ACL). ACL omogućava imenovanje jedne ili grupe IP adresa, podmreža ili drugih ACL lista. Na primjer, moguće je definirati koje IP adrese unutar mreže mogu pristupiti servisu *bind* ili omogućiti cijeloj mreži rekurzivne upite.

U sljedećem primjeru omogućen je transfer zona za dvije lokalne mreže i jednu javnu IP adresu.

```
acl "omoguci" {
  192.168.0.0/24;   // mreza1
  192.168.1.0/24;   // mreza2
  192.168.2.150;   // privatna_ip
  161.53.2.70;   // javna_ip
};
zone domena.com  {
  allow-transfer { omoguci; };
};
```

Nakon dodavanja konfiguracije u `/etc/bind/named.conf` potrebno je napraviti ponovno učitavanje konfiguracije servisa bind:

```
$ sudo rndc reload
```

ACL liste

BIND ima nekoliko ACL lista koje su unaprijed definirane:

`none` – ne podudara se ni s jednom IP adresom, mrežom ili računalom

`any` – podudara se s bilo kojom IP adresom, mrežom ili računalom

`localhost` – podudara se s IP adresama na računalu na kojemu je instaliran BIND. Ako računalo ima jedno mrežno sučelje s IP adresom 192.168.2.55, tada će podudaranje biti za spomenutu adresu i za 127.0.0.1 (*loopback* adresa)

`localnets` – podudara se sa svim IP adresama podmreže prema IP adresi i podmreži na kojoj je instaliran BIND. Ako računalo ima mrežno sučelje s IP adresom 192.168.2.3. i podmrežom 255.255.255.0 (ili 192.168.2.2/24), tada će localnets pokriti opseg IP adresa od 192.168.2.0 do 192.168.2.255 i 127.0.0.1 (*localhost*).

Negativne ACL liste

Za izostavljanje jedne IP adrese ili podmreže iz liste za kontrolu pristupa koristi se uskličnik. U sljedećem primjeru onemogućit će se transfer zona IP adresi 192.168.2.55 i mreži 10.0/16, a omogućit će se pristup svim ostalim IP adresama.

```
acl "omoguci" {
  !192.168.2.55;
  !10.0/16;
```

```
  any;
}
zone domena.com  {
  allow-transfer { omoguci; };
};
```

Grupiranje ACL listi

U ACL listi moguće je navesti druge ACL liste:

```
acl "podmreza" {
  192.168.0.0/24;
};
acl "ipadresa" {
  192.168.1.53;
};
acl "sve" {
  "podmreza";
  "ipadresa";
};
```

Onemogućavanje pristupa rekurzivnim upitima

Ako DNS servis nema traženu informaciju, može biti napravljen rekurzivni upit prema drugim DNS poslužiteljima. Nakon što je informacija dohvaćena, DNS je prosljeđuje klijentu.

Ovisno o svrsi DNS poslužitelja rekurzija može biti onemogućena ili omogućena:

```
allow-recursion { none; };
allow-recursion { all; };
```

Također, rekurzija se može uključiti samo za lokalne podmreže:

```
acl podmreza1 {
  192.168.1.0/24;
};
allow-recursion { podmreza1; };
```

2.3.2. Servis elektroničke pošte

Postfix omogućava definiranje liste pristupa za svaki korak SMTP komunikacije:

- nakon uspostavljanja TCP veze (`smtpd_client_restrictions`)
- kada klijent pošalje naredbu MAIL FROM (`smtpd_sender_restrictions`)
- kada klijent pošalje naredbu RCPT TO (`smtpd_recipient_restrictions`)
- kao i kontroliranje korištenja *postfixa* kao relaya (`smtpd_relay_restrictions`).

Sve konfiguracije se dodaju i mijenjaju u `/etc/postfix/main.cf` nakon čega je potrebno napraviti ponovno učitavanje konfiguracije servisa: `$ sudo postfix reload`.

Sljedeća konfiguracija definira podmreže koje će *postfix* smatrati sigurnima i one će se koristiti u svim ostalim primjerima.

```
sigurne-podmreze = 10.0.0.0/8 127.0.0.0/8 192.168.1.0/24
```

Dopuštanje čitanja elektroničke pošte samo sa sigurnih podmreža, a sve ostale onemogući:

```
smtpd_client_restrictions =
  permit_sigurne-podmreze,
  reject
```

Sljedeća konfiguracija će onemogućiti slanje s nepostojećih domena:

```
smtpd_sender_restrictions =
  reject_unknown_sender_domain
```

Omogućavanje primanja elektroničke pošte sa sigurnih mreža i autenticiranim *sasl* korisnicima te razne preporučene zabrane:

```
smtpd_recipient_restrictions =
   permit_sigurne-podmreze,
   permit_sasl_authenticated,
   # razne zabrane
   reject_non_fqdn_hostname,
   reject_non_fqdn_sender,
   reject_non_fqdn_recipient,
   reject_unauth_destination,
   reject_unauth_pipelining,
   reject_invalid_hostname,
   reject_rbl_client bl.spamcop.net,
   reject_rbl_client cbl.abuseat.org,
   reject_rbl_client dnsbl.sorbs.net,
   reject_rbl_client zen.spamhaus.org,
   # dopusti sve ostalo
   permit
```

Omogućavanje korisnicima koji su navedeni u `/etc/postfix/access` i `/etc/postfix/sender_access` da mogu koristiti *postfix relay*, kao i korisnicima koji se uspješno autenticiraju i koji dolaze sa sigurnih podmreža:

```
smtpd_relay_restrictions =
  check_sender_access hash:/etc/postfix/sender_checks,
  check_client_access hash:/etc/postfix/client_checks,
  permit_sigurne-podmreze,
  permit_sasl_authenticated,
  # razne zabrane
  reject_invalid_hostname,
  reject_unknown_sender_domain,
  reject_unknown_recipient_domain,
  reject_unauth_pipelining,
  reject_unauth_destination,
  # dopusti sve ostalo
  permit
```

2.3.3. Web-servis

Apache2 modul *mod_access* može omogućiti ili onemogućiti pristup direktorijima, datotekama ili lokacijama prema IP adresi, podmreži, imenu računala itd. Konfiguracija upisuje u datoteci virtualnoga hosta `/etc/apache2/sites-available/<ime_virtualnog_hosta>.conf`.

Primjer onemogućavanja pristupa direktoriju `./www` prema IP adresama i domeni:

```
<Directory /www>
  Order Deny,Allow
  Deny from 192.168.1.99 192.168.1.100
  Deny from google.com
</Directory>
```

Primjer omogućavanja pristupa prema podmreži i imenu hosta:

```
<Directory /www>
  Order Allow,Deny
  Allow from 10.1.0.0/16
  Allow from test.primjer.hr
</Directory>
```

Direktiva `order` ima dvije mogućnosti, `Allow` i `Deny`. Ovisno o poretku, pristup direktoriju će biti omogućen ili onemogućen.

Kod poretka `"Order Allow, Deny"` prvo se uzimaju u obzir sve `Allow` direktive. Ako su ime hosta ili IP adresa navedeni u `Allow from` direktivi pristup će im biti omogućen. Zatim se uzimaju

u obzir `Deny` direktive te se host ili IP adresa odbijaju. Na kraju, svaki zahtjev koji se ne podudara s `Allow` i `Deny` direktivama bit će odbijen.

Kod poretka `"Order Deny, Allow"` prvo se uzimaju u obzir sve `Deny` direktive. Ako su ime hosta ili IP adresa navedeni u `Deny from` direktivi njima će biti onemogućen pristup i obratno. Na kraju, svaki zahtjev koji se ne podudara s `Deny` i `Allow` direktivama bit će omogućen.

Nakon izmjena konfiguracija potrebno je ponovno pokrenuti *web*-servis naredbom: `$ sudo systemctl reload apache2`

2.3.4. Sustavi za upravljanje bazama podataka

Sustavi za upravljanje bazama podataka (npr. MariaDB, MySQL) mogu se koristiti lokalno, tj. bez potrebe da se na njih spaja preko mreže. U tom slučaju u datoteku `/etc/my.cnf` potrebno je dodati liniju `skip-networking` koja onemogućava spajanje protokolom TCP/IP.

Za udaljeno spajanje na bazu podataka potrebno je zakomentirati liniju `skip-networking` i podesiti bind-address što je IP adresa poslužitelja te dozvoliti pristup korisniku unutar baze podataka s određene IP adrese:

```
# promjena konfiguracije
vi /etc/my.cnf
bind-address = 192.168.1.50
# skip-networking

# nakon izmjena konfiguracija potrebno je ponovno pokrenuti servis
$ sudo systemctl restart mysql

# spajanje na servis mysql
$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 2
Server version: 10.1.26-MariaDB-0+deb9u1 Debian 9.1

# stvaranje baze podataka
MariaDB [(none)]> CREATE DATABASE test_db;
Query OK, 1 row affected (0.00 sec)

# dodjeljivanje prava korisniku test_user i IP adresi 192.168.1.55 za spajanje
na bazu test_db
MariaDB [(none)]> GRANT ALL ON test_db.* TO test_user@'192.168.1.55' IDENTIFIED
BY 'PASSWORD';
Query OK, 0 rows affected (0.01 sec)

# izlaz iz baze podataka
MariaDB [(none)]> exit
Bye
```

2.3.5. Zanimljivi izvori

Poveznice:

- http://www.aitechsolutions.net/dnsservertips.html
- http://httpd.apache.org/docs/2.0/mod/mod_access.html
- https://www.tecmint.com/mysql-mariadb-security-best-practices-for-linux/

2.3.6. Vježba 4: Ograničavanje pristupa virtualnom hostu

1. Prije početka rada odaberite sliku stanja virtualnoga računala (Snapshot) **slika_jedan** za početak vježbe.
2. Prijavite se na računalo kao korisnik **linux1**. U GUI-ju pokrenite **Terminal** (*Activities* → **Terminal**). Izvršite **su** - naredbu da postanete administrator (lozinka: linux1).
3. Provjerite *iptables* pravila.
4. Ako je politika lanaca postavljena na ACCEPT, promijenite ih na DROP. Propustite sav promet za port 80, a za port 22 propustite samo IP adresu Vašeg računala, 192.168.2.1.

```
# vim /etc/iptables/rules.v4
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
--append INPUT --protocol tcp --source 192.168.2.1 --dport 22 --match state \n
--state NEW,ESTABLISHED --jump ACCEPT
--append OUTPUT --protocol tcp --sport 22 --match state --state ESTABLISHED --jump ACCEPT

--append INPUT --protocol tcp --dport 80 --match state --state NEW,ESTABLISHED --jump ACCEPT
--append OUTPUT --protocol tcp --sport 80 --match state --state NEW,ESTABLISHED --jump ACCEPT

COMMIT

# iptables-apply /etc/iptables/rules.v4
```

5. Provjerite otvara li se testna *web*-stranica *web*-servisa tako da otvorite *web*-preglednik u *Windows* okruženju i upišite URL

   http://localhost

6. Provjerite možete li se spojiti koristeći program putty u Windows okruženju na IP adresu kao linux1.

   linux1@192.168.2.1

Stvorite dva direktorija, **/var/www/html/onemoguci/** i **/var/www/html/omoguci**. I u tim direktorijama, stvorite datoteke **index.html** s proizvoljnim sadržajem.

```
# vim /etc/apache2/sites-enabled/000-default.conf
<Directory /var/www/html/omoguci> Order Allow,Deny
Allow from 192.168.2.0/24
```

```
</Directory>

<Directory /var/www/html/onemoguci> Order Allow,Deny
Deny from 192.168.2.0/24
</Directory>
```

7. Nakon promjene konfiguracije ponovno učitajte konfiguraciju *web*-servisa:

   ```
   # systemctl reload apache2
   ```

8. Provjerite otvaraju li se web-stranice tako da otvorite web- preglednik u *Windows* okruženju i upišite URL-ove http://localhost./omoguci i http://localhost./onemoguci

9. Prikazuju li se obje web-stranice? Što je sve ispisano u web- pregledniku za onemogućenu web-stranicu?

   _____

   _____

10. Što će se dogoditi ako se okrene poredak **Order** na **Deny**, **Allow**? Promijenite konfiguraciju, ponovno učitajte konfiguraciju *web*-servisa i testiranje rezultate.

    _____

    _____

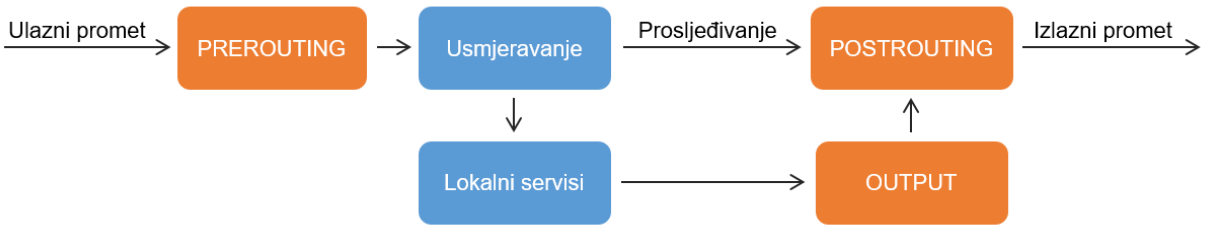
2.4. Onemogućavanje izravnog pristupa

2.4.1. Mehanizam NAT

Računala koja se nalaze u lokalnoj mreži (npr. 192.168.0.0/16) mogu međusobno komunicirati, ali ako se žele spojiti na Internet, njihova lokalna IP adresa mora biti translatirana u javnu IP adresu. Najčešće ovu promjenu adresa obavlja usmjerivač kako bi se računala iz lokalnih mreža spojila na Internet. Usmjerivač translatira izvorišnu IP adresu paketa u svoju javnu IP adresu, zabilježi zahtjev u svojoj memoriji i pošalje paket prema poslužitelju na Internetu. Kad dođe odgovor, usmjerivač provjeri zahtjev u svojoj memoriji i translatira odredišnu IP adresu (javnu IP adresu usmjerivača) u IP adresu računala koji je iniciralo komunikaciju.

NAT (*Network Address Translation*) koristi se za translaciju izvorišnih i/ili odredišnih IP adresa paketa koji prolazi kroz usmjerivač ili vatrozid. *Linux kernel framework netfilter* omogućava korištenje NAT-a kroz naredbu *iptables*. Na ovaj način *Linux* možemo konfigurirati da se koristi kao usmjerivač.

Iptables može kreirati kompleksna pravila za modificiranje i filtriranje paketa koji se nalaze u tablici za translaciju mrežnih adresa – NAT tablici. U tablici postoje tri lanca: PREROUTING, OUTPUT i POSTROUTING.



Paketi koji dolaze na mrežno sučelje prolaze kroz lanac PREROUTING u kojem se odlučuje hoće li se paket proslijediti na drugo računalo ili će ga koristiti lokalni proces u operacijskom sustavu. Nakon što paket prođe fazu PREROUTING, donosi se odluka o usmjerivanju. U slučaju da je paket naslovljen na lokalni sustav, paket će biti proslijeđen lokalnom procesu i to ne uključuje NAT pravila. Ako je odredišna IP adresa paketa u istoj podmreži kao i drugo mrežno sučelje, taj paket će se proslijediti na to sučelje (ako je tako konfigurirano na operacijskom sustavu). I prije nego što proslijeđeni paket izađe iz mrežnog sučelja prolazi kroz POSTROUTING lanac.

Lokalno generirani paketi prolaze kroz OUTPUT pa i kroz POSTROUTING lanac.

Tablica Nat podržava:

- REDIRECT i DNAT (u lancima PREROUTING I OUTPUT)
- MASQUERADE (u lancu POSTRUTING)
- SNAT (u lancima POSTROUTING i OUTPUT).

Najčešće akcije koje se koriste u tablici NAT:

Akcija	Opis
REDIRECT	Translatira odredišnu IP adresu kako bi paket došao do lokalnih servisa, tj. IP adresa se translatira na 127.0.0.1..
DNAT	Translatira javnu IP adresu računala koje je iniciralo komunikaciju u definiranu IP adresu.
MASQUERADE	Translatira IP adresu paketa na IP adresu odabranoga mrežnog sučelja.
SNAT	Translatira izvorišnu IP adresu paketa na odabranu IP adresu.

Po zadanome, na operacijskijom sustavu *Debian*, mogućnost translatiranja IP adresa je onemogućeno jer na većini sustava ova opcija nije potrebna. Prije stvaranja *iptables* pravila potrebno je uključiti mogućnost ip_forward, tj. aktivirati mogućnost translatiranja IP adresa:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Translatacija IP adrese na mrežno sučelje

MASQUERADE translatira IP adresu paketa na IP adresu odabranoga mrežnog sučelja. Na primjer, na mrežnom sučelju poslužitelja eth0 prima se promet iz lokalne podmreže te se nakon translatacije šalje prema Internetu preko mrežnog sučelja eth1.

Naredba:

```
$ sudo iptables --table nat --append POSTROUTING --out-interface eth1 --
jump MASQUERADE
```

Translatacija izvorišne IP adrese

Static SNAT translatira izvorišnu IP adresu paketa na odabranu IP adresu, također se može koristiti u svrhu spajanja računala iz lokalne mreže na Internet.

Naredba:

```
$ sudo iptables --table nat --append POSTROUTING --out-interface eth0 --
source 192.168.0.0/24 --jump SNAT --to-source 123.123.123.123
```

Kao alternativa može se koristiti i dinamični SNAT, gdje se umjesto jedne IP adrese može postaviti nekoliko IP adresa u koje će se izvorišne IP adrese translatirati.

```
$ sudo iptables --table nat --append POSTROUTING --out-interface eth0 --
source 192.168.0.0/24 --jump SNAT --to-source 1.1.1.1-1.1.1.5
```

Translacija odredišne IP adrese

U slučaju MASQUERADE-a i SNAT-a, komunikaciju inicira računalo unutar lokalne podmreže i samo tako inicirana komunikacija bit će uspješno izvršena. Ako računalo na Internetu želi inicirati komunikaciju s računalima unutar lokalne mreže to može koristeći mogućnost DNAT. DNAT translatira javnu IP adresu računala koje je iniciralo komunikaciju u definiranu IP adresu *Linux* usmjerivača i tako promijenjen paket prosljeđuje se na definiranu privatnu IP adresu.

U sljedećem primjeru sav promet koji dolazi na IP adresu 1.1.1.11 bit će preusmjeren na 192.168.0.3.

```
$ sudo iptables --table nat --append PREROUTING --destination 1.1.1.11 -
-jump DNAT --to-source  192.168.0.3
```

Moguće je definirati DNAT pravila prema servisu, tj. prema portu na kojem taj servis sluša. Na sljedećem primjeru je promet s Interneta dopušten prema IP adresi 1.1.1.11 i portu 80 te će se isti preusmjeriti na 192.168.0.3 na kojem je poslužitelj s otvorenim portom 80.

```
$ sudo iptables --table nat --append PREROUTING --destination 1.1.1.11 -
-protocol tcp --dport 80 --jump DNAT --to-source 192.168.0.3
```

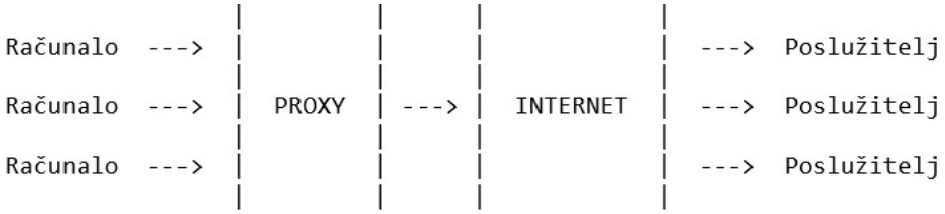
Primjer prikazuje izradu DNAT tablice koja translatira SSH pakete koji dolaze na IP adresu 1.1.1.11 i port 8532 pa ih preusmjerava na lokalnu IP adresu 192.168.0.3 i port 22.

```
$ sudo iptables --table nat --append PREROUTING --destination 1.1.1.11 -
-protocol tcp --dport 8532 --jump DNAT --to-source 192.168.0.3:22
```

2.4.2. Servis proxy

Proxy je servis koji posreduje između klijentskih zahtjeva i poslužitelja. Klijentsko računalo se povezuje sa servisom *proxy* tražeći neki resurs, kao što je *web*-stranica, SSH veza ili FTP zahtjev. Servis *proxy* procjenjuje zahtjev i ako je odobren, zahtjev se prosljeđuje. Prema tome klijent nikada ne komunicira izravno s vanjskim poslužiteljem i svaki nedozvoljeni zahtjev se onemogućava. Jedna od koristi je zaštita lokalnih računala jer je *proxy* poslužitelj jedini eksponiran prema Internetu.

Osim kontrole pristupa, *proxy* sprema sadržaj zahtjeva (*web*-stranice, slike, videa itd.) i tako smanjuje vrijeme kasnijega dohvaćanja istoga sadržaja čime smanjuje mrežni promet.



Squid proxy poslužitelj

Squid je *proxy* servis za *Linux* distribucije. *Squid* je najčešće instaliran na zasebnom poslužitelju, odvojen od sadržaja koje zahtijevaju klijenti. Prilikom prvoga pokretanja, *squid* će djelovati kao posrednik, prosljeđujući mrežni promet između klijenta i poslužitelja i spremajući ga u privremenu memoriju. Ako klijenti zatraže isti sadržaj prije nego se obriše s poslužitelja, *squid* automatski servira zahtjev.

Liste za kontrolu pristupa (ACL, *Access Control Lists*)

Listama za kontrolu pristupa onemogućava se pristup određenim *web*-stranicama, poslužiteljima, podmrežama ili IP adresama.

Sintaksa za liste za kontrolu pristupa: `acl aclname acltype argument ...`

- `aclname`: ime mora biti jedinstveno i preporučljivo je da bude opisno
- `acltype`: vrsta liste na osnovi koje se filtrira. Na primjer, IP adresa, domena, vrijeme itd. Sve mogućnosti mogu se pronaći na http://www.visolve.com/squid/squid24s1/access_controls.php
- `argument`: na čemu se izvršava filtriranje. Može biti niz IP adresa, regularni izraz ili lista domena. Može biti i kombinacija svega navedenog.

Primjer liste za kontrolu pristupa koje se kreiraju u `/etc/squid/squid.conf`:

```
# filtriranje po domeni
acl pristup_za_srce_hr dstdomain .srce.hr

# filtriranje po više domena
acl pristup_prema_trazilicama dstdomain .bing.com .yahoo.com .google.com
acl domena_piratebay_org dstdomain .piratebaty.org

# filtriranje po podmreži izvorišne ip adrese paketa
acl pristup_lokalnoj_podmrezi_101 src 10.53.0.0/16
```

Moguće je koristi i listu argumenta koja se nalazi u datoteci:

```
$ sudo vim /etc/squid/lista_trazilica.txt
.duckduckgo.com
.google.com
.yahoo.com
.vivisimo.com
.dogpile.com
.yippy.com
```

U tom slučaju lista za kontrolu pristupa će se definirati prema putanji tekstualne datoteke:

```
acl accessess_to_search_engines dstdomain
"/etc/squid/lista_trazilica.txt"
```

Pristupne liste

Da bi liste za kontrolu pristupa bile funkcionalne, potrebno je dodati pristupne liste. Pristupnim listama se dodaju `allow` ili `deny`, te i jedan ili više `aclname`.

Sintaksa je sljedeća:

```
access_list allow|deny aclname1 AND aclname2 ...
```

U sljedećem primjeru definirane su pristupne liste koje se referiraju na liste za kontrolu pristupa iz prethodnog primjera:

```
# dozvoli http pristup i spremanje u privremenu memoriju za domenu
srce.hr
http_access allow  pristup_za_srce_hr

# zabrani http pristup domeni piratebay.org
http_access deny domena_piratebay_org

# zabrani sve ostale zahtjeve
http_access deny all
```

Pristupne liste provjeravaju se po redu kako su definirane. Ako jedna lista odgovara zahtjevu, ostale liste se ne provjeravaju. Ako ni jedna lista ne odgovara zahtjevu, zahtjev se tretira obratno od onog kako je definirano u zadnjoj pristupnoj listi.

Preporuča se da zadnja lista bude izričita, tj. da omogući ili onemogući sve zahtjeve koje nisu odgovarale prijašnjim zahtjevima (kao što je i navedeno u prijašnjem primjeru).

Kombiniranje pristupnih lista

Pristupne liste se mogu kombinirati s logičkim operatorima I ili ILI, tako da se I stavlja unutar istog reda, a ILI koristeći različite linije.

U sljedećem primjeru zahtjev za dohvaćanjem *web*-stranica iz srce.hr domene mora doći iz lokalne mreže.

```
http_access allow domena_srce_hr pristup_lokalnoj_podmrezi_101
```

Za korištenje operatora ILI potrebno je staviti pristupnu listu jednu ispod druge, prema tome pristup *web*-stranicama je moguć prema domeni srce.hr ili prema bilo kojoj domeni iz lokalne podmreže:

```
http_access allow domena_srce_hr
http_access allow pristup_lokalnoj_podmrezi_101
```

2.4.3. Zanimljivi izvori

Poveznice:

- http://www.internet-computer-security.com/Firewall/NAT.html
- https://whatis.techtarget.com/definition/proxy-server

3. Sigurnosne postavke

Trajanje poglavlja:
185 min

Po završetku ove cjeline moći ćete:

- prepoznati aspekte informacijske sigurnosti na kojima se zasniva kriptografija
- razlikovati vrste kriptografskih algoritama i protokola
- koristiti asimetrične ključeve za spajanje na udaljena računala
- upotrijebiti samopotpisni certifikat u svrhu testiranja apache2 virtualnoga hosta
- primijeniti načelo najmanjih ovlasti ovisno o korisničkim potrebama koristeći naredbu sudo
- upotrijebiti metodu chroot jail za ograničavanje procesa modificiranjem korijenskoga direktorija
- navesti preporuke za stvaranje sigurne lozinke i testirati njenu jačinu.

Ova cjelina obrađuje aspekte informacijske sigurnosti koji su vezani za kriptografiju, algoritme i protokole. Asimetrični kriptografski algoritam koristit će se za spajanje na udaljeno računalo i bit će obrađena implementacija samopotpisanoga (self-signed) certifikata i osiguravanje kriptografskih postavki.

Upoznajemo se s načelima najmanjih ovlasti i njihovom primjenom koristeći naredbu sudo i chroot jail za ograničavanje procesa. Na kraju cjeline nalaze se preporuke za izradu sigurne lozinke i testiranje njene jačine.

3.1. Kriptografska zaštita

3.1.1. Što je kriptografija

Svrha računalne kriptografije jest omogućavanje sigurnoga komuniciranja između dvaju sustava ili osoba preko nesigurnih mreža gdje neovlaštena osoba ili računalni sustav može nadzirati taj kanal komunikacije. Pošiljatelj kriptira poruku, tj. mijenja sadržaj poruke da bi isti bio nečitljiv trećim osobama, koristeći unaprijed dogovorenu metodu i ključ. Tako promijenjen sadržaj poruke primatelj može dekriptirati koristeći tu istu metodu i ključ koji je prethodno razmijenio s pošiljateljem.

Jednostavni primjer uporabe kriptografije na *Linux* distribucijama jest enkripcija lozinke. Za prijavu u operacijski sustav korisnik odabire lozinku koja se kriptira i sprema u datoteku `/etc/shadow`, tako da drugi korisnici ne mogu pročitati odabranu lozinku. Tijekom prijave korisnika upisana lozinka se kriptira i uspoređuje s odabranom lozinkom koja je spremljena u `/etc/shadow`. Ako se lozinke podudaraju, korisnik može pristupiti sustavu.

Aspekti informacijske sigurnosti na kojima se zasniva moderna kriptografija su:

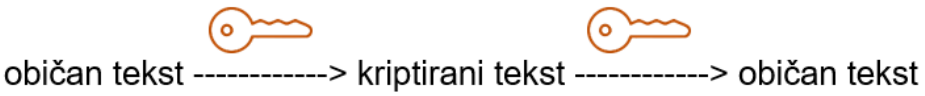
1) Autentikacija (*authentication*) – dokazivanje identiteta osobe, servisa ili operacijskog sustava.

2) Razmjena ključeva (*key exchange*) – sigurna metoda razmjene kriptografskih ključeva između pošiljatelja i primatelja.
3) Povjerljivost (*confidentiality*) – osiguranje da nitko neće moći pročitati poruku osim onoga kome je ona namijenjena. Čak i ako poruku netko presretne dok se šalje nesigurnim mrežama Interneta, ta poruka mora biti nečitljiva osim ako primatelj poruke ne posjeduje kriptografski ključ.
4) Integritet (*integrity*) – provjeravanje je li primatelj primio originalnu poruku, tj. poruka mora ostati nepromijenjena na putu od pošiljatelja do primatelja.
5) Provjereni pošiljatelj (*non-repudiation*) – metoda dokazivanja da je poruka doista poslana od određenog pošiljatelja.

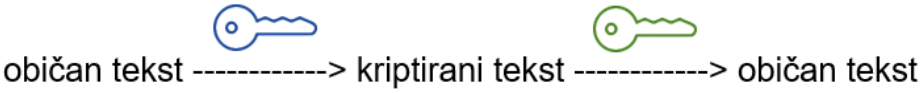
3.1.2. Kriptografski algoritmi

Kriptografske algoritme možemo podijeliti po broju ključeva koji se koriste za kriptiranje i dekriptiranje:

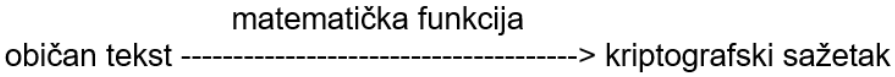
- simetrični kriptografski algoritmi ili algoritmi tajnoga ključa (*symmetric or secret key cryptography*) koriste samo jedan ključ za kriptiranje i dekriptiranje sadržaja



- asimetrični kriptografski algoritmi ili algoritmi javnoga ključa (*asymmetric or public key cryptography*) koriste javni ključ za kriptiranje, a privatni za dekriptiranje



- kriptografski sažetci (*cryptographic hash function*) ne koriste ključ već matematičku funkciju za stvaranje digitalnoga potpisa za provjeru integriteta sadržaja ili poruke



Simetrični kriptografski algoritmi

Prije slanja poruke, na primjer, preko Interneta ili neke druge nesigurne mreže, pošiljatelj mora kriptirati poruku koristeći kriptografski algoritam i privatni ključ. Ta je poruka nečitljiva svima, osim pošiljatelju koji koristi isti kriptografski algoritam i privatni ključ s kojim dekriptira poruku. Kriptografski algoritmi su javno dostupni, kao i javni ključ, ali privatni ključ mora ostati tajan inače bi svi koji ga imaju mogli pročitati poruku. Kako bi se uspostavio sigurni komunikacijski kanal, dvije strane moraju prvo razmijeniti privatni ključ ili lozinku, što je osnovni problem simetričnih algoritama. Za razmjenu privatnoga ključa ili lozinke na siguran način mogu se koristiti asimetrični kriptografski algoritmi.

Najpoznatiji simetrični algoritmi su DES (*Data Encryption Standard*), 3DES (*Triple Data Encryption Algorithm*), AES (*Advanced Encryption Standard*) i IDEA (*International Data Encryption Algorithm*). DES koristi 56 bitnih ključeva koji se lagano mogu dekriptirati grubom silom koristeći moderni hardver, pa je zamijenjen 3DES-om. 3DES koristi isti algoritam tri puta, svaki put s različitim ključem, prema tome njegova veličina ključa je 168 bita. Zbog drugih ranjivosti 3DES-a, NIST (*National Institute of Standards and Technology*) je za novi kriptografski standard odabrao AES. AES je kompaktan i brz, a koristi ključeve od 128, 192, i 256 bita. IDEA je još jedan kriptografski algoritam koji se često koristi i smatra se vrlo sigurnim. Koristi 128 bitne ključeve i osnovni je dio PGP (*Pretty Good Privacy*) kriptografskoga sustava.

Asimetrični kriptografski algoritmi

Asimetrični kriptografski algoritmi koriste dva ključa, javni ključ i privatni ključ. Svaka informacija koja se kriptira javnim ključem može se dekriptirati samo privatnim ključem i obratno. Na ovaj način bilo tko tko posjeduje javni ključ može kriptirati ili dekriptirati poruku ako je kriptirana privatnim ključem. Kako privatni ključ ne napušta svojega vlasnika, riješen je problem nesigurne razmjene ključeva koji postoji kod simetričnih kriptografskih algoritama. Nedostatak asimetričnih algoritama jest da je sporiji od simetričnih.

Najpopularniji asimetrični algoritam je RSA (*Rivest–Shamir–Adleman*). Njegova sigurnost se zasniva na težini (ili teškoći) faktorizacije dvaju velikih prirodnih brojeva s kojom se izračunavaju javni i privatni ključ. Na ovaj je način gotovo nemoguće izračunati originalne ključeve, tj. brojeve.

Uz asimetrične kriptografske ključeve neodvojive su organizacije koje izdaju i potvrđuju validnost javnih ključeva. CA (*certificate authority*) su organizacije koje potvrđuju da javni ključ pripada određenoj organizaciji, poduzeću, računalu, servisu ili osobi izdavanjem digitalnih certifikata. Certifikat posjeduje informacije kao što su vlasnik certifikata, izdavač certifikata, način enkripcije i druge relevantne informacije. Česti način korištenja CA je digitalno certificiranje javnih ključeva koji se koriste u protokolu HTTPS. Prilikom unošenja *web*-domene koja posjeduje certifikat, *web*-preglednik provjerava posjeduje li CA javni ključ koji je povezan s tim certifikatom. Ako je certifikat valjan, *web*-preglednik označava vezu sigurnom, najčešće lokotom ili riječi „Sigurno“ koja se nalazi lijevo od URL-a.

Kriptografski sažetci

Za izračunavanje kriptografskih sažetaka koriste se matematičke funkcije koje koriste podatke kao ulaznu varijablu i generiraju niz znakova, najčešće u heksadekadskoj notaciji. Podatak za koji se izračunava sažetak može biti bilo koja datoteka, poruka ili binarni podaci. Svaka mala promjena uvijek generira drugačiji kriptografski sažetak, čak i ako se koristi ista kriptografska funkcija. Svrha kriptografskih funkcija jest generiranje kriptografskih sažetaka i potvrđivanje integriteta podataka jer je gotovo nemoguće dobiti dva ista kriptografska sažetka. U praksi se može dogoditi da različiti podaci daju isti kriptografski sažetak, ali vjerojatnost takvog slučaja je zanemarivo mala. Osim za datoteke, kriptografski sažetci, tj. matematičke funkcije koriste se u digitalnim potpisima i PKI sustavima.

Kriptografski sažetci razlikuju se po algoritmima koji koriste i po dužini sažetka. Najpoznatiji su MD5 (*Message Digest Algorithm 5*) koji generira 128 bitni sažetak i SHA1 (*Secure Hash Algorithm160-bit hash*) sa 160 bitnim sažetkom. Oba spomenuta algoritma za generiranje

kriptografskih sažetaka su ranjiva i ne preporuča ih se koristiti. Umjesto njih preporuča se upotreba SHA-256, SHA-384, SHA-512 ili SHA-3.

3.1.3. Kriptografski protokoli

Na *Linux* i ostalim operacijskim sustavima postoje standardizirani i provjereni protokoli koji se koriste za zaštitu podataka ili zaštitu komunikacijskih kanala. Najkorišteniji su IPSec (*Internet Protocol Security*), SSL/TLS (*Secure Sockets Layer / Transport Layer Security*), SSH, S/MIME (*Secure / Multipurpose Internet Mail Extensions*), OpenPGP/GnuPG/PGP (*Pretty Good Privacy*) i Kerberos. Neke funkcionalnosti spomenutih protokola se poklapaju, ali svaki od njih se koristi za specifičnu namjenu.

IPSec

IPSec omogućuje enkripciju i autentikaciju na nivou IP paketa kod protokola TCP i UDP, a najčešće se koristi za komunikaciju između dvaju računala. Na protokolu IPSec se bazira VPN (*Virtual Private Network*) koji stvara sigurni komunikacijski tunel između više korisnika ili računala.

SSH

SSH je protokol za prijavljivanje, izvršavanje naredbi i izmjenu podataka na udaljenim računalima koji koristi protokol TCP i port 22. SSH je sigurna alternativa nesigurnim protokolima za udaljeno upravljanje kao što su telnet, rlogin i rsh. Ovi nesigurni protokoli komuniciraju u čistom tekstu, tako da je moguće presresti komunikaciju između dvaju računala i otkriti informacije koje razmjenjuju, kao što su lozinke.

Također, SSH omogućuje autentikaciju računala tako da svaka strana zna točno s kim razmjenjuje informacije, što sprječava ubacivanje posrednika u komunikaciju između dvaju računala. Osim prijave s korisničkim imenom i lozinkom, moguće je i spajanje korištenjem asimetričnoga kriptografskog algoritama pomoću javnog i privatnog ključa.

Prethodno navedene nesigurne alate za udaljeno upravljanje zamjenjuje sigurni paket alata OpenSSH koji uključuju servise *ssh*, *scp*, *sftp*. Također, sadrži sshd (SSH poslužitelj), ssh-agent, ssh-keygen i ssh-add koji generira i upravlja ključevima.

OpenPGP i S/MIME

SMTP (*Simple Mail Transfer Protocol*) je protokol za razmjenu elektroničke pošte i ima malo sigurnosnih mogućnosti. Za kriptiranje, dekriptiranje i potpisivanje elektroničke pošte koriste se OpenPGP i S/MIME. Oba protokola koriste asimetrične protokole, a razlika je u tome kako do njih dolaze. S protokolom S/MIME CA potvrđuje identitet korisnika, a kod OpenPGP-a drugi korisnici potvrđuju identitet.

SSL i TLS

Jedni od najpoznatijih načina korištenja asimetrične enkripcije i digitalnih potpisa za kriptiranu komunikaciju jesu protokoli SSL i TLS. SSL/TLS radi putem protokola TCP kriptirajući promet na portu 443, autenticira računala i provjerava integritet razmijenjenih podataka. Svaki put kad se

upiše ‘https://’ u *web*-preglednik, koristi se SSL ili TLS za zaštitu prometa. Uz *web*-promet SSL/TLS se često koristi i za druge programe i protokole, kao što su poslužitelji elektroničke pošte (protokoli SMTP, POP i IMAP), FTP, programi za razmjenu poruka (protokol XMPP), virtualne privatne mreže (TLS/SSL VPN), mrežni uređaji itd.

SSL/TLS pregovara o kriptografskom algoritmu i ključevima između dvaju računala i uspostavlja kriptirani tunel. Kroz tunel se razmjenjuje promet drugih protokola. Aktualni protokol SSL je verzije 3 i najčešće se koristi za sigurniji pregled *web*-stranica, ali se sve više napušta zbog otkrivenih ranjivosti. TLS je poboljšana verzija koja učvršćuje sigurnost i unaprjeđuje fleksibilnost te sve više zamjenjuje protokol SSL. Kod TLS-a nije preporučeno koristiti verzije 1.0 i 1.1. zbog ranjivosti.

Samo korištenje SSL/TLS enkripcija ne čini komunikaciju potpuno sigurnom niti je *web*-poslužitelj otporan na napade. Korištenjem slabe enkripcije, nemogućnosti provjere certifikata, sigurnosni propusti u servisima ili SSL bibliotekama čine *web*-poslužitelj ranjivim.

3.1.4. Osiguravanje kriptografskih postavki

Mnogo je zastarjelih i ranjivih kriptografskih metoda i algoritama koji su se nekada smatrali sigurnim, ali su dokazano ranjivi ili slabi. Sljedeće preporuke kriptografskih standarda smatraju se sigurnim za korištenje, a oni nesigurni su u većini slučajeva onemogućeni prilikom instalacija novih programa. Kod operacijskih sustava ili programa koji nisu aktualni ili nadograđeni postoji mogućnost da je ostao dio konfiguracije koji sadrži nesigurne kriptografske metode. Iz tog razloga potrebno je provjeriti konfiguracije programa i uskladiti ih s kriptografskim metodama koje su sigurne. Kod pretraživanja informacija o sigurnosti kriptografskih metoda potrebno je obratiti pozornost na datum pisanja članka ili knjige da preporuke budu aktualne.

SSH

OpenSSH ima implementirane sve kriptografske metode koje su potrebni za kompatibilnost s protokolom SSH, ali oni koji su slabi ili ranjivi nisu omogućeni. Kada se SSH klijent spaja na poslužitelj, svaka strana nudi listu parametara koje je potrebno uskladiti za ostvarivanje komunikacije. Ti parametri se nalaze u `/etc/ssh/ssh_config` i `/etc/ssh/sshd_config`. `sshd_config` je serverska konfiguracija koja se primjenjuje kad se udaljena računala spajaju na lokalno. `ssh_config` je klijentska konfiguracija koja se primjenjuje kad se s lokalnog računala spaja na udaljeno računalo. Svaki korisnik pojedinačno može konfigurirati svoj SSH klijent u datoteci `~/.ssh/config` koja će nadjačati `ssh_config`.

Parametri koje je potrebno promijeniti za osiguravanje kriptografskih postavki su:

- *KexAlgorithms* – metoda razmjene ključeva koja se koristi za generiranje ključeva prije povezivanja
- *Ciphers* – kriptografski algoritmi
- MAC (*message authentication code)* – algoritam koji se koristi za zaštitu integriteta podataka
- *PubkeyAcceptedKeyTypes* – algoritam koji je korišten za generiranje javnoga ključa kojim se poslužitelj identificira lokalnom računalu.

Kako bi povezivanje bilo uspješno za svaki parametar, mora postojati barem jedan izbor koji je međusobno kompatibilan.

Preporučena osigurana kriptografska konfiguracija za `sshd_config`:

```
KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-
nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256

Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-
gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-
etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com

PubkeyAcceptedKeyTypes ssh-ed25519,ssh-rsa,ecdsa-sha2-nistp256,ecdsa-sha2-
nistp384,ecdsa-sha2-nistp521,ssh-ed25519-cert-v01@openssh.com,ssh-rsa-cert-
v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-
cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com
```

Nakon promjena kripografskih metoda potrebno je ponovno pokrenuti servis `sshd`:

```
$ sudo systemctl restart sshd
```

Za pregled stanja kriptografskih metoda serverske konfiguracije koristi se naredba `sshd`:

```
$ sudo sshd -T | grep "\(ciphers\|macs\|kexalgorithms\)"

ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-
gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
macs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128
-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com

kexalgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-
nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256
```

Preporučena osigurana kriptografska konfiguracija za `ssh_config` ili `~/.ssh/config` za pojedinog korisnika:

```
HostKeyAlgorithms ssh-ed25519-cert-v01@openssh.com,ssh-rsa-cert-
v01@openssh.com,ssh-ed25519,ssh-rsa,ecdsa-sha2-nistp521-cert-
v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp256-
cert-v01@openssh.com,ecdsa-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2-
nistp256
KexAlgorithms diffie-hellman-group-exchange-sha256
MACs hmac-sha2-512,hmac-sha2-256
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
```

SSL/TLS na *web*-servisu

Za definiranje kriptografskih metoda na *web*-servisu *apache2* koristi se *cipher suite*. *Cipher suite* je kombinacija metoda razmjene ključeva, autentikacije, enkripcije i zaštite integriteta podataka unutar protokola SSL/TLS.

Slijedi primjer konfiguracije za *cipher suite*:

```
Cipher suite TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
```

Dodatna objašnjenja svakoga dijela primjera:

- TLS: protokol za koji je definiran Cipher suite
- DHE: algoritam za generiranje i razmjenu ključeva
- RSA: algoritam za autentikaciju
- AEC_256_GCM: algoritam za enkripciju podataka
- SHA384: algoritam za generiranje kriptografskih sažetaka koji se koristi za zaštitu integriteta podataka

Prije odabira Cipher suitea potrebno je odrediti na koliko je starim *web*-preglednicima potrebno pregledavati *web*-stranice koje će se posluživati preko *web*-servisa, tj. potrebno je odrediti koliko će *web*-sjedište biti sigurno. S povećanjem sigurnosti *web*-sjedišta smanjuje se broj *web*-preglednika na kojima je moguće pregledavati zaštićene *web*-stranice.

Slijedi preporučena osigurana *apache2* konfiguracija koja omogućuje pregled *web*-stranica na sljedećim i višim verzijama klijenata: *Firefox 27*, *Chrome 30*, *IE 11* na *Windows 7*, *Edge*, *Opera 17*, *Safari 9*, *Android 5.0* i *Java 8*.

```
SSLProtocol             all -SSLv3 -TLSv1 -TLSv1.1
SSLCipherSuite          ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-
AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-
RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256
SSLHonorCipherOrder     on
SSLCompression          off
SSLSessionTickets       off
```

Sljedeća konfiguracija se preporuča ako je potrebno prikazivati *web*-sadržaj na starijim verzijama klijenata, kao što su: *Firefox 1*, *Chrome 1*, *IE 7*, *Opera 5*, *Safari 1*, *Windows XP IE8*, *Android 2.3*, *Java 7* i na svim verzijama koje su više od navedenih.

```
SSLProtocol             all -SSLv3
SSLCipherSuite          ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-
POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-
AES256-GCM-SHA384:ECDHE-ECDSA-
AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-
SHA384:ECDHE-RSA-AES128-SHA:ECDHE-
ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-
```

```
SHA256:DHE-RSA-AES128-SHA:DHE-
RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-
CBC3-SHA:EDH-RSA-DES-CBC3-SHA:
AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-
SHA:AES256-SHA:DES-CBC3-SHA:!DSS
SSLHonorCipherOrder     on
SSLCompression          off
```

Sve gore navedene konfiguracije definiraju se u `/etc/apache2/mods-available/ssl.conf` datoteci. Nakon izmjena u datoteci preporučeno je provjeriti ispravnost konfiguracije, zatim napraviti ponovno učitavanje konfiguracije *web*-servisa:

```
$ sudo apachectl configtest && apachectl -k graceful
Syntax OK
```

Za provjeru implementacije protokola SSL i TLS, te ciphera na *web*-sjedištu i daljnje preporuke koristi se nekoliko *web*-stranica koje se mogu naći na sljedećem linku https://geekflare.com/ssl-test-certificate/.

3.1.5. Generiranje ključeva za servis za udaljeni rad

Javni ključ se postavlja na računala kojima je potrebno udaljena administracija. Korisnik je autenticira koristeći privatni ključ, koji uvijek mora biti na sigurnom mjestu i preporučeno je da se zaštiti lozinkom. Ako se javni i privatni ključ podudaraju, korisniku će se omogućiti pristup udaljenom računalu.

Alat *ssh-agent* upravlja korisničkim ključevima i lozinkama, tako da ih se može kostiti za udaljenu administraciju bez potrebe za ponovnim upisivanje lozinke od strane korisnika. Također se koristi za upravljanje i generiranje kriptografskih ključeva naredbom `ssh-keygen` na operacijskim sustavima *Linux*.

Slijedi procedura:

1. Korisnik generira svoj javni i privatni ključ lozinkom naredbom `ssh-keygen`.

```
korisnik@debian:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/korisnik/.ssh/id_rsa):
Created directory '/home/korisnik/.ssh'.
Enter passphrase (empty for no passphrase): ***********
Enter same passphrase again: ***********
Your identification has been saved in /home/korisnik/.ssh/id_rsa.
Your public key has been saved in /home/korisnik/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:ad+bqMnOs3fvyKB0694gfS3DIqqCGPhB1cIWj8/eGIM korisnik@debian
The key's randomart image is:
+---[RSA 2048]----+
|   ..o           |
```

```
|    =o.          |
|   o...          |
|  .  +   .       |
|..  E = S        |
|o .  . * o o .   |
|.+ .  o = B * .  |
|o o    =.*.X.*   |
|   .....OB=.*oo  |
+----[SHA256]-----+
```

Ključ se može generirati i bez lozinke što omogućuje korištenje OpenSSH naredbi u poslovima u servisu *Cron* i skriptama bez potrebe korisničke interakcije. Ovakva praksa čini ključeve manje sigurnim.

2. Potrebno je zaštiti privatni ključ da ga samo korisnik može koristiti:

```
korisnik@debian:~$ chmod 600 /home/korisnik/.ssh/id_rsa
```

3. Za dodavanje javnoga ključa na udaljeno računalo postoji specijalizirana naredba `ssh-copy-id`.

```
korisnik@debian:~$ ssh-copy-id korisnik@192.168.56.201
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed:
"/home/korisnik/.ssh/id_rsa.pub"
The authenticity of host '192.168.56.201 (192.168.56.201)' can't be
established.
ECDSA key fingerprint is
SHA256:rYWGxUBkdtcB741rEnFfBpLPGaEDE3pfaiaXmE2e1Ec.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to
filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you
are prompted now it is to install the new keys
korisnik@192.168.56.201's password:

Number of key(s) added: 1
Now try logging into the machine, with:   "ssh
'korisnik@192.168.56.201'"
and check to make sure that only the key(s) you wanted were added.
```

Može se primijetiti da je ovo bilo prvo spajanje na udaljeno računalo jer je potrebna privola korisnika prilikom razmjene ključeva računala.

Javni ključ korisnika dodaje se u datoteku `$HOME/.ssh/authorized_keys`.

```
[korisnik@localhost ~]$ cat ~/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQD1di4StDDwPE7UXckfMu+gTSrmjZ7+n1qMyMjgzQXf/yUVY3X
saMqAWiRW77Y4qjvc5LK4BfKqTTBmcRSNXEWljBVgvUqjs1xuSgAW2zr1T4riTiIn9VoWn6I39Xim7W
9aRRY7kDOsA2oZYDGVvQ/wAKj9IDQteRkM40ikzr2aXNIbjF9YyETlpIhbFOFXOy7MeeyKlPLoPNjG0
sAoR7p0Ye6KLp44RsAhXqEI49XF4k0hTEOA7GJbzvmKjhAQCJOgxDVaRBg+9VuRHTirXn8YHW6pYZHd
pucAgVZv8gIWULwzKF3zeqik3jSt9MEbvm+BHsodtaE3PvIX9F2T80TV korisnik@debian
```

4. Slijedi povezivanje koristeći lozinku:

```
korisnik@debian:~$ ssh korisnik@192.168.56.201
Enter passphrase for key '/home/korisnik/.ssh/id_rsa': ***********
Last login: Fri Jun  1 13:20:49 2018
[korisnik@localhost ~]$
```

3.1.6. Dodavanje samopotpisanih certifikata na apache2 virtualni host

Samopotpisani certifikat ili onaj koji je potpisao CA može se koristiti za spajanje na konzolu poslužitelja, servise elektroničke pošte, *web*-servise itd. Nakon što je generiran s*amopotpisani* certifikat u sljedećem primjeru će se implementirati u virtualni host *web*-servisa.

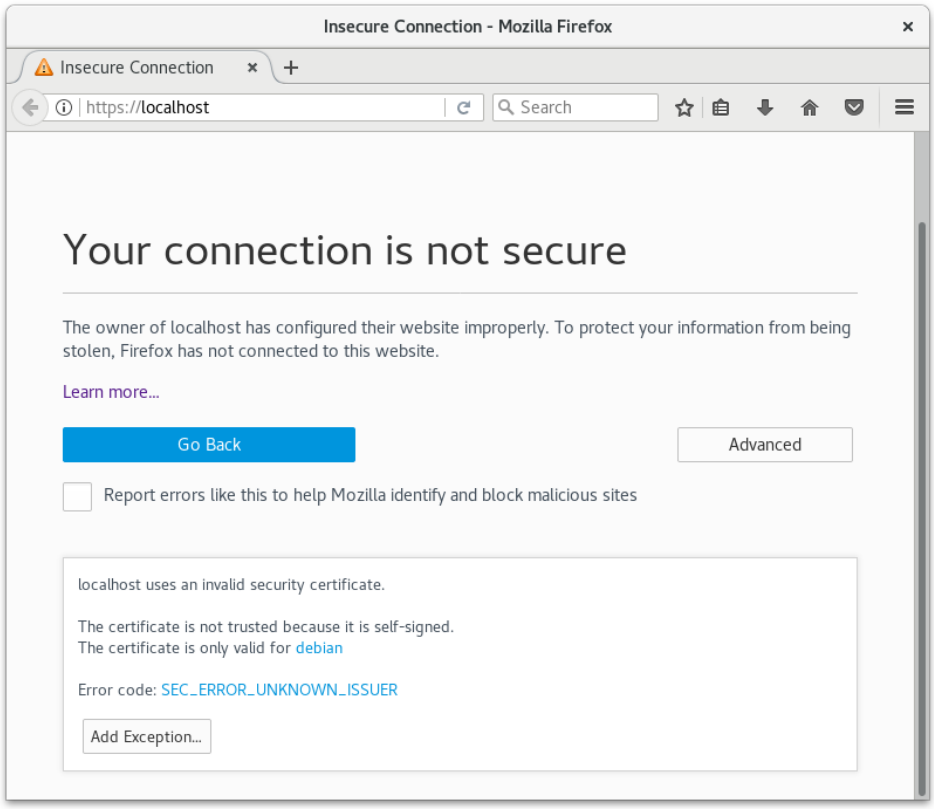
Prvo je potrebno instalirati *apache2* i omogućiti ssl modul te ponovno pokrenuti *web*-servis.

```
$ sudo apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-data apache2-utils
Suggested packages:
  apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-data apache2-utils
...

$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create
self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2

$ sudo systemctl restart apache2
```

Za sljedeći primjer koristit će se zadani virtualni host `default-ssl` koji je potrebno omogućiti pomoću sljedećih naredbi:

```
$ sudo a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2

$ sudo systemctl reload apache2
```

Za pregled virtualnoga hosta `default-ssl` (https://localhost) *web*-preglednik će ispisati poruku *"Your connection is not secure":*



U konfiguracijskoj datoteci virtualnoga hosta `default-ssl` postavljena je putanja do certifikata koji je generiran prilikom instalacije *web*-servisa. Te certifikate potrebno je zamijeniti za samopotpisani certifikat ili onaj potpisan od strane CA-a.

```
$ sudo cat /etc/apache2/sites-available/default-ssl.conf

<VirtualHost _default_:443>
  ServerAdmin webmaster@localhost

  DocumentRoot /var/www/html

  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/access.log combined

  SSLEngine on
  SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
  SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
<VirtualHost>
```

Za implementaciju SSL certifikata potrebno ga je generirati `openssl` naredbom i premjestiti javni i privatni ključ u direktorije `/etc/ssl/certs` i `/etc/ssl/private`.

```
sudo openssl req -new -x509 -days 30 -sha256 -newkey rsa:2048 -nodes -
keyout localhost.key -out localhost.crt -subj '/CN=localhost'

Generating a 2048 bit RSA private key
.......................+++
.....................................................................
..................................+++
writing new private key to 'localhost.key'
-----

$ sudo mv localhost.key /etc/ssl/private/
$ sudo mv localhost.crt /etc/ssl/certs/
```

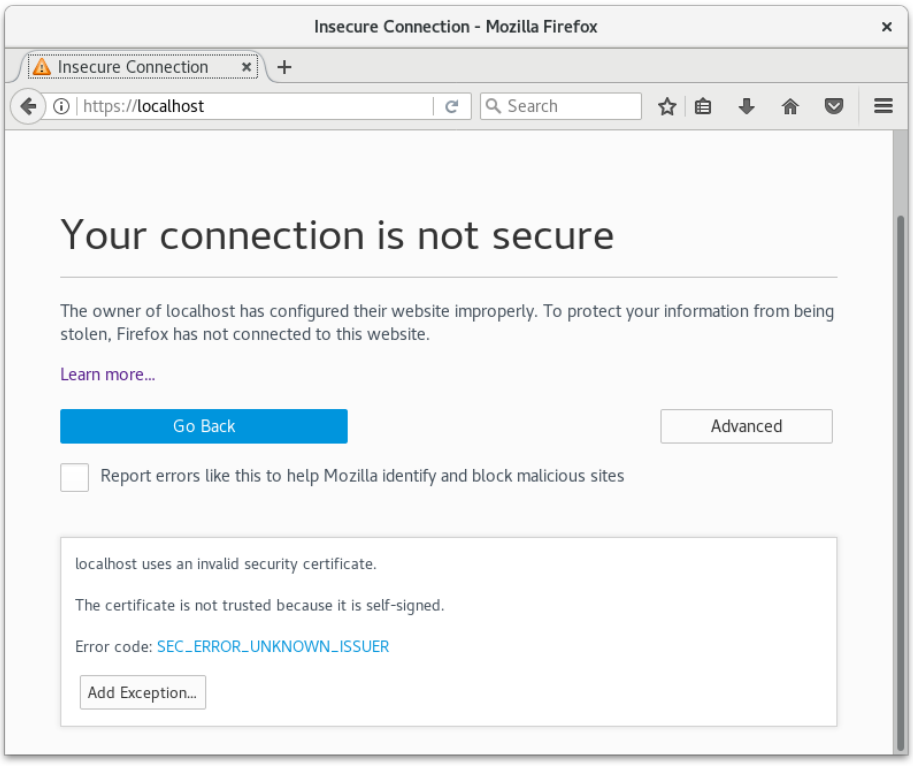
Za osiguravanje prava direktorija i datoteka vezano za certifikate preporučene su sljedeće postavke:

```
$ sudo chmod 755 /etc/ssl
$ sudo chmod 710 /etc/ssl/private

$ sudo chown -R root:root /etc/ssl/
$ sudo chown -R root:ssl-cert /etc/ssl/private/

$ sudo chmod 644 /etc/ssl/certs/*.crt
$ sudo chmod 640 /etc/ssl/private/*.key
```

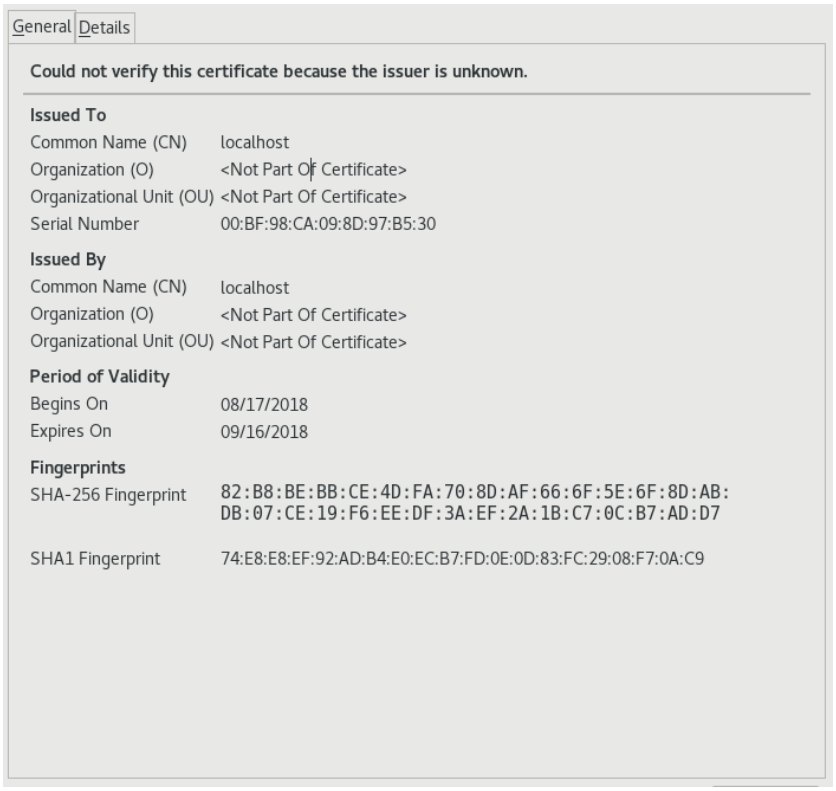
Za promjenu putanje do certifikata u `default-ssl.conf` potrebno je korigirati SSLCertificateFile i SSLCertificateKeyFile konfiguraciju i napraviti ponovno učitavanje konfiguracije web-servisa.

```
$ sudo vim /etc/apache2/sites-available/default-ssl.conf
 <VirtualHost _default_:443>

  ServerAdmin webmaster@localhost

  DocumentRoot /var/www/html

  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/access.log combined

  SSLEngine on
  SSLCertificateFile /etc/ssl/certs/localhost.crt
  SSLCertificateKeyFile /etc/ssl/private/localhost.key

<VirtualHost>

$ sudo systemctl reload apache2
```

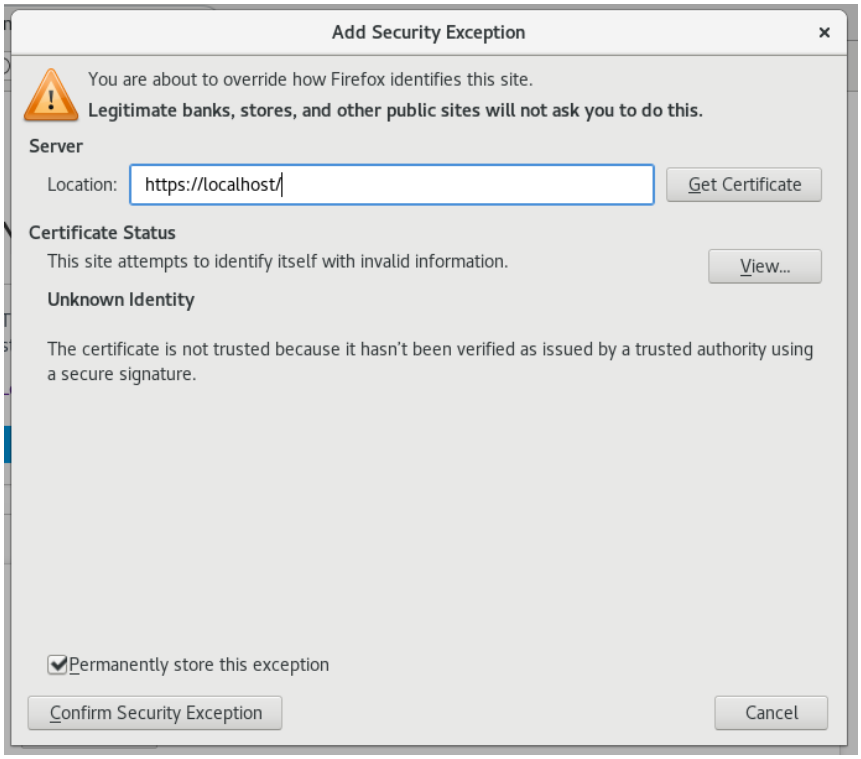
Nakon dodavanja samopotpisanoga certifikata preglednik još uvijek smatra vezu nesigurnom:

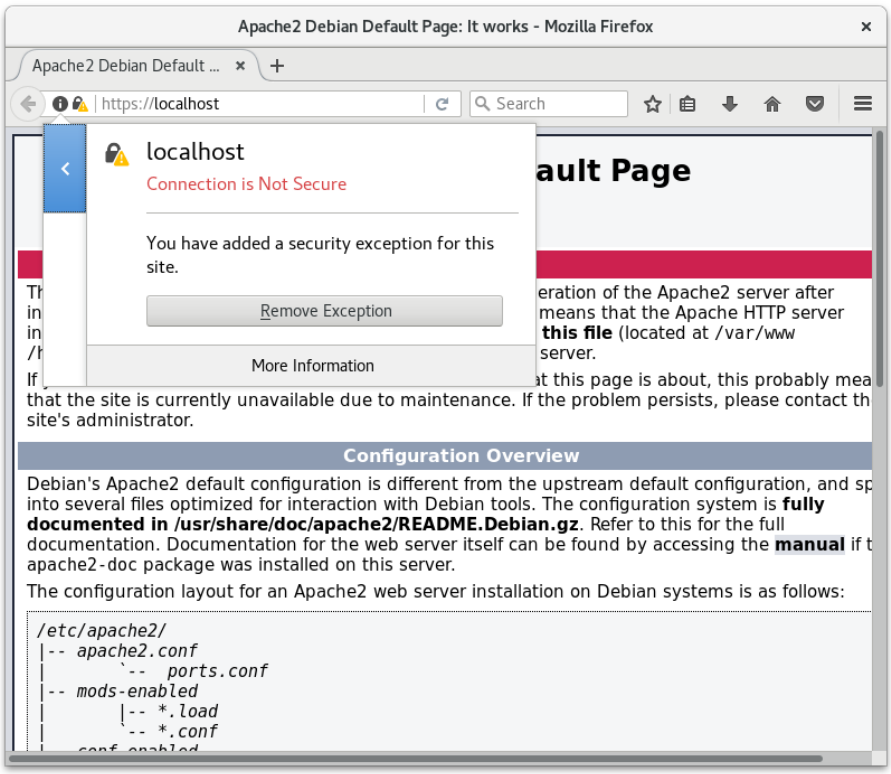


Odabirom "Add Exception" i "View" za pregled certifikata može se uočiti da je certifikat promijenjen.



S odabirom "Confirm Security Exception" *web*-stranica će se prikazati.





Ali će još uvijek prikazivati "Connection is Not Secure" oznaku jer *web*-preglednik samopotpisani certifikat ne smatra sigurnim, ali se može koristi u fazi testiranja.

3.1.7. Zanimljivi izvori

Poveznice:

- https://www.juniper.net/documentation/en_US/junos/topics/concept/certificate-digital-understanding.html
- https://www.namecheap.com/support/knowledgebase/article.aspx/786/38/what-is-an-ssl-certificate-and-what-is-it-used-for
- https://www.digicert.com/ssl/
- https://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslciphersuite

3.2. Postavke vezane za korisnike

3.2.1. Načelo najmanjih ovlasti

Jedna od glavnih uloga administriranja *Linux* poslužitelja (ili drugih informacijskih sustava) jest upravljanje korisnicima, tj. omogućavanje ili onemogućavanje korištenja funkcija operacijskog sustava, aplikacija ili podataka ovisno o korisničkim potrebama. Slučajno ili namjerno korisnici mogu naštetiti sustavu ili narušiti sigurnost sustava. To može biti obična korisnička greška, na primjer, pokretanje loše programirane skripte pod *root* ovlastima ili zlonamjerno korištenje sistemskih resursa od strane napadača ili legitimnoga korisnika.

Da bi se izbjegle neželjene situacije, preporuča se koristiti načelo najmanjih ovlasti prilikom dodjeljivanja prava. Kod primjene ovlasti, korisnici, programi ili procesi imaju minimalne ovlasti koje su potrebne za pristup informacijama ili resursima koje su potrebne za obavljanje njihovih zadataka. Na primjer, administrator ili više njih moraju imati *root*, tj. super korisničke ovlasti kako bi mogli obavljati sve potrebne zadaće na poslužitelju, ali ostalim korisnicima to nije potrebno. Za ostale korisnike može se koristiti naredba sudo gdje se može definirati koje naredbe korisnik može koristiti. Također, nije potrebno da svaki korisnik ima pristup svakom računalu na mreži, ako za to ne postoji valjani razlog.

Neki programi imaju sistemski korisnički račun pod kojim se pokreću procesi i taj račun može imati ograničene ovlasti na operacijskom sustavu. Na primjer, *apache2* treba imati *root* ovlasti kako bi otvorio port koji je manji od 1024, na primjer, 80 ili 443. Nakon što je port otvoren, *apache2* obrađuje standardne zahtjeve kao neprivilegirani korisnik, na primjer, www-data. Na ovaj način, ako poslužitelj bude kompromitiran, napadač neće imati *root* ovlasti.

Linux je iznimno fleksibilan kod dodjeljivanja prava korisnicima. Moguće je dodati nekoliko *root* korisnika ili više korisnika dodati u istu grupu s posebnim pravima. Također je moguće promijeniti prava čitanja, pisanja ili pokretanja za datoteke i direktorije, koji mogu biti definirani za vlasnika, grupu ili sve korisnike.

Načelo najmanjih ovlasti može se primijeniti na svih razinama operacijskih sustava i infrastrukture, kao što su korisnici, operacijski sustavi, procesi, mreže, baze podataka, programi itd

3.2.2. Naredba sudo

Rad kao `root` korisnik moguć je naredbom `su`, nakon upisane `root` lozinke. `Root` je korisnik koji nema ograničenja na *Linux* operacijskom sustavu te ga zbog sigurnosnog rizika i sprječavanja potencijalne štete nije preporučeno koristiti. Kao alternativa se koristi naredba `sudo` koja omogućava korisnicima i grupama izvršavanje naredbi kao neki drugi korisnik. Najčešće je taj drugi korisnik root korisnik, pa se korisnicima daju *root* ovlasti bez potrebe da se prijavljuju kao root korisnik ili da znaju root lozinku.

Naredba `sudo` koristi datoteku `/etc/sudoers` u kojoj se nalaze konfiguracije koje dolaze s instalacijom i direktorij `/etc/sudoers.d/` u koji se stavljaju dodatne korisničke konfiguracije. Za uređivanje sudo konfiguracijskih datoteka preporučuje se naredba `visudo` koja ima ugrađenu provjeru grešaka u sintaksi konfiguracije jer je moguće slučajno zabraniti pristup i sva prava `root` korisniku. Naredba `visudo` provjerava sintaksu prilikom spremanja datoteke.

Za omogućavanje korisničkih sudo ovlasti potrebno je kreirati datoteku unutar direktorija `/etc/sudoers.d/`, dati joj preporučene dozvole i dodati potrebnu konfiguraciju:

```
root@debian:~# touch /etc/sudoers.d/korisnik1
root@debian:~# chmod 440 /etc/sudoers.d/korisnik1
root@debian:~# visudo -f /etc/sudoers.d/korisnik1

korisnik1    ALL=(ALL:ALL) ALL
```

Nakon dodavanja ili promjene konfiguracije spajanjem kao korisnik1 testira se ima li korisnik ista prava kao i `root`:

```
root@debian:~# su - korisnik1

korisnik1@debian:~$ apt-get install htop
E: Could not open lock file /var/lib/dpkg/lock - open (13: Permission denied)
E: Unable to lock the administration directory (/var/lib/dpkg/), are you root?

korisnik1@debian:~$ sudo apt-get install htop
[sudo] password for korisnik1:
Reading package lists... Done
Building dependency tree
Reading state information... Done
htop is already the newest version (2.0.2-1).
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
```

Korisnik s naredbom `sudo -l` može provjeriti koje su mu naredbe omogućene:

```
korisnik1@debian:~$ sudo -l
[sudo] password for korisnik1:
Matching Defaults entries for te korisnik1 on debian:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User korisnik1 may run the following commands on debian:
    (ALL : ALL) ALL
```

Slijedi objašnjenje sintakse konfiguracije.

`korisnik1 ime_racunala=(korisnik2:grupa) naredba`

- `korisnik1` – ime korisnika na koji se primjenjuje konfiguracija.
- `ime_racunala` – ime računala sa koji se korisnik može spojiti.
- `korisnik2` – ime korisnika pod kojim korisnik može izvršavati naredbe.
- `grupa` – ime grupe pod kojom korisnik može izvršavati naredbe.

- `naredba` – naredba na koju se odnose prethodna pravila.
- `ALL` – ovisno o mjestu na kojem se nalazi u sintaksi, označava bilo koje ime računala, korisnika, grupu ili naredbu.

Slijedi nekoliko primjera konfiguracije i njihova objašnjenja:

`root ALL=(ALL:ALL) ALL` – zadana konfiguracija koja dolazi s instalacijom paketa, a definira *root* prava za root korisnika, ne preporuča se mijenjati.

`korisnik2 ALL=(ALL:ALL) /usr/bin/apt-get` – korisnik2 može izvršiti naredbu `apt-get` kao bilo koji drugi korisnik ili grupa s bilo kojega udaljenog računala.

`korisnik3 ALL=NOPASSWD:/usr/bin/updatedb` - korisnik3 može izvršiti naredbu `updatedb` bez korištenja lozinke kao root korisnik. Ako nakon znaka jednakosti "=" nije naveden korisnik ili grupa, naredba se pokreće pod root korisnikom.

`%sudo ALL=(ALL:ALL) ALL` – zadana konfiguracija koja dolazi s instalacijom paketa, a definira *root* prava za grupu sudo, tj. svaki korisnik u grupi imati će *root* ovlasti.

`%grupa1 sudo ALL=/usr/bin/systemctl restart apache2` – korisnici iz grupe grupa1 moći će ponovno pokrenuti *web*-servis.

3.2.3. Korisnička ograničenja

U trenutku kad se sumnja na (ozbiljan) sigurnosni incident, moguće je svim korisnicima (osim `roota`) zabraniti pristup terminalima. Ako postoji datoteka `/etc/nologin`, zaustavit će se svi pokušaji prijave na konzolu. Ako se korisnik uspješno autenticira, dobit će kao poruku sadržaj datoteke `/etc/nologin`.

Direktorij `/etc/security` sadrži niz datoteka koje omogućavaju administratoru ograničavanje korisničke potrošnje resursa. U direktoriju je ukupno osam konfiguracijskih datoteka:

```
$ ls /etc/security |grep conf
access.conf
capability.conf
group.conf
limits.conf
namespace.conf
pam_env.conf
sepermit.conf
time.conf
```

Najvažnije su datoteke:

- `access.conf` – onemogućava pristup korisnicima i grupama
- `group.conf` – konfiguracijska datoteka za upravljanje ovlastima članova grupa

- `limits.conf` – najvažnija datoteka koja omogućava ograničavanje brojnih parametara poput veličine datoteka, CPU-vremena, adrese, broja procesa, broj otvorenih datoteka, količina zauzete memorije i slično nad korisnicima i grupama. Po zadanome sve konfiguracije koje su definirane u datoteci `limits.conf` su nadjačane konfiguracijama u datotekama koje imaju nastavak `.conf` u direktroiju `/etc/security/limits.d/`. Preporuča se definiranje svih novih konfiguracija u spomenutom direktoriju.

Onemogućavanje pristupa korisnicima i grupama

Sintaksa svake linije konfiguracijske datoteke `access.conf` sadrži tri postavke odvojene dvotočkom: `<prava>:<korisnik/grupa>:<izvor>`

Slijedi objašnjenje dijelova sintakse:

- prava: može biti + za dozvoljavanje pristupa ili – za onemogućavanje pristupa.
- korisnik/grupa: može biti definiran jedan ili više korisnika ili grupa, te ALL što označava sve korisnike i grupe. Grupe se definiraju unutar zagrada kako bi se razlikovale od korisnika.
- izvor: može sadržavati *tty* imena, imena računala, imena domena, IP adrese, ALL za sve, LOCAL itd.

Slijedi primjer korisnika root, koji može koristiti cron, X11 terminal :0, tty1-6:

```
+ : root : crond :0 tty1 tty2 tty3 tty4 tty5 tty6
```

Upravljanje ovlastima članova grupa

Sintaksa svake linije konfiguracijske datoteke group.conf sadrži sljedeće postavke: `<servisi>;<tty>;<korisnici>;<vremena>;<grupe>`

Slijedi primjer gdje korisnik marko ima pristup grupi games na terminalu xsh izvan radnog vremena: `xsh;tty*;marko;!Wk0900-1700;games`

Upravljanje procesima korisnika

Sljedeća sintaksa odnosi se na datoteku `/etc/security/limits.conf` i sve datoteke koje imaju nastavak `.conf` u direktoriju `/etc/security/limits.d`

`<domena> <tip> <stavka> <vrijednost>`

Slijedi objašnjenje dijelova sintakse:

- <domena>: definira se korisničko ime, grupa, * za sve unose itd.
- <tip>: može biti hard pa korisnik ne može koristiti veće limite od onih koje su definirane, ili soft pa se korisnik može kretati unutar dovoljenog raspona već postojećim hard limitima.
- <stavka>: mogu biti razne stavke, na primjer, veličina datoteke, maksimalni broj procesa, maksimalni broj spajanja itd. Popis svih stavki nalazi se na poveznici: https://linux.die.net/man/5/limits.conf
- <vrijednost>: definira vrijednost stavke.

3.2.4. Jail

Alat *Chroot* omogućava promjenu korijenskoga direktorija *root* za procese i njegovu djecu tako da mijenja korijenski direktorij (koji je najčešće /) na direktorij *chroot* (npr., `/home/korisnik/radni`). Kako je promijenjeni korijenski direktorij u vrhu strukture datotečnoga sustava, programi koji koriste *chroot* ne mogu pristupiti direktorijima koji su viši od direktorija *root*. Prema tome, program ne može pristupiti datotekama izvan svog modificiranog korijenskog direktorija, a tako promijenjeno okruženje nazva se *chroot jail*. Okruženje *chroot jail* ne koristiti za procese koji se pokreću pod korisnikom `root`, jer se `root` može jednostavno izvući iz tog okruženja.

Chroot jail je koristan za testiranje programa koji potencijalno mogu promijeniti bitne sistemske datoteke ili osiguravanje okuženja kako legitimni proces ne bi kompromitirao ostatak sustava, ako se u njega provali. *Chroot jail* se može složiti za ograničavanje direktorija koje korisnik može vidjeti kad se spojiti protokolom SSH, na primjer, omogućava mu se pristup samo svome home direktoriju. Također je moguće ograničiti transfer datoteka samo na neke direktorije protokolom SFTP ili napraviti *chroot jail* za apache2, *postfix*, bind servise itd.

Konfiguracija *chroot jail* za /bin/bash naredbu

Kako bi *chroot jail* imao sve funkcionalnosti koje su mu potrebne za izvršavanje određene naredbe, nužno je dodati sve programske datoteke, konfiguracije i biblioteke.

Za stvaranje *chroot jail* okruženja prvo je nužno kopirati određenu naredbu, u ovom slučaju *bash*, u direktorij za tu svrhu.

```
$ sudo mkdir /home/korisnik/jail/bin -p
$ sudo cp /bin/bash /home/korisnik/jail/bin/
```

Naredba `/bin/bash` dinamički je povezana s dijeljenim bibliotekama, pa je i te biblioteke potrebno kopirati u direktorij gdje će se primijeniti *chroot jail*. Naredbom `ldd` provjerava se koje biblioteke koristi naredba `/bin/bash`.

```
$ sudo ldd /bin/bash
       linux-vdso.so.1 (0x00007ffe183ef000)
       libtinfo.so.5 => /lib/x86_64-linux-gnu/libtinfo.so.5
(0x00007f975a3cf000)
       libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2
(0x00007f975a1cb000)
       libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f9759e2c000)
       /lib64/ld-linux-x86-64.so.2 (0x00007f975a5f9000)

$ sudo mkdir /home/korisnik/jail/lib/x86_64-linux-gnu/ -p
$ sudo mkdir /home/korisnik/jail/lib64

$ sudo cp /lib/x86_64-linux-gnu/libtinfo.so.5
/home/korisnik/jail/lib/x86_64-linux-gnu/
```

```
$ sudo cp /lib/x86_64-linux-gnu/libdl.so.2
/home/korisnik/jail/lib/x86_64-linux-gnu/
$ sudo cp /lib/x86_64-linux-gnu/libc.so.6
/home/korisnik/jail/lib/x86_64-linux-gnu/
$ sudo cp /lib64/ld-linux-x86-64.so.2 /home/korisnik/jail/lib64
```

Nakon kopiranja svih potrebnih biblioteka naredbom `chroot` stvaramo novo okruženje za naredbu `/bin/bash`.

```
$ sudo chroot /home/korisnik/jail /bin/bash
bash-4.4#
```

Naredbom `pwd` može se provjeriti lokacija direktorija:

```
bash-4.4# pwd
/
```

Naredba `pwd` prikazuje korijenski direktorij `root`, premda je korisnikova lokacija u `/home/korisnik/jail`.

Naredba `pwd` može se pokrenuti jer je uključena u naredbu `shell`, ali za bilo koju drugu naredbu ljuska će javiti grešku jer unutar *chroot jail* okruženja nije moguće pronaći naredbe niti dinamički povezane biblioteke. Ovo je dokaz da korisnik ne može pristupiti ostalim dijelovima operacijskog sustava:

```
bash-4.4# ls
bash: ls: command not found
```

3.2.5. Lozinke

Autentikacija lozinkom glavni je način potvrde korisničkog identiteta na *Linux* distribucijama. Kvalitetno upravljanje lozinkama jako je važno za zaštitu korisnika, računala i mreže.

Lozinke moraju biti takve da ih je teško pogoditi pretraživanjem svih mogućih rješenja koristeći napad grubom silom (*brute force*) ili uspoređivanjem s izrazima iz rječnika. Sigurna lozinka stvara se prema sljedećim preporukama:

- dužina lozinke treba biti minimalno 12 do 14 znakova
- potrebno je koristiti specijalne znakove (npr. !"#$%&/()=?*), brojeve te velika i mala slova
- izbjegavati česte (https://en.wikipedia.org/wiki/List_of_the_most_common_passwords) lozinke kao što su “password”, “123456”, “admin123” itd.
- izbjegavati ime, prezime ili bilo koje druge informacije koje su osobno vezane za korisnika, na primjer, adresa stanovanja, imena rodbine, datum rođenja, imena kućnih ljubimaca itd.
- izbjegavati jezične i značenjsko smislene izraze, tj. riječi koji se mogu pronaći u rječniku ili njihove obrnute verzije

- izbjegavati ponavljanje istih izraza u istoj lozinci, npr. “adminadmin”
- izbjegavati korištenje iste lozinke za više programa, korisničkih računa itd., zbog toga što napadač, nakon uspješnog kompromitiranja jedne lokacije, može iskoristiti istu lozinku na više lokacija
- izbjegavati davanje lozinke drugim osobama, a u slučajevima kada je to nužno, potrebno je promijeniti lozinku nakon što ju je druga osoba prestala koristiti
- ne spremati lozinke u tekstualnom obliku u tablicama, tekstualnim dokumentima, fotografijama, papirićima itd., već je za upravljanje i spremanje lozinki preporučeno koristiti profesionalne alate za tu svrhu koji čuvaju lozinke u kriptiranom obliku
- mijenjati lozinke svakih nekoliko mjeseci kako bi se otežali napadi grubom silom tijekom dužeg vremena
- nova, promijenjena lozinka, ne smije imati iste znakove kao i stara
- ako je moguće koristiti mehanizam verifikacija s dvama ili više faktora, tj. kombinaciju nečega što korisnik zna (lozinka, PIN...), nečega što korisnik ima (npr. pametni telefon na kojem se generira token) ili neka fizička obilježja korisnika (zjenica oka, otisak prsta...).

Ako lozinka nije sigurna, postoji nekoliko načina na koji je napadač može saznati:

- Gruba sila – napad grubom silom testira svaku moguću kombinaciju brojeva, slova i specijalnih znakova kako bi se saznala točna lozinka. Današnja računala imaju mogućnost testirati veliki broj kombinacija u kratkom vremenu. Dužina lozinke i raznovrsnost znakova znatno utječe na smanjenje mogućnosti otkrivanja lozinke. Kad se duljina lozinke povećava, prosječno vrijeme pronalaska lozinke eksponencijalno se povećava.
- Rječnici – korištenje rječnika slično je napadu grubom silom uz pomoć standardnih riječi ili čestih lozinki. Kako bi se saznala lozinka, koriste se gotovi rječnici (npr. hrvatski, engleski, njemački...), liste čestih lozinki (npr. admin, 1234, password) i njihove kombinacije.
- Socijalni inženjering – uključuje otkrivanje lozinke koristeći osobne podatke korisnika kao što su ime, prezime, adresa stanovanja, imena rodbine, datum rođenja, imena kućnih ljubimaca itd.

Lozinke na *Linux* distribucijama

Prilikom odabira korisničke lozinke na *Linux* distribucijama izračuna se kriptografski sažetak i spremi u `/etc/shadow`. Za izračun sažetka koriste se algoritmi MD2, MD5, SHA-1, SHA-256 i SHA-512. MD2 i MD5 smatraju se ranjivim, a SHA-1 koristi premali broj bitova (160 bitova) za sažetak, pa ih se ne preporuča koristiti.

Prilikom instalacije *Debiana* konfigurira se algoritam SHA-512 koji izračunava 512 bitne kriptografske sažetke i sprema ih u `/etc/shadow`. Pravo na čitanje te datoteke ima samo korisnik `root`. Preporučeno je da se ove postavke ne mijenjaju. Napadač može pokušati doznati lozinku spajanjem na računalo preko mreže, koristeći protokole SSH ili FTP. Ovakav način napada je spor i ostavlja trag u dnevničkim zapisima, a može se spriječiti korištenjem programa unutar sustava HIDS (*host-based intrusion detection system*). Čak i ako sustav zaštite HIDS nije implementiran, napadač neće moći saznati sigurnu lozinku.

Kriptografski sažeci mogu se spremati u `/etc/passwd`, ali pravo na čitanje te datoteke imaju svi korisnici i programi na tom računalu. Ovaj način spremanja sažetaka omogućava napadaču da preuzme sažetke lozinki i na svom računalu pokuša pogoditi lozinku koristeći alate za tu svrhu. Ako je lozinka slaba, samo je pitanje vremena kada će je napadač doznati.

Uz kriptografske sažetke lozinki, u datoteci `/etc/shadow` nalaze se informacije o tome kada ističe lozinka, je li mijenjana, minimalno i maksimalno vrijeme između promjene lozinke i sl.

Stvaranje sigurne lozinke

Sigurna lozinka može se stvoriti slijedeći gore prethodno navedena pravila. Alternativa su generatori sigurnih lozinki koji imaju već implementirana pravila, tj. generiraju sigurne lozinke.

Jedan od generatora je *pwgen* i instalira se na *Debianu* naredbom `apt-get`:

```
$ sudo apt-get install pwge
```

Naredba za generiranje nekoliko sigurnih lozinki, duljine 14 znakova, jest:

```
$ pwgen -ysBv 14
Rn4nH,cV$@K|Lk \'=3Kr:/PX&T[d Ftg<!%#R3@_+,- wwJ-^sXPHM$`;7 [c!MT./\,$3}>%
fn)/PJ7|NN(XkN C(m\'{3)v<w}F7 >3`Rn93&K:,q?+ Tt7s}>[.f#+HJH qH;7FCk=<3)'
Csw3{)R? cJ%[Hb<vx"w9h& 9Rr]<3vp+v|xgN x.7||^.vq+9qWq 9L`(FvPn"F?xnJ
sPx93shN|L\!qm %d,%_3V@T#`-mV ]]h~(Hjv3#+FMk fW)X"|\{9{:_P< rL"&[T"]=<`*w7
}jRH"W"w\$ms3# !}~rp>,4TxhCV4 hq]X%@4kVP9{xq t>jc7.vs>gc?KH 7qj]}T~!h|}]c*
p);'{f#|^&wLL4 z)L('r'N)?4q#' *^c=('>,JMr4j' J%dVq4JRmFg*`? %7rmp_wfprJ9#$
HM[k7VzX`4\\?n [bddJLs;n9wh-| X<_;W3np,&?b t]kW`."]-4Pk<]
Js{{{MLH.[]{4< 3[@gVvp/`>`"fL "tkts][7*R~)V" <}hwz7?p;dH)wF J*^}k:9P7KbW)j
```

Provjeru jačine lozinke izvrsno odrađuje *web*-stranica https://howsecureismypassword.net/. Nakon upisane lozinke prikazuje se vrijeme potrebno za otkrivanje lozinke i savjeti kako poboljšati lozinku.

Sljedeći je primjer za lozinku test1234:

I primjer lozinke HM[k7VzX`4\\?n:

Forsiranje sigurne lozinke i provjera prema rječniku

Ako korisnici sami upisuju svoje lozinke, moguće je s *Linux PAM* modulom *pam_cracklib.so* forsirati korištenje sigurne lozinki. Ovaj modul također provjerava pojavljuje li se u lozinki neka riječ koja je navedena u rječniku i na taj način dodatno osigurava stvaranje sigurne lozinke. Mogu se postaviti minimalni uvjeti za lozinku kao što su dužina, broj slova, specijalnih znakova i brojeva.

Modul *pam_cracklib.so* instalira se naredbom `apt-get`:

```
$ sudo apt-get install libpam-cracklib
```

Konfiguracijska datoteka je `/etc/pam.d/common-password`, a linija koja se mijenja je:

```
password required pam_cracklib.so minlen=12 dcredit=-2 ucredit=-2
lcredit=-2 ocredit=-2 difok=6 retry=2
```

Objašnjenje konfiguracije:

- `minlen=12`: lozinka mora imati najmanje 12 znakova
- `dcredit=-2`: lozinka mora imati najmanje dva broja
- `ucredit=-2`: lozinka mora imati najmanje dva mala slova
- `lcredit=-2`: lozinka mora imati najmanje dva velika slova
- `ocredit=-2`: lozinka mora imati najmanje dva specijalna znaka
- `retry=2`: korisnik može pokušati upisati lozinku 2 puta prije nego što alat javi grešku
- `difok=6`: broj istih znakova u novoj lozinki u odnosu na staru

Naredba `passwd` mijenja staru lozinku, nakon upisa trenutačne lozinke:

```
$ passwd korisnik
Changing password for test1.
(current) UNIX password: fsd$5fdg$%!
New password: admin1234
BAD PASSWORD: it is too simplistic/systematic
New password: 1234
BAD PASSWORD: it is too short
New password: %7rmP_wfprJ9#$
Retype new password: %7rmP_wfprJ9#$
passwd: password updated successfully
```

Napomena

Ljuska ne ispisuje upisane korisničke lozinke, gornje lozinke su prikazane kako bi se bolje razumjele greške.

Testiranje jačine lozinke

Jakost lozinke može se testirati besplatnim alatom *John the Ripper*. Alat otkriva slabe lozinke koristeći kriptografske sažetke operacijskoga sustava *Linux*, na primjer, iz `/etc/shadow`, ali podržava i mnoge druge. Za svaku mogućnost lozinke izračunava se kriptografski sažetak koristeći razne algoritme i uspoređuje ih se sa sažetkom lozinke. Ako su sažeci isti, lozinka je pogođena.

Alat *John the Ripper* ima nekoliko načina rada, a ovo je zadani poredak kojim otkriva lozinke:

- *Single crack mod* pokušava doznati lozinku koristeći informacije iz `/etc/passwd` gdje se može naći korisničko ime, puno ime, adresa e-pošte itd.

- *Wordlist mod* koristi izraze iz rječnika poznatih svjetskih jezika ili često korištene lozinke. Alat može kombinirati izraze, lozinke i brojeve te je moguće koristiti vlastite liste izraza.
- *Incremental mod* grubom silom isprobava sve moguće kombinacije slova, brojeva i specijalnih znakova.

Alat *John the Ripper* instalira se naredbom `apt-get`, a naredba `unshadow` kreira datoteku koja je prilagođena za otkrivanje lozinki:

```
$ sudo apt-get install john

$ sudo /usr/sbin/unshadow /etc/passwd /etc/shadow > /tmp/sazeci_lozinki

$ cat /tmp/sazeci_lozinki
marko:$6$7hnlV8Uj$zybG9uxgHSeRwWKbG1nv8PkiPGHca0aGHUhihe7cXNdO5XD.RFZAa.D.MLq30
Ui4JWUJ/W7Jyx7qsJ25b6WsE1:1005:1005:Marko Markic:/home/marko:/bin/bash

mario:$6$3Vj6NanR$JnMmb1F8MnZJmZpTevzLOf0EmM1TRrWmNQ9TxKTpbs7yRUe.0GW2YwjeL1
NcHhP52DYllU0iD5HMvgh9moZAT/:1006:1006:Mario Maric:/home/mario:/bin/bash

dario:$6$GhrzwKIl$eOOoaXsla7cL1MS0e3NUkxxZwxD6ruGgn37zRiy12LafLRmtkVz5CufozYQPGe50
ED.8v8rIhg4E/A6RnfqyL.:1007:1007:Dario Daric:/home/dario:/bin/bash

marina:$6$0FzwfOKJ$mEbxgfW15qSeXoQF8mKAAmAYfq7ZzNxJx1Ofk2sjTvG2eOU.ty4BRQgey1o
JciHYVXLGGu6HGl/Nq6QMTatlM0:1008:1008:Marina Marinic:/home/marina:/bin/bash

maja:$6$AfwsPZ7b$IvqpXM39iuGB7.sUPsmKEaypsMyifenRirTPBsaq5ZNnUh1JosMAi4Zi4/nNbbemx
Kx9LrPlAZqRhA80ifRi/0:1009:1009:Maja Majic:/home/maja:/bin/bash

mirna:$6$6GfzKIWV$xIWBoLYU.T/z1LtyBShQUUwhkRGYe9QfgfJm28gFmhDzEoVJDDoGDG1eyiT
NgPqlCIrGQzMm1zr3gVbWx7acJ/:1010:1010:Mirna Mirnic:/home/mirna:/bin/bash
```

Naredbom `john` počinje pogađanje lozinke, a one koje se otkriju ispišu se na ekranu zajedno s korisničkim imenom. Pritiskom bilo koje tipke može se vidjeti stanje procesa, na primjer, broj pogođenih lozinki, utrošeno vrijeme itd.

```
$ sudo john --show /tmp/sazeci_lozinki
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
majamja          (maja)
mario1234        (mario)
2g 0:00:05:25 5% 2/3 0.006150g/s 132.1p/s 206.0c/s 206.0C/s heathers..boxerses
adminadmin       (marina)
3g 0:01:45:20 3/3 0.000474g/s 75.84p/s 219.2c/s 219.2C/s powis..ponta
```

Ovisno o jačini, neke lozinke nije moguće otkriti pa se proces može zaustaviti pomoću [ctrl] + [c], a sljedeća naredba prikazuje otkrivene lozine:

```
$ sudo john --show /tmp/sazeci_lozinki
mario:mario1234:1006:1006:Mario Maric:/home/mario:/bin/bash
```

```
marina:adminadmin:1008:1008:Marina Marinic:/home/marina:/bin/bash
maja:majamja:1009:1009:Maja Majic:/home/maja:/bin/bash
3 password hashes cracked, 3 left
```

3.2.6. Zanimljivi izvori

Poveznice:

- https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance
- https://en.wikipedia.org/wiki/Sudo
- https://en.wikipedia.org/wiki/Chroot
- https://smallbiztrends.com/2017/08/password-policy-best-practices.html
- https://linux.die.net/man/1/pwgen
- https://howsecureismypassword.net/
- http://www.deer-run.com/~hal/sysadmin/pam_cracklib.html
- https://linuxconfig.org/password-cracking-with-john-the-ripper-on-linux

3.2.7. Vježba 5: Generiranje i implemantacija SSL certifikata za virtualni host web-servisa

1. Prije početka rada odaberite sliku stanja virtualnoga računala **slika_jedan** za početak vježbe. Prijavite se na računalo kao korisnik **linux1**.
2. U GUI-ju pokrenite **Terminal** (*Activities* → **Terminal**). Izvršite **su -** naredbu da postanete administrator (lozinka: linux1).
3. Instalirajte *web*-servis, omogućite modul SSL i ponovno učitajte konfiguraciju *web*-servisa:

```
# apt-get install apache2
# a2enmod ssl
# systemctl reload apache2
```

4. Omogućite virtualni host **default-ssl** i ponovno učitajte konfiguraciju *web*-servisa:

```
# a2ensite default-ssl.conf
# systemctl reload apache2
```

5. U **apache2.conf** dodajte localhost pod **ServerName**, provjerite sintaksu *web*-servisa i ponovno učitajte konfiguraciju *web*- servisa:

```
# echo "ServerName localhost" >> /etc/apache2/apache2.conf
# apachectl configtest && apachectl -k graceful
```

6. Otvorite *web*-preglednik (*Activities* → *Firefox*) i upišite URL http://localhost i https://localhost. Što se prikazuje u web- pregledniku kad se otvori *web*-stranica http://localhost, a što kad se otvori https://localhost?

_____

_____

7. Generirajte asimetrične ključeve s protokolom SSL koristeći **openssl** naredbu i premjestite ih u **/etc/ssl/private/** i **/etc/ssl/certs/**:

```
# openssl req -new -x509 -days 30 -sha256 -newkey rsa:2048 \n
-nodes -keyout localhost.key -out localhost.crt \n
-subj '/CN=localhost'

# mv localhost.key /etc/ssl/private/
# mv localhost.crt /etc/ssl/certs/
```

8. Promijenite prava direktorija i datoteka za sigurnije postavke certifikata:

```
# chmod 755 /etc/ssl
# chmod 710 /etc/ssl/private

# chown -R root:root /etc/ssl/
# chown -R root:ssl-cert /etc/ssl/private/

# chmod 644 /etc/ssl/certs/*.crt
# chmod 640 /etc/ssl/private/*.key
```

9. Promijenite putanju do certifikata za **SSLCertificateFile** i **SSLCertificateKeyFile** i ponovno učitajte konfiguraciju *web*- servisa:

```
# vim /etc/apache2/sites-available/default-ssl.conf

SSLEngine on
SSLCertificateFile /etc/ssl/certs/localhost.crt
SSLCertificateKeyFile /etc/ssl/private/localhost.key

# systemctl reload apache2
```

10. Otvorite web-preglednik (*Activities* → *Firefox*) i upišite URL https://localhost. Odaberite „Advanced“, „Add Exception“ i „View“, te provjerite ispravnost certifikata. Koji je *Common Name* i kada certifikat ističe?

    _____

    _____

11. Dodajte iznimku klikom na „**Confirm Security Exception**“ i *web*-preglednik više neće prikazivati da *web*-stranica nije sigurna.

12. Provjerite verziju web-servisa:

    ```
    # dpkg -l | grep apache2
    ```

13. Otvorite *web*-stranicu https://ssl-config.mozilla.org/, upišite verziju *web*-servisa, odaberite „Apache“ i „Modern“.

14. U datoteci **/etc/apache2/mods-available/ssl.conf** i u datotekama virtualnih hostova ažurirajte konfiguraciju prema preporukama iz prethodnog koraka.
15. Provjerite ispravnost konfiguracije i ponovno učitajte konfiguraciju *web*-servisa:

```
# apachectl configtest && apachectl -k graceful
```

3.2.8. Vježba 6: Omogućavanje root ovlasti koristeći naredbu sudo

1. Prije početka rada odaberite sliku stanja virtualnoga računala **slika_jedan** za početak vježbe.
2. Prijavite se na računalo kao korisnik **linux1**. U GUI-ju pokrenite **Terminal** (*Activities* → **Terminal**). Izvršite **su -** naredbu da postanete administrator (lozinka: linux1).
3. Stvorite dva korisnika, maju i marka sa lozinkom linux1.

```
root@debian:~# adduser maja
```

```
root@debian:~# adduser marko
```

4. Instalirajte paket **sudo**:

```
root@debian:~# apt-get install sudo
```

5. Kreirajte datoteku **/etc/sudoers.d/maja**, promijenite prava i umetnite konfiguraciju:

```
root@debian:~# touch /etc/sudoers.d/maja
root@debian:~# chmod 440 /etc/sudoers.d/maja
root@debian:~# visudo -f /etc/sudoers.d/maja
maja   ALL=(ALL:ALL) ALL
```

6. Promijenite korisnika i kreirajte grupu instalacija:

```
root@debian:~# su - maja
```

```
maja@debian:~$ addgroup instalacija
```

7. Koja greška se ispisuje na ekranu i zašto?

_____

_____

8. Kreirajte grupu instalacija i dodajte korisnika marko u grupu koristeći naredbu **sudo**:

```
maja@debian:~$ sudo addgroup instalacija
maja@debian:~$ sudo vim /etc/group
instalacija:x:1006:marko
```

9. Kreirajte datoteku instalacija, promijenite prava. Zatim dodajte grupi instalacija prava za instalaciju paketa:

```
maja@debian:~$ sudo touch /etc/sudoers.d/instalacija
maja@debian:~$ sudo chmod 440 /etc/sudoers.d/instalacija
maja@debian:~$ sudo visudo -f /etc/sudoers.d/instalacija
%instalacija ALL=(ALL:ALL) /usr/bin/apt-get
```

10. Promijenite korisnika na marka i testirajte naredbu **apt-get**

```
maja@debian:~$ sudo su - marko
```

```
marko@debian:~$ sudo apt-get install htop
```

3.2.9. Vježba 7: Kreiranje i forsiranje sigurne lozinke

1. Prije početka rada odaberite sliku stanja virtualnoga računala **slika_jedan** za početak vježbe.

2. Prijavite se na računalo kao korisnik **linux1**. U GUI-ju pokrenite **Terminal** (*Activities* → **Terminal**). Izvršite **su -** naredbu da postanete administrator (lozinka: linux1).

3. Instalirajte programe *pwgen*, *libpam-cracklib* i *john*

```
# apt-get install pwgen libpam-cracklib john
```

4. Kreirajte korisnike ana i darko s lozinkom 'admin'

```
# adduser ana
# adduser darko
```

5. Koju grešku naredba **adduser** ispisuje na ekranu nakon upisa lozinke?

_____

_____

6. U datoteci **/etc/pam.d/common-password** pronađite liniju s **pam_cracklib.so** konfiguracijom i promijenite je u:

```
password required pam_cracklib.so minlen=12 dcredit=-2
ucredit=-2 lcredit=-2 ocredit=-2 difok=6 retry=2
```

7. Kao korisnik darko pokušajte promijeniti lozinu na 'test'.

8. Promijenite lozinku korisnika darko na 'test'.

```
# passwd darko
New password:test
```

9. Koju grešku naredba **passwd** ispisuje na ekranu nakon upisa lozinke i je li lozinka prihvaćena?

_____

10. Izvršite su - naredbu da postanete administrator (lozinka: linux1). Promijenite lozinku korisnika darko na 'test'.

11. Naredbom **pwgen** generirajte lozinku. Ako je potrebno, promijenite generiranu lozinku tako da ispunjava gore navedena pravila i postavite je za korisnika marko.

```
# pwgen -ysBv 12
```

12. Naredbom **unshadow** kreirajte datoteku koja će se koristiti za doznavanje lozinki:

```
/usr/sbin/unshadow /etc/passwd /etc/shadow >
/tmp/sazeci_lozinki
```

13. U *vimu* otvorite datoteku **/tmp/sazeci_lozinki** i obrišite sve linije osim onih koji u sebi sadrže korisnike ana i darko.

```
# vim /tmp/sazeci_lozinki
```

14. Naredbom **john** pokušajte saznati lozinke:

```
john --format=crypt /tmp/sazeci_lozinki
```

15. Je li *John the Ripper* otkrio neku od lozinki?

_____

_____

Prekinite proces tipkom **q**.

4. Zaštita od napada

Trajanje poglavlja:
260 min

Po završetku ovoga poglavlja moći ćete:

- razlikovati vrste mehanizama za detekciju i odbijanje napada na operacijski sustav
- objasniti kako NIDS detektira i odbija napade na mrežnoj razini
- upotrijebiti alat snort za zaštitu od mrežnih napada
- upotrijebiti Fail2ban za zaštitu od napada grubom silom
- opisati prijetnje koje virusi i neželjena pošta imaju na operacijski sustav Linux
- koristiti servise Antivirus i AntiSPAM za rješavanje prijetnji od virusa i neželjene pošte
- koristiti filtriranje neželjenih privitaka, adresa i pošiljatelja
- kriptirati pristup kroz protokol HTTPS koristeći SSL certifikat
- primijeniti preporuke za osiguravanje konfiguracije web-servisa
- primijeniti aplikativni vatrozid web-servisa u svrhu odbijanja zloćudnih upita i napada grubom silom
- koristiti servise proxy i reverse proxy za prosljeđivanje web prometa prema backend servisima ili poslužiteljima.

Ova cjelina obrađuje načine odbijanja i detekecije napada na mrežnoj razini. Obradit će se i zaštita elektroničke pošte koristeći servise Antivirus i AntiSPAM te zaštita *web*-servisa enkripcijom i očvršćivanjem konfiguracijskih postavki.

4.1. Odbijanje mrežnih napada

4.1.1. Otkrivanje i sprječavanje napada u mrežnom prometu

IDS

Zbog povećanja mrežnoga prometa na Internetu i između lokalnih računala te kompleksnosti napada na informacijske sustave potrebno je odabrati rješenja za obranu od napadača i drugih sigurnosnih prijetnji. Iako postoji veliki broj alata i metodologija, dva su najčešća načina obrane od zloćudnih aktivnosti, vatrozid i sustav za otkrivanje i sprječavanje napada (*intrusion detection systems, IDS*). Vatrozid nadzire odlazni i dolazni mrežni promet te ovisno o pravilima omogućava ili onemogućava pristup nekom računalu ili podmreži. Nakon što ga vatrozid propusti, IDS provjerava sumnjive aktivnosti u mrežnom prometu ili na lokalnim računalima. Ako otkrije zloćudne aktivnosti IDS može blokirati promet i prijaviti napad administratorima.

Dvije su osnovne vrste IDS-a:

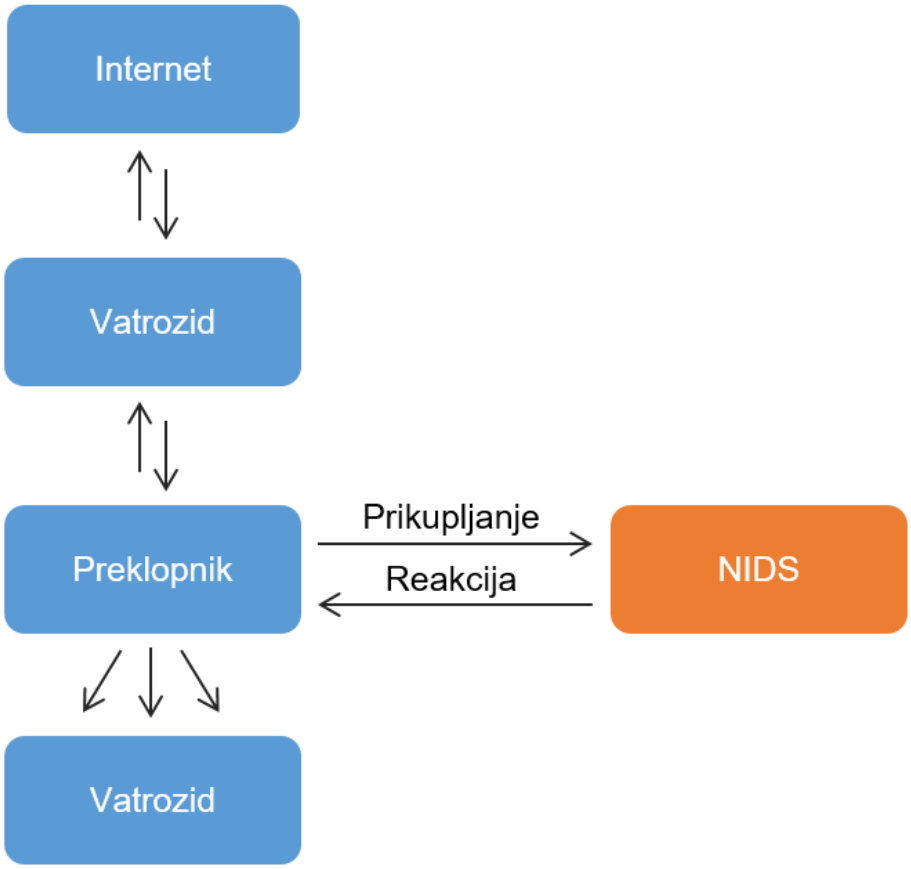
- mrežni IDS (*Network Based Intrusion Detection System, NIDS*) analizira mrežni promet i uspoređuje ga s bazom poznatih napada
- računalni IDS (*Host Based Intrusion Detection System, HIDS*) analizira dnevničke zapise operacijskoga sustava i programa te blokira zloćudne ili nestandardne aktivnosti.

NIDS

NIDS, identificira zloćudne aktivnosti ili razne anomalije koristeći samo mrežni promet. Dva su glavna načina rada NIDS-a, provjera potpisa i otkrivanje anomalija. Provjera potpisa (*checksums*) obuhvaća poznate i dokumentirane napade, a NIDS uspoređuje potpise ili uzorke znakova (čisti tekst ili regularne izraze) koje je pretražio u mrežnom prometu i one koje ima u svojoj bazi poznatih napada. Kako bi provjera bila potpuna, baza podataka mora biti kontinuirano nadograđivana novim napadima. Administrator može dodavati ili prilagođavati potpise i uzorke kada se otkrije da su zloćudni. Prilikom otkrivanja anomalija, NIDS prvo mora pratiti normalan tok mrežnoga prometa i na osnovi njega definira osnovno stanje sustava. Osnovno stanje mogu definirati i mrežni administratori po vlastitoj procjeni mrežnoga prometa. Nakon što je to stanje definirano, analizom prometa otkrivaju se otkloni od osnovnog stanja, tj. NIDS prati sve anomalije. Nakon otkrivanja napada ili anomalija, zadatak NIDS-a je zaustaviti tu aktivnosti i obavijestiti administratora sustava.

Unutar lokalne mreže, NIDS može biti instaliran na operacijskom sustavu *Linux* i prikupljati mrežni promet koji je namijenjen svim računalima u toj mreži. NIDS može biti spojen na hub, preklopnik ili TAP (*Terminal Access Point*) od kojih prima mrežni promet i analizirati ga.

Na sljedećem primjeru NIDS je spojen u lokalnoj mreži nakon vatrozida:



Sljedeći NIDS alati koriste se za instalaciju na operacijskim sustavima *Linux*:

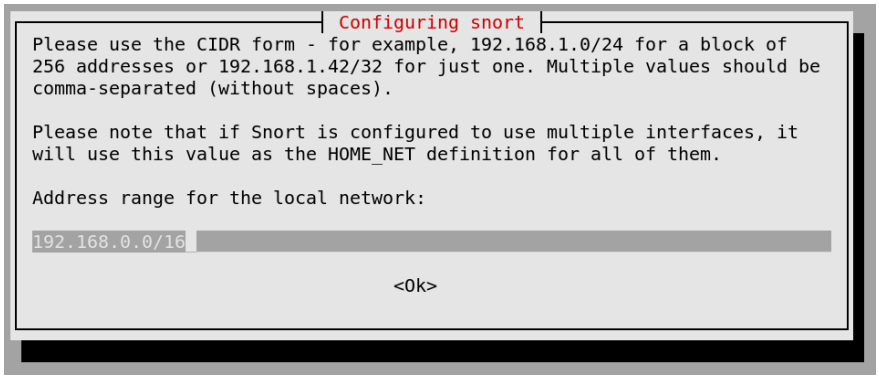
- *Snort*
- *Suricata*
- *Sagan*
- *Open WIPS-NG*
- *Bro*
- *Security Onion*

4.1.2. Alat snort

Alat *snort* je program otvorenoga kôda i koristi se za otkrivanje i sprječavanje upada u sustav analizom mrežnoga prometa u stvarnom vremenu. Također omogućuje prisluškivanje (*sniffing*) mrežnoga prometa i bilježenje paketa u dnevničke zapise. U načinu rada alat za prisluškivanje čita sve mrežne pakete i prikazuje ih na ekranu, a *packet logger* zapisuje te pakete na disk ili u bazu podataka. NIDS način rada omogućava analizu tih paketa, tj. provjerava podudaraju li se mrežni paketi prema unaprijed određenim pravilima. Načini otkrivanja zloćudnih aktivnosti temelje se na usporedbi s popisa već postojećih napada ili otkrivanje anomalija u mrežnom prometu. Alat *snort* pri instalaciji aktivira svoja pravila, ali je moguće dodati i vlastita. Nakon analize, paket se može ignorirati, zabilježiti u dnevničkom zapisu i/ili postali obavijest administratorima o njegovu prisustvu.

Alat *snort* se instalira sljedećom naredbom, a tijekom instalacije potrebno je definirati koje mrežno sučelje će se pratiti kao i podmrežu.

```
$ sudo apt-get install snort
```



Prisluškivanje

Alat *snort* u prisluškivačkom načinu rada čita mrežne pakete i prikazuje ih na ekranu. Slijedi nekoliko korisnih naredbi koje u ovom načinu rada:

- Ispis TCP/IP zaglavlja:

```
$ sudo snort -v
Commencing packet processing (pid=2728)
09/14-20:51:38.637419 192.168.56.203:22 -> 192.168.56.1:51918
TCP TTL:64 TOS:0x10 ID:11258 IpLen:20 DgmLen:124 DF
***AP*** Seq: 0x31BCB306  Ack: 0x71C0AFEC  Win: 0xFB  TcpLen: 20
```

- Ispis sadržaja paketa:

```
$ sudo snort -v
Commencing packet processing (pid=2728)
09/14-20:51:38.637419 192.168.56.203:22 -> 192.168.56.1:51918
TCP TTL:64 TOS:0x10 ID:11258 IpLen:20 DgmLen:124 DF
***AP*** Seq: 0x31BCB306  Ack: 0x71C0AFEC  Win: 0xFB  TcpLen: 20
80 E7 3C BF 20 53 BF 1B 21 FD A4 CB 91 C5 BF 1A  ..<. S..!.......
D9 80 59 E8 B5 A2 E0 D1 B4 5B FE C9 F1 6E 10 F7  ..Y......[...n..
3B DE 9C D1 25 2A BE 63 AE 41 35 18 16 57 A5 64  ;...%*.c.A5..W.d
54 C6 9C 1D BD A7 45 76 03 DD 26 04 5D 80 58 89  T.....Ev..&.].X.
1C 7E FD 1F D6 76 40 57 F7 A7 08 BF 36 AD 3D E1  .~...v@W....6.=.
91 75 7F 68 9D 22 D9 51 36 16 99 6B E5 E4 5C A7  .u.h.".Q6..k..\.
15 4E C5 CE EE 4E 39 72 B4 31 8A 8C 0A 6F AB 6C  .N...N9r.1...o.l
AB B0 89 AD ED F8 CA C1 EE 7C B3 B7 16 EB C0 12  .........|......
39 02 8E D7 7A A9 11 71 15 16 F0 6E 9E 96 50 78  9...z..q...n..Px
27 08 32 C3 28 97 C9 E7 5A 07 04 73 FD 34 88 51  '.2.(...Z..s.4.Q
E5 57 3B B0 6C AF C4 CC B1 BD CF 56 D9 E7 BA 11  .W;.l......V....
A2 81 C0 6A 5B 66 E0 BC 06 E8 0A 6F 03 CA EC CF  ...j[f.....o....
3E 31 B9 C0 46 F4 29 A4 B4 EB 3E 5A CE 5C F6 A7  >1..F.)...>Z.\..
BC 86 5A 29 BB 9D A8 19 D3 BF B8 56 08 96 74 AC  ..Z).......V..t.
EA 98 FA 76 8D 9B 27 E8 0A FB 3E 42 59 D4 E6 A4  ...v..'...>BY...
B1 3C 6B F1 94 AF 16 A7 67 46 2C C4 F8 88 25 91  .<k.....gF,...%.
03 03 9F F9 6D 0D 81 A6 86 1A EC 30 17 20 A9 DA  ....m......0. ..
3D 15 2D C6 42 22 78 CA 35 BC 66 D9 0A 84 03 37  =.-.B"x.5.f....7
92 1B 67 1B 12 73 05 6B 80 4B 20 6A 03 2D EE 1E  ..g..s.k.K j.-..
A4 23 C3 9F 0E B3 B9 77 25 12 22 8E 34 73 0B 2A  .#.....w%."4s.*
B7 26 70 9F F6 47 16 1D CA 6C 26 56 7B A5 9C 18  .&p..G...l&V{...
D8 DC 39 B6 6B B6 0A 1E 75 1A 85 48 29 AD 43 72  ..9.k...u..H).Cr
1C 26 EB 2B 56 5E 88 CA 84 25 8B 01 34 6A 86 61  .&.+V^...%..4j.a
FC 6F 2C 2A DE F0 CB D3 1C E2 63 61 06 F1 52 27  .o,*......ca..R'
2F DA 73 65 34 03 B3 A2 F7 6B E0 D7 BB 52 9D D9  /.se4....k...R..
04 A0 B7 17 3C B7 8D D3 F3 9B BA 37 C0 A2 66 99  ....<......7..f.
B5 D5 73 38 01 F5 C5 2A 2C 3F 84 8A 34 32 8C 15  ..s8...*,?..42..
D2 D3 91 79 B4 D6 31 FD 6C 96 E8 A1 2B B0 17 99  ...y..1.l...+...
17 8E 1B A8 BB C7 3C 8A 0D D2 C0 FE 8A 68 F7 84  ......<......h..
4C 47 22 94 97 FE 7A 3B 07 0E B2 CE BE B0 4B 08  LG"...z;......K.
9D 5C B8 72 4B 72 8D 52 E9 1D E7 C8 00 D0 EE D4  .\.rKr.R........
B6 1B C9 AE C1 CA C2 F3 61 3B 75 17 79 51 67 8B  ........a;u.yQg.
80 8C AD E2 EB 6E 92 1A 40 D1 52 65 2E EA AD 5F  .....n..@.Re..._
02 2C 0F E6 7D 24 91 8F 50 68 49 53 90 E2 40 ED  .,..}$..PhIS..@.
27 D2 1F 31                                      '..1
```

- Ispis zaglavlja podatkovnoga sloja:

```
$ sudo snort -e
Commencing packet processing (pid=2716)
09/14-20:47:35.868556 08:00:27:D6:44:BA -> 0A:00:27:00:00:15 type:0x800 len:0x7A
192.168.56.203:22 -> 192.168.56.1:51918 TCP TTL:64 TOS:0x10 ID:11204 IpLen:20
DgmLen:108 DF
***AP*** Seq: 0x31BC69AA  Ack: 0x71C0AC7C  Win: 0xFB  TcpLen: 20
```

- naredba `snort -vde` je kombinacija svih gore navedenih naredbi

Bilježenje paketa

Alat *snort* omogućuje spremanje svih podataka koje je prikupio prisluškivanjem. Sljedeća naredba bilježi ispis naredbe u prethodno stvoren direktorij:

```
$ sudo snort -vde -l /var/log/snort
```

Za spremanje velike količine mrežnoga prometa, u svrhu smanjivanja datoteke, zapis se može spremiti u binarnom zapisu gdje se zapisuje cijeli paket:

```
$ sudo snort -l /var/log/snort -b
```

Za čitanje spremljenih zapisa koristi se argument `-r`:

```
$ sudo snort -r /tmp/log/snort.log.1536964272
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to read-file.
Acquiring network traffic from "/tmp/log/snort.log.1536964272".

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.8.1
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.8

Commencing packet processing (pid=1241)
09/15-00:31:12.498773 192.168.56.203:22 -> 192.168.56.1:50219
TCP TTL:64 TOS:0x10 ID:18313 IpLen:20 DgmLen:108 DF
***AP*** Seq: 0xCEEFCF53  Ack: 0xCE89A884  Win: 0xFB  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
WARNING: No preprocessors configured for policy 0.
09/15-00:23:09.851248 192.168.56.1:50219 -> 192.168.56.203:22
TCP TTL:128 TOS:0x0 ID:7468 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xCE898C5C  Ack: 0xCEEF2597  Win: 0xFF  TcpLen: 20
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/15-00:23:10.834634 192.168.56.203:22 -> 192.168.56.1:50219
TCP TTL:64 TOS:0x10 ID:18020 IpLen:20 DgmLen:156 DF
***AP*** Seq: 0xCEEF2597  Ack: 0xCE898C5C  Win: 0xFB  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
09/15-00:23:10.877202 192.168.56.1:50219 -> 192.168.56.203:22
TCP TTL:128 TOS:0x0 ID:7469 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xCE898C5C  Ack: 0xCEEF260B  Win: 0xFF  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/15-00:23:11.856609 192.168.56.203:22 -> 192.168.56.1:50219
TCP TTL:64 TOS:0x10 ID:18021 IpLen:20 DgmLen:156 DF
***AP*** Seq: 0xCEEF260B  Ack: 0xCE898C5C  Win: 0xFB  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

===============================================================================
Run time for packet processing was 0.49571 seconds
Snort processed 304 packets.
Snort ran for 0 days 0 hours 0 minutes 0 seconds
   Pkts/sec:          304
===============================================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       782336
  Bytes in mapped regions (hblkhd):      12906496
  Total allocated space (uordblks):      671728
  Total free space (fordblks):           110608
  Topmost releasable block (keepcost):   100240
===============================================================================
Packet I/O Totals:
   Received:          304
   Analyzed:          304 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:          304 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:          304 (100.000%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:            0 (  0.000%)
        TCP:          296 ( 97.368%)
        IP6:            0 (  0.000%)
…
   IP4 Disc:            8 (  2.632%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
```

```
All Discard:            8 (  2.632%)
      Other:            0 (  0.000%)
Bad Chk Sum:          108 ( 35.526%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:            0 (  0.000%)
     S5 G 2:            0 (  0.000%)
      Total:          304
===============================================================================
Snort exiting
```

Ispis naredbe prikazuje načina rada alata *snort*, lokaciju datoteke, te listu informacija o paketima uključujući IP adresu i TCP/UDP/ICMP zaglavlja. Iza liste svih paketa, sumarno se ispisuju broj paketa uključujući protokole, fragmentacijsku statistiku itd.

Način rada NIDS-a

Analiziranje mrežnoga prometa prema unaprijed određenim pravilima i izvođenje reakcije vrši se sljedećom naredbom:

```
$ sudo snort -A console -c /etc/snort/snort.conf -l /var/log/snort -i enp0s3
```

Argumenti naredbe su:

- `-A console` ispisuje na ekranu pravila koja se podudaraju
- `-c /etc/snort/snort.conf` datoteka konfiguracije
- `-i enp0s3` mrežno sučelje koje se analizira
- `-l /var/log/snort` datoteka spremanja zapisa

Kada se pokrene naredba na računalu s velikim mrežnim prometom, može se vidjeti prikaz pravila koja se aktiviraju. Kao na primjer, prikaz sljedećega mrežnog skeniranja:

```
$ sudo snort -A console -c /etc/snort/snort.conf -l /var/log/snort -i enp0s3
09/15-01:48:02.788553  [**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3] {UDP}
192.168.56.1:64673 -> 239.255.255.250:1900
09/15-01:48:03.788957  [**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3] {UDP}
192.168.56.1:64673 -> 239.255.255.250:1900
09/15-01:48:04.789950  [**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3] {UDP}
192.168.56.1:64673 -> 239.255.255.250:1900
09/15-01:48:05.790800  [**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3] {UDP}
192.168.56.1:64673 -> 239.255.255.250:1900
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

U prethodnom primjeru alat *snort* koristi sva pravila koja su već definirana u: `/etc/snort/snort.conf`

Alat *snort* ima opciju stvaranja prilagođenih pravila kojima se testira ispravan rad servisa ili se prati stanje neuobičajenoga mrežnog prometa. Sva lokalna pravila konfiguriraju se u datoteci `$ sudo vim/etc/snort/rules/local.rules` i sljedeća linija konfiguracije će prikazati obavijest ako netko pokuša pingati računalo:

```
$ sudo vim /etc/snort/rules/local.rules
alert icmp any any -> $HOME_NET any (msg:"Pokusaj pinganja";
sid:1000099;)
```

Nakon pokretanja naredbe može se primijetiti aktivirano pravilo:

```
$ sudo snort -A console -c /etc/snort/snort.conf -l /var/log/snort -i enp0s3

09/15-01:46:49.013125  [**] [1:382:7] ICMP PING Windows [**] [Classification:
Misc activity] [Priority: 3] {ICMP} 192.168.56.1 -> 192.168.56.203
09/15-01:46:49.013125  [**] [1:1000002:1] Pokusaj pinganja [**] [Priority: 0]
{ICMP} 192.168.56.1 -> 192.168.56.203
09/15-01:46:49.013125  [**] [1:384:5] ICMP PING [**] [Classification: Misc
activity] [Priority: 3]
{ICMP} 192.168.56.1 -> 192.168.56.203
09/15-01:46:49.013145  [**] [1:1000002:1] Pokusaj pinganja [**] [Priority: 0]
{ICMP} 192.168.56.203 -> 192.168.56.1
09/15-01:46:49.013145  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc
activity] [Priority: 3]
{ICMP} 192.168.56.203 -> 192.168.56.1
09/15-01:46:50.014462  [**] [1:382:7] ICMP PING Windows [**] [Classification:
Misc activity] [Priority: 3]
{ICMP} 192.168.56.1 -> 192.168.56.203
09/15-01:46:50.014462  [**] [1:1000002:1] Pokusaj pinganja [**] [Priority: 0]
{ICMP} 192.168.56.1 -> 192.168.56.203
09/15-01:46:50.014462  [**] [1:384:5] ICMP PING [**] [Classification: Misc
activity] [Priority: 3]
{ICMP} 192.168.56.1 -> 192.168.56.203
09/15-01:46:50.014481  [**] [1:1000002:1] Pokusaj pinganja [**] [Priority: 0]
{ICMP} 192.168.56.203 -> 192.168.56.1
09/15-01:46:50.014481  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc
activity] [Priority: 3]
{ICMP} 192.168.56.203 -> 192.168.56.1
09/15-01:46:51.016001  [**] [1:382:7] ICMP PING Windows [**] [Classification:
Misc activity] [Priority: 3]
{ICMP} 192.168.56.1 -> 192.168.56.203
```

Pravila

Sintaksa za izradu pravila je jednostavna i fleksibilna, a pomoću postojećih ili vlastitih pravila razlikujemo normalni mrežni promet od zloćudnog. Svako pravilo mora imati sljedeće komponente u točno navedenom poretku:

- Reakciju kad se pravilo aktivira u usporedbi s mrežnim prometom, a može biti obavijest (*alert*), zapis (*log*), ignoriranje (*pass*).
- Protokol, TCP, UDP, ICMP, ili IP.
- Izvorišna IP adresa, podmreža ili više njih.
- Izvorišni port ili više njih.
- Operator smjera specificira smjer prometa, na primjer -> definira kretanje s IP adrese koja je prva napisana do druge IP adrese, a <> definira promet koji se i šalje i prima s obiju IP adresa.
- Odredišna IP adresa, podmreža ili više njih.
- Odredišni port ili više njih.
- Poruka koja će se ispisati na ekranu ili se zabilježiti u dnevničkom zapisu.
- Sid – jedinstveni identifikacijski broj pravila.
- Sadržaj paketa.

Sljedeće pravilo poslat će obavijest i zapisati mrežni promet u dnevnički zapis ako s bilo koje IP adrese (*any*) i bilo kojega porta (*any*) netko *pinga* (protokol ICMP) IP adresu ($HOME_NET) koja je navedena u `/etc/snort/snort.debian.conf`. Poruka koja će se ispisati stavlja se u navodnike iza msg.

```
alert icmp any any -> $HOME_NET any (msg:"Pokusaj pinganja"; sid:1000099;)
```

Sav promet protokolom TCP koji nije s podmreže 10.0.0.1/8, a dolazi na IP adresu 192.168.53.201, bit će zabilježen u dnevničkom zapisu:

```
log tcp !10.0.0.1/8 any -> 192.168.53.201 any (msg: "Nezeljeni promet"; sid:1000098; )
```

Obavijest će se poslati ako se u sadržaju paketa pronađe sadržaj "90E8 C0FF FFFF" paketa s bilo koje IP adrese prema podmreži 192.168.53.0/24 i portu 143.

```
alert tcp any any -> 192.168.53.0/24 143 (msg:”IMAP Buffer overflow!”;content:”90E8
C0FF FFFF”; sid:1000097;)
```

4.1.3. Zaštita od napada grubom silom

Napad grubom silom koristi se za otkrivanje lozinke na udaljenim računalima ili otkrivanje skrivenih *web*-stranica i sadržaja unutar *web*-aplikacija. U svojoj osnovi napad se temelji na isprobavanju svih mogućih kombinacija (npr. za otkrivanje lozinke može koristiti alat *John the Ripper*), dok jedna kombinacija slova, posebnih znakova i brojeva ne uspije. Uspješnost je veća ako se generira više kombinacija u kraće vrijeme ili produljivanjem vremena utrošenog u napad. Takav napad može potrajati, ali ako operacijski sustav i njegovi resursi nisu osigurani, bit će kompromitirani. Također se mogu koristiti rječnici ili lista čestih lozinki kako bi se skratilo vrijeme otkrivanja lozinke.

Napad grubom silom najčešće se vrši na udaljeno računalo pokušajima spajanja protokolom SSH ili FTP. Za smanjivanje mogućnosti otkrivanja lozinke pri takvom napadu preporučeno je koristiti što duže i kompleksnije lozinke, ali i smanjiti broj mogućih spajanja za pojedinog korisnika. Ako je

maksimalan broj pokušaja namješten na 3 pokušaja, napadač nakon 3. pokušaja određen vremenski period neće više moći isprobavati mogućnosti. U ovom slučaju legitimni korisnik, ili više njih, se također neće moći spojiti. *Web*-stranice dopuštaju velik broj mogućih spajanja, pa nije moguće zabraniti pristupe po korisniku, jer legitimni korisnici često ne bi imali mogućnosti pristupa *web*-stranici.

Moguće je da napadač pokušava istu lozinku za više korisnika. Najčešći su pokušaji za korisnike koji imaju česta imena, npr. root, admin, administrator, mysql itd., pa se preporučuje ne koristiti takva imena. Općenito se korisniku root treba onemogućiti spajanje s udaljenih računala. Udaljeno računalo se dodatno može zaštititi ako se omogući spajanje samo s pojedinih IP adresa ili korištenje kombinacije privatnog i javnog ključa.

Fail2ban

Osim navedenih preporuka, postoje alati koji su specijalizirani za sprečavanje napada grubom silom. Najpopularniji alat koji se koristi za operacijski sustav *Linux* jest *Fail2ban*. Alat pregledava autentikacijske zapise, na primjer, `/var/log/auth.log` i `/var/log/apache2/access.log` te onemogućava promet s IP adresa koje imaju mnogobrojne pokušaje spajanja. *Fail2ban* prilikom instalacije aktivira mnoge predefinirane *jailove* za razne servise, npr. *ssh, ftp, apache2, named, squid, mysql, nagios* itd. Nakon što se jedan od tih *jailova* aktivira, IP adresa se na određeno vrijeme dodaje u *iptables* i šalje se elektronička pošta administratorima.

Servis *Fail2ban* instalira se apt-get, a pokreće naredbom `systemctl`:

```
$ sudo apt-get install fail2ban
$ sudo systemctl restart fail2ban
```

Kako bi se servis pokrenuo nakon ponovnog pokretanja računala potrebno je pokrenuti naredbu:

```
$ sudo systemctl enable fail2ban
```

Konfiguracije servisa *Fail2ban* nalaze se u direktoriju `/etc/fail2ban`, a glavna konfiguracijska datoteka je `jail.conf` koja ima predefinirane *jailove*. Za primjenu lokalne konfiguracije potrebno je kopirati navedenu datoteku u `/etc/fail2ban/jail.local`, jer će nadogradnja servisa *Fail2ban* obrisati sve promijenjene konfiguracije iz `jail.conf`.

Nakon kopiranja datoteke, jail.local će prikazivati zadane konfiguracije koje dolaze s instalacijom:

```
[DEFAULT]
ignoreip = 127.0.0.1/8
bantime  = 600
findtime  = 600
maxretry = 5
destemail = root@localhost
```

Više o konfiguraciji:

- `ignoreip`: dodavanje IP adresa ili podmreža koje se ne blokiraju, čak i ako napad dolazi s njih
- `maxretry`: broj neuspješnih spajanja s neke IP adrese prije nego što se ista blokira
- `findtime`: vremenski period za iskorištavanje maksimalnoga broja spajanja, na primjer, ako se korisnik neuspješno pokušava spojiti 5 (*maxretry*) puta unutar 600 sekundi (*findtime*), IP adresa će se blokirati
- `bantime`: vrijeme na koje će se IP adresa blokirati u sekundama, ako je brojka negativna, IP adresa će zauvijek biti blokirana
- `destemail`: adresa elektroničke pošte na koju će se poslati obavijest o blokiranju IP adrese.

Zaštita za pojedine servise dodaje se u direktorij `jail.d`. Radi preglednosti preporučeno je da sve konfiguracije za jedan servis budu u jednoj datoteci. Te datoteke moraju imati datotečni nastavak `.conf`. Pri instalaciji *Fail2ban* paketa uključena je zaštita za servisni proces *sshd*:

```
$ cat /etc/fail2ban/jail.d/defaults-debian.conf
[sshd]
enabled = true
```

Trenutačno stanje uključenih *jailova* provjerava se naredbom:

```
$ sudo fail2ban-client status
Status
|- Number of jail:   1
`- Jail list:  sshd
```

Za provjeru stanja blokiranih IP adresa uz gornju naredbu potrebno je dodati ime *jaila*:

```
$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed:     0
|  |- Total failed:  15
|  `- File list:     /var/log/auth.log
`- Actions
   |- Currently banned:     1
   |- Total banned:  3
   `- Banned IP list:       192.168.56.1
```

Jedna IP adresa je blokirana, 192.168.56.1, što se može potvrditi naredbom `iptables`:

```
$ sudo iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
f2b-sshd   tcp  --  0.0.0.0/0            0.0.0.0/0            multiport dports
22

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain f2b-sshd (1 references)
target     prot opt source               destination
REJECT     all  --  192.168.56.1         0.0.0.0/0            reject-with icmp-
port-unreachable
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
```

Za deblokiranje IP adrese prije konfiguriranog isteka vremena (*bantime*) koristi se argument `set` s navedenim *jailom* i `unbanip` nakon kojeg se specificira IP adresa:

```
$ sudo fail2ban-client set sshd unbanip 192.168.56.1
192.168.56.1
```

Konfiguriranje i aktiviranje *jaila*

Svi postojeći *jailovi* koji se mogu aktivirati navedeni su unutar uglatih zagrada u `jail.conf`, a mogu se prikazati naredbom:

```
$ grep -Ris '^\[' /etc/fail2ban/jail.conf | grep -v 'INCLUDES\|DEFAULT'
[sshd]
[sshd-ddos]
[dropbear]
[selinux-ssh]
[apache-auth]
[apache-badbots]
[apache-noscript]
[apache-overflows]
[apache-nohome]
[apache-botsearch]
[apache-fakegooglebot]
[apache-modsecurity]
[apache-shellshock]
[openhab-auth]
[nginx-http-auth]
```

```
[nginx-limit-req]
[nginx-botsearch]
[php-url-fopen]
.....
```

Za aktiviranje pojedinoga *jaila* potrebno je stvoriti datoteku unutar direktorija `jail.d` i postaviti početne konfiguracije:

```
$ sudo vim /etc/fail2ban/jail.d/apache-auth.conf
[apache-auth]
enabled  = true
```

Nakon promjene konfiguracije potrebno je ponovno pokrenuti servis *Fail2ban*:

```
$ sudo systemctl restart fail2ban
```

4.1.4. Zanimljivi izvori

Poveznice:

- https://linuxsecurityblog.com/2018/05/24/setting-up-a-snort-ids-on-debian-linux/
- https://www.linode.com/docs/security/using-fail2ban-for-security/
- https://www.comparitech.com/net-admin/network-intrusion-detection-tools/

4.1.5. Vježba 8: Zaštita od napada grubom silom

1. Prije početka rada odaberite sliku stanja virtualnoga računala **slika_jedan** za početak vježbe.
2. Prijavite se na računalo kao korisnik **linux1**. U GUI-ju pokrenite **Terminal** (*Activities* → **Terminal**). Izvršite **su -** naredbu da postanete administrator (lozinka: linux1).
3. Instalirajte servis *Fail2ban* i ponovno pokrenite servis *Fail2ban*.

   ```
   # apt-get install fail2ban
   # systemctl restart fail2ban
   ```

4. Provjerite je li servis aktivan naredbom:

   `# systemctl status fail2ban`

5. Kreirajte novu konfiguraciju datoteku jail.local

   `# touch /etc/fail2ban/jail.local`

6. Zašto je potrebno kreirati novu konfiguraciju?

7. U `local.jail` dodajte konfiguraciju da se nakon dva pogrešna unosa lozinke IP adresa blokira na 20 minuta.

   Ponovno pokrenite servis *Fail2ban*.

```
# vim /etc/fail2ban/jail.local
[DEFAULT]
bantime = 1200
maxretry = 2
```

8. Provjerite je li omogućen *sshd jail*. Ako nije, omogućite ga i ponovno pokrenite servis *Fail2ban*.

```
# fail2ban-client status
# vim /etc/fail2ban/jail.d/defaults- debian.conf
[sshd] enabled = true
# systemctl restart fail2ban
```

9. Stvorite korisnika marko s proizvoljnim postavkama.

```
# adduser marko
```

10. Uključite praćenje dnevničkih zapisa servisa Fail2ban **tail** naredbom:

```
# tail -f /var/log/fail2ban.log
```

11. Koristeći program **putty** u *Windows* okruženju pokušajte se spojiti na IP adresu kao korisnik marko koristeći krivu lozinku.

    marko@192.168.2.1

12. Što se dogodi nakon što nekoliko puta upišete krivu lozinku?

13. Što je zabilježeno u dnevničkom zapisu?

14. Je li ista IP adresa zabilježena u servisu *iptables* i kao ispis naredbe **fail2ban-cilent**?

```
# iptables -nL
# fail2ban-client status sshd
```

15. Uklonite IP adresu **fail2ban-cilent** naredbom i **unbanip** atributom.

```
# fail2ban-client set sshd unbanip x.x.x.x
```

4.2. Zaštita elektroničke pošte

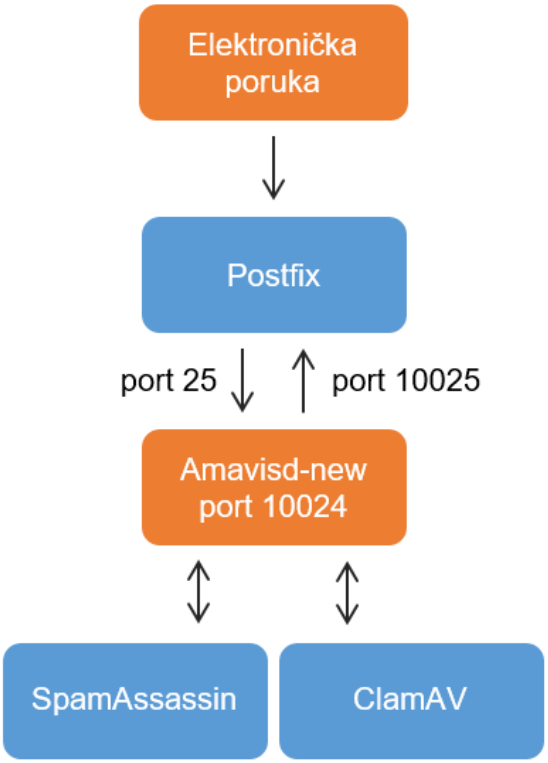
4.2.1. Servis Antivirus

Virusi su programi instalirani na računalu žrtve koji vrše zloćudne aktivnosti i repliciraju se ako je to moguće. Jedan od načina preuzimanja virusa je putem privitka elektroničke pošte. Korisnik, misleći da otvara legitimni sadržaj, otvori program i inficira svoje računalo. Virus se može replicirati tako da se pošalje na sve adrese elektroničke pošte iz žrtvinog adresara.

Procesi servisa elektroničke pošte na operacijskom sustavu *Linux* nemaju *root* ovlasti, pa virusi koji su napisani za *Linux* mogu imati prava koja ima i servis elektroničke pošte. Takva prava nisu dovoljna da se virus proširi na cijeli sustav pa je s tim i njegovo djelovanje ograničeno, ali to ne znači da takvi virusi ne postoje. *ClamAV*, uz bazu virusa pisanih za *Linux*, ima i one viruse koji se mogu naći na operacijskom sustavu *Windows* jer se klijenti i s njega spajaju na poslužitelj elektroničke pošte.

Jedan od najpopularnijih antivirusnih alata za *Linux* je *ClamAV*, a koristiti se za agente elektroničke pošte *Sendmail* ili *postfix*. *ClamAV* je besplatni alat otvorenoga kôda koji svoju bazu virusa aktivno nadopunjuje. Uz automatsku nadogradnju baze virusa, postoje još mnoge mogućnosti, na primjer, skener iz naredbene linije, podršku za većinu formata elektroničke pošte te skeniranje izvršnih i arhivskih datoteka. Kako bi *ClamAV* skenirao svaku elektroničku poruku, potreban mu je servis *amavi*s koji vrši ulogu SMTP *proxyja*. Servis *amavis* svaku elektroničku poruku prosljeđuje *ClamAVu* i nakon provjere vraća ga servisu *postfix*.

Prikaz kretanja elektroničke pošte kroz servise Antivirus i AntiSPAM (servis će biti opisan u idućem poglavlju):



Instalacija i konfiguracija alata *ClamAV* i servisa *amavis*

Naredba za instalaciju je

```
$ sudo apt-get install clamav clamav-daemon amavisd-new
```

Servis *amavis* će kroz naredbu `hostname --fqdn` doznati ime računala i upotrijebiti ga u konfiguraciji. Ako se radi o lokalnom računalu koji se koristi za testiranje, potrebno je promijeniti `$myhostname` u `/etc/amavis/conf.d/05-node_id` i ponovno pokrenuti servis *amavis*:

```
$ sudo vim /etc/amavis/conf.d/05-node_id
$myhostname = "localhost";

$ sudo systemctl restart amavis
```

Potrebno je pokrenuti servisni proces *clamav-daemon*:

```
$ sudo systemctl restart clamav-daemon
```

Po zadanome servisni proces *freshclam* se pokreće nakon instalacije i svakih sat vremena provjerava postoji li nadogradnja baze virusa koju može preuzeti. Učestalost nadogradnje baze virusa mijenja se u `/etc/clamav/freshclam.conf`:

```
$ less /etc/clamav/freshclam.conf | grep Check
# Check for new database 24 times a day
Checks 24
```

Za potpuno funkcioniranje servisa *clamav-freshclam* mora imati sva prava kao i servis *amavis* i obratno:

```
$ sudo adduser clamav amavis
Adding user `clamav' to group `amavis' ...
Adding user clamav to group amavis
Done.

$ sudo adduser amavis clamav
Adding user `amavis' to group `clamav' ...
Adding user amavis to group clamav
Done.
```

Nakon promjene prava potrebno je ponovno pokrenuti servis *clamav-freshclam*:

```
$ sudo systemctl restart clamav-freshclam
```

U konfiguraciji servisa *amavis* `/etc/amavis/conf.d/15-content_filter_mode` aktivira se pretraživanje virusa tako da se obriše komentar (#) ispred linije konfiguracije u primjeru i ponovno pokrene servis *amavis*:

```
$ sudo vim /etc/amavis/conf.d/15-content_filter_mode
@bypass_virus_checks_maps = (
   \%bypass_virus_checks, \@bypass_virus_checks_acl,
\$bypass_virus_checks_re);

$ sudo systemctl restart amavis
```

Integracija sa servisom *postfix*

Postfix, nakon što primi elektroničku poruku, mora ju proslijediti servisu *amavis* za provjeru virusa. U `/etc/postfix/main.cf` dodaje se `content_filter` konfiguracija:

```
$ sudo vim /etc/postfix/main.cf
content_filter = smtp-amavis:[127.0.0.1]:10024
```

U `/etc/postfix/master.cf` upisuje se sljedeća konfiguracija (na sljedećoj poveznici nalaze se detaljnije informacije: http://www.postfix.org/master.5.html):

```
$ sudo vim /etc/postfix/master.cf

smtp-amavis unix -      -       n       -       2       smtp
    -o smtp_data_done_timeout=1200
    -o smtp_send_xforward_command=yes
    -o disable_dns_lookups=yes
    -o smtp_line_length_limit=0
    -o notify_classes=protocol,resource,software
    -o max_use=10

127.0.0.1:10025 inet n  -       n       -       -       smtpd
    -o content_filter=
    -o local_recipient_maps=
    -o relay_recipient_maps=
    -o smtpd_restriction_classes=
    -o smtpd_delay_reject=no
    -o smtpd_client_restrictions=permit_mynetworks,reject
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o smtpd_data_restrictions=reject_unauth_pipelining
    -o smtpd_end_of_data_restrictions=
    -o mynetworks=127.0.0.0/8
    -o smtpd_error_sleep_time=0
    -o smtpd_soft_error_limit=1001
    -o smtpd_hard_error_limit=1000
    -o smtpd_client_connection_count_limit=0
    -o smtpd_client_connection_rate_limit=0
    -o
receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```

```
    -o strict_rfc821_envelopes=yes
```

Nakon dodavanja konfiguracija u `main.cf` i `master.cf` potrebno je ponovno pokrenuti servis *postfix*:

```
$ sudo systemctl restart postfix
```

Provjera rada servisa

Za funkcionalnu provjeru virusa svake elektroničke poruke svi servisi moraju biti pokrenuti, što se može provjeriti sljedećim naredbama:

```
$ sudo systemctl status clamav-daemon
$ sudo systemctl status clamav-freshclam
$ sudo systemctl status amavis
$ sudo systemctl status postfix
```

Provjera rada porta

Provjera rada servisa *amavis* provodi se korištenjem programa `telnet`:

```
$ telnet localhost 10024
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 [127.0.0.1] ESMTP amavisd-new service ready
^]
telnet> quit
telnet> Connection closed.
```

Rješavanje problema

Servis *amavis* ima način rada traženja pogrešaka (*debug mode*) gdje se prikazuju svi koraci prilikom pokretanja servisa i prikazat će se greške koje mogu pomoći pri rješavanju problema. Prije uključivanja *debug moda* potrebno je zaustaviti servis:

```
$$ sudo /etc/init.d/amavis stop
[ ok ] Stopping amavis (via systemctl): amavis.service.

$ sudo /etc/init.d/amavis debug
Trying to run amavisd-new in debug mode...
head: cannot open '/etc/mailname' for reading: No such file or directory
Sep 19 07:56:46.248 localhost /usr/sbin/amavisd-new[16259]: logging
initialized, log level 0, syslog: amavis.mail
```

```
Sep 19 07:56:46.251 localhost /usr/sbin/amavisd-new[16259]: starting.
/usr/sbin/amavisd-new at localhost amavisd-new-2.10.1 (20141025), Unicode
aware, LANG="en_US.UTF-8"
Sep 19 07:56:46.255 localhost /usr/sbin/amavisd-new[16259]: perl=5.024001,
user=, EUID: 121 (121);  group=, EGID: 127 127 (127 127)
Sep 19 07:56:46.355 localhost /usr/sbin/amavisd-new[16259]: INFO: no optional
modules: unicore::lib::Nt::De.pl Unix::Getrusage
Sep 19 07:56:46.356 localhost /usr/sbin/amavisd-new[16259]: socket module
IO::Socket::IP, protocol families available: INET, INET6
Sep 19 07:56:46.364 localhost /usr/sbin/amavisd-new[16259]: bind to
/var/lib/amavis/amavisd.sock|unix, 127.0.0.1:10024/tcp, [::1]:10024/tcp
.......
```

Testiranje

Za testiranje rada antivirusa šalje se elektronička poruka s jednog korisnika drugome. Prvo se stvori dodatni korisnik kojemu će `root` korisnik poslati elektroničku poruku.

```
$ sudo adduser andro
$ sudo mail -s "Da li je ovo virus?" -- andro@localhost  < /dev/null
```

Naredbom `mail` može se pregledati poslana elektronička poruka, nakon spajanja kao korisnik `andro`:

```
$ sudo su - andro
andro@debian:~$ mail
"/var/mail/andro": 1 message 1 new
>N   1 root               Wed Sep 19 09:34  24/872   Da li je ovo virus?
? 1
Return-Path: <root@debian>
X-Original-To: andro@localhost
Delivered-To: andro@localhost
Received: from localhost (localhost [127.0.0.1])
       by debian (Postfix) with ESMTP id DF38C170B
       for <andro@localhost>; Wed, 19 Sep 2018 09:34:06 +0200 (CEST)
X-Virus-Scanned: Debian amavisd-new at
Received: from debian ([127.0.0.1])
       by localhost (localhost [127.0.0.1]) (amavisd-new, port 10024)
       with ESMTP id BrKpf3eHFr00 for <andro@localhost>;
       Wed, 19 Sep 2018 09:34:06 +0200 (CEST)
Received: by debian (Postfix, from userid 0)
       id ABE3916F5; Wed, 19 Sep 2018 09:34:06 +0200 (CEST)
Date: Wed, 19 Sep 2018 09:34:06 +0200
From: root <root@debian>
To: andro@localhost
Subject: Da li je ovo virus?
Message-ID: <20180919073406.lngndu4am3htf2om@debian>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
```

```
Content-Disposition: inline
User-Agent: NeoMutt/20170113 (1.7.2)

test
```

Iz tijela elektroničke poruke može se vidjeti da ju je provjerio servis *amavis* i da u njoj nema virusa:

```
X-Virus-Scanned: Debian amavisd-new at
Received: from debian ([127.0.0.1])
 by localhost (localhost [127.0.0.1]) (amavisd-new, port 10024)
 with ESMTP id BrKpf3eHFr00 for <andro@localhost>;
 Wed, 19 Sep 2018 09:34:06 +0200 (CEST)
```

Za testiranje prepoznaje li *ClamAV* viruse potrebno je skinuti jedan i poslati elektroničku poruku s virusom u privitku:

```
$ wget https://secure.eicar.org/eicar.com.txt -P /tmp/eicar.com.txt
$ mail -A /tmp/eicar.com.txt -s "virus" andro@localhost < /dev/null
```

Ako servis *amavis* pronađe virus, korisnik neće primiti elektroničku poruku, a poruka s privitkom spremit će se u karantenu u direktorij `/var/lib/amavis/virusmails`

```
$ less /var/lib/amavis/virusmails/a/virus-avuQ8ee2kDBP
Return-Path: <root@debian>
Delivered-To: virus-quarantine
X-Envelope-To: <andro@localhost>
X-Envelope-To-Blocked: <andro@localhost>
X-Quarantine-ID:
X-Amavis-Alert: INFECTED, message contains virus: Eicar-Test-Signature
X-Spam-Flag: NO
X-Spam-Score: 0
X-Spam-Level:
X-Spam-Status: No, score=x tag=x tag2=x kill=x tests=[] autolearn=unavailable
Received: from debian ([127.0.0.1])
        by localhost (localhost [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id avuQ8ee2kDBP for <andro@localhost>;
        Thu, 20 Sep 2018 08:35:00 +0200 (CEST)
Received: by debian (Postfix, from userid 0)
        id 1B578171B; Thu, 20 Sep 2018 08:35:00 +0200 (CEST)
Content-Type: multipart/mixed; boundary="2008610139-1537425300=:721"
MIME-Version: 1.0
Subject: virus
To: <andro@localhost>
X-Mailer: mail (GNU Mailutils 3.1.1)
Message-Id: <20180920063500.1B578171B@debian>
Date: Thu, 20 Sep 2018 08:35:00 +0200 (CEST)
From: root@debian (root)

--2008610139-1537425300=:721
```

```
Content-ID: <20180920083500.721@debian>
Content-Type: text/plain

--2008610139-1537425300=:721
Content-ID: <20180920083500.721.1@debian>
Content-Type: application/octet-stream; name=eicar.com.txt
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=eicar.com.txt

WDVPIVAlQEFQWzRcUFpYNTQoUF4pN0NDKTd9JEVJQ0FSLVNUQU5EQVJELUFOVElWSVJVUy1URVNU
LUZJTEUhJEgrSCo=
--2008610139-1537425300=:721--
```

4.2.2. Servis AntiSPAM

Neželjena elektronička poruka (*spam* ili *junk*) je poruka poslana na više adresa elektroničke pošte sa svrhom oglašavanja, napada (*phishing*) ili dijeljenja zlonamjernih poveznica. Neželjene elektroničke poruke mogu sadržavati i zlоćudne skripte ili druge izvršne datoteke.

SpamAssassin je alat za analiziranje elektroničke pošte u svrhu pronalaženja i filtriranja neželjenih elektroničkih poruka. Na osnovi usporedbe sadržaja elektroničke poruke s velikom bazom pravila, *SpamAssassin* boduje svaku elektroničku poruku. Što više bodova dobije od različitih pravila veća je vjerojatnost da je elektronička poruka neželjena. Ovisno o broju bodova, elektronička poruka će se označiti kao neželjena ili će se proslijediti korisniku.

Alat je fleksibilan pa je moguće podesiti koliko koje pravilo donosi bodova ili izraditi svoja pravila. Također se može prilagoditi okolini i prepoznati legitimne pošiljatelje i identificirati nove vrste neželjene elektroničke pošte. Ako je alat označio elektroničku poruku kao neželjenu, njegov naslov i zaglavlje će se promijeniti. Automatizirani sistemi AntiSPAM nisu savršeni pa mogu proglasiti neželjenima i one elektroničke poruke koje to nisu. Prema tome, administrator može podesiti pravila kako bi se takvi slučajevi izbjegli u budućnosti.

Instalacija

SpamAssassin se integrira u servis elektroničke pošte p*ostfix*. Kao i kod alata za provjeru virusa, potrebno je instalirati servis *amavis*, koji je posrednik između servisa *postfix* i *spamassassin*.

Uz servis *SpamAssassin* instalira se i servis *amavis*:

```
$ sudo apt-get install spamassassin amavisd-new
```

Za aktiviranje potrebno je obrisati komentar (#) ispred sljedeće linije u datoteci `/etc/amavis/conf.d/15-content_filter_mode` i ponovno pokrenuti servis *amavisd-new*:

```
@bypass_spam_checks_maps = (
   \%bypass_spam_checks, \@bypass_spam_checks_acl,
\$bypass_spam_checks_re);

$ sudo systemctl restart amavis
```

Integracija s *postfixom*, provjera rada servisa, provjera rada porta i rješavanje problema je identična kao i kod instalacije antivirusnog alata *ClamAV*, opisanog u prethodnom poglavlju.

Testiranje

Tekst za testiranje mora se staviti u datoteku i poslati elektroničkom poštom:

```
$ echo 'XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-
EMAIL*C.34X' > /tmp/poruka
$ mail -s "Da li je ovo spam?" -- andro@localhost  < /tmp/poruka
```

Iz datoteke za bilježenje događaja vezanih za elektroničku poštu `/var/log/mail.log` prati se stanje provjere:

```
$ less /var/log/mail.log
...
Sep 20 11:35:10 debian amavis[944]: (00944-01) DSN: FILTER 554 Spam,
spam level
1003.231 exceeds cutoff 10, <root@debian> -> <andro@localhost>
Sep 20 11:35:10 debian amavis[944]: (00944-01) Blocked SPAM
{NoBounceInbound,Quarantined}, [127.0.0.1] <root@debian> ->
<andro@localhost>,
quarantine: t/spam-tnN6HTa2iZXV.gz, Message-ID:
<20180920093509.78A7C1720@debian>,
mail_id: tnN6HTa2iZXV, Hits: 1003.231, size: 383, 1209 ms
```

Može se primijetiti da je neželjena poruka, koja je poslana na andro@localhost, dobila 1000.231 bodova. Po zadanoj konfiguraciji, sve elektroničke poruke koje imaju preko 10 bodova stavljaju se u karantenu u direktorij `/var/lib/amavis/virusmails/`, a iz zapisa se vidi i u kojoj je datoteci spremljena: `t/spam-tnN6HTa2iZXV.gz`.

Prosljeđivanje neželjene elektroničke pošte

Filteri nisu savršeni pa je moguće legitimnu elektroničku poruku označi kao neželjenu. Preporučeno je da se neželjene elektroničke poruke spremaju u odvojenu datoteku *spam* ili *junk*. Konfiguracija za prosljeđivanje neželjenih elektroničkih poruka korisniku, bez obzira na to kako je označena, umeće se u `/etc/amavis/conf.d/50-user`, nakon čega je potrebno ponovno pokrenuti servis *amavis*:

```
$ sudo vim /etc/amavis/conf.d/50-user
$final_spam_destiny       = D_PASS;

$ sudo systemctl restart amavis
```

Sada će neželjena elektronička pošta završiti u korisničkom pretincu s prefiksom naslova ***SPAM***:

```
$ mail -s "Da li je ovo spam 56?" -- andro@localhost  < /tmp/poruka
$ sudo su - andro
andro@debian:~$ mail
"/var/mail/andro": 1 message 1 new
>N   1 root               Thu Sep 20 12:53  28/1190  ***SPAM*** Da li je ovo
spam 56?
? 1
Return-Path: <root@debian>
X-Original-To: andro@localhost
Delivered-To: andro@localhost
Received: from localhost (localhost [127.0.0.1])
        by debian (Postfix) with ESMTP id C10151727
        for <andro@localhost>; Thu, 20 Sep 2018 12:53:46 +0200 (CEST)
X-Quarantine-ID: <3txfhd26e3do>
X-Virus-Scanned: Debian amavisd-new at
X-Spam-Flag: YES
X-Spam-Score: 1003.231
X-Spam-Level: ************************************************************
X-Spam-Status: Yes, score=1003.231 tagged_above=-999 required=6.31
        tests=[GTUBE=1000, NO_RELAYS=-0.001, PYZOR_CHECK=1.985,
        TO_MALFORMED=1.247] autolearn=no autolearn_force=no
Received: from debian ([127.0.0.1])
        by localhost (localhost [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id 3TXfHd26E3do for <andro@localhost>;
        Thu, 20 Sep 2018 12:53:45 +0200 (CEST)
Received: by debian (Postfix, from userid 0)
        id 6295F1713; Thu, 20 Sep 2018 12:53:45 +0200 (CEST)
Subject: ***SPAM*** Da li je ovo spam 56?
To: <andro@localhost>
X-Mailer: mail (GNU Mailutils 3.1.1)
Message-Id: <20180920105345.6295F1713@debian>
Date: Thu, 20 Sep 2018 12:53:45 +0200 (CEST)
From: root@debian (root)

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

4.2.3. Crne liste

Servisi AntiSPAM, kao što je *SpamAssassin*, mogu filtrirati velik broj neželjene elektroničke pošte, ali neke se poruke mogu provući kroz njihove mehanizme. Korak više u rješavanju problema s neželjenom elektroničkom poštom jest aktiviranje crnih listi ili RBL-ova (*Real-time Blackhole*). RBL je baza IP adresa i podmreža s kojih se šalje ili prosljeđuje neželjena elektronička pošta. To mogu biti i kompromitirani poslužitelji sa zlođudnim programima. Većina servisa elektroničke pošte može se konfigurirati tako da blokira elektroničke poruke koje dolaze s mreža koje su navedene u RBL bazama.

Servis *postfix* može se konfigurirati i tako da prepoznaje zlođudne IP adrese i blokira sumnjive elektroničke poruke. Konfiguracija se postavlja u `/etc/postfix/main.cf`:

```
$ sudo vim /etc/postfix/main.cf

smtpd_recipient_restrictions =
     permit_sigurne-podmreze,
     permit_sasl_authenticated,
     reject_non_fqdn_hostname,
     reject_non_fqdn_sender,
     reject_non_fqdn_recipient,
     reject_unauth_destination,
     reject_unauth_pipelining,
     reject_invalid_hostname,
     reject_rbl_client bl.spamcop.net,
     reject_rbl_client cbl.abuseat.org,
     reject_rbl_client dnsbl.sorbs.net,
     reject_rbl_client zen.spamhaus.org
     permit
```

Nakon linija konfiguracije koje primaju sve elektroničke poruke sa sigurnih IP adresa ili autenticiranih korisnika te linija koje blokiraju sve nepravilno poslane elektroničke poruke, umeću se linije s `reject_rbl_client`. Svaka linija definira domenu koja sadrži crne liste. Svaka elektronička poruka koja nije obuhvaćena zabranama koje su definirane u prethodnim linijama, provjerit će se na crnim listama. Ako se utvrdi da IP adresa ili podmreža s koje elektronička poruka dolazi nije na crnim listama, poruka će se propustiti korisniku ili servisima Antivirus i/ili AntiSPAM, ovisno o konfiguraciji.

Nakon dodavanja spomenutih linija potrebno je ponovno pokrenuti servis *postfix:*

```
$ systemctl restart postfix
```

4.2.4. Filtriranje neželjenih privitaka

Servis *postfix* ima mogućnosti blokiranja neželjenih privitaka ovisno o datotečnom nastavku. Najčešće se blokiraju izvršne datoteke kao što su `.exe` ili `.bat` koje mogu sadržavati zloćudne programe.

U `/etc/postfix/main.cf` dodaje se lokacija datoteke koja sadrži pravila provjere MIME zaglavlja. Ta pravila izrađena su od regularnih izraza:

```
$ sudo vim /etc/postfix/main.cf
mime_header_checks = regexp:/etc/postfix/mime_header_checks

$ sudo vim /etc/postfix/mime_header_checks
/name=[^>]*\.(bat|com|exe|dll|vbs)/ REJECT
```

Uputom REJECT sve elektroničke poruke koje imaju definirane datotečne nastavke neće biti dostavljene primatelju, a pošiljatelj će primiti poruku o grešci. Za primjenu konfiguracije potrebno je ponovno pokrenuti servis *postfix*:

```
$ sudo systemctl restart postfix
```

Nakon poslane elektroničke poruke s datotekom zabranjenoga datotečnog nastavka, u zapisu se može primijetiti da je elektronička poruka odbijena:

```
$ mail -A /tmp/virus.exe -s "provjera datotecnog nastavka"
andro@localhost < /dev/null

$ tail /var/log/mail.log
...
Sep 21 10:29:39 debian postfix/cleanup[3062]: 152D217AE: reject: header
Content-Type: application/octet-stream; name=virus.exe from local;
from=<root@debian>: 5.7.1 message content rejected
Sep 21 10:29:39 debian postfix/cleanup[3062]: 152D217AE:
to=<andro@localhost>,
relay=none, delay=0.04, delays=0.04/0/0/0, dsn=5.7.1, status=bounced
(message content rejected)
...
```

Pošiljatelj će primiti elektroničku poruku da njegova poruka nije dostavljena primatelju:

```
$ mail
"/var/mail/root": 1 messages 1 new
>N   1 Mail Delivery Syst Fri Sep 21 10:28  70/2143  Undelivered Mail
Returned to Sender
1

Return-Path: <>
X-Original-To: root@debian
Delivered-To: root@debian
Received: by debian (Postfix)
       id 24C2F17AA; Fri, 21 Sep 2018 10:28:25 +0200 (CEST)
Date: Fri, 21 Sep 2018 10:28:25 +0200 (CEST)
From: MAILER-DAEMON@debian (Mail Delivery System)
Subject: Undelivered Mail Returned to Sender
To: root@debian
Auto-Submitted: auto-replied
MIME-Version: 1.0
Content-Type: multipart/report; report-type=delivery-status;
       boundary="14B4E17A7.1537518505/debian"
Content-Transfer-Encoding: 8bit
Message-Id: <20180921082825.24C2F17AA@debian>

This is a MIME-encapsulated message.
```

```
--14B4E17A7.1537518505/debian
Content-Description: Notification
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: 8bit

This is the mail system at host debian.

I'm sorry to have to inform you that your message could not
be delivered to one or more recipients. It's attached below.

For further assistance, please send mail to postmaster.

If you do so, please include this problem report. You can
delete your own text from the attached returned message.

                   The mail system

<andro@localhost>: message content rejected

--14B4E17A7.1537518505/debian
Content-Description: Delivery report
Content-Type: message/delivery-status

Reporting-MTA: dns; debian
X-Postfix-Queue-ID: 14B4E17A7
X-Postfix-Sender: rfc822; root@debian
Arrival-Date: Fri, 21 Sep 2018 10:28:25 +0200 (CEST)

Final-Recipient: rfc822; andro@localhost
Original-Recipient: rfc822;andro@localhost
Action: failed
Status: 5.7.1
Diagnostic-Code: X-Postfix; message content rejected

--14B4E17A7.1537518505/debian
Content-Description: Undelivered Message Headers
Content-Type: text/rfc822-headers
Content-Transfer-Encoding: 8bit

Return-Path: <root@debian>
Received: by debian (Postfix, from userid 0)
       id 14B4E17A7; Fri, 21 Sep 2018 10:28:25 +0200 (CEST)
Content-Type: multipart/mixed; boundary="1306334045-1537518505=:3059"
MIME-Version: 1.0
Subject: provjera virusa
To: <andro@localhost>
X-Mailer: mail (GNU Mailutils 3.1.1)
Message-Id: <20180921082825.14B4E17A7@debian>
```

```
Date: Fri, 21 Sep 2018 10:28:25 +0200 (CEST)
From: root@debian (root)

--14B4E17A7.1537518505/debian--
```

4.2.5. Filtriranje adresa i pošiljatelja

Servis *postfix*, prema zadanim postavkama, prihvaća elektroničke poruke sa svih adresa i pošiljatelja. Uz zaštitu servisima Antivirus i AntiSPAM i crnim listama, nekada je potrebno napraviti i vlastitu listu adresa i pošiljatelja kojima se onemogućava slanje elektroničkih poruka prema poslužitelju koji je potrebno zaštititi. Moguće je i omogućiti primanje elektroničkih poruka s adresa koje su završile na crnim listama, ako su tamo završile jer im je bio kompromitiran poslužitelj u nekom periodu.

Postoji više načina filtriranja elektroničkih poruka, a dva se najčešće koriste. S atributom `check_client_access` može se filtrirati po IP adresi, podmreži ili imenu računala s kojeg se šalje elektronička poruka, a s atributom `check_sender_access` se filtrira po adresi pošiljatelja koji se nalazi u FROM polju elektroničke poruke.

Svaka opcija filtriranja ima svoju datoteku, najčešće se sprema u direktorij `/etc/postfix`, a referenciraju se u `/etc/postfix/main.cf`:

```
$ sudo vim /etc/postfix/main.cf

smtpd_recipient_restrictions =
     check_sender_access hash:/etc/postfix/sender_checks,
     check_client_access hash:/etc/postfix/client_checks,
     permit_sigurne-podmreze,
     permit_sasl_authenticated,
     reject_non_fqdn_hostname,
     reject_non_fqdn_sender,
     reject_non_fqdn_recipient,
     reject_unauth_destination,
     reject_unauth_pipelining,
     reject_invalid_hostname,
     reject_rbl_client bl.spamcop.net,
     reject_rbl_client cbl.abuseat.org,
     reject_rbl_client dnsbl.sorbs.net,
     reject_rbl_client zen.spamhaus.org,
     permit
```

Preporuča se da reference na filtere budu među prvima u `smtpd_recipient_restrictions`. Na ovaj način elektronička poruka neće biti uhvaćena kasnijim filterima.

Liste se definiraju u zasebnim datotekama:

```
$ sudo vim /etc/postfix/sender_checks
korisnik@domena.hr      REJECT
domena.hr               REJECT
.domena.hr              REJECT
primjer.hr              OK

$ sudo vim /etc/postfix/client_checks
192.168.56.34         REJECT
10.0.0.1/8            REJECT
192.168.56.50         OK
```

Definirani su filteri po adresi pošiljatelja, domeni, poddomeni, IP adresi i podmreži. REJECT onemogućuje dostavljanje elektroničkih poruka primatelju, a OK omogućuje.

Za ažuriranje postavki potrebno je pokrenuti naredbu postmap i napraviti ponovno učitavanje konfiguracije servisa *postfix*:

```
$ sudo postmap /etc/postfix/sender_checks
$ sudo postmap /etc/postfix/client_checks
$ sudo systemctl reload postfix
```

4.2.6. Zanimljivi izvori

Poveznice:

- https://www.tecmint.com/integrate-clamav-and-spamassassin-to-protect-postfix-mails-from-viruses/
- http://www.postfix.org/SMTPD_ACCESS_README.html

4.2.7. Vježba 9: Zaštita servisa elektroničke pošte: podešavanje antispam i antivirus alata

1. Prije početka rada odaberite sliku stanja virtualnoga računala **slika_jedan** za početak vježbe.
2. Prijavite se na računalo kao korisnik **linux1**. U GUI-ju pokrenite **Terminal** (*Activities* → **Terminal**). Izvršite **su -** naredbu da postanete administrator (lozinka: linux1).
3. Instalirajte antispam i antivirus servise:

   ```
   # apt-get install clamav clamav-daemon amavisd-new spamassassin
   ```

4. Promijenite ime računala u **localhost** da se može koristiti na lokalnom virtualnom računalu:

   ```
   vim /etc/amavis/conf.d/05-node_id
   ```

```
$myhostname = "localhost";
```

5. Dodajte sljedeću liniju konfiguracije kako bi se primatelju dostavila elektronička poruka čak i ako je neželjena:

```
# vim /etc/amavis/conf.d/50-user

$final_spam_destiny     = D_PASS;
```

6. Ponovno pokrenite servis **amavis** i provjerite je li ispravno pokrenut naredbom **systemctl status**:

```
# systemctl restart amavis
# systemctl status amavis
```

7. Dodajte clamav korisnika u amavis grupu i obratno:

```
# adduser clamav amavis
# adduser amavis clamav
```

8. U datoteci **/etc/amavis/conf.d/15-content_filter_mode** obrišite komentar (**#**) ispred sljedećih konfiguracija i ponovno pokrenite servis amavis:

```
@bypass_virus_checks_maps = (
\%bypass_virus_checks,
\@bypass_virus_checks_acl,
\$bypass_virus_checks_re);

@bypass_spam_checks_maps = (
\%bypass_spam_checks,
\@bypass_spam_checks_acl,
\$bypass_spam_checks_re);

# systemctl restart amavis
```

9. Testirajte sluša li *amavisd-new* na portu 10024:

```
# telnet localhost 10024
```

10. Kakav ispis se dobije od **telnet** naredbe?

_____

_____

11. Dodajte sljedeću konfiguraciju u **main.cf** i **master.cf** (konfiguracija za master.cf nalazi su u datoteci **/root/master.cf**), te ponovno pokrenite servis *postfix*.

```
# vim /etc/postfix/main.cf
content_filter = smtp-amavis:[127.0.0.1]:10024

# vim /etc/postfix/master.cf
smtp-amavis unix - -      n      -  2   smtp
```

```
  -o smtp_data_done_timeout=1200
  -o smtp_send_xforward_command=yes
  -o disable_dns_lookups=yes
  -o smtp_line_length_limit=0
  -o notify_classes=protocol,resource,software
  -o max_use=10

127.0.0.1:10025 inet n -  n      - -    smtpd
  -o content_filter=
  -o local_recipient_maps=
  -o relay_recipient_maps=
  -o smtpd_restriction_classes=
  -o smtpd_delay_reject=no
  -o smtpd_client_restrictions=permit_mynetworks,reject
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o smtpd_data_restrictions=reject_unauth_pipelini ng
  -o smtpd_end_of_data_restrictions=
  -o mynetworks=127.0.0.0/8
  -o smtpd_error_sleep_time=0
  -o smtpd_soft_error_limit=1001
  -o smtpd_hard_error_limit=1000
  -o smtpd_client_connection_count_limit=0
  -o smtpd_client_connection_rate_limit=0
  -o
receive_override_options=no_header_body_checks,no_unknown_recipi
ent_checks
  -o strict_rfc821_envelopes=yes

# systemctl restart postfix
```

12. Provjerite stanje svih servisa:

```
# systemctl status clamav-daemon
# systemctl status clamav-freshclam
# systemctl status spamassassin
# systemctl status amavis
# systemctl status postfix
```

13. Jesu li svi servisi aktivni? Ako nisu, ponovno ih pokrenite.

14. Dodajte korisnika mario i pošaljite mu elektroničku poruku:

```
# adduser mario
# mail -s "test" -- mario@localhost < /dev/null
```

15. Koje linije u zaglavlju elektroničke poruke je potrebno provjeriti kako bi se uvjerili da antispam i antivirus servisi funkcioniraju?

16. U GUI-ju pokrenite **Terminal** (*Activities* → **Terminal**). Izvršite **su- mario** naredbu kako bi se spojili kao korisnik mario.

17. Provjerite elektroničku poštu naredbom **mail** i otvorite poruku tipkom **1**. Postoje li u zaglavlju poruke linije koje ukazuju na antispam i antivirus zaštitu? Ima li elektronička poruka u sebi virus ili je neželjena elektronička poruka?

18. Vratite se u **Terminal** gdje ste spojeni kao ***root*** korisnik i pošaljite sljedeću elektroničku poruku:

```
# echo 'XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X' >
/root/poruka

# mail -s "Da li je ovo spam?" -- mario@localhost < /root/poruka
```

19. U GUI-ju pokrenite **Terminal** (*Activities* → **Terminal**). Izvršite **su- mario** naredbu kako bi se spojiti kao korisnik mario.

20. Provjerite elektroničku poštu naredbom **mail** i otvorite poruku tipkom **1**. Ima li elektronička poruka u sebi virus ili je neželjena elektronička poruka? Koje sve informacije možete saznati iz zaglavlja?

4.3. Zaštita web servisa

4.3.1. Enkripcija pristupa kroz protokol HTTPS

Sav *web* promet između klijenta i poslužitelja može se kriptirati protokolom HTTPS koji koristi SSL certifikate. U suprotnom, treća strana može prisluškivati *web* promet i otkriti korisničke informacije, lozinke, broj kreditne kartice i ostale osjetljive informacije. Za *web* sjedišta s takvim osjetljivim informacijama nužno je korištenje SSL certifikata za kriptiranje prometa. Sigurni i valjani certifikati nabavljaju se od CA organizacija (*certificate authorities*), kao što su *Comodo*, *IdenTrust*, *Symantec* itd.

Prije slanja zahtjeva CA za izdavanje SSL certifikata potrebno je generirati CSR (*Certificate Signing Request*). CSR je enkriptirana datoteka koja sadrži javni ključ i informacije o tvrtki i ime domene. Naredba za generiranje CSR je `openssl`:

```
$ sudo  openssl req -new -newkey rsa:2048 -nodes -out primjer_hr.csr -keyout
primjer_hr.key
Generating a 2048 bit RSA private key
..............................+++
........+++
writing new private key to 'primjer_hr.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:HR
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:Zagreb
Organization Name (eg, company) [Internet Widgits Pty Ltd]:edu4it
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:www.primjer.hr
Email Address []:test@primjer.hr
```

Datoteka s datotečnim nastavkom .csr šalje se CA organizaciji koja izdaje SSL certifikat i dostavlja javni ključ koji se koristi za *apache2* virtualni host. Primjer CRS datoteke:

```
$ cat primjer_hr.csr
-----BEGIN CERTIFICATE REQUEST-----
MIICwjCCAaoCAQAwfTELMAkGA1UEBhMCSFIxEzARBgNVBAgMClNvbWUtU3RhdGUx
DzANBgNVBAcMBlphZ3JlYjEPMA0GA1UECgwGZWR1NGl0MRcwFQYDVQQDDA53d3cu
cHJpbWplci5ocjEeMBwGCSqGSIb3DQEJARYPdGVzdEBwcmltamVyLmhyMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAumzwzn49f0mT/bbjF32vs06oAlac
g5q/uYMMyoyeYAzgdDV/aOlzz9k5swmX6FfW3AVlC/9g9phs6DjD44btsj7IVoAV
aTNlp9Er83Rcw469kegFgLjRGh6Oeyc0F/6tX0zDIcfiQshmHj5NzktW8KuN/YMH
zKQF/qE73tm4asnXN9dzvUOt6bZCM6Aab/Z1o8EAu3AvRjMNaxgGToPADd3RTQpv
```

```
QocJ1UqrEnjftjx3rF4kaw9Pg5rMF2Uv0e1bocIKV01/J+Jifa9qFqPOmetdJSME
BP+OVIzsRsQaT87zAwzTfzYErpx79uLd2z6ssCVHndEblP9h56Avo4Y8NQIDAQAB
oAAwDQYJKoZIhvcNAQELBQADggEBAGPBjF7fDz+BJ3nlu5DBer/T6eQpUrQ1QFX/
wdiQmr6imeXNqhNk6xSKsLbz29sHxSi6cLbnSJ6aeeQL8y/d0CyjJDg5IhDextcf
WnVDYYal6PuROwAgU+o2YdrAw5WnAt72Xn0RFPnG1n0ZskvKGceMViR9P1vRY+Sq
S03FINHMsoUr4pDO+4lGMHlqqWsRze4DbwfZNth3zLJ5xPbMk9nITUONK9NbN3QR
84FNJThXqp3opnFFaSRr2RzDr6GSxKpf3xZrFL6GIyBbjH5PNhM8Dj2DVwuZAtfO
PwM3dD5Sd8QHTiTntdITGdxfPngR/8v1ebxDh3NhUQuNYID8XvY=
-----END CERTIFICATE REQUEST-----
```

CRS datoteka je nečitljiva, ali sa sljedećom naredbom možemo vidjeti njene detalje:

```
$ openssl req -in primjer_hr.csr -noout -text
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = HR, ST = Some-State, L = Zagreb, O = edu4it, CN =
www.primjer.hr, emailAddress = test@primjer.hr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ba:6c:f0:ce:7e:3d:7f:49:93:fd:b6:e3:17:7d:
                    af:b3:4e:a8:02:56:9c:83:9a:bf:b9:83:0c:ca:8c:
                    9e:60:0c:e0:74:35:7f:68:e9:73:cf:d9:39:b3:09:
                    97:e8:57:d6:dc:05:65:0b:ff:60:f6:98:6c:e8:38:
                    c3:e3:86:ed:b2:3e:c8:56:80:15:69:33:65:a7:d1:
                    2b:f3:74:5c:c3:8e:bd:91:e8:05:80:b8:d1:1a:1e:
                    8e:7b:27:34:17:fe:ad:5f:4c:c3:21:c7:e2:42:c8:
                    66:1e:3e:4d:ce:4b:56:f0:ab:8d:fd:83:07:cc:a4:
                    05:fe:a1:3b:de:d9:b8:6a:c9:d7:37:d7:73:bd:43:
                    ad:e9:b6:42:33:a0:1a:6f:f6:75:a3:c1:00:bb:70:
                    2f:46:33:0d:6b:18:06:4e:83:c0:0d:dd:d1:4d:0a:
                    6f:42:87:09:d5:4a:ab:12:78:df:b6:3c:77:ac:5e:
                    24:6b:0f:4f:83:9a:cc:17:65:2f:d1:ed:5b:a1:c2:
                    0a:57:4d:7f:27:e2:62:7d:af:6a:16:a3:ce:99:eb:
                    5d:25:23:04:04:ff:8e:54:8c:ec:46:c4:1a:4f:ce:
                    f3:03:0c:d3:7f:36:04:ae:9c:7b:f6:e2:dd:db:3e:
                    ac:b0:25:47:9d:d1:1b:94:ff:61:e7:a0:2f:a3:86:
                    3c:35
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         63:c1:8c:5e:df:0f:3f:81:27:79:e5:bb:90:c1:7a:bf:d3:e9:
         e4:29:52:b4:35:40:55:ff:c1:d8:90:9a:be:a2:99:e5:cd:aa:
         13:64:eb:14:8a:b0:b6:f3:db:db:07:c5:28:ba:70:b6:e7:48:
```

```
        9e:9a:79:e4:0b:f3:2f:dd:d0:2c:a3:24:38:39:22:10:de:c6:
        d7:1f:5a:75:43:61:86:a5:e8:fb:91:3b:00:20:53:ea:36:61:
        da:c0:c3:95:a7:02:de:f6:5e:7d:11:14:f9:c6:d6:7d:19:b2:
        4b:ca:19:c7:8c:56:24:7d:3f:5b:d1:63:e4:aa:4b:4d:c5:20:
        d1:cc:b2:85:2b:e2:90:ce:fb:89:46:30:79:6a:a9:6b:11:cd:
        ee:03:6f:07:d9:36:d8:77:cc:b2:79:c4:f6:cc:93:d9:c8:4d:
        43:8d:2b:d3:5b:37:74:11:f3:81:4d:25:38:57:aa:9d:e8:a6:
        71:45:69:24:6b:d9:1c:c3:af:a1:92:c4:aa:5f:df:16:6b:14:
        be:86:23:20:5b:8c:7e:4f:36:13:3c:0e:3d:83:57:0b:99:02:
        d7:ce:3f:03:37:74:3e:52:77:c4:07:4e:24:e7:b5:d2:13:19:
        dc:5f:3e:78:11:ff:cb:f5:79:bc:43:87:73:61:51:0b:8d:60:
        80:fc:5e:f6
```

Privatni ključ ima datotečni nastavak `.key` i važno je da bude na sigurnom mjestu, tj. na računalu za koji se koristi. Slijedi primjer privatnoga ključa:

```
$ cat primjer_hr.key
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC6bPDOfj1/SZP9
tuMXfa+zTqgCVpyDmr+5gwzKjJ5gDOB0NX9o6XPP2TmzCZfoV9bcBWUL/2D2mGzo
OMPjhu2yPshWgBVpM2Wn0SvzdFzDjr2R6AWAuNEaHo57JzQX/q1fTMMhx+JCyGYe
Pk3OS1bwq439gwfMpAX+oTve2bhqydc313O9Q63ptkIzoBpv9nWjwQC7cC9GMw1r
GAZOg8AN3dFNCm9ChwnVSqsSeN+2PHesXiRrD0+DmswXZS/R7VuhwgpXTX8n4mJ9
r2oWo86Z610lIwQE/45UjOxGxBpPzvMDDNN/NgSunHv24t3bPqywJUed0RuU/2Hn
oC+jhjw1AgMBAAECggEAYavx/j3lumqyPpszH3uaMjdjjtYR6mGJUYh3iydhUrFs
Z3Yf6rdlFeCZelPsYq6iw2OQLVj/VDNH2+LhvrNSlbCPBcLVdOiYufO9MzAj6dE/
QNJvD6HE7ApWW++OO4QTEXsGQQyYXqTf27iIyyxtwGohWlDsJStKeL3AwGERXeC7
hSELszsRRjz/rfY0JHV0sK+2WnEbF+14TJydI6sNol//hbu0f+3okwKB7ViU7NPS
Z6GZsr355LJXooF/fEL0bKowGC/iU8AxEFJP3BzTTBiOflLV1JpMRRGF1KZtX3un
xhjHuPfhpvlxHNshAxEcGYOpIowk31GmUYV3wfuQAQKBgQD1mdvdVOahsxZFgH7t
LQkZQb0KQAPZ+GMuRZo+ZeLTJsRi48MPT+O4SNIXZXspzQtWnNAB6v92quAvOqSu
3DspNnsZkeLRo8Q3En2+nvFgMAYEa4Dr/t2p6Ox9qZylUK8av0u51Td6tKxqQAhC
RI9zaIGvIdtxJGYoWE4vuTUooQKBgQDCUaljrUN8Vn0cHGuZYSfdaSPhaTw3pvp1
BV1/2rrNT0I3BGTDeDoKNJb1nYYp0nYV4ZkZhV9wkNL5wSCjVRx7Eg6os4Xqzg9X
bvx23yXKcLn2+VM2B66mZLlm7uWXySMhfyhNyA8KlNCim1NYzHgeAIsAddYeETxf
taT1H52HFQKBgQC32H6OxdkGveo0CKX6oLWo5F6/5396kMadgpidkOMkMGbdp6UC
N0k9T7WEsgBqIAUWxremV+T3TZ4XfIx+IHlgtlmboGrrhu2AVCUwpgYFfK1kbZzK
C7SeVa+BuY966FTLbtseto6bGdfeiSQlhvDi8R3ynSOJJDgch02vx7IVQQKBgGs0
3Ixmog3uNZYVw/NaG8FW6XnKMnPNxu5a6GvKhDcTXEe4P9Nr+DF7NDIMF2HpgEaw
MWRYJgCXlh4+w7/5C/6GRtoiOWcDConFbLo0gMgAi0jL43GyqVOZzIQSl063pI8t
dVH8ZvgChFzB7yjVnguHZyj42gm6nqF7OKgYKjPFAoGAM3rLfQLS2bGmFEGrD6Nh
zFBxM0hYjO83WEpojWr3qZHn8LPBLDEmCXnHuvvtHWkpOUtIq1zhPFz03AB9uTTH
ROzn5g3K5WAOfvD89AYf568M66ATxnTJa3eeBNTmJNU8roqwFRMuhp4Wbm0r5AXh
5n0CAQwhMUJDvT1Nss45SNY=
-----END PRIVATE KEY-----
```

Privatni i javni ključ (koji se dobije od CA) postavlja se u `/etc/ssl/private` i `/etc/ssl/certs` sa sljedećim pravima direktorija i datoteka:

```
$ sudo chmod 755 /etc/ssl
$ sudo chmod 710 /etc/ssl/private

$ sudo chown -R root:root /etc/ssl/
$ sudo chown -R root:ssl-cert /etc/ssl/private/

$ sudo chmod 644 /etc/ssl/certs/*.crt
$ sudo chmod 640 /etc/ssl/private/*.key
```

Potrebno je instalirati *web*-servis, omogućiti modul, dodati virtualni *host* i ponovno pokrenuti *web*-servis:

```
$ sudo apt-get install apache2
$ sudo a2enmod ssl
$ sudo a2ensite default-ssl.conf
$ sudo systemctl reload apache2
```

Za preusmjeravanje HTTP *web* prometa na HTTPS potrebno je dodati konfiguraciju u virtualni host koji sluša na portu 80:

```
$ sudo vim /etc/apache2/sites-available/000-default.conf
<VirtualHost *:80>
  ServerName www.primjer.hr
  Redirect / https://www.primjer.hr
</Virtualhost>
```

Za promjenu putanje do certifikata u `default-ssl.conf` potrebno je korigirati `SSLCertificateFile` i `SSLCertificateKeyFile` konfiguraciju i ponovno pokrenuti *web*-servis:

```
$ sudo vim /etc/apache2/sites-available/default-ssl.conf
<VirtualHost _default_:443>

  ServerName www.primjer.hr
  ServerAdmin webmaster@localhost

  DocumentRoot /var/www/html

  SSLEngine on
  SSLCertificateFile /etc/ssl/certs/primjer_hr.crt
  SSLCertificateKeyFile /etc/ssl/private/primjer_hr.key

<VirtualHost _default_:443>
```

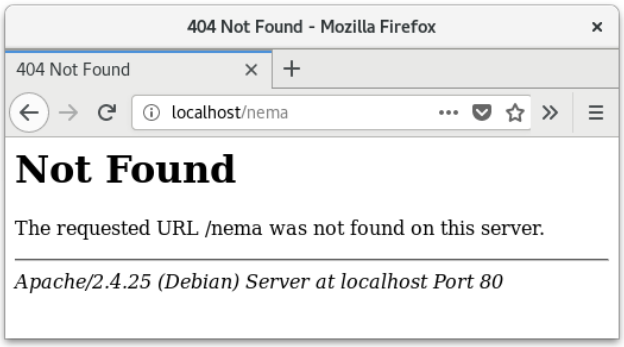
```
$ sudo systemctl reload apache2
```

4.3.2. Prilagodba sigurnosnih postavki web-servisa

Zadane postavke tek instaliranih servisa mogu napadaču dati vrijedne informacije o stanju *web* poslužitelja koje može koristiti za daljnje napade. Uz redovitu nadogradnju servisa preporučeno je i učvrstiti konfiguraciju *web*-servisa.

Skrivanje verzije *web*-servisa i imena operacijskog sustava

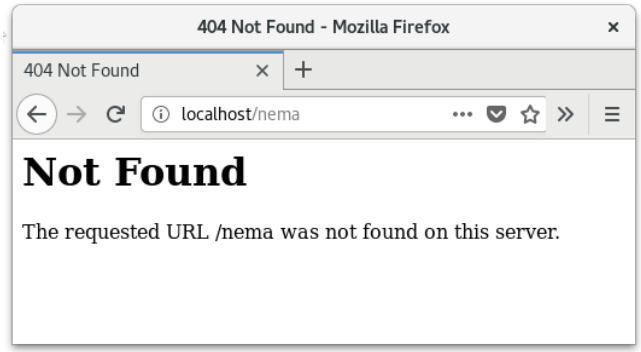
Po zadanome, *web*-servis prikazuje verziju i ime operacijskoga sustava za *web* putanje koje ne postoje. Na primjer, ako korisnik upiše krivi URL u preglednik, dobit će grešku 404, tj. obavijest da ta stranica ne postoji:



Za skrivanje osjetljivih informacija potrebno je dodati sljedeću konfiguraciju na kraj datoteke `apache2.conf` i ponovno pokrenuti *web*-servis:

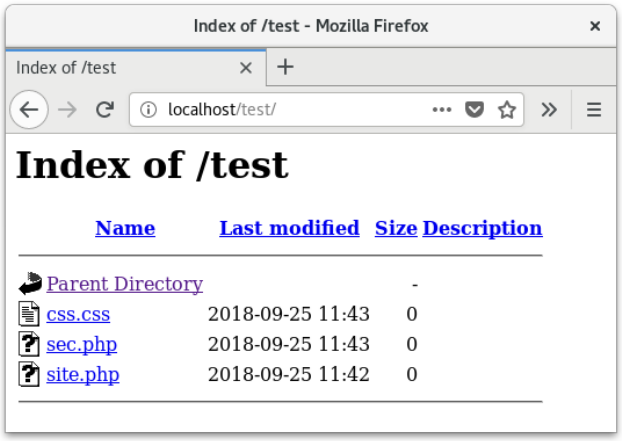
```
$ sudo vim /etc/apache2/apache2.conf
ServerSignature Off
ServerTokens Prod
$ sudo systemctl reload apache2
```

Nakon promjene konfiguracije verzija *web*-servisa i ime operacijskog sustava neće se prikazivati:



Onemogućavanje prikaza sadržaja direktorija

Po zadanome, prikazuje se sadržaj direktorija root i poddirektorija ako u njima nema datoteke s prefiksom `index.*`:



Za onemogućavanje prikaza direktorija, konfiguracija se stavlja u virtualni host, nakon čega je potrebno ponovno učitati konfiguraciju:

```
$ sudo vim /etc/apache2/sites-available/default-ssl.conf
<VirtualHost _default_:443>

  DocumentRoot /var/www/html

  <Directory /var/www/html>
    Options -Indexes

  </Directory>

 </VirtualHost>
$ sudo systemctl reload apache2
```

Nakon primjenjivanja konfiguracije, prikaz sadržaja direktorija će biti onemogućen, a korisnik će dobiti sljedeću obavijest:

Onemogućavanje simboličnih poveznica

Po zadanome, *web*-servis ima omogućeno praćenje simboličnih poveznica. Ako *web* sjedište ima lošu organizaciju datoteka, korisnik može praćenjem simbolične poveznice izaći iz root direktorija. U gorem slučaju, napadač može iskoristiti ranjivost *web*-aplikacije i stvoriti datoteku sa simboličnom poveznicom na neki osjetljiviji direktorij unutar operacijskoga sustava i kompromitirati ga.

Za onemogućavanje simboličnih poveznica, konfiguracija se stavlja u konfiguracijsku datoteku virtualnog hosta, nakon čega je potrebno ponovno učitati konfiguraciju:

```
$ sudo vim /etc/apache2/sites-available/default-ssl.conf
<VirtualHost _default_:443>

  DocumentRoot /var/www/html
<Directory /var/www/html>
     Options -Indexes -FollowSymLinks
</Directory>

 </VirtualHost>

 $ sudo systemctl reload apache2
```

Etag

Ako je *Etag* uključen, napadač može saznati informacije kao što je broj *inoda*, proces dijete kroz *Etag* zaglavlje i *multipart MIME boundary*. Ova ranjivost se može riješiti sljedećom konfiguracijom:

```
$ sudo vim /etc/apache2/apache2.conf
Header unset ETag
FileETag None

$ sudo systemctl reload apache2
```

Onemogućavanje *Trace HTTP Request*

Omogućen *TraceEnable* može potencijalno dati napadaču opciju krađe informacija o kolačićima. Ako je onemogućen, modul *mod_proxy* će napadaču javiti grešku 405 (metoda nije dozvoljena).

TraceEnable se onemogućuje sljedećom konfiguracijom:

```
$ sudo vim /etc/apache2/apache2.conf
Header unset ETag
TraceEnable off
```

```
$ sudo systemctl restart apache2
```

Onemogućavanje nekorištenih modula

Po zadanome, *web*-servis, ima omogućeno nekoliko modula koji nisu potrebni za normalan rad. Uvijek je dobro smanjiti šanse za napadom, pa se preporučuje onemogućiti module koji se ne koriste.

Popis modula može se dobiti naredbom:

```
$ sudo apache2ctl -M
Loaded Modules:
 core_module (static)
 so_module (static)
 watchdog_module (static)
 http_module (static)
 log_config_module (static)
 logio_module (static)
 version_module (static)
 unixd_module (static)
 access_compat_module (shared)
 alias_module (shared)
 auth_basic_module (shared)
 authn_core_module (shared)
 authn_file_module (shared)
 authz_core_module (shared)
 authz_host_module (shared)
 authz_user_module (shared)
 autoindex_module (shared)
 deflate_module (shared)
 dir_module (shared)
 env_module (shared)
 filter_module (shared)
 mime_module (shared)
 mpm_event_module (shared)
 negotiation_module (shared)
 reqtimeout_module (shared)
 setenvif_module (shared)
 socache_shmcb_module (shared)
 ssl_module (shared)
```

Ovisno o svrsi *web*-poslužitelja, pojedini modul se može onemogućiti naredbom:

```
$ sudo a2dismod autoindex -f
```

```
Module autoindex disabled.
To activate the new configuration, you need to run:
  systemctl restart apache2

$ sudo systemctl restart apache2
```

Pokretanje *web*-servisa pod sistemskim korisnikom

Po zadanome, *web*-servis se pokreće pod korisnikom www-data:

```
$ ps -ef | grep apache
root      3236     1  0 14:23 ?        00:00:00 /usr/sbin/apache2 -k
start
www-data  3237  3236  0 14:23 ?        00:00:00 /usr/sbin/apache2 -k
start
www-data  3238  3236  0 14:23 ?        00:00:00 /usr/sbin/apache2 -k
start
```

Prvi proces, tj. roditeljski proces mora biti pod *root* ovlastima jer upravlja procesima djecom. Ti procesi djeca koji se pokreću pod korisnikom www-data obavljaju sve zadatke *web*-poslužitelja.

Ako gore spomenuta konfiguracija nije implementirana, potrebno je stvoriti korisnika i konfigurirati *web*-servis da ga koristi:

```
$ sudo adduser www-data

$ sudo vim /etc/apache2/apache2.conf
User www-data
Group www-data

$ sudo systemctl reload apache2
```

Napomena

Potrebno je promijeniti prava svim direktorijima i datotekama koje koristi *web*-servis.

Onemogućavanje udaljenog izvršavanja kôda

Opcije *Server Side Includes* i *CGI Execution* omogućuju hakerima udaljeno izvršavanje zloćudnoga kôda ili preopterećenje poslužitelja. Ako nisu potrebni, *Server Side Includes* i *CGI Execution* mogu se onemogućiti za cijeli *web*-servis ili za pojedini direktorij:

```
$ sudo vim /etc/apache2/apache2.conf
```

```
Options -Includes
Options -ExecCGI

$ sudo vim /etc/apache2/sites-available/default-ssl.conf
<VirtualHost _default_:443>

  DocumentRoot /var/www/html

  <Directory /var/www/html>
    Options -Indexes -FollowSymLinks -Includes -ExecCGI
    </Directory>

</VirtualHost>

$ sudo systemctl reload apache2
```

Ograničavanje HTTP zahtjeva

Po zadanome, *web*-servis, nema konfigurirano ograničenje za HTTP zahtjeve. Napadač može poslati velike datoteke i tako prouzročiti napad DoS koji će ostalim legitimnim korisnicima onemogućiti korištenje usluge.

LimitRequestBody ograničava veličinu zahtjeva, a može se konfigurirati za cijeli *web*-poslužitelj ili direktorij:

```
$ sudo vim /etc/apache2/apache2.conf

LimitRequestBody 204800

$ sudo vim /etc/apache2/sites-available/default-ssl.conf
<VirtualHost _default_:443>

  DocumentRoot /var/www/html

  <Directory /var/www/html>
    LimitRequestBody 204800
   </Directory>

</VirtualHost>

$ sudo systemctl reload apache2
```

Vrijednost ograničenja može biti od 0 (neograničeno) do 2147483647 (2 GB).

Skeniranje ranjivosti i očvršćivanje konfiguracija

Postoji mnogo *web*-stranica koje skeniraju *web*-sjedišta u potrazi za sigurnosnim ranjivostima. Preporučljivo je, nakon primjenjivanja prethodno navedenih konfiguracija, testirati *web*-sjedište u svrhu otkrivanja ranjivosti i aktualnih preporuka očvršćivanja konfiguracija. Na sljedećoj *web*-stranici je popis najpoznatijih *web*-stranica za skeniranje: https://geekflare.com/online-scan-website-security-vulnerabilities/.

4.3.3. Aplikativni vatrozid

Moduli *mod_security* i *mod_evasive* koriste se za pojačavanje sigurnosti *web*-servisa. Modul *mod_security* je vatrozid koji sprječava brojne zloćudne aktivnosti kao što su SQL *injection*, *cross-site* skriptiranje i *session hijacking*, a *mod_evasive* štiti *web*-servis od napada grubom silom i napada DDoS.

Modul mod_security

Modul *mod_security* je besplatni alat otvorenoga kôda koji prati *web*-promet u realnom vremenu te prepoznaje i sprječava zloćudne aktivnosti. Uz HIDS, *mod_security* ima mogućnost praćenja HTTP prometa i spremanja u dnevničke zapise, pasivne sigurnosne provjere u svrhu otkrivanja ranjivosti i abnormalnih aktivnosti te očvršćivanja konfiguracija.

Modul se instalira naredbom `apt-get` koja ga automatski omogućava, što se može provjeriti naredbom `apachectl -M`:

```
$ sudo apt-get install libapache2-modsecurity

$ sudo apachectl -M | grep sec
 security2_module (shared)
```

Instalacija donosi preporučenu konfiguraciju, koju je potrebno preimenovati kako bi se mogla primijeniti. Kako bi se aktivirala, konfiguraciju je potrebno ponovno učitati:

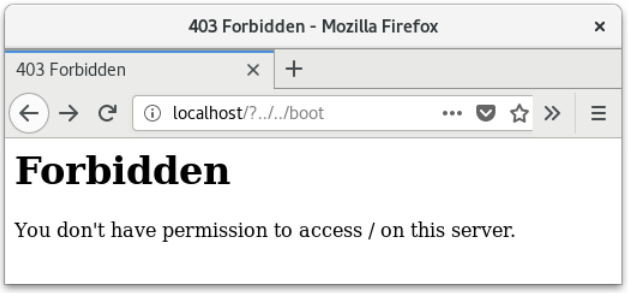
```
$ sudo mv /etc/modsecurity/modsecurity.conf-recommended
/etc/modsecurity/modsecurity.conf

$ sudo systemctl reload apache2
```

Zadana konfiguracija za *mod_security* je `DetectionOnly`, koja bilježi u dnevnički zapis podudara li se *web*-promet s određenim pravilom. Ali DetectionOnly ne blokira zloćudni promet i to se može promijeniti u `modsecurity.conf`:

```
$ sudo vim /etc/modsecurity/modsecurity.conf
SecRuleEngine On

$ sudo systemctl reload apache2
```

CRS (*Core Rule Set*) su pravila koja dolaze s instalacijom modula *mod_security* i njihova lokacija je `/usr/share/modsecurity-crs/rules/` .

Prema zadanim postavkama sva pravila u spomenutoj datoteci su aktivirana. Rad modula *mod_security* može se testirati uz pomoć sljedećeg *web*-upita:



Kao što je prikazano u pregledniku, korisniku je zabranjen pristup *web*-stranici sa sumnjivim upitom (napadač pokušava izaći iz direktorija gdje se nalazi *web* stranica i otvoriti sistemski direktorij boot), a više informacija se može vidjeti u dnevničkom zapisu:

```
/var/log/apache2/modsec_audit.log:
$ tail -f /var/log/apache2/modsec_audit.log

--7da2e347-A--
[25/Sep/2018:17:57:27 +0200] W6pa538AAQEAAA-w-dEAAABI 127.0.0.1 47712 127.0.0.1
80
--7da2e347-B--
GET /?../../boot HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Mon, 20 Aug 2018 09:40:16 GMT
If-None-Match: "29cd-573dab264bb20-gzip"
Cache-Control: max-age=0

--7da2e347-F--
HTTP/1.1 403 Forbidden
Content-Length: 209
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

--7da2e347-E--
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /
on this server.<br />
</p>
</body></html>

--7da2e347-H--
Message: Warning. Pattern match
"(?i)(?:\\x5c|(?:%(?:c(?:0%(?:[2aq]f|5c|9v)|1%(?:[19p]c|8s|af))|2(?:5(?:c(?:0%25
af|1%259c)|
2f|5c)|%46|f)|(?:(?:f(?:8%8)?0%8|e)0%80%a|bg%q)f|%3(?:2(?:%(?:%6|4)6|F)|5%%63)|u
(?:221
[56]|002f|EFC8|F025)|1u|5c)|0x(?:2f|5c)|\\/))(?:%(?:(?:f(?:(?:c%80|8)%8)?0%8
..." at REQUEST_URI_RAW.
[file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-
LFI.conf"] [line "50"] [id "930100"]
[rev "3"] [msg "Path Traversal Attack (/../)"] [data "Matched Data: /?../ found
within
REQUEST_URI_RAW: /?../../boot"] [severity "CRITICAL"] [ver "OWASP_CRS/3.0.0"]
[maturity "9"]
[accuracy "7"] [tag "application-multi"] [tag "language-multi"] [tag "platform-
multi"] [tag "attack-lfi"]
[tag "OWASP_CRS/WEB_ATTACK/DIR_TRAVERSAL"]
Message: Warning. Matched phrase
"../" at REQUEST_URI. [file "/usr/share/modsecurity-crs/rules/REQUEST-930-
APPLICATION-ATTACK-LFI.conf"]
[line "77"] [id "930110"] [rev "1"] [msg "Path Traversal Attack (/../)"] [data
"Matched Data: ../ found within
REQUEST_URI: /?../../boot"] [severity "CRITICAL"] [ver "OWASP_CRS/3.0.0"]
[maturity "9"] [accuracy "7"]
[tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag
"attack-lfi"] [tag "OWASP_CRS/WEB_ATTACK/DIR_TRAVERSAL"]
Message: Warning. Matched phrase
"../" at REQUEST_URI. [file "/usr/share/modsecurity-crs/rules/REQUEST-930-
APPLICATION-ATTACK-LFI.conf"]
[line "77"] [id "930110"] [rev "1"] [msg "Path Traversal Attack (/../)"] [data
"Matched Data: ../ found within REQUEST_URI:
/?../../boot"] [severity "CRITICAL"] [ver "OWASP_CRS/3.0.0"] [maturity "9"]
[accuracy "7"] [tag "application-multi"]
[tag "language-multi"] [tag "platform-multi"] [tag "attack-lfi"] [tag
"OWASP_CRS/WEB_ATTACK/DIR_TRAVERSAL"]
Message: Access denied with code 403 (phase 2).
Operator GE matched 5 at TX:anomaly_score. [file "/usr/share/modsecurity-
crs/rules/REQUEST-949-
BLOCKING-EVALUATION.conf"] [line "57"] [id "949110"] [msg "Inbound Anomaly Score
Exceeded
(Total Score: 15)"] [severity "CRITICAL"] [tag "application-multi"] [tag
```

```
"language-multi"] [tag "platform-multi"]
[tag "attack-generic"]
Message: Warning. Operator GE matched 5
at TX:inbound_anomaly_score. [file "/usr/share/modsecurity-crs/rules/RESPONSE-
980-CORRELATION.conf"]
[line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound
Score: 15 - SQLI=0,
XSS=0,RFI=0,LFI=15,RCE=0,PHPI=0,HTTP=0,SESS=0): Path Traversal Attack (/../)"]
[tag "event-correlation"]
Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client %s]
ModSecurity: %s%s [uri "%s"]%s
Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client %s]
ModSecurity: %s%s [uri "%s"]%s
Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client %s]
ModSecurity: %s%s [uri "%s"]%s
Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client %s]
ModSecurity: %s%s [uri "%s"]%s
Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client %s]
ModSecurity: %s%s [uri "%s"]%s
Action: Intercepted (phase 2)
Stopwatch: 1537891047278697 20402 (- - -)
Stopwatch2: 1537891047278697 20402; combined=5689, p1=692, p2=4781, p3=0, p4=0,
p5=216,
sr=21, sw=0, l=0, gc=0
Response-Body-Transformed: Dechunked
Producer: ModSecurity for Apache/2.9.1 (http://www.modsecurity.org/);
OWASP_CRS/3.0.0.
Server: Apache
Engine-Mode: "ENABLED"

--7da2e347-Z--
```

Modul mod_evasive

Modul prati *web*-promet i uspoređuje ga s tablicom sažetaka (*hash table*) IP adresa i URL-ova te blokira promet ako prelazi konfigurirani prag. U slučaju prelaženja toga praga, zlćudna aktivnost se bilježi ili se pošalje obavijest.

Modul se instalira naredbom `apt-get` i automatski je omogućava, što se može provjeriti `apachectl -M` naredbom:

```
$ sudo apt-get install libapache2-mod-evasive

$ sudo apachectl -M | grep evasive
 evasive20_module (shared)
```

Prema zadanim postavkama `mod_evasive` konfiguracija se nalazi u `/etc/apache2/mods-enabled/evasive.conf` i sve opcije su onemogućene. Ovisno o zaštiti koji je potrebna, potrebno je obrisati komentar (#) ispred pojedine opcije i ponovno pokrenuti *web*-servis:

```
$ sudo vim /etc/apache2/mods-enabled/evasive.conf
<IfModule mod_evasive20.c>
    DOSHashTableSize    3097
    DOSPageCount        2
    DOSSiteCount        50
    DOSPageInterval     1
    DOSSiteInterval     1
    DOSBlockingPeriod   10

    DOSEmailNotify      root@localhost
    #DOSSystemCommand    "su - someuser -c '/sbin/... %s ...'"
    DOSLogDir           "/var/log/mod_evasive"
</IfModule>

$ sudo systemctl reload apache2
```

Slijedi objašnjenje konfiguracije:

- `DOSHashTableSize`: specificira se veličina tablice sažetaka koja se koristi za praćenje aktivnosti po IP adresi. Povećanje će omogućiti brže praćenje *web*-stranica koje je klijent već posjetio, ali će trošiti puno računalnih resursa ako je vrijednost previsoka.
- `DOSPageCount`: broj identičnih upita prema istoj lokaciji na *web*-sjedištu koje korisnik smije napraviti u vremenskom intervalu koji je definiran u DOSPageInterval-u
- `DOSPageCount`: broj upita koje klijent smije napraviti na cijelom *web*-sjedištu u vremenskom intervalu koji je definiran u DOSSiteInterval-u
- `DOSPageInterval`: vremenski interval u sekundama
- `DOSSiteInterval`: vremenski interval u sekundama
- `DOSBlockingPeriod`: vremenski interval u sekundama, na koji će se blokirati korisnik ako pređe prag definiran u DOSPageCountu i DOSPageCountu
- `DOSSystemCommand:` naredba koja će se izvršiti nakon što je neka IP adresa blokirana
- `DOSEmailNotify`: adresa elektroničke pošte za slanje obavijesti o blokiranju IP adrese korisnika
- `DOSLogDir`: lokacija dnevničkoga zapisa.

Za omogućavanje bilježenja potrebno je stvoriti direktorij s vlasnikom www-data u kojem će ih modul zapisivati.

```
$ sudo mkdir /var/log/mod_evasive
$ sudo chown -R www-data:www-data /var/log/mod_evasive
$ sudo systemctl reload apache2
```

Ako gore objašnjene konfiguracije nisu dobro podešene, moguće je blokirati pristup legitimnim korisnicima. Zato je potrebno testirati razne konfiguracije dok se ne pronađe ona koja najviše odgovara trenutnom *web*-poslužitelju.

Za testiranje rada modula potrebno je promijeniti broj zahtjeva za istu *web*-stranicu u vremenskom periodu. Bit će dovoljno staviti da se korisnik blokira nakon 2 zahtjeva u sekundi:

```
$ sudo vim /etc/apache2/mods-enabled/evasive.conf
<IfModule mod_evasive20.c>
    DOSHashTableSize    3097
    DOSPageCount        2
    DOSSiteCount        50
    DOSPageInterval     10
    DOSSiteInterval     1
    DOSBlockingPeriod   10

    DOSEmailNotify      root@localhost
    #DOSSystemCommand    "su - someuser -c '/sbin/... %s ...'"
    DOSLogDir           "/var/log/mod_evasive"

</IfModule>

$ sudo systemctl reload apache2
```

Nakon ponovnoga pokretanja *web*-servisa, koristeći wget naredbu više od dva puta u 10 sekundi IP adresa će se zabraniti:

```
$ wget 127.0.0.1
--2018-09-26 12:47:52--  http://127.0.0.1/
Connecting to 127.0.0.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10701 (10K) [text/html]
Saving to: ‘index.html.7’

index.html.7
100%[=========================================
==========================================>]
10.45K  --.-KB/s    in 0s

2018-09-26 12:47:52 (197 MB/s) - ‘index.html.7’ saved [10701/10701]

$ wget 127.0.0.1
--2018-09-26 12:47:54--  http://127.0.0.1/
Connecting to 127.0.0.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10701 (10K) [text/html]
Saving to: ‘index.html.8’
```

```
index.html.8
100%[=========================================
=========================================>]
10.45K  --.-KB/s    in 0.001s

2018-09-26 12:47:54 (7.57 MB/s) - ‘index.html.8’ saved [10701/10701]

$ wget 127.0.0.1
--2018-09-26 12:47:56--  http://127.0.0.1/
Connecting to 127.0.0.1:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2018-09-26 12:47:56 ERROR 403: Forbidden.
```

O blokiranoj IP adresi poslat će se elektronička poruka:

```
$ mail
"/var/mail/root": 1 message 1 new
     1 www-data           Wed Sep 26 12:23  29/1071
? 1
Return-Path: <www-data@debian>
X-Original-To: root@localhost
Delivered-To: root@localhost
Received: from localhost (localhost [127.0.0.1])
       by debian (Postfix) with ESMTP id 56F0B17EC
       for <root@localhost>; Wed, 26 Sep 2018 12:23:39 +0200 (CEST)
X-Virus-Scanned: Debian amavisd-new at
X-Spam-Flag: NO
X-Spam-Score: 3.013
X-Spam-Level: ***
X-Spam-Status: No, score=3.013 tagged_above=-999 required=6.31
       tests=[MISSING_SUBJECT=1.767, NO_RELAYS=-0.001,
TO_MALFORMED=1.247]
       autolearn=no autolearn_force=no
Received: from debian ([127.0.0.1])
       by localhost (localhost [127.0.0.1]) (amavisd-new, port 10024)
       with ESMTP id WsDK0f0okxSo for <root@localhost>;
       Wed, 26 Sep 2018 12:23:38 +0200 (CEST)
Received: by debian (Postfix, from userid 33)
       id 8AF3817E1; Wed, 26 Sep 2018 12:23:38 +0200 (CEST)
To: <root@localhost>
X-Mailer: mail (GNU Mailutils 3.1.1)
Message-Id: <20180926102338.8AF3817E1@debian>
Date: Wed, 26 Sep 2018 12:23:38 +0200 (CEST)
From: www-data@debian (www-data)

To: root@localhost
Subject: HTTP BLACKLIST 127.0.0.1
```

```
mod_evasive HTTP Blacklisted 127.0.0.1
```

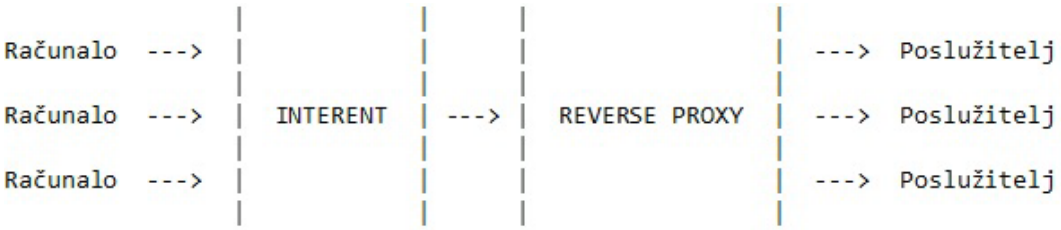
IP adresa ili podmreža na koju se neće primjenjivati navedena pravila dodaje se u `/etc/httpd/conf.d/mod_evasive.conf`:

```
$ sudo vim /etc/httpd/conf.d/mod_evasive.conf
<IfModule mod_evasive20.c>
    DOSWhitelist    192.168.0.53
    DOSWhitelist    127.0.0.*
    ...
</IfModule>

$ sudo systemctl reload apache2
```

4.3.4. Reverse proxy

Proxy je servis koji posreduje između klijentskih zahtjeva, najčešće u lokalnoj mreži, i poslužitelja. Klijentsko računalo se povezuje sa servisom *proxy* tražeći neki resurs, kao što je *web*-stranica. Servis *proxy* procjenjuje zahtjev i, ako je odobren, zahtjev se prosljeđuje do poslužitelja. Prema tome, klijent nikada ne komunicira izravno s vanjskim poslužiteljem i svaki nedozvoljeni zahtjev se onemogućava.

Reverse proxy radi u obrnutom smjeru, zahtjeve koji dolaze od klijenata koji se nalaze na Internetu prosljeđuje do poslužitelja koji je smješten u lokalnoj mreži. Između klijenta i poslužitelja smješten je poslužitelj *reverse proxy* koji distribuira zahtjeve na jedan ili više *backend* poslužitelja.



Na ovaj način klijent nikad ne komunicira direktno s *backend* poslužiteljima, a postoji mogućnost balansiranja zahtjeva na više poslužitelja što osigurava neprekidnost usluge i rasterećenje pojedinih poslužitelja. Poslužitelj *reverse proxy* ima i opciju privremene memorije ako se neki sadržaj često zahtjeva pa s time dodatno smanjuje opterećenje poslužitelja. Također je moguće kontrolirati pristup poslužitelju, tj. uspostaviti vatrozid.

Servis *proxy* se može uspostaviti na poslužitelju na kojem se nalaze aplikacije koje poslužuje, tako da zahtjev koji dođe na port 80 ili 443 *proxyjira* na neki drugi port na kojem radi željena aplikacija. *Web*-servis koristi nekoliko modula za sve navedene mogućnosti:

- *mod_proxy:* glavni modul za prosljeđivanje prometa raznim aplikacijama
- *mod_proxy_http*: omogućuje proxiranje HTTP prometa

- *mod_proxy_balancer* i *mod_lbmethod_byrequests*: omogućuje balansiranje prometa na više poslužitelja.

Moduli se aktiviraju naredbom `a2enmod`, nakon čega je potrebno ponovno pokrenuti *web*-servis:

```
$ sudo a2enmod proxy  proxy_http proxy_balancer lbmethod_byrequests
$ sudo systemctl reload apache2

$ sudo apachectl -M | grep
'proxy\|proxy_http\|proxy_balancer\|lbmethod_byrequests'
 lbmethod_byrequests_module (shared)
 proxy_module (shared)
 proxy_balancer_module (shared)
 proxy_http_module (shared)
```

Konfiguracija za *reverse proxy* definira se u virtualnom hostu na koji će stizati klijentski zahtjevi, u ovom slučaju to je zadani SSL virtualni host:

```
$ sudo vim /etc/apache2/sites-enabled/default-ssl.conf
<VirtualHost _default_:443>
  ProxyPreserveHost On

  ProxyPass / https://127.0.0.1:4433/
  ProxyPassReverse / https://127.0.0.1:4433/
</VirtualHost>

$ sudo systemctl reload apache2
```

Objašnjenje konfiguracije:

- `ProxyPreserveHost`: *web*-servis prosljeđuje originalno zaglavlje klijentovoga zahtjeva tako da *backend* poslužitelji ili aplikacije znaju njegovu IP adresu.
- `ProxyPas`: konfiguracija koja definira gdje se prosljeđuje zahtjev. U prethodnoj konfiguraciji sav promet koji dođe na https://127.0.0.1 proslijedit će se na https://127.0.0.1:4433 i vratit će željenu web-stranicu klijentu.
- `ProxyPassReverse`: mora biti isti kao i ProxyPass, a korigirat će zaglavlje koje dođe s *backend* poslužitelja. Tako će *web*-preglednik od klijenta dobiti IP adresu od *proxy* poslužitelja, a ne od *backend* poslužitelja.

Da *proxy* dobro prosljeđuje promet može se provjeriti u `error.log` dnevničkom zapisu nakon upisivanja https://127.0.0.1 u web-preglednik:

```
[Wed Sep 26 17:42:44.779313 2018] [proxy:error] [pid 7552:tid
139906918418176]
```

```
(111)Connection refused: AH00957: HTTPS: attempt to connect
to 127.0.0.1:4433 (127.0.0.1) failed
```

Web-servis pokuša doći do porta 4433, što je i konfigurirano, ali zbog nepostojanja aplikacije koja sluša na tom portu, ispisuje se greška.

Za korištenje balansera prometa koji prosljeđuje promet prema nekoliko poslužitelja koristi se sljedeća konfiguracija:

```
$ sudo vim /etc/apache2/sites-enabled/default-ssl.conf
<VirtualHost _default_:443>
  ProxyPreserveHost On

  ProxyPass / balancer://backend/
  ProxyPassReverse / balancer://backend/

  <Proxy balancer://backend>
    BalancerMember https://192.168.0.50:443
    BalancerMember https://192.168.0.51:443
  </Proxy>
</VirtualHost>

$ sudo systemctl reload apache2
```

Atributi `ProxyPass` i `ProxyPassReverse` sada sadržavaju direktivu (balancer://backend) koja se referencira na posebnom bloku konfiguracija (<Proxy></Proxy>). U bloku se definira više lokacija prema kojima će se promet balansirati.

Iz `error.log` zapisa može se provjeriti prosljeđuje li *proxy* dobro promet, ali zbog nepostojanja aplikacije koja sluša na tom portu, ispisuje se greška.

```
[Wed Sep 26 17:50:30.687771 2018] [proxy:error] [pid 7635:tid
140571102627584]
(110)Connection timed out: AH00957: HTTP: attempt to connect to
192.168.0.51:443 (192.168.0.51) failed192.168.0.51:443 (192.168.0.51)
failed
```

4.3.5. Zanimljivi izvori

Poveznice:

- https://www.sslshopper.com/what-is-a-csr-certificate-signing-request.html
- https://www.tecmint.com/apache-security-tips/
- https://geekflare.com/10-best-practices-to-secure-and-harden-your-apache-web-server/

4.3.6. Vježba 10: Prilagodba sigurnosnih postavki web-servisa

1. Prije početka rada odaberite sliku stanja virtualnoga računala **slika_jedan** za početak vježbe.
2. Prijavite se na računalo kao korisnik **linux1**. U GUI-ju pokrenite **Terminal** (*Activities* → **Terminal**). Izvršite **su -** naredbu da postanete administrator (lozinka: linux1).
3. Provjerite ispravnost pokretanja web-servisa:

```
# systemctl status apache2
```

4. Otvorite *web*-preglednik u *Windows* okruženju i upišite URL http://localhost/nema.
5. Koje sve informacije možete saznati s otvorene web-stranice? Jesu li to osjetljive informacije i zašto?

_____

_____

6. Kako bi zakrpali ranjivost upišite sljedeću konfiguraciju na kraj datoteke **apache2.conf** i ponovno učitajte konfiguraciju *web*- servisa:

```
# vim /etc/apache2/apache2.conf
ServerSignature Off
ServerTokens Prod

# systemctl reload apache2
```

7. Otvorite *web*-preglednik u *Windows* okruženju i upišite URL http://localhost/nema. Jesu li sada prikazane osjetljive informacije?

_____

8. Stvorite nekoliko proizvoljnih datoteka i direktorija u direktoriju **/var/www/html/test/**.

```
# mkdir /var/www/html/test
# touch /var/www/html/test/css.css
# touch /var/www/html/test/sec.php
# touch /var/www/html/test/site.php
# mkdir /var/www/html/test/dir
```

9. Otvorite *web*-preglednik u *Windows* okruženju i upišite URL http://localhost/test. Jesu li prikazane datoteke i direktoriji? Jesu li to osjetljive informacije i zašto?

_____

_____

10. U datoteci zadanoga virtualnog hosta *web*-servisa dodajete konfiguraciju **Options – Indexes** za direktorij **/var/www/html**. Zatim ponovno učitajte konfiguraciju web-servisa.

```
# vim /etc/apache2/sites-available/000-default.conf

<VirtualHost *:80>
    DocumentRoot /var/www/html
    <Directory /var/www/html>
           Options -Indexes
    </Directory>
</VirtualHost>

# systemctl reload apache2
```

11. Otvorite *web*-preglednik u Windows okruženju i upišite URL http://localhost/test. Jesu li prikazane datoteke i direktoriji? Što se sada prikazuje na web-stranici?

_____

12. Dodajte ostale preporuke za sigurniju konfiguraciju: _____

a. Onemogućavanje simboličnih poveznica

```
# vim /etc/apache2/sites-available/000-default.conf

<VirtualHost *:80>
   DocumentRoot /var/www/html

   <Directory /var/www/html>
          Options -Indexes -FollowSymLinks
   </Directory>
</VirtualHost>

# systemctl reload apache2
```

b. Onemogućavanje *Etaga*:

```
# vim /etc/apache2/apache2.conf
Header unset ETag
FileETag None

# systemctl reload apache2
```

c. Onemogućavanje *Trace HTTP Request*

```
# vim /etc/apache2/apache2.conf
Header unset ETag
TraceEnable off

# systemctl reload apache2
```

d. Onemogućavanje Server Side Includes i CGI Execution

```
# vim /etc/apache2/sites-available/000-default.conf
<VirtualHost *:80>
   DocumentRoot /var/www/html
   <Directory /var/www/html>
          Options -Indexes -FollowSymLinks -Includes -ExecCGI
   </Directory>
</VirtualHost>
```

e. Ograničavanje HTTP zahtjeva

```
# vim /etc/apache2/apache2.conf
LimitRequestBody 204800

# vim /etc/apache2/sites-available/000-default.conf

<VirtualHost *:80>
   DocumentRoot /var/www/html
   <Directory /var/www/html>
          LimitRequestBody 204800
   </Directory>
</VirtualHost>

# systemctl reload apache2
```

4.3.7. Vježba 11: Aplikativni vatrozid web- servisa

1. Prije početka rada odaberite sliku stanja virtualnoga računala **slika_jedan** za početak vježbe.
2. Prijavite se na računalo kao korisnik **linux1**. U GUI-ju pokrenite **Terminal** (*Activities* → **Terminal**). Izvršite **su -** naredbu da postanete administrator (lozinka: linux1).
3. Provjerite ispravnost pokretanja *web*-servisa:

   ```
   # systemctl status apache2
   ```

4. Instalirajte module *libapache2-modsecurity libapache2-mod- evasive web*-servisa i naredbom **apachectl –M** provjerite jesu li aktivirani:

```
# apt-get install libapache2-mod-security2 libapache2-mod-
evasive
# apachectl -M | grep 'evasive\|sec'
```

5. Premjestite preporučenu konfiguracijsku datoteku modula *security2* i ponovno učitajte konfiguraciju web-servisa:

```
# mv /etc/modsecurity/modsecurity.conf-recommended
/etc/modsecurity/modsecurity.conf

# systemctl reload apache2
```

6. Naredbom tail -f pratite dnevničke zapise modula security2:

```
# tail -f /var/log/apache2/modsec_audit.log
```

7. Otvorite web-preglednik u Windows okruženju i upišite URL http://localhost/?../../boot. Prikazuje li se web-stranica? Što se bilježi u dnevničkom zapisu nakon **'Engine-Mode**'?

_____

_____

8. U datoteci **modsecurity.conf** promijenite konfiguraciju kako bi se aktivirala zaštita. Zatim ponovno učitajte konfiguraciju *web*-servisa:

```
# vim /etc/modsecurity/modsecurity.conf
SecRuleEngine On
```

9. Naredbom **tail -f** pratite dnevničke zapise modula *security2*:

```
# tail -f /var/log/apache2/modsec_audit.log
```

10. Otvorite *web*-preglednik u Windows okruženju i upišite URL http://localhost/?../../boot. Prikazuje li se web-stranica? Što se bilježi u dnevničkom zapisu nakon 'Engine-Mode'?

_____

_____

11. Stvorite datoteku koja će koristiti modul *evasive* za bilježenje svojih aktivnosti u dnevnički zapis:

```
# mkdir /var/log/mod_evasive
```

```
# chown -R www-data:www-data /var/log/mod_evasive
```

12. Promijenite konfiguracije modula *evasive* i ponovno učitajte konfiguraciju *web*-servisa:

```
# vim /etc/apache2/mods-enabled/evasive.conf
<IfModule mod_evasive20.c>
DOSHashTableSize  3097
DOSPageCount      3
DOSSiteCount      50
DOSPageInterval   10
DOSSiteInterval   1
DOSBlockingPeriod 10

DOSEmailNotify
root@localhost
#DOSSystemCommand "su - someuser -c
'/sbin/... %s ...'"
DOSLogDir  "/var/log/mod_evasive"
</IfModule>

# systemctl reload apache2
```

13. Prema gore promijenjenoj konfiguraciji, nakon koliko pokušaja otvaranja *web*-stranice u i kojem vremenskom intervalu će korisniku biti onemogućen pristup web-stranici?

_____

14. Otvorite *web*-preglednik u *Windows* okruženju i otvorite nekoliko puta URL http://localhost/. Koji je maksimalni broj otvaranja web-stranice?

_____

15. Dodajte konfiguraciju za *whitelist* IP adresa s kojim se pristupa web-servisu i ponovno učitajte konfiguraciju *web*-servisa:

```
# vim /etc/apache2/mods-enabled/evasive.conf
<IfModule mod_evasive20.c>
DOSWhitelist      192.168.2.1
DOSWhitelist      127.0.0.*
</IfModule>

# systemctl reload apache2
```

16. Otvorite *web*-preglednik u *Windows* okruženju i otvorite nekoliko puta URL http://localhost/. Koji je maksimalni broj otvaranja *web*-stranice?

5. Nadzor sigurnosti

Trajanje poglavlja:
205 min

Po završetku ovoga poglavlja moći ćete:

- opisati način rada i nabrojati alate za otkrivanje sigurnosnih prijetnji i anomalija u dnevničkim zapisima
- implementirati alat Wazuh za analiziranje dnevničkih zapisa i reagiranje na prijetnje
- definirati rad provjere integriteta datoteka, te koristiti alat Wazuh za tu svrhu
- primijeniti alate ClamAV i Chkrootkit za otkrivanje zlonamjernih programa
- opisati važnost skeniranja otvorenih portova te za tu svrhu koristiti alate Wazuh i nmap
- navesti kako može doći do nesigurnih konfiguracija i koristiti alate za automatsku provjeru konfiguracija
- razlikovati lokalne i udaljene sigurnosne ranjivosti te razliku između iskoristivih i neiskoristivih ranjivosti
- upotrijebiti alat Lynis za skeniranje lokalnih ranjvosti.

Ova cjelina obrađuje načine nadzora sustava kroz praćenje dnevničkih zapisa, skeniranje zlonamjernih programa i provjeru integriteta datoteka. U drugom dijelu cjeline obrađuje se učvršćivanje i provjera konfiguracije poslužitelja, te provjera svih obrađenih sigurnosnih standarda skeniranjem ranjivosti i provjera otvorenih portova.

5.1. Nadzor sustava i servisa

5.1.1. Računalni IDS

Računalni IDS (HIDS, *Host Based Intrusion Detection System*) aktivno provjerava tragove koje napadač ostavlja u dnevničkim zapisima, prilikom promjene konfiguracija, izvršavanja naredbi, pokretanja skripti, instaliranja programa itd., te pokušava spriječiti njegove daljnje aktivnosti i poslati upozorenje administratorima sustava. HIDS uključuje nekoliko razina zaštite i mogućnosti za operacijske sustave:

- otkrivanje sigurnosnih prijetnji i anomalija u dnevničkim zapisima i reakcija na prijetnje
- provjera integriteta datoteka
- otkrivanje zlonamjernih programa
- provjera izlaza naredbi.

Lista mogućnosti računalnih IDSova je poduža i često se proširuje mogućnostima koje nisu usko vezane za otkrivanje napada u realnom vremenu. Te mogućnosti mogu biti i provjera otvorenih portova, skeniranje ranjivosti, provjera konfiguracija u svrhu osiguravanja itd.

HIDS se u mreži implementira nakon mrežnoga IDS-a i vatrozida, tj. direktno na operacijski sustav. U mrežama s nekoliko računala HIDS se može implementirati na odvojenom računalu koje prikuplja sve sistemske i aplikacijske zapise te reagira na prijetnje.

HIDS alati koji se mogu instalirati na operacijskim sustavima *Linux* su *Wazuh*, OSSEC, *Security Onion*, *Samhain*, *Sagan*, *Fail2Ban* itd.

Wazuh

Alat *Wazuh* je HIDS otvorenoga kôda i može se koristiti na svim poznatijim operacijskim sustavima. Instalira se na računalo kojem je potrebna zaštita ili na zasebno računalo koje prikuplja dnevničke zapise od ostalih računala, analizira ih i reagira na prijetnje.

U slučaju distribuirane arhitekture gdje se u mreži nalazi više računala kojima je potrebna zaštita, servis *wazuh-manager* instalira se na zasebnom računalu, a na svim ostalim računalima instalira se servis *wazuh-agent* koji prosljeđuje dnevničke zapise, informacije o integritetu datoteka, popis otvorenih portova itd. servisu *wazuh-manager*. Nakon analize dnevničkih zapisa ili drugih provjera, *wazuh-manger* može reagirati na prijetnju tako da blokira napadača i može poslati obavijesti prijetnji ili o nekoj drugoj anomaliji.

Instalacija servisa *wazuh-manager*

Za instalaciju servisa *wazuh-manager* potrebno je dodati repozitorij za *Wazuh* pakete:

```
$ sudo apt-get update
$ sudo apt-get install curl apt-transport-https lsb-release
$ sudo curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -
$ sudo echo "deb https://packages.wazuh.com/3.x/apt/ stable main" | tee -a
/etc/apt/sources.list.d/wazuh.list
$ sudo apt-get update
```

Napomena

Wazuh je nastao iz OSSEC-a i zbog toga se još uvijek koristi njegovo ime u imenovanju datoteka, direktorija, servisnoga procesa itd.

Zatim se naredbom `apt-get` instalira servis *wazuh-manger* te se provjeri njegov status:

```
$ sudo apt-get install wazuh-manager
$ sudo systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/etc/systemd/system/wazuh-manager.service; enabled; vendor
preset: enabled)
   Active: active (running) since Wed 2018-10-03 15:35:14 CEST; 58s ago
   CGroup: /system.slice/wazuh-manager.service
           ├─18660 /var/ossec/bin/wazuh-db
           ├─18674 /var/ossec/bin/ossec-execd
```

```
           ├─18680 /var/ossec/bin/ossec-analysisd
           ├─18684 /var/ossec/bin/ossec-syscheckd
           ├─18689 /var/ossec/bin/ossec-remoted
           ├─18693 /var/ossec/bin/ossec-logcollector
           ├─18697 /var/ossec/bin/ossec-monitord
           └─18718 /var/ossec/bin/wazuh-modulesd

Oct 03 15:35:12 debian env[18644]: Started wazuh-db...
Oct 03 15:35:12 debian env[18644]: Started ossec-execd...
Oct 03 15:35:12 debian env[18644]: Started ossec-analysisd...
Oct 03 15:35:12 debian env[18644]: Started ossec-syscheckd...
Oct 03 15:35:12 debian env[18644]: Started ossec-remoted...
Oct 03 15:35:12 debian env[18644]: Started ossec-logcollector...
Oct 03 15:35:12 debian env[18644]: Started ossec-monitord...
Oct 03 15:35:12 debian env[18644]: Started wazuh-modulesd...
Oct 03 15:35:14 debian env[18644]: Completed.
Oct 03 15:35:14 debian systemd[1]: Started Wazuh manager.
```

Konfiguracija servisa *wazuh-manager*

Zadana konfiguracija servisa *wazuh-manager* nalazi se u datoteci `/var/ossec/etc/ossec.conf`:

```
<ossec_config>
  <global>
</global>


    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>ossecm@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <queue_size>131072</queue_size>
</global>


 <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>12</email_alert_level>
  </alerts>
  ...
</ossec_config></ossec_config>
```

Pojašnjenje važnijih mogućnosti konfiguracije:

- `jsonout_output`: Ako je postavljeno na yes, bilježi alertove u formatu JSON u datoteku dnevničkoga zapisa: `/var/ossec/logs/archives/archives.json`. Preporučeno je postaviti na no, osim ako postoji potreba za korištenjem.
- `alerts_log`: bilježi alertove u dnevnički zapis: /var/ossec/logs/alerts/alerts.log ako je postavljeno na yes.
- email_notification: uključuje ili isključuje slanje obavijesti elektroničkom poštom.
- `smtp_server`: adresa poslužitelja elektroničke pošte za slanje alertova
- `email_from`: upis pošiljatelja elektroničke pošte za alertova
- `email_to`: primatelj elektroničke poruke koje sadrže alertove
- `email_maxperhour`: maksimalni broj elektroničkih poruka koje će se poslati po satu. Ako broj alertova prijeđe maksimalni broj, alertovi će se grupirati u jednoj elektroničkoj poruci i poslati na kraju tekućega sata.
- `log_alert_level`: postavlja se minimalna razina za alertove koji će se zapisati u dnevničkim zapisima u alerts.log ili archives.json (razina od 1 do 16)
- `email_alert_level`: postavlja se minimalna razina za alertove koji će se slati elektroničkom poštom (razina od 1 do 16).

Nakon pokušaja spajanja s nepostojećim korisnikom protokolom SSH, *Wazuh* je zabilježio sljedeće alertove:

```
$ tail -f /var/ossec/logs/alerts/alerts.log

** Alert 1538590789.26718: mail  -
syslog,sshd,invalid_login,authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,
pci_dss_10.6.1,gpg13_7.1,gdpr_IV_35.7.d,gdpr_IV_32.2,
2018 Oct 03 20:19:49 debian->/var/log/auth.log
Rule: 5710 (level 5) -> 'sshd: Attempt to login using a non-existent user'
Src IP: 192.168.56.1
Src Port: 65223
Oct  3 20:19:48 debian sshd[563]: Invalid user asdf from 192.168.56.1 port 65223

** Alert 1538590793.27126: mail  -
pam,syslog,authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,
gpg13_7.8,gdpr_IV_35.7.d,gdpr_IV_32.2,
2018 Oct 03 20:19:53 debian->/var/log/auth.log
Rule: 5503 (level 5) -> 'PAM: User login failed.'
Src IP: 192.168.56.1
Oct  3 20:19:52 debian sshd[563]: pam_unix(sshd:auth): authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
uid: 0
euid: 0
tty: ssh

** Alert 1538590795.27541: mail  -
syslog,sshd,invalid_login,authentication_failed,pci_dss_10.2.4,
pci_dss_10.2.5,pci_dss_10.6.1,gpg13_7.1,gdpr_IV_35.7.d,gdpr_IV_32.2,
2018 Oct 03 20:19:55 debian->/var/log/auth.log
Rule: 5710 (level 5) -> 'sshd: Attempt to login using a non-existent user'
```

```
Src IP: 192.168.56.1
Oct  3 20:19:54 debian sshd[563]: Failed password for invalid user asdf from
192.168.56.1 port 65223 ssh2
```

Također je poslao elektroničku poruku za pravila 5710 i 5503:

```
Return-Path: <root@localhost>
X-Original-To: root@localhost
Delivered-To: root@localhost
Received: from notify.ossec.net (localhost [127.0.0.1])
        by debian.home (Postfix) with SMTP id BA21D4E
        for <root@localhost>; Wed,  3 Oct 2018 20:20:08 +0200 (CEST)
To: <root@localhost>
From: Wazuh <root@localhost>
Date: Wed, 03 Oct 2018 20:20:08 +0200
Subject: OSSEC Notification - debian - Alert level 5
Message-Id: <20181003182008.BA21D4E@debian.home>


Wazuh Notification.
2018 Oct 03 20:19:49

Received From: debian->/var/log/auth.log
Rule: 5710 fired (level 5) -> "sshd: Attempt to login using a non-existent user"
Src IP: 192.168.56.1
Portion of the log(s):

Oct  3 20:19:48 debian sshd[563]: Invalid user asdf from 192.168.56.1 port 65223



 --END OF NOTIFICATION



Wazuh Notification.
2018 Oct 03 20:19:53

Received From: debian->/var/log/auth.log
Rule: 5503 fired (level 5) -> "PAM: User login failed."
Src IP: 192.168.56.1
```

Iz prethodnog primjera možemo doznati detaljne informacije:

- `2018 Oct 03 20:19:49`: vrijeme alerta.
- `Received From: debian->/var/log/auth.log`: alert je došao s računala imena debian i iz dnevničkog zapisa /var/log/auth.log.

- `Rule: 5710 fired (level 5) -> "sshd: Attempt to login using a non-existent user"`: alert ima id 5710 i pete je razine, a može se vidjeti i detaljnije objašnjenje alerta.
- `Src IP: 192.168.56.1`: IP adresa s koje potječe neuspjeli pokušaj spajanja.

Servis *wazuh-client*

U prethodnom primjeru instaliran je servis *wazuh-manager* koji ima sve mogućnosti za zaštitu jednoga računala. Ako je potrebna zaštita na više računala (agenata), potrebno je instalirati servis *wazuh-agent* i spojiti ga sa servisom *wazuh-manager* na središnjem računalu.

Za instalaciju servisa *wazuh-agent* potrebno je na računalu koje treba zaštititi dodati repozitorij za *Wazuh* pakete i instalirati ga naredbom `apt-get`:

```
$ sudo apt-get update
$ sudo apt-get install curl apt-transport-https lsb-release
$ curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -
$ echo "deb https://packages.wazuh.com/3.x/apt/ stable main" | tee -a
/etc/apt/sources.list.d/wazuh.list
$ sudo apt-get update

$ sudo apt-get install wazuh-agent
```

Svako računalo s instaliranim servisom *wazuh-agent*, komunicira sa servisom *wazuh-manager* kriptiranim porukama koje se kriptiraju dijeljenim (*pre-shared*) ključem. Svi načini registracije agenata navedeni su na poveznici: https://documentation.wazuh.com/current/user-manual/index.html. Proces registracije agenta na središnje računalo uključuje generiranje ključa, upis IP adrese agenta i ime računala, a pokreće se sljedećom naredbom na središnjem računalu:

```
$ sudo /var/ossec/bin/manage_agents

****************************************
* Wazuh v3.6.1 Agent manager.          *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: a
```

Opcija A otvara izbornik za dodavanje novog agenta:

```
- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: test.primjer.hr
   * The IP Address of the new agent: 192.168.2.202
   * An ID for the new agent[001]:
Agent information:
   ID:001
   Name:test.primjer.hr
   IP Address:192.168.2.202

Confirm adding it?(y/n): y
Agent added with ID 001.
```

Agent je dodan, a za prikazivanje ključa potrebno je upisati slovo E i odabrati id agenta:

```
****************************************
* Wazuh v3.6.1 Agent manager.          *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: e

Available agents:
   ID: 001, Name: test.primjer.hr, IP: 192.168.2.202
Provide the ID of the agent to extract the key (or '\q' to quit): 001

Agent key information for '001' is:
MDAxIHRlc3QucHJpbWplci5ociAxOTIuMTY4LjIuMjAyIGQ4NGVmYTAxM2ZmZDIwYTc4
NTJiMGQzNjE4OTIxYzk0NTNhZWE2ODIyMWQwMTdhNmRhNjhhMjkxODQxZjZmZDk=
```

Na agentu se istom naredbom dodaje ključ i upisuju podaci potrebni za komunikaciju:

```
$ sudo /var/ossec/bin/manage_agents

****************************************
* Wazuh v3.6.1 Agent manager.          *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
```

```
Choose your action: I or Q:
Select I to import a key and paste in the key that you extracted on the
manager:

Choose your action: I or Q: I

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit):
MDAxIHRlc3QucHJpbWplci5ociAxOTIuMTY4LjIuMjAyIGQ
4NGVmYTAxM2ZmZDIwYTc4NTJiMGQzNjE4OTIxYzk0NTNhZWE2ODIyMWQwMTdhNmRhNjhhMjk
xODQxZjZmZDk=

Agent information:
   ID:001
   Name:test.primjer.hr
   IP Address:192.168.2.202

Confirm adding it?(y/n): y
Added.
Select 'Q' to exit from manage_agents.
```

Za dovršetak konfiguracije u datoteci `/var/ossec/etc/ossec.conf` dodaje se IP adresa središnjega računala na kojem je instaliran servis *wazuh-manager*, nakon čega se ponovno pokreće *wazuh-agent*:

```
<client>
      <server-ip>192.168.2.201</server-ip>
</client>

$ sudo systemctl restart wazuh-agent
```

Wazuh dnevnički zapis, koji se koristi za rješavanje problema u radu servisa, nalazi se u datoteci `/var/ossec/logs/ossec.log`.

5.1.2. Otkrivanje sigurnosnih prijetnji i anomalija u dnevničkim zapisima i reagiranje na prijetnje

Analizom dnevničkih zapisa izdvajaju se i imenuju informacije o raznim procesima unutar operacijskog sustava i aplikacija. Svrha procesa izdvajanja informacija jest identificiranje sistemskih i aplikacijskih grešaka, napada na sustav i ostalih sigurnosnih problema.

Prema tim izdvojenim infromacijama izrađuju se pravila. Kada HIDS naiđe na dnevnički zapis koji odgovara pravilima, aktivira se alert te HIDS pokreće jednu od sljedećih mogućnosti:

- slanje elektroničke poruke o alertu administatorima
- bilježenje alerta u dnevnički zapis
- pokretanje reakcije na prijetnje, tj. zabranjuje se promet s IP adrese napadača
- ili kombinacija dviju ili više gore navedenih mogućnosti.

Lokacija dnevničkih zapisa

Kod središnjeg *Wazuh* poslužitelja i agenata, konfiguracija lokacija za prikupljanje dnevničkih zapisa nalazi se u datoteci `/var/ossec/etc/ossec.conf` .

```
$ cat /var/ossec/etc/ossec.conf

<ossec_config>

   ...

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/error.log</location>
  </localfile>

  </localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/access.log</location>
  </localfile>

  </localfile>
    <log_format>syslog</log_format>
    <location>/var/ossec/logs/active-responses.log</location>
  </localfile>

  </localfile>
    <log_format>syslog</log_format>
   <location>/var/log/messages</location>
  </localfile>

  </localfile>
    <log_format>syslog</log_format>
    <location>/var//log/auth.log</location>
  </localfile>

  </localfile>
    <log_format>syslog</log_format>
    /var/log/syslo<location>/var/log/syslog</location>
  </localfile>

  </localfile>
    <log_format>syslog</log_format>
   <location>/var/log/mail.info</location>
```

```
</localfile>

</localfile>
    <log_format>syslog</log_format>
    <location>/var/log/dpkg.log</location>
  </localfile>

  </localfile>
    <log_format>syslog</log_format>
    <location>/var/log/kern.log</location>
  </localfile>

  </ossec_config>
```

Location može biti direktna putanja do datoteke (npr. /var/log/kern.log) ili se regularnim izrazom obuhvaća više datoteka u istom direktoriju, npr. /var/log/*.log. Formati dnevničkih zapisa (log_format) mogu biti *syslog*, *apache2*, *json*, itd. Nakon promjene ili dodavanja novoga dnevničkog zapisa, potrebno je ponovno pokrenuti servis *wazuh-agent* ili *wazuh-manager*.

Analiza dnevničkih zapisa

Za testiranje analize dnevničkih zapisa koristi se naredba `/var/ossec/bin/wazuh-logtest` te se upisuje jedan zapis iz dnevničkog zapisa:

```
$ sudo /var/ossec/bin/wazuh-logtest
2018/10/04 12:47:09 ossec-testrule: INFO: Started (pid: 25558).
ossec-testrule: Type one log per line.

Oct  3 20:19:48 debian sshd[563]: Invalid user asdf from 192.168.56.1 port 65223


**Phase 1: Completed pre-decoding.
       full event: 'Oct  3 20:19:48 debian sshd[563]: Invalid user asdf from
192.168.56.1 port 65223'
       timestamp: 'Oct  3 20:19:48'
       hostname: 'debian'
       program_name: 'sshd'
       log: 'Invalid user asdf from 192.168.56.1 port 65223'

**Phase 2: Completed decoding.
       decoder: 'sshd'
       srcuser: 'asdf'
       srcip: '192.168.56.1'
       srcport: '65223'

**Phase 3: Completed filtering (rules).
       Rule id: '5710'
       Level: '5'
       Description: 'sshd: Attempt to login using a non-existent user'
**Alert to be generated.
```

Kao što je vidljivo iz ispisa naredbe, dnevnički zapis mora proći tri faze analize: *pre-decoding*, *decoding* i *rule matching*.

U fazi *pre-decoding* izvlače se statičke informacije iz poznatih dijelova zapisa. *Syslog*, *apache* i ostali poznati formati dnevničkih zapisa neke informacije zapisuju uvijek na istom mjestu. Iz prethodnog primjera dnevničkoga zapisa, informacije koje se dobiju u fazi *pre-decoding* su:

```
timestamp: 'Oct  3 20:19:48'
hostname: 'debian'
program_name: 'sshd
```

U fazi *decoding* se iz ostatka dnevničkoga zapisa identificira vrsta dnevničkoga zapisa i izvlače preostale informacije. Iz prethodnog primjera dnevničkoga zapisa informacije koje se dobiju u fazi *decoding* su:

```
decoder: 'sshd'
srcuser: 'asdf'
srcip: '192.168.56.1'
srcport: '65223'
```

Faza *rule matching* informacije dobivene iz prethodnih dviju faza uspoređuje s pravilima. Informacije dobivene iz prethodnog primjera dnevničkoga zapisa navedene su u sljedećim pravilima:

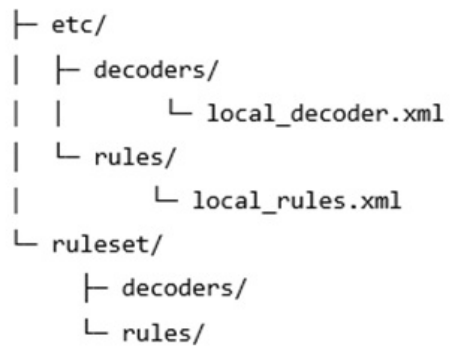
```
<rule id="5710" level="5">
    <if_sid>5700</if_sid>
   <match>illegal user|invalid user</match>
    <description>sshd: Attempt to login using a non-existent user</description>


<group>invalid_login,authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,...</gr
oup>
      </rule>
```

Kada se dnevnički zapis podudara s pravilom, servis *wazuh-manager* aktivirat će sljedeći alert:

```
** Alert 1538590789.26718: mail  -
syslog,sshd,invalid_login,authentication_failed,
pci_dss_10.2.4,pci_dss_10.2.5,...
2018 Oct 03 20:19:49 debian->/var/log/auth.log
Rule: 5710 (level 5) -> 'sshd: Attempt to login using a non-existent user'
Src IP: 192.168.56.1
Src Port: 65223
Oct  3 20:19:48 debian sshd[563]: Invalid user asdf from 192.168.56.1 port 65223
```

Datoteke pravila i dekodera

Struktura datoteka i direktorija servisa *wazuh-manager* je:



Zadani dekoderi i pravila nalaze se u direktoriju ruleset i njih se ne preporuča mijenjati jer će svaka napravljena promjena biti obrisana prilikom nadogradnje paketa. Novi dekoderi i pravila ili promjene postojećih stavljaju se unutar direktorija etc u pripadajuće datoteke:

`/var/ossec/etc/rules/local_rules.xml` i `/var/ossec/etc/decoders/local_decoder.xml`.

Dodavanje novih dekodera i pravila

Na sljedećem primjeru dnevničkoga zapisa koji se upisuje u naredbu za testiranje zapisa napravit će se novi dekoder i pravilo:

```
$ sudo /var/ossec/bin/wazuh-logtest
2018/10/05 12:49:25 ossec-testrule: INFO: Started (pid: 1051).
ossec-testrule: Type one log per line.

Jan 08 09:51:11 webserver zoltan[12345]: Korisnik 'mario'
logirao se sa '192.168.2.222'

**Phase 1: Completed pre-decoding.
       full event: 'Jan 08 09:51:11 webserver zoltan[54891]: Korisnik 'mario'
se logirao sa '192.168.2.222''
       timestamp: 'Jan 08 09:51:11'
       hostname: 'webserver'
       program_name: 'zoltan'
       log: 'Korisnik 'mario' logirao se sa '192.168.2.222''

**Phase 2: Completed decoding.
       No decoder matched.
```

Iz faze *pre-decoding* može se doznati vrijeme, ime računala, ime programa i ostatak dnevničkoga zapisa. Po tim informacijama napravit će se novi dekoder koji se upisuje u datoteku `/var/ossec/etc/decoders/local_decoder.xml`:

```
$ sudo vim /var/ossec/etc/decoders/local_decoder.xml

<decoder name="zoltan">
   <program_name>^zoltan</program_name>
</decoder>

<decoder name="spajanje_korisnika">
  <parent>zoltan</parent>
  <regex>Korisnik '(\w+)' logirao se sa '(\d+.\d+.\d+.\d+)'</regex>
  <order>user, srcip</order>
</decoder>
```

Prvi dekoder odnosi se na ime programa, a drugi dekoder obuhvaća detaljnije informacije iz dnevničkog zapisa. Na ovaj način prvi dekoder može se iskoristiti kao baza za neke druge dekodere koji će imati drugačiju svrhu od primjera. Naredba `logtest` dat će sljedeće rezultate:

```
$ sudo /var/ossec/bin/wazuh-logtest
2018/10/05 12:51:30 ossec-testrule: INFO: Started (pid: 1064).
ossec-testrule: Type one log per line.

Jan 08 09:51:11 webserver zoltan[12345]: Korisnik 'mario' logirao
se sa '192.168.2.222'


**Phase 1: Completed pre-decoding.
       full event: 'Jan 08 09:51:11 webserver zoltan[12345]:
Korisnik 'mario' logirao se sa '192.168.2.222''
       timestamp: 'Jan 08 09:51:11'
       hostname: 'webserver'
       program_name: 'zoltan'
       log: 'Korisnik 'mario' logirao se sa '192.168.2.222''

**Phase 2: Completed decoding.
       decoder: 'zoltan'
       dstuser: 'mario'
       srcip: '192.168.2.222'
```

Objašnjenja svih mogućnosti koje se mogu koristiti u fazi *decoder* nalaze se na poveznici: https://documentation.wazuh.com/current/user-manual/ruleset/ruleset-xml-syntax/decoders.html?highlight=decoder.

Na osnovi informacija izvučenih fazama *pre-decoding* i *decoding* stvaraju se pravila. Slijedi primjer:

```
$ sudo vim /var/ossec/etc/rules/local_rules.xml:

<rule id="111111" level="0">
  <program_name>zoltan</program_name>
<description>korisnik se uspjesno spojio na posluzitelj<description>
</rule>
```

Ime programa uzet će se kao jedini uvjet za aktiviranje alerta. Budući da je razina namještena na 0, alert se neće spremiti u dnevnički zapisi niti će se poslati elektroničkom porukom.

Naredbom `logtest` testira se napisano pravilo:

```
$ sudo /var/ossec/bin/wazuh-logtest
2018/10/05 14:55:26 ossec-testrule: INFO: Started (pid: 1501).
ossec-testrule: Type one log per line.

Jan 08 09:51:11 webserver zoltan[12345]: Korisnik 'mario'
logirao se sa '192.168.2.222'


**Phase 1: Completed pre-decoding.
       full event: 'Jan 08 09:51:11 webserver zoltan[12345]: Korisnik 'mario'
logirao se sa '192.168.2.222''
       timestamp: 'Jan 08 09:51:11'
       hostname: 'webserver'
       program_name: 'zoltan'
       log: 'Korisnik 'mario' logirao se sa '192.168.2.222''

**Phase 2: Completed decoding.
       decoder: 'zoltan'
       dstuser: 'mario'
       srcip: '192.168.2.222'

**Phase 3: Completed filtering (rules).
       Rule id: '111111'
       Level: '0'
       Description: 'korisnik se uspijesno spojio na posluzitelj'
```

Objašnjenja svih opcija koje se mogu koristiti pri izradi pravila nalaze se na poveznici: https://documentation.wazuh.com/current/user-manual/ruleset/ruleset-xml-syntax/rules.html#rules-syntax.

Nakon dodavanja novih pravila potrebno je ponovno pokrenuti servis *wazuh-manager*:

```
$ sudo systemctl restart wazuh-manager
```

Reakcija na prijetnje

Prilikom aktivacije nekoga pravila ili pravila koja su na određenoj razini, moguće je automatski izvesti željenu naredbu (*active response*). Najčešće je to reakcija na prijetnje gdje se blokira napadač ako izvršava neke zloćudne radnje. Ova mogućnost mora se oprezno implementirati jer može doći do lažno pozitivnih prijetnji (*false positive*), gdje se legitimnim korisnicima blokira pristup servisu ili poslužitelju.

Wazuh ima nekoliko predefiniranih naredbi koje se mogu povezati s određenim pravilima ili razinama. Najčešće reakcije na prijetnje su:

- `disable-account.sh`: Onemogućava korisnika naredbom `passwd --lock <ime_korisnika>`
- `firewall-drop.sh` ili `default-firewall-drop.sh`: Blokiranje prometa po IP adresi koristeći servis *iptables*
- `firewalld-drop.sh`: Blokiranje prometa po IP adresi koristeći servis *firewalld*
- `host-deny.sh`: Blokiranje prometa po IP adresi dodajući je u datoteku **/etc/hosts.deny**
- `ip-customblock.sh`: administrator može dodati svoju skriptu za prilagođenu reakciju
- `restart-ossec.sh`: Skripta za automatsko ponovno pokretanje servisa *wazuh-manager* ili *wazuh-agent* nakon promjene konfiguracijske datoteke `ossec.conf`.

Konfiguracija reakcije na prijetnje nalazi se u datoteci `/var/ossec/etc/ossec.conf` , a u blokovima command su dodatne konfiguracije za pojedine naredbe:

```
<ossec_config>
  <command>
    <name>disable-account</name>
    <executable>disable-account.sh</executable>
    <expect>user</expect>
    <timeout_allowed>yes</timeout_allowed>
  </command>

<command>
    <name>restart-ossec</name>
    <executable>restart-ossec.sh</executable>
    <expect></expect>
 </command>

</command>
     <name>host-deny</name>
    <executable>host-deny.sh</executable>
     <expect>srcip</expect>
     <timeout_allowed>yes</timeout_allowed>
  </command>

<command>
    <name>firewall-drop</name>
    <executable>firewall-drop.sh</executable>
    <expect>srcip</expect>
    <timeout_allowed>yes</timeout_allowed>
```

```
</command>
...
</ossec_config>
```

U bloku command definira se:

- `firewall-drop`: ime reakcije na prijetnje (`firewall-drop`) koje će koristiti kasnije u bloku active-response
- `Executable`: definira ime datoteke skripte, unutar direktorija **/**`var/ossec/active-response/bin`
- `srcip`: IP adresa koju koristi skripta
- `timeout_allowed`: omogućava se deblokiranje IP adrese nakon određenog vremena, što se može specificirati u bloku `active-response`.

U bloku `active-response` definira se gdje i kada će se naredba izvršiti. U sljedećem primjeru naredba `firewall-drop` pokrenut će se samo na lokalnom računalu ako bilo koje pravilo razine 7 i iznad bude aktivirano. Nakon 300 sekundi IP adresa će biti deblokirana.

```
<ossec_config>
  <active-response>
      <disabled>no</disabled>
      <command>firewall-drop</command>
      <location>local</location>
      <level>7</level>
      <timeout>300</timeout>
  </active-response>
 ...
</ossec_config>
```

Slijedi detaljnije objašnjenje svih mogućnosti bloka active-response:

- `disabled`: omogućava ili onemogućava reakciju na prijetnje. Ako je namješteno na yes na središnjem *Wazuh* računalu, reakcija na prijetnje bit će onemogućena za sve agente. Ako je yes samo na *Wazuh* agentu, na njemu će biti onemogućena reakcija na prijetnje.
- `command`: poveznica s imenom bloka `command`.
- `location`
    - `local`: naredba se pokreće na agentu na kojem se aktiviralo pravilo
    - `server`: naredba se pokreće na središenjem *Wazuh* računalu kada se aktivira pravilo
    - `defined-agent`: naredba se pokreće na agentu koji je definiran identifikatorom agenta (agent_id)
    - `all`: naredba se pokreće na svim agentima, bez obzira na to gdje se aktivira pravilo
- `agent_id`: identifikator agenta, koristi se s opcijom `defined-agent`

- `level`: ako se aktivira pravilo koje je na navedenoj ili većoj razini, naredba će se pokrenuti; razina može biti od 1 do 16
- `rules_group`: ako aktivira pravilo koje je u navedenoj grupi, naredba će se pokrenuti
- `rules_id`: definira je jedno ili više pravila koja se moraju aktivirati za pokretanje naredbe
- `timeout`: vrijeme u sekudama koje je potrebno da se izvrši naredba za deblokiranje.

Za neke IP adrese, iza kojih su računala ili mreže za koje se zna da ne predstavljaju prijetnju, moguće je onemogućiti reakciju na prijetnje. Te IP adrese navode se unutar bloka global datoteke ossec.conf. U sljedećem primjeru definirat će se IP adresa, podmreža te ime lokalnog i domena računala:

```
<ossec_config>
<global>
 ...
  <white_list>127.0.0.1</white_list>
  <white_list>^localhost.localdomain$</white_list>
  <white_list>192.168.0.1/24</white_list>
 </global>
</ossec_config>
```

Nakon promjene konfiguracije potrebno je ponovno pokrenuti servis *wazuh-manager*:

```
$ sudo systemctl restart wazuh-manager
```

Dnevnički zapis servisa *wazuh-manager* i *wazuh-agent* vezan za reakcije na prijetnje nalazi se u datoteci `/var/ossec/logs/active-response.log`. Iz dnevničkog zapisa može se doznati vrijeme blokiranja i deblokiranja, koja je naredba korištena,

Napomena

U nekim verzijama servisa *wazuh-manager*, skripta **`firewall-drop.sh`** ima naziv **`default-firewall-drop.sh`**. Zbog toga je potrebno ispraviti konfiguraciju bloka command i ponovno pokrenuti servis *wazuh-manager.*

IP adresa i pravilo koje je aktivirano (na kraju zapisa). Slijedi primjer:

```
Sat Oct  6 21:23:35 CEST 2018 /var/ossec/active-response/bin/firewall-drop.sh add
 - 192.168.1.222 1538853815.183786236 31508
Sun Oct  7 07:23:36 CEST 2018 /var/ossec/active-response/bin/firewall-drop.sh delete
 - 192.168.1.222 1538853815.183786236 31508
```

```
<ossec_config>
  <command>
    <name>firewall-drop</name>
    <executable>default-firewall-drop.sh</executable>
    <expect>srcip</expect>
   <timeout_allowed>yes</timeout_allowed>
 <command>
...
<ossec_config>
$ sudo  systemctl restart wazuh-manager
```

5.1.3. Integritet datoteka

Nadzor integriteta datoteka (komponenta *syscheck*) provodi se usporedbom kriptografskoga sažetka legitimne datoteke s kriptografskim sažetkom datoteke koju je potrebno provjeriti. Ako kriptografski sažetci nisu isti, datoteka je promijenjena i aktivira se alert. Također se može provjeravati promjena veličine, promjena vlasnika i grupe te promjena ovlasti nad datotekama. Uz provjeru promjena, moguće je pratiti i dodavanje i brisanje datoteka.

Wazuh agenti, po zadanome, provjeru integriteta datoteka vrše svakih 12 sati. Moguće je konfigurirati i provjeru u realnom vremenu, ali samo za cijele direktorije i sve datoteke u njemu. Središnje *Wazuh* računalo sprema kriptografske sažetke i svojstva datoteka te uspoređuje aktualne prikupljene vrijednosti s onima koje su prikupljene u prošlom nadzoru. Postoji i mogućnost slanja alerta s promijenjenim stanjem datoteke, pa administrator tako odmah može vidjeti što je promijenjeno.

Konfiguracija nadzora integriteta datoteka nalazi se u datoteci `/var/ossec/etc/ossec.conf` u bloku `syscheck`:

```
<ossec_config>

  <!-- File integrity monitoring -->
  <syscheck>
    <disabled>no</disabled>

    <!-- Frequency that syscheck is executed default every 12 hours -->
    <frequency>43200</frequency>

    <scan_on_start>yes</scan_on_start>

    <!-- Generate alert when new file detected -->
    <alert_new_files>yes</alert_new_files>

    <!-- Don't ignore files that change more than 'frequency' times -->
    <auto_ignore frequency="10" timeframe="3600">no</auto_ignore>

    <!-- Directories to check  (perform all possible verifications) -->
   <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
    <directories check_all="yes">/bin,/sbin,/boot</directories>
```

```
    <!-- Files/directories to ignore -->
    <ignore>/etc/mtab</ignore>
    <ignore>/etc/hosts.deny</ignore>
    <ignore>/etc/mail/statistics</ignore>
    <ignore>/etc/random-seed</ignore>
    <ignore>/etc/random-seed</ignore>
    <ignore>/etc/adjtime</ignore>
    <ignore>/etc/httpd/logs</ignore>
    <ignore>/etc/utmpx</ignore>
    <ignore>/etc/wtmpx</ignore>
    <ignore>/etc/cups/certs</ignore>
    <ignore>/etc/dumpdates</ignore>
    <ignore>/etc/svc/volatile</ignore>
    <ignore>/sys/kernel/security</ignore>
    <ignore>/sys/kernel/debug</ignore>

    <!-- Check the file, but never compute the diff -->
    <nodiff>/etc/ssl/private.key</nodiff>

    <skip_nfs>yes</skip_nfs>

   <!-- Remove not monitored files -->
<remove_old_diff>yes</remove_old_diff>

  <!-- Allow the system to restart Auditd after installing the plugin -->
  <restart_audit>yes</restart_audit>
</syscheck>

</ossec_config>
```

Slijedi objašnjenje važnijih zadanih opcija i njihovih mogućnosti:

- `disabled`: omogućavanje ili onemogućavanje nadzora integriteta datoteka
- `frequency`: frekvencija nadzora integriteta datoteka
- `scan_on_start`: omogućavanje ili onemogućavanje nadzora integriteta datoteka nakon pokretanja servisa *wazuh-agent* ili *wazuh-manager*
- `alert_new_files`: omogućavanje aktiviranja alerta nakon stvaranja novih datoteka
- `directories`: definiranje liste direktorija ili datoteka nad kojima se vrši nadzor
    - `check_all="yes"`: provjerava veličinu datoteke, dozvole, atribute, inode, zadnje vrijeme promjene i sve kripotgrafske sažetke (MD5, SHA1 i SHA256)
- `ignore`: definiranje liste datoteka i direktorija nad kojima se ne vrši nadzor.

Kako bismo dobili alert elektroničkom porukom, u trenutačne promjene datoteke, a zajedno sa sadržajem te datoteke, potrebno je dodati `realtime` i `report_changes` konfiguracije:

```
<directories check_all="yes" realtime="yes"
report_changes="yes">/tmp/test</directories>
```

Slijedi primjer alerta za promijenjenu datoteku:

```
** Alert 1538929714.85841: mail
- ossec,syscheck,pci_dss_11.5,gpg13_4.11,gdpr_II_5.1.f,
2018 Oct 07 18:28:34 debian->syscheck
Rule: 550 (level 7) -> 'Integrity checksum changed.'
Integrity checksum changed for: '/tmp/test/debian.conf'
Size changed from '35' to '36'
Old md5sum was: '77f3f8c87d3a62c4b57713697c9b8a07'
New md5sum is : '65175d573ece6fbc0290a9042c4b2a3f'
Old sha1sum was: '6ae492b23b78509075701057a2308ba3599a9756'
New sha1sum is : '6c041a6bd677530c1c29e33213e8d5d3ed8f867c'
Old sha256sum was:
'537741471f5594a76aa67b1b4ce41e4f32c79945cd6099e1d447283d1a4808e3'
New sha256sum is :
'1a327b490ab8950e2e019fd753e69712e8e6654df09c59c0df9444b78410de27'
What changed:
1c1
< ovo je originalni sadrzaj datoteke
---
> ovo je promijenjeni sadrzaj datoteke

Attributes:
 - Size: 36
 - Permissions: 100644
 - Date: Sun Oct  7 18:28:34 2018
 - Inode: 5254
 - User: root (0)
 - Group: root (0)
 - MD5: 65175d573ece6fbc0290a9042c4b2a3f
 - SHA1: 6c041a6bd677530c1c29e33213e8d5d3ed8f867c
 - SHA256:
1a327b490ab8950e2e019fd753e69712e8e6654df09c59c0df9444b78410de27
```

Aktivirano pravilo 550 sadrži informacije o promjeni datoteke `/tmp/test/debian.conf`. Uz nekoliko starih i novih kriptografskih sažetaka, vidi se i promijenjeni sadržaj datoteke te trenutne dozvole i atributi nad datotekom.

Nakon promjene konfiguracije potrebno je ponovno pokrenuti servis *wazuh-manager*:

```
$ sudo systemctl restart wazuh-manager
```

5.1.4. Otkrivanje zlonamjernih programa

Operacijski sustav *Linux*, mada puno rjeđe od operacijskog sustava *Windows*, može biti inficiran zloćudnim programima. Zloćudni programi (virusi, *spyware* i *adware*) onemogućuju normalan rad operacijskog sustava, prikazuju reklamne poruke, pokušavaju kompromitirati osjetljive informacije, omogućavaju neovlašteni pristup na udaljeno računalo itd.

Postoji nekoliko alata otvorenoga kôda, koji se koriste za skeniranje operacijskoga sustava *Linux*, u potrazi za zloćudnim programima. Alat za skeniranje mora imati ažurnu bazu zloćudnih programa kako bi bio efektivan i mora obuhvatiti što više virusa. Kako ni jedan alat nije savršeno rješenje za skeniranje, preporuča se koristiti nekoliko njih za što bolje rezultate.

ClamAV

ClamAV je alat koji se već spominjao na tečaju pri implementaciji sa servisima za elektroničku poštu. Uz aktivno skeniranje svakoga privitka u svrhu otkrivanja zloćudnih programa, *ClamAV* ima i ručni način rada i moguće je skenirati cijeli datotečni sustav.

ClamAV se instalira naredbom `apt-get` zajedno sa servisnim procesom *clamav-freshclam* koji služi za ažuriranje baze zloćudnih programa:

```
$ sudo apt-get install clamav clamav-freshclam
```

Slijedi objašnjenje najčešćih naredbi za skeniranje:

- `clamscan -r /`: skeniraju se svi dokumenti datotečnoga sustava i prikazuje se svaka datoteka
- `clamscan -r -i /`: skeniraju se svi dokumenti datotečnoga sustava i prikazuju se samo zlonamjerne datoteke
- `clamscan -r --move=/ /tmp/viruses`: skeniraju se svi dokumenti datotečnoga sustava i sve zlonamjerne datoteke se premještaju u /tmp/viruses
- `clamscan -r --remove /home/`: skeniraju se svi dokumenti unutar direktorija home i zlonamjerne datoteke se brišu.

Slijedi primjer skeniranja s pronađenim zlonamjernim programom:

```
$ sudo clamscan -r /tmp
/tmp/eicar.com: Eicar-Test-Signature FOUND

----------- SCAN SUMMARY -----------
Known viruses: 6675181
Engine version: 0.100.1
Scanned directories: 15
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 38.700 sec (0 m 38 s)
```

Chkrootkit

Alatom *Chkrootkit* dodatno će se provjeriti postojanje zlonamjernih programa i dodatno provjerava ima li promjena u sistemskim bibliotekama, provjerava je li mrežno sučelje u prisluškivačkom načinu rada, ima li znakova brisanja dnevničkoga zapisa lastlog itd.

U ispisu naredbe kod svake provjere prikazuju se sljedeće informacije:

- `INFECTED`: test je našao ranjivost
- `not infected`: test nije našao ranjivost
- `not tested`: test nije napravljen
- `not found`: naredba koja je potrebna da se napravi test nije dostupna
- `Vulnerable but disabled`: pronađena je zloćudna naredba, ali ne se koristi.

Nakon instalacije, pokreće se skeniranje koje ispisuje detaljan izvještaj:

```
$ sudo apt-get install chkrootkit
$ sudo chkrootkit
ROOTDIR is `/'
Checking `amd'...                                           not found
Checking `basename'...                                      not infected
Checking `biff'...                                          not found
Checking `chfn'...                                          not infected
Checking `chsh'...                                          not infected
Checking `cron'...                                          not infected
Checking `crontab'...                                       not infected
Checking `date'...                                          not infected
Checking `du'...                                            not infected
Checking `dirname'...                                       not infected
Checking `echo'...                                          not infected
Checking `egrep'...                                         not infected
Checking `env'...                                           not infected
Checking `find'...                                          not infected
Checking `fingerd'...                                       not found
Checking `gpm'...                                           not found
Checking `grep'...                                          not infected
Checking `hdparm'...                                        not infected
Checking `su'...                                            not infected
Checking `ifconfig'...                                      not infected
Checking `inetd'...                                         not infected
Checking `inetdconf'...                                     not found
Checking `identd'...                                        not found
Checking `init'...                                          not infected
Checking `killall'...                                       not infected
Checking `ldsopreload'...                                   not infected
Checking `login'...                                         not infected
Checking `ls'...                                            not infected
Checking `lsof'...                                          not infected
Checking `mail'...                                          not infected
Checking `mingetty'...                                      not found
Checking `netstat'...                                       not infected
Checking `named'...                                         not found
Checking `passwd'...                                        not infected
Checking `pidof'...                                         not infected
Checking `pop2'...                                          not found
Checking `pop3'...                                          not found
Checking `ps'...                                            not infected
Checking `pstree'...                                        not infected
```

```
Checking `rpcinfo'...                                       not found
Checking `rlogind'...                                       not found
Checking `rshd'...                                          not found
Checking `slogin'...                                        not infected
Checking `sendmail'...                                      not infected
Checking `sshd'...                                          not infected
Checking `syslogd'...                                       not tested
Checking `tar'...                                           not infected
Checking `tcpd'...                                          not infected
Checking `tcpdump'...                                       not infected
Checking `top'...                                           not infected
Checking `telnetd'...                                       not found
Checking `timed'...                                         not found
Checking `traceroute'...                                    not infected
Checking `vdir'...                                          not infected
Checking `w'...                                             not infected
Checking `write'...                                         not infected
Checking `aliens'...                                        no suspect files
Searching for sniffer's logs, it may take a while...        nothing found
Searching for rootkit HiDrootkit's default files...         nothing found
Searching for rootkit t0rn's default files...               nothing found
Searching for t0rn's v8 defaults...                         nothing found
Searching for rootkit Lion's default files...               nothing found
Searching for rootkit RSHA's default files...               nothing found
Searching for rootkit RH-Sharpe's default files...          nothing found
Searching for Ambient's rootkit (ark) default files and dirs... nothing found
Searching for suspicious files and dirs, it may take a while... The following
suspicious files and directories were found:
/usr/lib/jvm/.java-1.8.0-openjdk-amd64.jinfo

Searching for LPD Worm files and dirs...                    nothing found
Searching for Ramen Worm files and dirs...                  nothing found
Searching for Maniac files and dirs...                      nothing found
Searching for RK17 files and dirs...                        nothing found
Searching for Ducoci rootkit...                             nothing found
Searching for Adore Worm...                                 nothing found
Searching for ShitC Worm...                                 nothing found
Searching for Omega Worm...                                 nothing found
Searching for Sadmind/IIS Worm...                           nothing found
Searching for MonKit...                                     nothing found
Searching for Showtee...                                    nothing found
Searching for OpticKit...                                   nothing found
Searching for T.R.K...                                      nothing found
Searching for Mithra...                                     nothing found
Searching for LOC rootkit...                                nothing found
Searching for Romanian rootkit...                           nothing found
Searching for Suckit rootkit...                             nothing found
Searching for Volc rootkit...                               nothing found
Searching for Gold2 rootkit...                              nothing found
Searching for TC2 Worm default files and dirs...            nothing found
Searching for Anonoying rootkit default files and dirs...   nothing found
Searching for ZK rootkit default files and dirs...          nothing found
Searching for ShKit rootkit default files and dirs...       nothing found
Searching for AjaKit rootkit default files and dirs...      nothing found
```

```
Searching for zaRwT rootkit default files and dirs...       nothing found
Searching for Madalin rootkit default files...              nothing found
Searching for Fu rootkit default files...                   nothing found
Searching for ESRK rootkit default files...                 nothing found
Searching for rootedoor...                                  nothing found
Searching for ENYELKM rootkit default files...              nothing found
Searching for common ssh-scanners default files...          nothing found
Searching for Linux/Ebury - Operation Windigo ssh...        nothing found
Searching for 64-bit Linux Rootkit ...                      nothing found
Searching for 64-bit Linux Rootkit modules...               nothing found
Searching for suspect PHP files...                          nothing found
Searching for anomalies in shell history files...           nothing found
Checking `asp'...                                           not infected
Checking `bindshell'...                                     not infected
Checking `lkm'...                                           chkproc: nothing
detected
chkdirs: nothing detected
Checking `rexedcs'...                                       not found
Checking `sniffer'...                                       lo: not promisc and
no packet sniffer sockets
enp0s3: not promisc and no packet sniffer sockets
enp0s8: PACKET SNIFFER(/sbin/dhclient[461])
Checking `w55808'...                                        not infected
Checking `wted'...                                          chkwtmp: nothing
deleted
Checking `scalper'...                                       not infected
Checking `slapper'...                                       not infected
Checking `z2'...                                            chklastlog: nothing
deleted
Checking `chkutmp'...                                        The tty of the
following user process(es) were not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! Debian-+     1890 tty1   /usr/lib/xorg/Xorg vt1 -displayfd 3 -auth
/run/user/116/gdm/
Xauthority -background none -noreset -keeptty -verbose 3
! Debian-+     1888 tty1   /usr/lib/gdm3/gdm-x-session gnome-session --autostart
/
usr/share/gdm/greeter/autostart
! Debian-+     1919 tty1   /usr/lib/gnome-session/gnome-session-binary --
autostart /
usr/share/gdm/greeter/autostart
! Debian-+     1984 tty1   /usr/lib/gnome-settings-daemon/gnome-settings-daemon
! Debian-+     1939 tty1   /usr/bin/gnome-shell
chkutmp: nothing deleted
Checking `OSX_RSPLUG'...                                    not infected
```

5.1.5. Zanimljivi izvori

Poveznice:

- https://documentation.wazuh.com/current/index.html
- https://www.comparitech.com/net-admin/network-intrusion-detection-tools/
- https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-01-287.pdf

5.1.6. Vježba 12: Nadzor sistema i servisa: Podešavanje alata Wazuh i osiguravanje konfiguracija

1. Prije početka rada odaberite sliku stanja virtualnoga računala **slika_jedan** za početak vježbe.
2. Prijavite se na računalo kao korisnik **linux1**. U GUI-ju pokrenite **Terminal** (*Activities* → **Terminal**). Izvršite **su -** naredbu da postanete administrator (lozinka: linux1).
3. Za instalaciju servisa wazuh-manager potrebno je dodati repozitorij za Wazuh pakete.

```
# apt-get update
# apt-get install curl apt-transport-https lsb-release
# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-
default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --
import && chmod 644 /usr/share/keyrings/wazuh.gpg
# echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg]
https://packages.wazuh.com/4.x/apt/ stable main" | tee -a
/etc/apt/sources.list.d/wazuh.list
# apt-get update
```

4. Naredbom **apt-get** instalirajte *wazuh-manager* i provjerite status servisa:

```
# apt-get install wazuh-manager
# systemctl status wazuh-manager
```

5. Omogućite slanje elektroničke pošte na root@localhost i podesite level za slanje elektroničke pošte i bilježenje u dnevnički zapis:

```
# vim /var/ossec/etc/ossec.conf
<global>
<jsonout_output>no</jsonout_output>
<email_notification>yes</email_notification>
<smtp_server>localhost</smtp_server>
<email_from>root@localhost</email_from>
<email_to>root@localhost</email_to>
<email_maxperhour>300</email_maxperhour>
...
</global>
<alerts>
```

```
<log_alert_level>2</log_alert_level>
<email_alert_level>2</email_alert_level>
</alerts>
```

6. Da bi se primijenile konfiguracije, ponovno pokrenite servis *wazuh-manager*.

```
# systemctl restart wazuh-manager
```

7. Pregledajte alertove u datoteci **/var/ossec/logs/alerts/alerts.log**. Koje se preporuke za osiguravanje konfiguracija prikazuju?

_____

_____

8. Primjenite konfiguraciju za sljedeću preporuku 'CIS Benchmark for Debian/Linux 10: Ensure SSH root login is disabled'.

```
# vim /etc/ssh/sshd_config
PermitRootLogin no

# systemctl restart sshd
```

9. Kako bi servis *wazuh-manager* ponovno provjerio konfiguracije, potrebno ga je ponovno pokrenuti:

```
# systemctl restart wazuh-manager
```

10. Pregledajte alertove u datoteci **/var/ossec/logs/alerts/alerts.log**. Koje se sada preporuke prikazuju?

_____

_____

11. Koji još alertovi se prikazuju? Zašto su oni korisni?

_____

_____

12. Promijenite *level* na pravilu 502 da ne prikazuje aletrove. U datoteku /var/ossec/etc/rules/local_rules.xml upišite sljedeću konfiguraciju:

```
<group name="ossec,">
  <rule id="502" level="0" overwrite="yes">
    <if_sid>500</if_sid>
```

```
    <match>Ossec started</match>
    <description>Ossec server started.</description>
    <group>pci_dss_10.6.1,gpg13_10.1,gdpr_IV_35.7.d,</group>
  </rule>
</group>
```

13. Objasnite svaku liniju prethodne konfiguracije.

14. Pokrenite novi **Terminal** (*Activities* → **Terminal**). Naredbom **tail** pratite upis u datoteku **/var/ossec/logs/alerts/alerts.log**, dok u drugom terminalu ponovno pokrećete servis *wazuh-manager*:

```
# tail –f /var/ossec/logs/alerts/alerts.log
# systemctl restart wazuh-manager
```

15. Prikazuju li se alertovi za pokretanje Wazuh agenta?

16. Da li se prikazuju alerti za pravilo 1002? Ako je odgovor da, napravite novi *rule id* za te alertove.

5.1.7. Vježba 13: Nadzor sistema i servisa: Podešavanje reakcije na prijetnje u servisu Wazuh

1. Naredbom **tail** pratite upis u datoteku **var/ossec/logs/alerts/alerts.log**

```
# tail -f /var/ossec/logs/alerts/alerts.log
```

2. Koristeći program **putty** u *Windows* okruženju pokušajte se spojiti na IP adresu kao nepostojeći korisnik marko.

```
marko@192.168.2.1
```

3. Koji se alert prikazuje za pokušaj spajanja s nepostojećim korisnikom? Što se može iz njega saznati?

4. Za pokušaj spajanja s nepostojećim korisnikom konfigurirajte reakciju na prijetnje koja će blokirati IP adresu napadača.

   Dodajte sljedeću konfiguraciju u datoteku **ossec.conf** umjesto zakomentirane konfiguracije *active-responsea*.

```
<active-response>
<disabled>no</disabled>
<command>firewall-drop</command>
<location>local</location>
<rules_id>5710</rules_id>
<timeout>300</timeout>
</active-response>
```

5. Objasnite svaku liniju prethodne konfiguracije.

6. U nekim verzijama servisa *wazuh-manager*, skripta **firewall-drop.sh** ima naziv **default-firewall-drop.sh**. Provjerite naziv skripte u direktoriju **/var/ossec/active-response/bin/** i ispravite konfiguraciju bloka **command** ako je potrebno:

```
<ossec_config>
<command>
<name>firewall-drop</name>
<executable>default-firewall-drop.sh</executable>
<expect>srcip</expect>
<timeout_allowed>yes</timeout_allowed>
```

```
</command>
...
<ossec_config>
# systemctl restart wazuh-manager
```

7. Naredbom tail pratite upis u datoteku **/var/ossec/logs/alerts/alerts.log**.

```
# tail –f /var/ossec/logs/alerts/alerts.log
```

8. Koristeći program **putty** u *Windows* okruženju pokušajte se spojiti na IP adresu kao nepostojeći korisnik marko.

```
marko@192.168.2.1
```

9. Koje se informacije mogu saznati iz zadnjeg zapisa u datoteci **/var/ossec/logs/active-responses.log**?

_____

_____

10. U kojim se lancima servisa *iptables* nalazi blokirana IP adresa?

_____

_____

11. Koristeći naredbu *iptables* uklonite IP adresu iz vatrozida:

```
# iptables -D INPUT -s 192.168.2.1 -j DROP
# iptables -D FORWARD -s 192.168.2.1 -j DROP
```

12. Provjerite uklanjanje IP adrese iz vatrozida naredbom **iptables – nL**.
13. Dodajte konfiguraciju za *whitelist* IP adrese u datoteku **ossec.conf** i ponovno pokrenite servis *wazuh-manager*:

```
<ossec_config>
<global>
<white_list>192.168.2.1</white_list>
</global>
</ossec_config>
# systemctl restart wazuh-manager
```

14. Koristeći program **putty** u *Windows* okruženju pokušajte se spojiti na IP adresu kao nepostojeći korisnik marko.

    ```
    marko@192.168.2.1
    ```

15. Je li IP adresa blokirana? Na koje se sve načine može provjeriti je li IP adresa blokirana ili ne?

    _____

    _____

5.1.8. Vježba 14: Nadzor sistema i servisa: Stvaranje novih pravila

U prethodnoj vježbi, svaki korisnik koji se pokuša spojiti s nepostojećim korisničkim imenom, bit će blokiran na 300 sekundi. Ako se legitimni korisnici slučajno pokušaju spojiti s krivim korisničkim imenom, nakon kratkog roka od 300 sekundi, moći će pokušati opet. Postoji puno pokušaja, gdje se napadači žele spojiti s čestim korisničkim imenima, kao što su admin, root, mysql, www-data itd. Za te pokušaje ćemo napraviti novo pravilo koje će zabraniti promet po IP adresi na tjedan dana.

1. Naredbom **tail** pratite upis u datoteku **/var/log/auth.log**:

    ```
    # tail –f /var/log/auth.log
    ```

2. Koristeći program **putty** u *Windows* okruženju pokušajte se spojiti na IP adresu kao nepostojeći korisnik admin.

    ```
    admin@192.168.2.1
    ```

3. Iz dnevničkog zapisa kopirajte prvi zapis koji se pojavi nakon pokušaja spajanja. Na primjer:

```
Oct 30 10:20:58 debian sshd[30706]: Invalid user admin from
192.168.2.1 port 65029
```

4. Za analizu dnevničkoga zapisa koristite naredbu **/var/ossec/bin/wazuh-logtest** i zalijepite kopirani zapis:

```
# /var/ossec/bin/wazuh-logtest
2018/10/30 10:21:42 wazuh-testrule: INFO: Started (pid: 30714).
wazuh-testrule: Type one log per line.

Oct 30 10:20:58 debian sshd[30706]: Invalid user admin from
192.168.2.1 port 65029
```

5. Koje polje se može iskoristiti za stvaranje pravila opisanog u uvodu?

_____

6. U datoteku **/var/ossec/etc/rules/local_rules.xml** upišite sljedeće pravilo:

```
<group name="local,sshd,attack,">
  <rule id="100002" level="12">
  <if_sid>5710</if_sid>
  <user>^root$|^admin$|^mysql$|^backup$|^test$|^ postgres$|^ftp$|^www-
data$|^pi$|^guest$|^jenkins$|^git$|^server$|^team$|^dev$|^oracle$|^user$
|^student$|^web$|^us er1$|^ubuntu$</user>
  <program_name>sshd</program_name>
  <group>attack,</group>
  <description>Ssh connect attempt with general user names</description>
  </rule>
</group>
```

7. Za analizu dnevničkoga zapisa koristite naredbu **/var/ossec/bin/wazuh-logtest** i zalijepite zapis. Je li se promijenilo pravilo?

_____

8. Za pokušaj spajanja s čestim korisničkim imenima konfigurirajte reakciju na prijetnje koja će blokirati IP adresu napadača.

```
<active-response>
<disabled>no</disabled>
<command>firewall-drop</command>
```

```
<location>local</location>
<rules_id>100002</rules_id>
<timeout>604800</timeout>
</active-response>
```

9. U nekim verzijama servisa *wazuh-manager*, skripta **firewall-drop.sh** ima naziv **default-firewall-drop.sh**. Provjerite naziv skripte u direktoriju **/var/ossec/active-response/bin/** i ispravite konfiguraciju bloka **command** ako je potrebno:

```
<ossec_config>
<command>
<name>firewall-drop</name>
<executable>default-firewall-drop.sh</executable>
<expect>srcip</expect>
<timeout_allowed>yes</timeout_allowed>
</command>
...
<ossec_config>

# systemctl restart wazuh-manager
```

10. Ako je dodana, zakomentirajte (ili obrišite) konfiguraciju za *whitelist* IP adrese u datoteku **ossec.conf** i ponovno pokrenite servis *wazuh-manage*r:

```
# vim ossec.conf
<ossec_config>
<global>
<!-- <white_list>192.168.2.1</white_list> -->

</global>
</ossec_config>

# systemctl restart wazuh-manager
```

11. Naredbom tail pratite upis u datoteku **/var/ossec/logs/alerts/alerts.log**:

```
# tail -f /var/ossec/logs/alerts/alerts.log
```

12. Koristeći program **putty** u *Windows* okruženju pokušajte se spojiti na IP adresu kao nepostojeći korisnik **admin**.

```
admin@192.168.2.1
```

13. Je li IP adresa blokirana?

5.2. Sigurnosne provjere

5.2.1. Otvoreni portovi

Skeniranje otvorenih portova je proces pokušaja spajanja na jedan ili više portova u svrhu provjere otvorenoga porta i servisa koji ga koristi. Svaki otvoreni port, koji nije dio standardnoga rada računala, može biti dokaz provaljivanja u sustav. Potrebno je vršiti periodičke provjere otvorenih portova.

Dva su načina provjere otvorenih portova: lokalno ili preko mreže. Lokalna provjera, naredbama `lsof -i` ili `netstat -plunt`, nije pouzdana jer naredbe provjeravaju je li port otvoren na računalu, a ne je li dostupan preko mreže. Napadač može zamijeniti alat za skeniranje otvorenih portova i tako onemogućiti otkrivanje stvarnoga stanja otvorenih portova.

Wazuh, ako je instaliran na računalu, ima zadanu konfiguraciju da svakih 12 sati prati stanje portova. Slijedi primjer alerta o otvorenosti portova gdje je zapisano trenutačno i prijašnje stanje:

```
** Alert 1539078626.73304: -
ossec,pci_dss_10.2.7,pci_dss_10.6.1,gpg13_10.1,gdpr_IV_35.7.d,
2018 Oct 09 11:50:26 debian->netstat listening ports
Rule: 533 (level 7) -> 'Listened ports status (netstat) changed (new port opened
or closed).'

ossec: output: 'netstat listening ports':
tcp6 :::21 :::* 624/vsftpd
tcp 0.0.0.0:22 0.0.0.0:* 658/sshd
tcp6 :::22 :::* 658/sshd
tcp 0.0.0.0:25 0.0.0.0:* 1272/master
tcp6 :::25 :::* 1272/master
udp 0.0.0.0:68 0.0.0.0:* 461/dhclient
tcp6 :::80 :::* 708/apache2
udp 0.0.0.0:1514 0.0.0.0:* 534/ossec-remoted
udp 0.0.0.0:1900 0.0.0.0:* 649/minissdpd
udp 0.0.0.0:5353 0.0.0.0:* 1999/avahi-daemon
udp6 :::5353 :::* 1999/avahi-daemon
tcp 127.0.0.1:10024 0.0.0.0:* 1281/amavisd-new
tcp6 ::1:10024 :::* 1281/amavisd-new
tcp 127.0.0.1:10025 0.0.0.0:* 1272/master
udp6 :::54442 :::* 1999/avahi-daemon
udp 0.0.0.0:55120 0.0.0.0:* 1999/avahi-daemon

Previous output:
ossec: output: 'netstat listening ports':
tcp6 :::21 :::* 624/vsftpd
tcp 0.0.0.0:22 0.0.0.0:* 658/sshd
tcp6 :::22 :::* 658/sshd
tcp 0.0.0.0:25 0.0.0.0:* 1272/master
tcp6 :::25 :::* 1272/master
udp 0.0.0.0:68 0.0.0.0:* 461/dhclient
tcp6 :::80 :::* 708/apache2
udp 0.0.0.0:1514 0.0.0.0:* 534/ossec-remoted
```

```
udp 0.0.0.0:1900 0.0.0.0:* 649/minissdpd
udp 0.0.0.0:5353 0.0.0.0:* 1999/avahi-daemon
udp6 :::5353 :::* 1999/avahi-daemon
tcp 127.0.0.1:10024 0.0.0.0:* 1281/amavisd-new
tcp6 ::1:10024 :::* 1281/amavisd-new
tcp 127.0.0.1:10025 0.0.0.0:* 1272/master
udp 0.0.0.0:50905 0.0.0.0:* 231/systemd-timesyn
udp6 :::54442 :::* 1999/avahi-daemon
udp 0.0.0.0:55120 0.0.0.0:* 1999/avahi-daemon
```

Za pouzdaniju provjeru otvorenih portova preko mreže koristi se alat nmap. *Network Mapper*, nmap, je alat za skeniranje mreže i sigurnosnu reviziju, a može skenirati pojedinačna mrežna sučelja ili cijele mreže. Koristi se IP-paketima za pretraživanje mreže, pretraživanje lociranih uređaja, identificiranje aplikacija na portovima, prikupljanje detalja o operacijskom sustavu, vatrozidu i slično. Primjer skeniranja otvorenih portova naredbom `nmap`:

```
$ sudo nmap -sT -O localhost

Starting Nmap 7.40 ( https://nmap.org ) at 2018-10-09 14:04 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00077s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
10024/tcp open  unknown
10025/tcp open  unknown
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.8 - 4.6
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.46 seconds
```

5.2.2. Usklađivanje sa sigurnosnim standardima

Nakon instalacije i osiguravanja konfiguracije operacijskoga sustava i servisa, preporučeno je provjeriti odgovaraju li sve konfiguracije sigurnosnim standardima. Konfiguracije mogu imati sigurnosne probleme iz nekoliko razloga:

- zadane konfiguracije koje se primjenjuju tijekom instalacije operacijskoga sustava ili servisa nisu osigurane
- prilikom nadogradnje paketa konfiguracije servisa se mogu promijeniti tako da više ne budu po sigurnosnim standardima

- primijenjena "sigurna" konfiguracija je zastarjela i više se ne smatra sigurnom zbog otkrivenosti ranjivosti
- nikad nije ni primijenjena sigurnosno standardna konfiguracija.

Nekoliko je organizacija koje objavljuju sigurnosne standarde (*OpenSCAP*, CIS *Benchmarks*), tj. preporuke konfiguracija prema kojima se uspoređuju konfiguracije servisa ili operacijskoga sustava. Za implementaciju sigurnosnih standarda potrebno je instalirati alate koji provjeravaju stanje na računalu i obavještavaju o mogućim promjenama. Jedan od tih alata je *Wazuh*, kod kojeg je prema zadanim postavkama uključena provjera po CIS *Benchmarks* sigurnosnim standardima za konfiguraciju servisa *ssh*.

Ako *Wazuh* pronađe konfiguraciju koja nije po sigurnosnom standardu, generira se alert, koji se može vidjeti u dnevničkom zapisu u datoteci `/var/ossec/logs/alerts/alerts.log` ili poslati elektroničkom poštom. Primjer takvih alertova je:

```
** Alert 1539183408.64662: - ossec,rootcheck,gdpr_IV_30.1.g,
2018 Oct 10 16:56:48 debian->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: SSH Hardening - 3: Root can log in. File: /etc/ssh/sshd_config.
Reference: 3 .
title: SSH Hardening - 3: Root can log in.
file: /etc/ssh/sshd_config

** Alert 1539183408.64971: - ossec,rootcheck,gdpr_IV_30.1.g,
2018 Oct 10 16:56:48 debian->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: SSH Hardening - 4: No Public Key authentication {PCI_DSS: 2.2.4}.
File: /etc/ssh/sshd_config. Reference: 4 .
title: SSH Hardening - 4: No Public Key authentication
file: /etc/ssh/sshd_config

** Alert 1539183408.65322: - ossec,rootcheck,gdpr_IV_30.1.g,
2018 Oct 10 16:56:48 debian->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: SSH Hardening - 5: Password Authentication {PCI_DSS: 2.2.4}.
File: /etc/ssh/sshd_config. Reference: 5 .
title: SSH Hardening - 5: Password Authentication
file: /etc/ssh/sshd_config

** Alert 1539183408.65663: - ossec,rootcheck,gdpr_IV_30.1.g,
2018 Oct 10 16:56:48 debian->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: SSH Hardening - 6: Empty passwords allowed {PCI_DSS: 2.2.4}.
File: /etc/ssh/sshd_config. Reference: 6 .
title: SSH Hardening - 6: Empty passwords allowed
file: /etc/ssh/sshd_config

** Alert 1539183408.66004: - ossec,rootcheck,gdpr_IV_30.1.g,
2018 Oct 10 16:56:48 debian->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
```

```
System Audit: SSH Hardening - 7: Rhost or shost used for authentication
{PCI_DSS: 2.2.4}.
File: /etc/ssh/sshd_config. Reference: 7 .
title: SSH Hardening - 7: Rhost or shost used for authentication
file: /etc/ssh/sshd_config

** Alert 1539183408.66375: - ossec,rootcheck,gdpr_IV_30.1.g,
2018 Oct 10 16:56:48 debian->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: SSH Hardening - 8: Wrong Grace Time {PCI_DSS: 2.2.4}.
File: /etc/ssh/sshd_config. Reference: 8 .
title: SSH Hardening - 8: Wrong Grace Time
file: /etc/ssh/sshd_config

** Alert 1539183408.66702: - ossec,rootcheck,gdpr_IV_30.1.g,
2018 Oct 10 16:56:48 debian->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: SSH Hardening - 9: Wrong Maximum number of authentication attempts
{PCI_DSS: 2.2.4}. File: /etc/ssh/sshd_config. Reference: 9 .
title: SSH Hardening - 9: Wrong Maximum number of authentication attempts
file: /etc/ssh/sshd_config
```

U prethodnom primjeru može se vidjeti da su sve preporuke vezane za konfiguraciju servisa *sshd*, tj. za konfiguracijsku datoteku `/etc/ssh/sshd_config` i u svakom alertu iz naslova (*title*) može se doznati o kakvoj preporuci se radi.

Wazuh ima još ima nekoliko sigurnosnih provjera i sve se nalaze u direktoriju `/var/ossec/etc/rootcheck/`, a neke od njih su vezane za operacijski sustav *Debian* i servise na njemu. Za omogućavanje pojedinih provjera potrebno je u `ossec.conf` dodati punu putanju:

```
$ sudo vim /var/ossec/etc/ossec.conf

<ossec_config>

  ...

      <!-- Policy monitoring -->
            <rootcheck>
                <disabled>no</disabled>
<!—Frequency that rootcheck is executed - every 12 hours -->

    <frequency>43200</frequency>
    <system_audit>/var/ossec/etc/rootcheck/system_audit_ssh.txt</system_audit>

<system_audit>/var/ossec/etc/rootcheck/cis_debian_linux_rcl.txt</system_audit>
    <system_audit>/var/ossec/etc/rootcheck/cis_apache2224_rcl.txt</system_audit>
    <system_audit>/var/ossec/etc/rootcheck/cis_mysql5-
6_community_rcl.txt</system_audit>
    ...

  </rootcheck>
</ossec_config>
```

U `system_audit` dodane su provjere za operacijski sustav *Debian*, te *web*-servis i servis *mysql*.

Nakon ponovnog pokretanja servisa *wazuh-manager* ili *wazuh-agent*, *system_audit* vršit će provjere i za dodane sigurnosne standarde. Slijedi primjer alertova za *web*-servis i servis *mysql*, te operacijski sustav *Debian*:

```
** Alert 1539188927.148607: - ossec,rootcheck,gdpr_IV_30.1.g,
2018 Oct 10 18:28:47 debian->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: CIS - Apache Configuration - 9.1: Set TimeOut to 10 or less.
File: /etc/apache2/apache2.conf. Reference:
https://workbench.cisecurity.org/benchmarks/307,
https://workbench.cisecurity.org/benchmarks/308 .
title: CIS - Apache Configuration - 9.1: Set TimeOut to 10 or less.
file: /etc/apache2/apache2.conf

** Alert 1539188927.137829: - ossec,rootcheck,gdpr_IV_30.1.g,
2018 Oct 10 18:28:47 debian->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: CIS - Debian Linux - 1.4 - Robust partition scheme - /tmp is not
on its own partition {CIS: 1.4 Debian Linux}. File: /etc/fstab. Reference:
https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf .
title: CIS - Debian Linux - 1.4 - Robust partition scheme -
/tmp is not on its own partition
file: /etc/fstab

** Alert 1539188964.153842: - ossec,rootcheck,gdpr_IV_30.1.g,
2018 Oct 10 18:29:24 debian->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: CIS - MySQL Configuration - 6.1: log-error is not set in my.cnf.
File: /etc/mysql/my.cnf. Reference:
https://workbench.cisecurity.org/files/1310/download .
title: CIS - MySQL Configuration - 6.1: log-error is not set in my.cnf.
file: /etc/mysql/my.cnf
```

Alat *Lynis*

Alat *Lynis* je alternativa alatu *Wazuh* ako je potrebna povremena provjera sigurnosnih standarda za konfiguracije. Izvršava stotine testova i provjera konfiguracija prema *OpenSCAP* i CIS *Benchmarks* standardima, a skeniranje se prilagođava operacijskom sustavu i servisima koji su instalirani na njemu. Na primjer ako pronađe instalirani *web*-servis, bit će pokrenute provjere koje su vezane za taj servis. Provjere koje je provode nalaze se na elektroničkoj poveznici: https://cisofy.com/lynis/controls/.

Prije instalacije alata *Lynis* potrebno je dodati javni ključ i repozitorij paketa:

```
$ wget -O - https://packages.cisofy.com/keys/cisofy-software-public.key |
apt-key add -
$ sudo apt-get install apt-transport-https
```

```
$ sudo echo "deb https://packages.cisofy.com/community/lynis/deb/ stable
main" | tee /etc/apt/sources.list.d/cisofy-lynis.list
$ sudo apt-get update
$ sudo apt-get install lynis
$ sudo lynis show version
```

Za pokretanje provjera koristi se naredba `lynis audit system –quick`, a izvještaj će se ispisati na ekranu. U odjeljku *Warnings* bitna su upozorenja na koje je potrebno odmah obratiti pozornost, a u odjeljku *Suggestions* su dodane preporuke za osiguravanje raznih konfiguracija:

```
$ sudo lynis audit system --quick

[ Lynis 2.6.9 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           2.6.9
  Operating system:          Linux
  Operating system name:     Debian
  Operating system version:  9.5
  Kernel version:            4.9.0
  Hardware platform:         x86_64
  Hostname:                  debian
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /usr/share/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                                  [ NO UPDATE ]
```

```
[+] System Tools
------------------------------------
  - Scanning available tools...
  - Checking system binaries...

[+] Plugins (phase 1)
------------------------------------
Note: plugins have more extensive tests and may take several minutes to complete

  - Plugins enabled                                           [ NONE ]

[+] Boot and services
------------------------------------
  - Service Manager                                           [ systemd ]
  - Checking UEFI boot                                        [ DISABLED ]
  - Checking presence GRUB2                                   [ FOUND ]
    - Checking for password protection                        [ WARNING ]
  - Check running services (systemctl)                        [ DONE ]
        Result: found 29 running services
  - Check enabled services at boot (systemctl)                [ DONE ]
        Result: found 34 enabled services
  - Check startup files (permissions)                         [ OK ]

[+] Kernel
------------------------------------
  - Checking default run level                                [ RUNLEVEL 5 ]
  - Checking CPU support (NX/PAE)
    CPU support: PAE and/or NoeXecute supported               [ FOUND ]
  - Checking kernel version and release                       [ DONE ]
  - Checking kernel type                                      [ DONE ]
  - Checking loaded kernel modules                            [ DONE ]
      Found 61 active modules
  - Checking Linux kernel configuration file                  [ FOUND ]
  - Checking default I/O kernel scheduler                     [ FOUND ]
  - Checking for available kernel update                      [ OK ]
  - Checking core dumps configuration                         [ DISABLED ]
    - Checking setuid core dumps configuration                [ DEFAULT ]
  - Check if reboot is needed                                 [ NO ]

[+] Memory and Processes
------------------------------------
  - Checking /proc/meminfo                                    [ FOUND ]
  - Searching for dead/zombie processes                       [ OK ]
  - Searching for IO waiting processes                        [ OK ]

[+] Users, Groups and Authentication
------------------------------------
  - Administrator accounts                                    [ OK ]
  - Unique UIDs                                               [ OK ]
  - Consistency of group files (grpck)                        [ OK ]
  - Unique group IDs                                          [ OK ]
  - Unique group names                                        [ OK ]
  - Password file consistency                                 [ OK ]
  - Query system users (non daemons)                          [ DONE ]
```

```
  - NIS+ authentication support                                [ NOT ENABLED ]
  - NIS authentication support                                 [ NOT ENABLED ]
  - sudoers file                                               [ NOT FOUND ]
  - PAM password strength tools                                [ SUGGESTION ]
  - PAM configuration files (pam.conf)                         [ FOUND ]
  - PAM configuration files (pam.d)                            [ FOUND ]
  - PAM modules                                                [ FOUND ]
  - LDAP module in PAM                                         [ NOT FOUND ]
  - Accounts without expire date                               [ OK ]
  - Accounts without password                                  [ OK ]
  - Checking user password aging (minimum)                     [ DISABLED ]
  - User password aging (maximum)                              [ DISABLED ]
  - Checking expired passwords                                 [ OK ]
  - Checking Linux single user mode authentication             [ OK ]
  - Determining default umask
    - umask (/etc/profile)                                     [ NOT FOUND ]
    - umask (/etc/login.defs)                                  [ SUGGESTION ]
  - LDAP authentication support                                [ NOT ENABLED ]
  - Logging failed login attempts                              [ ENABLED ]

[+] Shells
------------------------------------
  - Checking shells from /etc/shells
    Result: found 4 shells (valid shells: 4).
    - Session timeout settings/tools                           [ NONE ]
  - Checking default umask values
    - Checking default umask in /etc/bash.bashrc               [ NONE ]
    - Checking default umask in /etc/profile                   [ NONE ]

[+] File systems
------------------------------------
  - Checking mount points
    - Checking /home mount point                               [ SUGGESTION ]
    - Checking /tmp mount point                                [ SUGGESTION ]
    - Checking /var mount point                                [ SUGGESTION ]
  - Query swap partitions (fstab)                              [ OK ]
  - Testing swap partitions                                    [ OK ]
  - Testing /proc mount (hidepid)                              [ SUGGESTION ]
  - Checking for old files in /tmp                             [ OK ]
  - Checking /tmp sticky bit                                   [ OK ]
  - Checking /var/tmp sticky bit                               [ OK ]
  - ACL support root file system                               [ ENABLED ]
  - Mount options of /                                         [ NON DEFAULT ]
  - Checking Locate database                                   [ FOUND ]
  - Disable kernel support of some filesystems
    - Discovered kernel modules: freevxfs hfs hfsplus jffs2 squashfs udf

[+] USB Devices
------------------------------------
  - Checking usb-storage driver (modprobe config)              [ NOT DISABLED ]
  - Checking USB devices authorization                         [ ENABLED ]
  - Checking USBGuard                                          [ NOT FOUND ]

[+] Storage
```

```
------------------------------------
  - Checking firewire ohci driver (modprobe config)           [ NOT DISABLED ]

[+] NFS
------------------------------------
  - Check running NFS daemon                                  [ NOT FOUND ]

[+] Name services
------------------------------------
  - Searching DNS domain name                                 [ UNKNOWN ]
  - Checking /etc/hosts
    - Checking /etc/hosts (duplicates)                        [ OK ]
    - Checking /etc/hosts (hostname)                          [ OK ]
    - Checking /etc/hosts (localhost)                         [ OK ]
    - Checking /etc/hosts (localhost to IP)                   [ OK ]

[+] Ports and packages
------------------------------------
  - Searching package managers
    - Searching dpkg package manager                          [ FOUND ]
      - Querying package manager
    - Query unpurged packages                                 [ NONE ]
  - Checking security repository in sources.list file         [ OK ]
  - Checking vulnerable packages (apt-get only)               [ DONE ]
  - Checking package audit tool                               [ INSTALLED ]
    Found: apt-get

[+] Networking
------------------------------------
  - Checking IPv6 configuration                               [ ENABLED ]
      Configuration method                                    [ AUTO ]
      IPv6 only                                               [ NO ]
  - Checking configured nameservers
    - Testing nameservers
      Nameserver: 161.53.252.41                               [ SKIPPED ]
      Nameserver: 161.53.252.43                               [ SKIPPED ]
    - Minimal of 2 responsive nameservers                     [ SKIPPED ]
  - Checking default gateway                                  [ DONE ]
  - Getting listening ports (TCP/UDP)                         [ DONE ]
      * Found 17 ports
  - Checking promiscuous interfaces                           [ OK ]
  - Checking waiting connections                              [ OK ]
  - Checking status DHCP client                               [ RUNNING ]
  - Checking for ARP monitoring software                      [ NOT FOUND ]

[+] Printers and Spools
------------------------------------
  - Checking cups daemon                                      [ NOT FOUND ]
  - Checking lp daemon                                        [ NOT RUNNING ]

[+] Software: e-mail and messaging
------------------------------------
  - Postfix status                                            [ RUNNING ]
    - Postfix configuration                                   [ FOUND ]
```

```
      - Postfix banner                                          [ WARNING ]

[+] Software: firewalls
------------------------------------
  - Checking iptables kernel module                             [ FOUND ]
    - Checking iptables policies of chains                      [ FOUND ]
    - Checking for empty ruleset                                [ WARNING ]
    - Checking for unused rules                                 [ OK ]
  - Checking host based firewall                                [ ACTIVE ]

[+] Software: webserver
------------------------------------
  - Checking Apache (binary /usr/sbin/apache2)                  [ FOUND ]
      Info: No virtual hosts found
    * Loadable modules                                          [ FOUND (115) ]
        - Found 115 loadable modules
          mod_evasive: anti-DoS/brute force                     [ NOT FOUND ]
          mod_reqtimeout/mod_qos                                [ FOUND ]
          ModSecurity: web application firewall                 [ NOT FOUND ]
  - Checking nginx                                              [ NOT FOUND ]

[+] SSH Support
------------------------------------
  - Checking running SSH daemon                                 [ FOUND ]
    - Searching SSH configuration                               [ FOUND ]
    - SSH option: AllowTcpForwarding                            [ SUGGESTION ]
    - SSH option: ClientAliveCountMax                           [ SUGGESTION ]
    - SSH option: ClientAliveInterval                           [ OK ]
    - SSH option: Compression                                   [ SUGGESTION ]
    - SSH option: FingerprintHash                               [ OK ]
    - SSH option: GatewayPorts                                  [ OK ]
    - SSH option: IgnoreRhosts                                  [ OK ]
    - SSH option: LoginGraceTime                                [ OK ]
    - SSH option: LogLevel                                      [ SUGGESTION ]
    - SSH option: MaxAuthTries                                  [ SUGGESTION ]
    - SSH option: MaxSessions                                   [ SUGGESTION ]
    - SSH option: PermitRootLogin                               [ OK ]
    - SSH option: PermitUserEnvironment                         [ OK ]
    - SSH option: PermitTunnel                                  [ OK ]
    - SSH option: Port                                          [ SUGGESTION ]
    - SSH option: PrintLastLog                                  [ OK ]
    - SSH option: Protocol                                      [ NOT FOUND ]
    - SSH option: StrictModes                                   [ OK ]
    - SSH option: TCPKeepAlive                                  [ SUGGESTION ]
    - SSH option: UseDNS                                        [ OK ]
    - SSH option: UsePrivilegeSeparation                        [ OK ]
    - SSH option: VerifyReverseMapping                          [ NOT FOUND ]
    - SSH option: X11Forwarding                                 [ SUGGESTION ]
    - SSH option: AllowAgentForwarding                          [ SUGGESTION ]
    - SSH option: AllowUsers                                    [ NOT FOUND ]
    - SSH option: AllowGroups                                   [ NOT FOUND ]

[+] SNMP Support
------------------------------------
```

```
  - Checking running SNMP daemon                              [ NOT FOUND ]

[+] Databases
------------------------------------
    No database engines found

[+] LDAP Services
------------------------------------
  - Checking OpenLDAP instance                                [ NOT FOUND ]

[+] PHP
------------------------------------
  - Checking PHP                                              [ NOT FOUND ]

[+] Squid Support
------------------------------------
  - Checking running Squid daemon                             [ NOT FOUND ]

[+] Logging and files
------------------------------------
  - Checking for a running log daemon                         [ OK ]
    - Checking Syslog-NG status                               [ NOT FOUND ]
    - Checking systemd journal status                         [ FOUND ]
    - Checking Metalog status                                 [ NOT FOUND ]
    - Checking RSyslog status                                 [ FOUND ]
    - Checking RFC 3195 daemon status                         [ NOT FOUND ]
    - Checking minilogd instances                             [ NOT FOUND ]
  - Checking logrotate presence                               [ OK ]
  - Checking log directories (static list)                    [ DONE ]
  - Checking open log files                                   [ DONE ]
  - Checking deleted files in use                             [ FILES FOUND ]

[+] Insecure services
------------------------------------
  - Checking inetd status                                     [ NOT ACTIVE ]

[+] Banners and identification
------------------------------------
  - /etc/issue                                                [ FOUND ]
    - /etc/issue contents                                     [ WEAK ]
  - /etc/issue.net                                            [ FOUND ]
    - /etc/issue.net contents                                 [ WEAK ]

[+] Scheduled tasks
------------------------------------
  - Checking crontab/cronjob                                  [ DONE ]

[+] Accounting
------------------------------------
  - Checking accounting information                           [ NOT FOUND ]
  - Checking sysstat accounting data                          [ NOT FOUND ]
  - Checking auditd                                           [ NOT FOUND ]

[+] Time and Synchronization
```

```
------------------------------------

[+] Cryptography
------------------------------------
  - Checking for expired SSL certificates [0/2]               [ NONE ]

[+] Virtualization
------------------------------------

[+] Containers
------------------------------------

[+] Security frameworks
------------------------------------
  - Checking presence AppArmor                                [ NOT FOUND ]
  - Checking presence SELinux                                 [ NOT FOUND ]
  - Checking presence grsecurity                              [ NOT FOUND ]
  - Checking for implemented MAC framework                    [ NONE ]

[+] Software: file integrity
------------------------------------
  - Checking file integrity tools
    - OSSEC (syscheck)                                        [ FOUND ]
  - Checking presence integrity tool                          [ FOUND ]

[+] Software: System tooling
------------------------------------
  - Checking automation tooling
  - Automation tooling                                        [ NOT FOUND ]
  - Checking for IDS/IPS tooling                              [ NONE ]

[+] Software: Malware
------------------------------------
  - Checking chkrootkit                                       [ FOUND ]
  - Checking Rootkit Hunter                                   [ FOUND ]
  - Checking ClamAV scanner                                   [ FOUND ]
  - Checking ClamAV daemon                                    [ FOUND ]
    - Checking freshclam                                      [ FOUND ]

[+] File Permissions
------------------------------------
  - Starting file permissions check

[+] Home directories
------------------------------------
  - Checking shell history files                              [ OK ]

[+] Kernel Hardening
------------------------------------
  - Comparing sysctl key pairs with scan profile
    - fs.protected_hardlinks (exp: 1)                         [ OK ]
    - fs.protected_symlinks (exp: 1)                          [ OK ]
    - fs.suid_dumpable (exp: 0)                               [ OK ]
    - kernel.core_uses_pid (exp: 1)                           [ DIFFERENT ]
```

```
    - kernel.ctrl-alt-del (exp: 0)                              [ OK ]
    - kernel.dmesg_restrict (exp: 1)                            [ OK ]
    - kernel.kptr_restrict (exp: 2)                             [ DIFFERENT ]
    - kernel.randomize_va_space (exp: 2)                        [ OK ]
    - kernel.sysrq (exp: 0)                                     [ DIFFERENT ]
    - kernel.yama.ptrace_scope (exp: 1 2 3)                     [ DIFFERENT ]
    - net.ipv4.conf.all.accept_redirects (exp: 0)               [ DIFFERENT ]
    - net.ipv4.conf.all.accept_source_route (exp: 0)            [ OK ]
    - net.ipv4.conf.all.bootp_relay (exp: 0)                    [ OK ]
    - net.ipv4.conf.all.forwarding (exp: 0)                     [ OK ]
    - net.ipv4.conf.all.log_martians (exp: 1)                   [ DIFFERENT ]
    - net.ipv4.conf.all.mc_forwarding (exp: 0)                  [ OK ]
    - net.ipv4.conf.all.proxy_arp (exp: 0)                      [ OK ]
    - net.ipv4.conf.all.rp_filter (exp: 1)                      [ DIFFERENT ]
    - net.ipv4.conf.all.send_redirects (exp: 0)                 [ DIFFERENT ]
    - net.ipv4.conf.default.accept_redirects (exp: 0)           [ DIFFERENT ]
    - net.ipv4.conf.default.accept_source_route (exp: 0)        [ DIFFERENT ]
    - net.ipv4.conf.default.log_martians (exp: 1)               [ DIFFERENT ]
    - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)             [ OK ]
    - net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)       [ OK ]
    - net.ipv4.tcp_syncookies (exp: 1)                          [ OK ]
    - net.ipv4.tcp_timestamps (exp: 0 1)                        [ OK ]
    - net.ipv6.conf.all.accept_redirects (exp: 0)               [ DIFFERENT ]
    - net.ipv6.conf.all.accept_source_route (exp: 0)            [ OK ]
    - net.ipv6.conf.default.accept_redirects (exp: 0)           [ DIFFERENT ]
    - net.ipv6.conf.default.accept_source_route (exp: 0)        [ OK ]

[+] Hardening
------------------------------------
    - Installed compiler(s)                                     [ FOUND ]
    - Installed malware scanner                                 [ FOUND ]

[+] Custom Tests
------------------------------------
  - Running custom tests...                                     [ NONE ]

[+] Plugins (phase 2)
------------------------------------

================================================================================

  -[ Lynis 2.6.9 Results ]-

  Warnings (2):
  ----------------------------
  ! Found some information disclosure in SMTP banner (OS or software name)
[MAIL-8818]
      https://cisofy.com/lynis/controls/MAIL-8818/

  ! iptables module(s) loaded, but no rules active [FIRE-4512]
      https://cisofy.com/lynis/controls/FIRE-4512/

  Suggestions (36):
  ----------------------------
```

```
  * Set a password on GRUB bootloader to prevent altering boot configuration
(e.g. boot in single user mode without password) [BOOT-5122]
      https://cisofy.com/lynis/controls/BOOT-5122/

  * Install a PAM module for password strength testing like pam_cracklib or
pam_passwdqc [AUTH-9262]
      https://cisofy.com/lynis/controls/AUTH-9262/

  * Configure minimum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/lynis/controls/AUTH-9286/

  * Configure maximum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/lynis/controls/AUTH-9286/

  * Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
      https://cisofy.com/lynis/controls/AUTH-9328/

  * To decrease the impact of a full /home file system, place /home on a
separate partition [FILE-6310]
      https://cisofy.com/lynis/controls/FILE-6310/

  * To decrease the impact of a full /tmp file system, place /tmp on a separate
partition [FILE-6310]
      https://cisofy.com/lynis/controls/FILE-6310/

  * To decrease the impact of a full /var file system, place /var on a separate
partition [FILE-6310]
      https://cisofy.com/lynis/controls/FILE-6310/

  * Disable drivers like USB storage when not used, to prevent unauthorized
storage or data theft [STRG-1840]
      https://cisofy.com/lynis/controls/STRG-1840/

  * Disable drivers like firewire storage when not used, to prevent unauthorized
storage or data theft [STRG-1846]
      https://cisofy.com/lynis/controls/STRG-1846/

  * Check DNS configuration for the dns domain name [NAME-4028]
      https://cisofy.com/lynis/controls/NAME-4028/

  * Install debsums utility for the verification of packages with known good
database. [PKGS-7370]
      https://cisofy.com/lynis/controls/PKGS-7370/

  * Consider running ARP monitoring software (arpwatch,arpon) [NETW-3032]
      https://cisofy.com/lynis/controls/NETW-3032/

  * You are advised to hide the mail_name (option: smtpd_banner) from your
postfix configuration. Use postconf -e or change your main.cf file
(/etc/postfix/main.cf) [MAIL-8818]
      https://cisofy.com/lynis/controls/MAIL-8818/

  * Disable the 'VRFY' command [MAIL-8820:disable_vrfy_command]
    - Details  : disable_vrfy_command=no
```

```
    - Solution : run postconf -e disable_vrfy_command=yes to change the value
      https://cisofy.com/lynis/controls/MAIL-8820/

  * Install Apache mod_evasive to guard webserver against DoS/brute force
attempts [HTTP-6640]
      https://cisofy.com/lynis/controls/HTTP-6640/

  * Install Apache modsecurity to guard webserver against web application
attacks [HTTP-6643]
      https://cisofy.com/lynis/controls/HTTP-6643/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowTcpForwarding (YES --> NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : ClientAliveCountMax (3 --> 2)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Compression (YES --> NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : LogLevel (INFO --> VERBOSE)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxAuthTries (6 --> 2)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxSessions (10 --> 2)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Port (22 --> )
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : TCPKeepAlive (YES --> NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : X11Forwarding (YES --> NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowAgentForwarding (YES --> NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Check what deleted files are still in use and why. [LOGG-2190]
      https://cisofy.com/lynis/controls/LOGG-2190/
```

```
  * Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
      https://cisofy.com/lynis/controls/BANN-7126/

  * Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
      https://cisofy.com/lynis/controls/BANN-7130/

  * Enable process accounting [ACCT-9622]
      https://cisofy.com/lynis/controls/ACCT-9622/

  * Enable sysstat to collect accounting (no results) [ACCT-9626]
      https://cisofy.com/lynis/controls/ACCT-9626/

  * Enable auditd to collect audit information [ACCT-9628]
      https://cisofy.com/lynis/controls/ACCT-9628/

  * Determine if automation tools are present for system management [TOOL-5002]
      https://cisofy.com/lynis/controls/TOOL-5002/

  * One or more sysctl values differ from the scan profile and could be tweaked
[KRNL-6000]
    - Solution : Change sysctl value or disable test (skip-test=KRNL-6000:)
      https://cisofy.com/lynis/controls/KRNL-6000/

  * Harden compilers like restricting access to root user only [HRDN-7222]
      https://cisofy.com/lynis/controls/HRDN-7222/

  Follow-up:
  ----------------------------
  - Show details of a test (lynis show details TEST-ID)
  - Check the logfile for all details (less /var/log/lynis.log)
  - Read security controls texts (https://cisofy.com)
  - Use --upload to upload data to central system (Lynis Enterprise users)

================================================================================

  Lynis security scan details:

  Hardening index : 66 [#############       ]
  Tests performed : 213
  Plugins enabled : 0

  Components:
  - Firewall               [V]
  - Malware scanner        [V]

  Lynis Modules:
  - Compliance Status      [?]
  - Security Audit         [V]
  - Vulnerability Scan     [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat
```

```
================================================================================

  Lynis 2.6.9

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

================================================================================

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see
/etc/lynis/default.prf for all settings)
```

Nakon svih testova (*tests performed*), alat boduje (*hardening index*) sigurnost svih konfiguracija. Što ima više bodova, to je sigurnija konfiguracija. Detalji svih testova mogu se vidjeti u dnevničkom zapisu u datoteci `/var/log/lynis.log`, a datoteka `/var/log/lynis-report.dat` sadrži kopiju izvještaja.

U izvještaju su dva upozorenja, jedan se odnosi na SMTP *banner* iz kojeg se može otkriti verzija operacijskog sustava ili servis koji se koristi za slanje elektroničke pošte, a drugi ukazuje na to da ne postoje pravila u servisu *iptables*:

```
Warnings (2):
  ----------------------------
  ! Found some information disclosure in SMTP banner (OS or software name)
[MAIL-8818]
      https://cisofy.com/lynis/controls/MAIL-8818/

  ! iptables module(s) loaded, but no rules active [FIRE-4512]
      https://cisofy.com/lynis/controls/FIRE-4512/
```

5.2.3. Sigurnosne ranjivosti

Nakon usklađivanja konfiguracija sa sigurnosnim politikama, preporučuje se redovito skenirati operacijski sustav i njegove servise u svrhu otkrivanja sigurnosnih ranjivosti. Ranjivost je propust u konfiguraciji ili kôdu nekoga programa, a postoje mnogi testovi koji ih mogu automatski otkriti. Ti testovi otkrivaju već poznate ranjivosti u interakciji sa servisom ili operacijskim sustavom.

Otkrivanje ranjivosti samo je jedan korak do sigurnijeg poslužitelja, ostatak ovisi o stručnosti osoblja kad je potrebno osigurati konfiguracije servisa i operacijskog sustava. Također je potrebno te iste konfiguracije, kojima se uklanjaju ranjivosti, primijeniti i na ostala računala u mreži. Ako su ranjivosti vezane za verzije programa, bitna je brza reakcija pri nadogradnji servisa i jezgre operacijskog sustava.

Ovisno o vrsti skeniranja, mogu se dobiti informacije o upaljenim računalima na mreži, operacijskim sustavima, otvorenim portovima, servisima i njihovim verzijama, vatrozidima itd. Sve

te informacije se koristite za definiranje ranjivosti i njihove ozbiljnosti. CVE (*Common Vulnerabilities and Exposures*) je javna baza podataka svih poznatih ranjivosti. Svaka ranjivost ima svoj identifikacijski broj, opis i javne reference, a cijela lista se može pronaći na *web*-stranici: cve.mitre.org/cve/. Većina alata za skeniranje ranjivosti koristi informacije s te liste i ako želi biti aktualna, mora imati usklađenu bazu ranjivosti s tom listom.

Dvije su vrste ranjivosti, lokalne i udaljene (*remote*).

Lokalne ranjivosti

Kod lokalnih ranjivosti potreban je pristup konzoli ili neka druga vrsta pristupa operacijskom sustavu u kojem korisnik može dobiti veće ovlasti nego što je inicijalno konfigurirano. To može biti pristup servisima ili datotekama za koje inače nema prava, tj. ograničeno mu je korištenje resursa na sustavu, a pomoću ranjivosti nastoji steći prava koja nema. Na primjer, ako postoji ranjivost u programu *passwd* koji mijenja lozinke korisnicima, korisnik koji nije root bi je mogao iskoristiti za dobivanje *root* ovlasti. Lokalne ranjivosti su manje kritične od udaljenih ranjivosti, ali u kombinaciji s uspješnim napadima na udaljene ranjivosti mogu omogućiti napadaču da proširi korisnička prava i dobije *root* ovlasti.

Udaljene ranjivosti

Udaljene ranjivosti mogu se iskoristiti bez lokalnog pristupa, ako se servisu može pristupiti preko mreže, na primjer servisimi za posluživanje *web*-sadržaja, elektroničke pošte, DNS-a, FTP-a itd. Takve ranjivosti mogu dovesti do kompromitiranja podataka, iskorištavanja resursa sustava, smanjenje mogućnosti korištenja za legitimne korisnike, interakciju sa sustavom ili čak neželjenu autentikaciju.

Zbog razvoja globalne mreže Internet, povećao se broj dostupnih *web*-aplikacija. Zbog toga se velik dio udaljenoga skeniranja odnosi na ranjivosti *web*-servisa. Neke od tih ranjivosti su:

- *cross-site scripting:* omogućuje napadačima izvršavanje zloćudnoga kôda u *web*-pregledniku korisnika. Umetanje zloćudnoga kôda vrši se u legitimne *web*-stranice koji se izvršavaju kod *web*-preglednika korisnika. Najranjivije *web*-stranice za *cross-site scripting* su forumi, oglasne ploče, i *web*-stranice koje dozvoljavaju komentiranje.
- *format string*: napadač iskorištava formu za upis kako bi izvršio naredbe preko *web*-stranice na poslužitelju.
- XML *injection:* omogućuje napadačima promjenom ili umetanjem XML sadržaja izmjenu strukture XML-a kako bi napravili zloćudnu radnju, najčešće je to promjena informacija o financijskim transakcijama ili neautorizirano povezivanje s administratorskim korisničkim računom.
- SQL *injection:* jedna od najčešćih ranjivosti koja iskorištava forme za upis na *web*-stranicama kako bi napadač izvršio SQL naredbe i došao do nedozvoljenih informacija.
- *command injection:* napadač izvršava naredbe na operacijskom sustavu putem ranjivih aplikacija, najčešće koristeći forme za upis, kolačiće (*cookies*), HTTP zaglavlja itd.
- *path traversal:* napadač pokušava izaći iz svog direktorija (npr. direktorij gdje se nalazi *web*-stranica) manipuliranjem varijablama koje sadrže putanju do direktorija.
- sve neosigurane konfiguracije *web*-servisa.

Alati

Postoji mnogo besplatnih i komercijalnih alata koji se koriste za skeniranje ranjivosti sa svojim prednostima i nedostatcima. Neki od tih alata su *Nessus*, *OpenVAS*, *Nexpose*, *Retina* itd. Specijalizirani alati za *web* ranjivosti su *Skipfish*, *Wapitija* i *Nikta*, a cijela lista alata može se pronaći na poveznici: https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools.

Neispravna analiza ranjivosti

Izvještaj skeniranja ranjivosti navodi/nabraja pronađene ranjivosti, nivo njihove ozbiljnosti, opis, a neki alati u izvještaju predlažu i moguća rješenja. Neke od pronađenih ranjivosti mogu biti lažno pozitivne (*false positives)* ili lažno negativne (*false negatives)*. Lažno pozitivna ranjivost ne postoji ali ju je pronašao alata za skeniranje, a lažno negativna je ranjivost koja postoji, ali je alat za skeniranje nije pronašao u svom skeniranju. Ni jedan alat nije savršen, pa je zato u izvještaju potrebno obratiti pozornost na ove izuzetke.

Penetracijsko testiranje

Činjenica da postoji ranjivost ne znači da se može iskoristiti za zloćudne radnje. Ako ranjivost ipak dovede do neovlaštenog pristupa sustava ili na bilo koji način utječe na rad aplikacije, kaže se da je ranjivost iskoristiva (*exploit*). Nakon skeniranja ranjivosti poželjno je učiniti i penetracijsko testiranje, koje koristi informacije iz skeniranja i pokušava oponašati stvarni napad i iskoristiti slabosti u informacijskim sustavima. Cilj napada je dobiti kontrolu nad sustavom ili ga bilo kako onemogućiti te napraviti protumjeru za isti napad.

Alat *Lynis*

Alat *Lynis* ima mogućnost pokretanja svojih skeniranja kao običan korisnik (bez *root* ovlasti) u tzv. *pentest modu*. U ovom neprivilegiranom skeniranju, testovi za koje su potrebne *root* ovlasti neće biti provjereni. Ovakvo skeniranje daje dobar uvid čemu običan korisnik ima pristup. Slijedi primjer izvještaja u *pentest modu*:

```
$ sudo lynis audit --pentest

[ Lynis 2.6.9 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]
```

```
  ---------------------------------------------------
  Program version:           2.6.9
  Operating system:          Linux
  Operating system name:     Debian
  Operating system version:  9.5
  Kernel version:            4.9.0
  Hardware platform:         x86_64
  Hostname:                  debian
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /usr/share/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                                [ NO UPDATE ]
Error, could not find helper

================================================================================

  -[ Lynis 2.6.9 Results ]-

  Great, no warnings

  No suggestions

================================================================================

  Lynis security scan details:

  Hardening index : 1 [#                   ]
  Tests performed : 0

  Components:
  - Firewall               [X]
  - Malware scanner        [X]

  Lynis Modules:
  - Compliance Status      [?]
  - Security Audit         [V]
  - Vulnerability Scan     [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

================================================================================
```

```
  Lynis 2.6.9

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

================================================================================

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see
/etc/lynis/default.prf for all settings)
```

5.2.4. Zanimljivi izvori

Poveznice:

- https://www.digitalocean.com/community/tutorials/how-to-use-nmap-to-scan-for-open-ports-on-your-vps
- https://www.cyberciti.biz/tips/linux-scanning-network-for-open-ports.html
- https://www.open-scap.org/
- https://www.cisecurity.org/cis-benchmarks/
- https://cisofy.com/lynis/
- https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

6. Sigurnosna pohrana

Trajanje poglavlja:
75 min

Po završetku ovoga poglavlja moći ćete:

- nabrojati postavke koje je potrebno uzeti u obzir pri odabiru sigurnosne pohrane
- koristiti alate Bacula i Rsync za implementiranje politike sigurnosne pohrane
- koristiti alat mysqldump i automysqlbackup za sigurnosnu pohranu baze podataka

Ova cjelina obrađuje politiku i alate za izvršavanje sigurnosne pohrane.

6.1. Sigurnosna pohrana datoteka i baza podataka

6.1.1. Strategije sigurnosne pohrane

Bez pouzdane i učestale sigurnosne pohrane, riskira se gubitak podataka. Razlozi gubitaka podataka mogu biti razni, od ljudske greške, grešaka u hardveru ili softveru, do virusa ili prestanka rada električne energije. Preporučeno je sigurnosnu pohranu raditi na udaljenoj lokaciji, tj. ne na računalu koje treba sigurnosno pohraniti. To može biti na dijeljenim mrežnim diskovima (*network-attached storage, NAS*), udaljenom računalu, magnetskim trakama, prijenosnim tvrdim diskovima itd.

Strategije sigurnosne pohrane mogu biti različite, a ovise o svrsi poslužitelja. Nekoliko postavki je potrebno uzeti u obzir pri odabiru strategije:

- učestalost sigurnosne pohrane, tj. točke oporavka podataka (svaki sat, dnevno, tjedno, mjesečno...)
- vrsta sigurnosne pohrane
- koje podatke je potrebno pohranjivati
- lokacija (udaljena ili lokalna) i uređaji na koje će se pohranjivati podaci (NAS, magnetske trake...)
- enkripcija i sažimanje tijekom prijenosa podataka na drugu lokaciju
- enkripcija i sažimanje sigurnosnih kopija
- vremenski period čuvanja podataka, nakon čega se podaci brišu
- povremeni testovi povratka podataka.

Postoji nekoliko vrsta sigurnosne pohrane:

- potpuna: pri svakoj sigurnosnoj pohrani spremaju se svi podaci.
- inkrementalna: prva sigurnosna kopija sastavljena je od svih datoteka nastalih ili izmijenjenih od zadnje potpune sigurnosne kopije. Nakon toga spremaju se sve datoteke izrađene ili izmijenjene od zadnje inkrementalne kopije.

- diferencijalna: pri svakoj sigurnosnoj pohrani spremaju se svi podaci koji su dodani ili mijenjani od zadnje potpune sigurnosne pohrane.

Potpuna pohrana obavezno se radi prilikom prve sigurnosne pohrane ili nakon većih promjena na operacijskom sustavu, nakon nadogradnje servisa ili velike promjene podataka. Potpuna sigurnosna pohrana najčešće se izvršava svakih tjedan ili mjesec dana, a potpune pohrane starije od određenog vremenskog razdoblja se brišu. Između potpunih sigurnosnih pohrana preporuča se izvršavati inkrementalne ili diferencijalne sigurnosne pohrane. Ako se izvršava diferencijalna pohrana, za potpuni povrat podataka potrebni su podaci iz posljednje potpune pohrane i posljednje diferencijalne pohrane. Mana diferencijalne pohrane jest da podaci mogu biti veliki, ali se brzo vraćaju nakon gubitka. Kod inkrementalne je nedostatak sporije vraćanje podataka, ali su zato pohranjeni podaci mnogo manji.

Postoje razni alati za izvršavanje sigurnosne pohrane na operacijskih sustavima *Linux*, kao što su naredbe `dd`, `dumo` , `tar`, `rsync` ili specijalizirani alati *Bacula*, *Amanda*, *Backupninja*, *Veritas Backup Exec*, *Veeam*, *Unitrends*, IBM *Spectrum Protect* itd.

6.1.2. Alat Bacula

Bacula je program otvorenoga kôda za sigurnosnu pohranu i oporavak koji se može koristiti lokalno ili preko mreže (arhitektura *agent-server*). Alat *Bacula* je efikasan i relativno jednostavan za upotrebu, uz mnogo naprednih mogućnosti upravljanja pohranom koja omogućava pretraživanje i oporavak obrisanih ili oštećenih podataka.

Komponente

Alat *Bacula* ima nekoliko komponenti i servisa:

- *bacula-director*: servis koji nadgleda sve sigurnosne pohrane, oporavke, arhiviranje i potvrde
- *bacula-sd (storage)*: servis koji pohranjuje i oporavlja podatke na mediju koji se koristi za sigurnosnu pohranu
- *bacula-fd (file)*: servisni proces se instalira na agentu na kojem se vrši sigurnosna pohrana
- *Bacula Console*: sučelje u naredbenom retku s kojim administrator upravlja servisom *Director*
- *Catalog*: servis koji upisuje i prati podatke koji su arhivirani kroz bazu podataka.

Kod lokalnog korištenja, sve komponente moraju biti instalirane na jednom računalu. Ako se koristi arhitektura agent-server, većina komponenti bit će instalirana samo na serveru, a na agentima je potreban samo servis *bacula-fd*.

Instalacija

Instalacija alata *Bacula* vrši se naredbom `apt-get`. Servis *bacula-director* za svoje podatke koristi SQL bazu podataka, pa je tijekom instalacije potrebno potvrditi konfiguraciju odabirom teksta <yes>:

```
$ sudo apt-get install bacula-server bacula-client

Configure database for bacula-director-sqlite3 with dbconfig-common?
 <Yes>     <No>
```

Za sigurnosnu pohranu i oporavak potrebni su odvojeni direktoriji sa sljedećim vlasnicima i pravima:

```
$ sudo mkdir -p /bacula/backup /bacula/restore
$ sudo chown -R bacula:bacula /bacula
$ sudo chmod -R 700 /bacula
```

Konfiguracija servisa *bacula-director*

Konfiguracijska datoteka servisa *bacula-director* nalazi se u `/etc/bacula/bacula-dir.conf` sa sljedećim blokovima konfiguracija:

- `Director`: generalna konfiguracija servisa
- `Pool`: logičke cjeline medija za pohranu, npr. sve trake gdje se radi potpuna sigurnosna pohrana smještaju se u jedan *pool* itd.
- `Job`: pojedinačni poslovi sigurnosnih pohrana i oporavaka
- `JobDefs`: zadane konfiguracije za poslove koje sve mogu referencirati unutar pojedinog *Joba*
- `Schedule`: vremenski period sigurnosne pohrane koji definira izvršavanje *Joba*
- `Client`: konfiguracije klijenta gdje će vršiti sigurnosna pohrana
- `FileSet`: definiranje direktorija ili datoteka koje će se pohraniti ili oporaviti, a koristit će se u pojedinom *Jobu*
- `Messages`: konfiguracija obavijesti koje se šalju elektroničkom poštom
- `Catalog:` konfiguracija baze podataka

Blok *Job*

Blok *Job* koristi se za definiranje poslova sigurnosne pohrane i oporavka.

Konfiguracija servisa *bacula-director* donosi zadane postavke *JobDefs*, koje se mogu referencirati u ostalim blokovima *Job*:

```
JobDefs {
  Name = "DefaultJob"
  Type = Backup
  Level = Incremental
  Client = debian-fd
  FileSet = "Full Set"
  Schedule = "WeeklyCycle"
  Storage = File1
  Messages = Standard
  Pool = File
  SpoolAttributes = yes
  Priority = 10
  Write Bootstrap = "/var/lib/bacula/%c.bsr"
}
```

Neke od mogućnosti su:

- `Name`: ime bloka JobDefs na koje se može referencirati u blokovima Job
- `Type`: sigurnosna pohrana (`Backup`) ili oporavak (`Restore`)
- `Level`: potpuni (`Full`), inkrementalni (`Incremental`) ili diferencijalni (`Differential`)
- `Client`, `Schedule`, `Storage` i ostala imena blokova: upisuje se ime bloka na koji se referencira

Sljedeći *Job* za pohranu je jednostavan, ima samo ime i referencira se na blok sa zadanim postavkama "DefaultJob":

```
Jobs {
  Name = "LokalnaPohrana"
  JobDefs = "DefaultJob"
}
```

Prema tome, njegova konfiguracija je ista kao i kod *DefaultJoba*.

Sljedeći *Job* koristi se za opravak, kako je i navedeno u mogućnosti Type, a oporavak će biti napravljen u prethodno stvorenom direktoriju /bacula/restore.

```
Job {
  Name = "LokalniOporavak"
  Type = Restore
  Client = debian-fd
  FileSet = "Full Set"
  Storage = File1
```

```
  Pool = File
  Messages = Standard
  Where = /bacula/restore
}
```

Blok FileSet

U bloku FileSet definiraju se datoteke i direktoriji nad kojima će se vršiti sigurnosna pohrana i one koje je potrebno izuzeti iz pohrane. Također je moguće dodati opciju sažimanja, enkripcije i kriptografskoga sažetka.

U bloku imena *DefaultJob* definirana je opcija `FileSet = "Full Set"`, pa će se i novi blok tako zvati:

```
FileSet {
  Name = "Full Set"
  Include {
    Options {
      signature = MD5
      compression = GZIP
    }
    File = /
  }
  Exclude {
    File = /var/lib/bacula
    File = /bacula
    File = /proc
    File = /tmp
    File = /sys
    File = /.journal
    File = /.fsck
  }
}
```

Sigurnosna pohrana vršit će se nad root direktorijem (/) i svim poddirektorijima, osim onih koji su izuzeti (Exclude). Većina izuzetih direktorija je zadana, a dodan je direktorij /bacula jer će se u njemu spremati pohranjeni i oporavljeni podaci. Za svaku datoteku izračunat će se kriptografski sažetak i ona će biti sažeta.

Blok Schedule

U bloku Schedule definira se koja će se vrsta sigurnosne pohrane izvršiti i kada:

```
Schedule {
  Name = "WeeklyCycle"
  Run = Full 1st sun at 23:05
  Run = Differential 2nd-5th sun at 23:05
  Run = Incremental mon-sat at 23:05
}
```

Napomena

Sve mogućnosti formata opcije Run objašnjene su na sljedećoj poveznici: https://www.bacula.org/9.4.x-manuals/en/main/Configuring_Director.html#SECTION00205000000000000000

Blok Storage

Sljedeća konfiguracija servisa *bacula-sd*, na koju se spaja servis *bacula-director*, zadana je i bit će dovoljna za lokalnu sigurnosnu pohranu:

```
Storage {
  Name = File1
# Do not use "localhost" here
  Address = localhost                # N.B. Use a fully qualified name here
  SDPort = 9103
  Password = "shDonQyasGrVTRUzZRO9ITgxkzk1qo0jR"
  Device = FileStorage
  Media Type = File
  Maximum Concurrent Jobs = 10         # run up to 10 jobs a the same time
}
```

Ako će se koristiti sigurnosna pohrana preko mreže, potrebno je promijeniti opciju `Address` da odgovara FQDN-u računala.

Sve opcije koje se mogu koristiti u konfiguracijskoj datoteci `/etc/bacula/bacula-dir.conf` objašnjene su na *web*-stranici:
http://www.bacula.org/5.2.x-manuals/en/main/main/Configuring_Director.html

Ispravnost konfiguracije testira se sljedećom naredbom:

```
$ sudo bacula-dir -tc /etc/bacula/bacula-dir.conf
```

Ako je sintaksa ispravna, naredba neće pokazati greške.

Konfiguracija servisa *bacula-sd*

Kako bi alat *Bacula* znao gdje će pohranjivati podatke, potrebno je konfigurirati servis *bacula-sd* u datoteci `/etc/bacula/bacula-sd.conf`.

Prema zadanim postavkama, u bloku Storage postavljena je SDAddress na 127.0.0.1, što je dovoljno za lokalnu upotrebu. Za drugu lokaciju potrebno je dodati FQDN računala.

```
Storage {
  Name = debian-sd
  SDPort = 9103
  WorkingDirectory = "/var/lib/bacula"
  Pid Directory = "/run/bacula"
  Maximum Concurrent Jobs = 20
  SDAddress = 127.0.0.1
}
```

Putanja za sigurnosnu pohranu dodaje se u blok Device:

```
Device {
  Name = FileStorage
  Media Type = File
  Archive Device = /bacula/backup
  LabelMedia = yes
  Random Access = no
  AutomaticMount = no
  RemovableMedia = no
  AlwaysOpen = no
}
```

Više informacija o konfiguracijama u prethodnom primjeru nalazi se na poveznici: https://www.bacula.org/9.4.x-manuals/en/main/Storage_Daemon_Configuratio.html#SECTION00223000000000000000.

Ispravnost konfiguracije testira se naredbom:

```
$ sudo bacula-sd -tc /etc/bacula/bacula-sd.conf
```

Ako je sintaksa ispravna, naredba neće pokazati greške.

Za primjenu konfiguracije potrebno je ponovno pokrenuti servise *bacula-director* i *bacula-sd*:

```
$ sudo systemctl restart bacula-director
$ sudo systemctl restart bacula-sd
```

Testiranje sigurnosne pohrane

Poželjno je testirati ispravnost sigurnosne pohrane nakon dodavanja konfiguracija. To se može napraviti naredbom `bconsole` koja otvara sučelje *Bacula Console*:

```
$ sudo bconsole
Connecting to Director localhost:9101
1000 OK: 102 debian-dir Version: 7.4.4 (20 September 2016)
Enter a period to cancel a command.
*
```

Zvjezdica (*) označava komandnu liniju *Bacula Console*.

Za početak je potrebno izvršiti naredbu `label` i odabrati Storage koji je definiran u bloku `JobDefs`. Nakon upisivanja proizvoljnog imena za Volume, potrebno je odabrati Pool koji je definiran u bloku `JobDefs`:

```
* label
Automatically selected Catalog: MyCatalog
Using Catalog "MyCatalog"
The defined Storage resources are:
     1: File1
     2: File2
Select Storage resource (1-2): 1
Enter new Volume name: Volume1
Defined Pools:
     1: Default
     2: File
     3: Scratch
Select the Pool (1-3): 2
Connecting to Storage daemon File1 at localhost:9103 ...
Sending label command for Volume "Volume1" Slot 0 ...
3000 OK label. VolBytes=194 VolABytes=0 VolType=1 Volume="Volume1"
Device="FileStorage" (/bacula/backup)
Catalog record for Volume "Volume1", Slot 0  successfully created.
Requesting to mount FileStorage ...
3906 File device ""FileStorage" (/bacula/backup)" is always mounted.
```

Nakon upisa naredbe `run` , otvara se izbornik za odabir *Joba*, u ovom slučaju to je LokalnaPohrana. Taj *Job* je potrebno potvrditi tipkom "yes".

```
* run
Automatically selected Catalog: MyCatalog
Using Catalog "MyCatalog"
A job name must be specified.
The defined Job resources are:
     1: LokalnaPohrana
     2: BackupCatalog
     3: LokalniOporavak
```

```
Select Job resource (1-3): 1
Run Backup job
JobName:  LokalnaPohrana
Level:    Incremental
Client:   debian-fd
FileSet:  Full Set
Pool:     File (From Job resource)
Storage:  File1 (From Job resource)
When:     2018-10-17 15:59:52
Priority: 10
OK to run? (yes/mod/no): yes
Job queued. JobId=9
You have messages.
```

Naredbom `status director` može se pratiti stanje budućih (*Scheduled Jobs*), trenutačnih (*Running Jobs*) i završenih (*Terminated Jobs*) poslova:

```
* status director
debian-dir Version: 7.4.4 (20 September 2016) x86_64-pc-linux-gnu debian 9.0
Daemon started 17-Oct-18 16:14, conf reloaded 17-Oct-2018 16:14:13
 Jobs: run=0, running=1 mode=0
 Heap: heap=135,168 smbytes=75,185 max_bytes=75,185 bufs=277 max_bufs=281

Scheduled Jobs:
Level          Type     Pri  Scheduled          Job Name           Volume
===================================================================================
Incremental    Backup    10  17-Oct-18 23:05    LokalnaPohrana     Volume1
Incremental    Backup    10  17-Oct-18 23:05    BackupClient1      Volume1
Full           Backup    11  17-Oct-18 23:10    BackupCatalog      Volume1
====

Running Jobs:
Console connected at 17-Oct-18 16:16
 JobId  Type Level     Files     Bytes  Name              Status
======================================================================
     1  Back Full          0         0  LokalnaPohrana    is running
====
No Terminated Jobs.
====
```

Iz statusa se može vidjeti da se izvršava potpuna sigurnosna pohrana imena LokalnaPohrana, a još 3 pohrane će se izvršiti iza 23 sata.

Nakon uspješno ili neuspješno izvršene pohrane poslat će se elektronička poruka s izvještajem. Ta poruka se može prikazati na ekranu naredbom `messages` u *Bacula Consoli*:

```
* messages
17-Oct 16:20 debian-dir JobId 1: No prior Full backup Job record found.
17-Oct 16:20 debian-dir JobId 1: No prior or suitable Full backup found in
catalog.
Doing FULL backup.
17-Oct 16:20 debian-dir JobId 1: Start Backup JobId 1, Job=LokalnaPohrana.
2018-10-17_16.20.57_03
17-Oct 16:20 debian-dir JobId 1: Using Device "FileStorage" to write.
17-Oct 16:20 debian-sd JobId 1: Wrote label to prelabeled Volume "Volume1" on
file
device "FileStorage" (/bacula/backup)
17-Oct 16:36 debian-fd JobId 1:      /dev is a different filesystem.
Will not descend from / into it.
17-Oct 16:36 debian-fd JobId 1:      /run is a different filesystem.
Will not descend from / into it.
17-Oct 16:36 debian-sd JobId 1: Elapsed time=00:15:16,
Transfer rate=1.961 M Bytes/second
17-Oct 16:36 debian-sd JobId 1: Sending spooled attrs to the Director.
Despooling 44,219,416 bytes ...
17-Oct 16:36 debian-dir JobId 1: Bacula debian-dir 7.4.4 (202Sep16):
  Build OS:               x86_64-pc-linux-gnu debian 9.0
  JobId:                  1
  Job:                    LokalnaPohrana.2018-10-17_16.20.57_03
  Backup Level:           Full (upgraded from Incremental)
  Client:                 "debian-fd" 7.4.4 (202Sep16) x86_64-pc-linux-
gnu,debian,9.0
  FileSet:                "Full Set" 2018-10-17 16:20:57
  Pool:                   "File" (From Job resource)
  Catalog:                "MyCatalog" (From Client resource)
  Storage:                "File1" (From Job resource)
  Scheduled time:         17-Oct-2018 16:20:46
  Start time:             17-Oct-2018 16:20:59
  End time:               17-Oct-2018 16:36:26
  Elapsed time:           15 mins 27 secs
  Priority:               10
  FD Files Written:       149,104
  SD Files Written:       149,104
  FD Bytes Written:       1,776,839,729 (1.776 GB)
  SD Bytes Written:       1,797,110,825 (1.797 GB)
  Rate:                   1916.8 KB/s
  Software Compression:   56.7% 2.3:1
  Snapshot/VSS:           no
  Encryption:             no
  Accurate:               no
  Volume name(s):         Volume1
  Volume Session Id:      1
  Volume Session Time:    1539785679
  Last Volume Bytes:      1,803,421,203 (1.803 GB)
  Non-fatal FD errors:    0
  SD Errors:              0
  FD termination status:  OK
```

```
  SD termination status:  OK
  Termination:            Backup OK

17-Oct 16:36 debian-dir JobId 1: Begin pruning Jobs older than 6 months .
17-Oct 16:36 debian-dir JobId 1: No Jobs found to prune.
17-Oct 16:36 debian-dir JobId 1: Begin pruning Files.
17-Oct 16:36 debian-dir JobId 1: No Files found to prune.
17-Oct 16:36 debian-dir JobId 1: End auto prune.
```

Datoteka sa sigurnosnom pohranom spremit će se u /bacula/backup pod imenom Volume1:

```
$ ls -alh /bacula/backup/Volume1
-rw-r----- 1 bacula tape 1.7G Oct 17 16:36 /bacula/backup/Volume1
```

Testiranje oporavka sigurnosne pohrane

Nakon uspješne sigurnosne pohrane bitno je testirati oporavak. Naredba restore otvara izbornik gdje se pod točkom 5 odabire zadnja izvršena sigurnosna pohrana:

```
* restore
Automatically selected Catalog: MyCatalog
Using Catalog "MyCatalog"

First you select one or more JobIds that contain files
to be restored. You will be presented several methods
of specifying the JobIds. Then you will be allowed to
select which files from those JobIds are to be restored.

To select the JobIds, you have the following choices:
     1: List last 20 Jobs run
     2: List Jobs where a given File is saved
     3: Enter list of comma separated JobIds to select
     4: Enter SQL list command
     5: Select the most recent backup for a client
     6: Select backup for a client before a specified time
     7: Enter a list of files to restore
     8: Enter a list of files to restore before a specified time
     9: Find the JobIds of the most recent backup for a client
    10: Find the JobIds for a backup for a client before a specified time
    11: Enter a list of directories to restore for found JobIds
    12: Select full restore to a specified Job date
    13: Cancel
Select item:  (1-13): 5
Automatically selected Client: debian-fd
Automatically selected FileSet: Full Set
+-------+-------+----------+------------+---------------------+------------+
| JobId | Level | JobFiles | JobBytes   | StartTime           | VolumeName |
+-------+-------+----------+------------+---------------------+------------+
| 1     | F     | 149104   | 1776839729 | 2018-10-17 16:20:59 | Volume1    |
+-------+-------+----------+------------+---------------------+------------+
```

```
You have selected the following JobId: 1

Building directory tree for JobId(s) 1 ...
++++++++++++++++++++++++++++++++++++++++
138,270 files inserted into the tree.

You are now entering file selection mode where you add (mark) and
remove (unmark) files to be restored. No files are initially added, unless
you used the "all" keyword on the command line.
Enter "done" to leave this mode.

cwd is: /
$
```

Naredba otvara virtualno stablo direktorija koje se može prikazati naredbom `Is` . Naredba `mark` s imenom direktorija ili datoteke označit će tu datoteku za oporavak. Ako je potrebno opraviti sve datoteke, naredba `mark*` će ih se sve označiti sa zvjezdicom (*):

```
$ mark *
149,104 files marked.
$ ls
*
*.cache
*bin/
*boot/
*dev
*etc/
*home/
*initrd.img
*initrd.img.old
*lib/
*lib64/
*lost+found
*media/
*mnt
*opt
*root/
*run
*sbin/
*srv/
*usr/
*var/
*vmlinuz
*vmlinuz.old
```

Označavanje se završava naredbom `done` koja otvara novi izbornik s ponuđenim *Jobovima*:

```
$ done
Bootstrap records written to /var/lib/bacula/debian-dir.restore.1.bsr
Bootstrap records written to /var/lib/bacula/debian-dir.restore.1.bsr

The Job will require the following (*=>InChanger):
   Volume(s)                 Storage(s)                SD Device(s)
===========================================================================

    Volume1                   File1                     FileStorage

Volumes marked with "*" are in the Autochanger.


149,104 files selected to be restored.

The defined Restore Job resources are:
     1: LokalniOporavak
     2: RestoreFiles
Select Restore Job (1-2): 1
Using Catalog "MyCatalog"
Run Restore job
JobName:         LokalniOporavak
Bootstrap:       /var/lib/bacula/debian-dir.restore.1.bsr
Where:           /bacula/restore
Replace:         Always
FileSet:         Full Set
Backup Client:   debian-fd
Restore Client:  debian-fd
Storage:         File1
When:            2018-10-17 18:03:44
Catalog:         MyCatalog
Priority:        10
Plugin Options:
OK to run? (yes/mod/no): yes
Job queued. JobId=2
```

Nakon odabira *Joba* LokalniOporavak i potvrde tipkom "yes", počet će oporavak.

Naredbom `status director` može se provjeriti stanje oporavka:

```
* status director
debian-dir Version: 7.4.4 (20 September 2016) x86_64-pc-linux-gnu debian 9.0
Daemon started 17-Oct-18 16:14, conf reloaded 17-Oct-2018 16:14:13
 Jobs: run=2, running=0 mode=0
 Heap: heap=73,728 smbytes=81,965 max_bytes=20,744,977 bufs=278 max_bufs=305

Scheduled Jobs:
Level          Type     Pri  Scheduled          Job Name           Volume
===================================================================================
Incremental    Backup    10  17-Oct-18 23:05    LokalnaPohrana     Volume1
Incremental    Backup    10  17-Oct-18 23:05    BackupClient1      Volume1
```

```
Full           Backup    11  17-Oct-18 23:10    BackupCatalog      Volume1
====

Running Jobs:
Console connected at 17-Oct-18 17:55
No Jobs running.
====

Terminated Jobs:
 JobId  Level    Files      Bytes   Status   Finished        Name
===================================================================
     1  Full    149,104    1.776 G  OK       17-Oct-18 16:36 LokalnaPohrana
     2  Restore  149,104    4.151 G  OK       17-Oct-18 18:06 LokalniOporavak

====
```

U `Terminated Jobsu` su dva odrađena posla i oba imaju *Status OK*. Posao LokalnaPohrana ima 4 puta manju veličinu što znači da se sve datoteke sažimaju prilikom sigurnosne pohrane.

Naredbom `exit` može se izaći iz sučelja *Bacula Console*. Uvidom u datoteku `/bacula/restore` može se provjeriti stanje oporavka:

```
*exit
You have new mail in /var/mail/root
$ ls -al /bacula/restore/
total 80
drwxr-xr-x  20 root   root   4096 Oct 17 16:09 .
drwx------   4 bacula bacula 4096 Oct 17 16:09 ..
drwxr-xr-x   2 root   root   4096 Oct 17 16:06 bin
drwxr-xr-x   3 root   root   4096 Oct 12 12:16 boot
drwx------   2 root   root   4096 Oct 11 14:39 .cache
drwxr-xr-x   2 root   root   4096 Oct 17 16:08 dev
drwxr-xr-x 123 root   root   4096 Oct 17 16:08 etc
drwxr-xr-x   3 root   root   4096 Oct 11 14:58 home
lrwxrwxrwx   1 root   root     29 Oct 17 18:03 initrd.img -> boot
/initrd.img-4.9.0-8-amd64
lrwxrwxrwx   1 root   root     29 Oct 17 18:06 initrd.img.old -> boot
/initrd.img-4.9.0-7-amd64
drwxr-xr-x  16 root   root   4096 Oct 12 12:15 lib
drwxr-xr-x   2 root   root   4096 Oct 11 14:23 lib64
drwx------   2 root   root   4096 Oct 11 14:23 lost+found
drwxr-xr-x   4 root   root   4096 Oct 11 14:23 media
drwxr-xr-x   2 root   root   4096 Oct 11 14:23 mnt
drwxr-xr-x   2 root   root   4096 Oct 11 14:23 opt
drwx------   4 root   root   4096 Oct 17 16:13 root
drwxr-xr-x   2 root   root   4096 Oct 17 16:08 run
drwxr-xr-x   2 root   root   4096 Oct 17 16:06 sbin
drwxr-xr-x   3 root   root   4096 Oct 12 11:00 srv
drwxr-xr-x  10 root   root   4096 Oct 11 14:23 usr
drwxr-xr-x  12 root   root   4096 Oct 12 10:59 var
lrwxrwxrwx   1 root   root     26 Oct 17 18:06 vmlinuz -> boot
/vmlinuz-4.9.0-8-amd64
```

```
lrwxrwxrwx   1 root   root     26 Oct 17 18:03 vmlinuz.old ->
boot/vmlinuz-4.9.0-7-amd64
```

6.1.3. Alat Rsync

Rsync (*Remote Sync*) jedan je od najkorištenijih alata za kopiranje, sinkronizaciju i sigurnosnu pohranu na operacijskim sustavima *Linux*. To je alat za lokalno i udaljeno kopiranje datoteka s opcijama sažimanja i raspakiravanja podataka radi smanjivanja mrežnoga prometa. Kopiranje može uključiti i simbolične poveznice te uređaje, skupa sa svojim vlasnicima, grupama i ovlastima.

Alat ima mogućnost protokola *remote-update* koji kopira samo razliku između dva seta podataka između izvora i odredišta. Prvo kopira sve podatke, a svaki sljedeći put kopira samo promijenjene datoteke i direktorije. Na ovaj način izvršava inkrementalnu sigurnosnu pohranu.

Sintaksa je:

rsync <opcije> <izvor> <odredište>

Slijedi objašnjenje opcija rsync naredbe:

Opcija	Značenje
-r	rekurzivno kopira podatke bez vlasnika, grupe i ovlasti
-l	kopiranje simboličkih poveznica.
-p	spremanje dozvole nad datotekama.
-t	spremanje vremena promjena
-g	spremanje grupe
-o	spremanje vlasnika
-D	spremanje uređaja i posebnih datoteka
-a	arhiviranje, zamjena za opcije –rlptgoD
-z	sažimanje podataka pri prijenosu
-h	prikazivanje detalja o prebacivanju podataka
--remove-source-files	brisanje izvornih podataka nakon kopiranja
--delete	brisanje odredišnih podataka kojih nema na izvorištu
--dry-run	vršenje testnog pokretanja
--bwlimit=1000	limitiranje mrežne propusnosti na 1000 bajtova po sekundi
--progress	prikazivanje napretka pri izvršavanju zadataka
--include 'ime*'	uključivanje pojedinih datoteka i direktorija
--exclude 'test*'	isključivanje pojedinih datoteka i direktorija
-v	prikazivanje informacija o datotekama koje se kopiraju u realnom vremenu i kratki sažetak o kopiranim podatcima
-v	Definiranje ljuske na udaljenom računalu

Naredba za instalaciju alata je:

```
$ sudo apt-get install rsync
```

Lokalno kopiranje

Slijedi primjer lokalnoga kopiranja datoteke i cijeloga direktorija:

```
$ rsync -avh /data/miner /backup/single/
sending incremental file list
created directory /backup/single
miner

sent 419.53M bytes  received 72 bytes  119.87M bytes/sec
total size is 419.43M  speedup is 1.00


$ rsync -avh /data/ /backup/data1/
sending incremental file list
./
nautilus
nm-applet
pulseaudio.desktop

sent 367.09M bytes  received 76 bytes  146.84M bytes/sec
total size is 367.00M  speedup is 1.00
```

Ako na odredištu ne postoji direktorij, rsync će ga stvoriti.

Udaljeno kopiranje

Primjer kopiranja na udaljeno računalo pod korisnikom linux1:

```
$ rsync -azvh /data/miner linux1@192.168.2.3:/home/linux1
linux1@192.168.2.3's password:
sending incremental file list
miner

sent 419.67M bytes  received 35 bytes  10.62M bytes/sec
total size is 419.43M  speedup is 1.00
```

Primjer kopiranja s udaljenog računala na lokalno:

```
$ rsync -azvh linux1@192.168.2.3:/home/linux1/extent /data/extent
linux1@192.168.2.3's password:
receiving incremental file list
```

```
extent

sent 43 bytes  received 419.67M bytes  8.84M bytes/sec
total size is 419.43M  speedup is 1.00
```

Za kriptirano slanje podataka može se koristiti protokol SSH dodavanjem opcije -e ssh:

```
$ rsync -azvhe ssh /data/qlen linux1@192.168.2.3:/home/linux1
linux1@192.168.2.3's password:
sending incremental file list
qlen

sent 10.49M bytes  received 35 bytes  2.33M bytes/sec
total size is 10.49M  speedup is 1.00
```

Za udaljeno je kopiranje potrebno svaki put upisati lozinku korisnika, što je moguće izbjeći korištenjem javnog i privatnog ključa bez lozinke za autentikaciju. Na ovaj način je jednostavno ostvariti periodičku izradu sigurnosnih kopija dodavanjem naredbe u *Cron*.

Automatizirana sigurnosna pohrana

Servis *Cron* se koristi za automatiziranje naredbi, u ovom slučaju automatizirat će se rsync kako bi se ostvarila periodička izrada sigurnosnih kopija. Naredbom `crontab-e` otvorit će se datoteka u koju se upisuje konfiguracija sljedećega formata:

`minute(0-59) sati(0-23) dan_u_mjesecu(1-31) mjesec(1-12) dan_u_tjednu(0-6) naredba`

Ta pravila postoje na svakom sustavu za korisnika root i omogućavaju da se u odgovarajući direktorij `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly`, `/etc/cron.monthly` jednostavno smjeste izvršne datoteke koje se trebaju izvršavati svaki sat, dan, tjedan ili mjesec.

Sljedeći *cron* sadrži naredbu koja će se izvršavati svake minute i svaki put će se izvršiti potpuna sigurnosna pohrana u novom direktoriju:

```
* * * * * rsync -a /data/ /backup/$(date '+\%y-\%m-\%d-\%H-\%M')

$ ls -al /backup/
total 51232
drwxr-xr-x  8 root root     4096 Oct 18 12:29 .
drwxr-xr-x 26 root root     4096 Oct 18 08:47 ..
drwxr-xr-x  2 root root     4096 Oct 18 12:01 18-10-18-12-26
drwxr-xr-x  2 root root     4096 Oct 18 12:01 18-10-18-12-27
drwxr-xr-x  2 root root     4096 Oct 18 12:01 18-10-18-12-28
drwxr-xr-x  2 root root     4096 Oct 18 12:01 18-10-18-12-29
```

Ako se izuzme dio za stvaranje novoga direktorija pri svakoj pohrani, posao u servisu *Cron* će prvi put napraviti potpunu sigurnosnu pohranu, a svaki sljedeći put će kopirati samo promijenjene i nove datoteke:

```
* * * * * rsync -a /data/ /backup/
ls -al /backup/
total 51208
drwxr-xr-x  2 root root     4096 Oct 18 12:01 .
drwxr-xr-x 26 root root     4096 Oct 18 08:47 ..
-rw-r--r--  1 root root 10485760 Oct 18 12:01 eqnl
-rw-r--r--  1 root root 10485760 Oct 18 12:01 leqn
-rw-r--r--  1 root root 10485760 Oct 18 12:01 lneq
-rw-r--r--  1 root root 10485760 Oct 18 12:00 qlen
-rw-r--r--  1 root root 10485760 Oct 18 12:00 qlne

$ touch /data/nova_datoteka

ls -al /backup/
total 51208
drwxr-xr-x  2 root root     4096 Oct 18 12:01 .
drwxr-xr-x 26 root root     4096 Oct 18 08:47 ..
-rw-r--r--  1 root root 10485319 Oct 18 12:36 eqnl
-rw-r--r--  1 root root 10485760 Oct 18 12:01 leqn
-rw-r--r--  1 root root 10485760 Oct 18 12:01 lneq
-rw-r--r--  1 root root        0 Oct 18 12:33 nova_datoteka
-rw-r--r--  1 root root 10485760 Oct 18 12:00 qlen
-rw-r--r--  1 root root 10485760 Oct 18 12:00 qlne
```

Naredba `rsync` može se kombinirati s naredbom `tar` koja sažima sve podatke prije sigurnosne pohrane:

```
* * * * * tar -cvf /tmp/backup/data_$(date '+\%y-\%m-\%d-\%H-\%M').tar
/data/ &&
rsync -a --remove-source-files /tmp/backup/ /backup/

$ ls -al /backup/
total 563340
drwxr-xr-x  2 root root     4096 Oct 18 13:06 .
drwxr-xr-x 26 root root     4096 Oct 18 08:47 ..
-rw-r--r--  1 root root 52439040 Oct 18 12:55 data_18-10-18-12-55.tar
-rw-r--r--  1 root root 52439040 Oct 18 12:57 data_18-10-18-12-57.tar
-rw-r--r--  1 root root 52439040 Oct 18 12:58 data_18-10-18-12-58.tar
-rw-r--r--  1 root root 52439040 Oct 18 12:59 data_18-10-18-12-59.tar
-rw-r--r--  1 root root 52439040 Oct 18 13:00 data_18-10-18-13-00.tar
```

Korištenjem mogućnost `--remove-source-files` obrisat će se izvorišne datoteke, u ovom slučaju s datotečnim nastavkom tar.

6.1.4. Sigurnosna pohrana baza podataka

Baze podataka, kao i ostale podatke, potrebno je redovito pohranjivati na sigurnu lokaciju da se može doći do podataka u slučaju havarije. Ovisno o svrsi baza podataka i poslužitelja potrebno je odrediti vremenski period između svakog izvršavanja sigurnosne pohrane.

Sigurnosna pohrana prvo izvozi bazu podatka kao logičke strukture baze podataka (kroz naredbe `create database`, `create table`) i sadržaj (naredbe `insert`), a zatim se ta datoteka kopira na udaljenu lokaciju. Izvezena baza podataka (ili više njih) je jedna datoteka koja sadrži sve podatke i kao takva može se uvesti u razne kompatibilne verzije sustava za upravljanje bazama poadataka. Ovakav način sigurnosne pohrane pogodan je za baze podataka s manje podataka, jer je sporiji uvoz i izvoz. Veće baze podataka potrebno je direktno integrirati sa sustavima za sigurnosnu pohranu.

Sigurnosna pohrana baze podataka na logički način može se izvršiti naredbom `mysqldump`, koja dolazi s instalacijom MySQL ili MariaDB baze podataka, ili koristeći specijalizirane alate, npr. *automysqlbackup*.

Izvoz baze podataka

Osnovna sintaksa naredbe za izvoz baze podataka je:

```
mysqldump -u <korisnicko_ime> -p <lozinka> <ime_baze_podataka> >
<ime_pohrane.sql>
```

Slijedi primjer izvoza baze podataka:

```
$ mysqldump -u root baza1 > /backup/ime_baze.sql

$ ls -al /backup/
total 12
drwxr-xr-x  2 root root 4096 Oct 18 14:20 .
drwxr-xr-x 26 root root 4096 Oct 18 08:47 ..
-rw-r--r--  1 root root 1290 Oct 18 14:46 baza1.sql
```

Za izvoz više baza podataka koristi se opcija `--databases`, a za izvoz svih baza koristi se opcija `--all-databases`:

```
$ mysqldump -u root --databases baza1 baza2 > /backup/baza1_baza2.sql
$ mysqldump -u root --all-databases > /backup/sve_baze.sq
```

Naredba `mysqldump` može se kombinirati s Cronom za izvršavanje periodičkih izvoza. Alternativa je korištenje alata *automysqlbackup* koji automatizira izvođenje izvoza jedne ili više baza podataka i sažima ih.

Uvoz baze podataka

Osnovna sintaksa naredbe za uvoz baze podataka:

```
mysqldump -u <korisnicko_ime> -p <lozinka> <ime_baze_podataka> <
<ime_pohrane.sql>
```

Za uvoz baze podataka potrebno se spojiti na bazu podataka naredbom `mysql`i stvoriti novu bazu s naredbom `create database restore_baze`:

```
$ sudo mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 6
Server version: 10.1.26-MariaDB-0+deb9u1 Debian 9.1

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE restore_baze;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> exit
Bye
```

Naredbom `mysql-p` uveze se pohranjena baza podataka:

```
$ sudo mysql -u root restore_baze < /backup/ime_baze.sql
```

Alat *automysqlbackup*

Instalacija se izvršava naredbom `apt-get`, a zadana konfiguracija nalazi se u datoteci `/etc/default/automysqlbackup`.

```
$ sudo apt-get install automysqlbackup

$ cat /etc/default/automysqlbackup

# Username to access the MySQL server e.g. dbuser
#USERNAME=`grep user /etc/mysql/debian.cnf | tail -n 1 | cut -d"=" -f2 | awk '
{print $1}'`

# Username to access the MySQL server e.g. password
#PASSWORD=`grep password /etc/mysql/debian.cnf | tail -n 1 | cut -d"=" -f2 |
awk '{print $1}'`
```

```
# Host name (or IP address) of MySQL server e.g localhost
DBHOST=localhost

# Backup directory location e.g /backups
BACKUPDIR="/var/lib/automysqlbackup"

# Email Address to send mail to? (user@domain.com)
MAILADDR="root"

# ============================================================
# === ADVANCED OPTIONS ( Read the doc's below for details )===
#============================================================

# List of DBBNAMES for Monthly Backups.
MDBNAMES="mysql $DBNAMES"

# List of DBNAMES to EXLUCDE if DBNAMES are set to all (must be in " quotes)
DBEXCLUDE=""

# Which day do you want weekly backups? (1 to 7 where 1 is Monday)
DOWEEKLY=6

# Choose Compression type. (gzip or bzip2)
COMP=gzip

# Which day do you want monthly backups? (01 to 31)
# If the chosen day is greater than the last day of the month, it will be done
# on the last day of the month.
# Set to 0 to disable monthly backups.
CONFIG_do_monthly="1"

# Set rotation of daily backups. VALUE*24hours
# If you want to keep only today's backups, you could choose 1, i.e. everything
older than 24hours will be removed.
CONFIG_rotation_daily=7

# Set rotation for weekly backups. VALUE*24hours
CONFIG_rotation_weekly=35

# Set rotation for monthly backups. VALUE*24hours
CONFIG_rotation_monthly=150
```

Slijedi objašnjenje opcija konfiguracije:

Opcija	Objašnjenje
USERNAME	Ime korisnika baze. Ako je korisnik root, USERNAME može ostati zakomentiran.
PASSWORD	Lozinka korisnika baze. Ako je korisnik root i ako nema loznike, PASSWORD može ostati zakomentiran.
DBHOST	Ime računala.
DBNAMES	Nazivi baza podataka koje će se izvesti. Prema zadanim postavkama to su sve baze podataka.
BACKUPDIR	Lokacija izvezenih baza podataka.
MAILADDR	Adresa elektroničke pošte za slanje obavijesti o izvršenim sigurnosnim pohranama.
MDBNAMES	Nazivi baza podataka koje će se izvesti svaki mjesec. Prema zadanim postavkama to su sve baze podataka koje su navedene u DBNAMES.
DBEXCLUDE	Baze podataka koje će se neće izvesti.
DOWEEKLY	Dan u tjednu za tjedno izvođenje. Vrijednosti su od 1 (ponedjeljak) do 7 (nedjelja).
COMP	Metoda sažimanja (gzip ili bzip2).
CONFIG_do_monthly	Dan u mjesecu za mjesečno izvođenje. Vrijednosti su od 1 do 31.
CONFIG_rotation_daily	Broj dana dnevne sigurnose pohrane koliko će se čuvati baze podataka prije nego što se obrišu.
CONFIG_rotation_weekly	Broj dana tjedne sigurnose pohrane koliko će se čuvati baze podataka prije nego što se obrišu.
CONFIG_rotation_monthly	Broj dana mjesečne sigurnose pohrane koliko će se čuvati baze podataka prije nego što se obrišu.

Prvo pokretanje izvršava se naredbom `automysqlbackup` nakon čega se stvaraju novi direktoriji u `/var/lib/automysqlbackup` koji odgovaraju dnevnim, tjednim i mjesečim sigurnosnim pohranama:

```
$ ls -al /var/lib/automysqlbackup/
total 20
drwxr-x---  5 root root 4096 Oct 19 14:48 .
drwxr-xr-x 47 root root 4096 Oct 19 14:48 ..
drwxr-xr-x  4 root root 4096 Oct 19 14:48 daily
drwxr-xr-x  2 root root 4096 Oct 19 14:48 monthly
drwxr-xr-x  4 root root 4096 Oct 19 14:48 weekly
```

```
$ ls -al /var/lib/automysqlbackup/daily/
total 16
drwxr-xr-x 4 root root 4096 Oct 19 14:48 .
drwxr-x--- 5 root root 4096 Oct 19 14:48 ..
drwxr-xr-x 2 root root 4096 Oct 19 14:48 ime_baze
drwxr-xr-x 2 root root 4096 Oct 19 14:48 restore_baze
```

Nakon prvog pokretanja napravit će se pohrana baza podataka i spremiti u direktorij `/var/lib/automysqlbackup/daily/`.

Ako se sigurnosna pohrana baza podataka kombinira sa sigurnosnom pohranom ostalih podataka, preporučeno je da se izvoz baza vrši prije pohrane.

6.1.5. Zanimljvi izvori

Poveznice:

- https://webmodelling.com/webbits/miscellaneous/bacula.aspx
- https://www.tecmint.com/rsync-local-remote-file-synchronization-commands/
- https://www.digitalocean.com/community/tutorials/how-to-backup-mysql-databases-on-an-ubuntu-vps
- https://www.linux.com/learn/how-do-painless-mysql-server-backups-automysqlbackup
- https://dev.mysql.com/doc/refman/8.0/en/backup-types.html

6.1.6. Vježba 15: Sigurnosna pohrana datoteka i baza podataka

1. Prije početka rada odaberite sliku stanja virtualnoga računala **slika_jedan** za početak vježbe.
2. Prijavite se na računalo kao korisnik **linux1**. U GUI-ju pokrenite **Terminal** (*Activities* → **Terminal**). Izvršite **su -** naredbu da postanete administrator (lozinka: linux1).
3. Instalirajte servis alat *automysqlbackup* naredbom **apt-get**:

   ```
   # apt-get install automysqlbackup
   ```

4. Dodajte sljedeće linije konfiguracije u datoteku **/etc/default/automysqlbackup**:

   ```
   # vim /etc/default/automysqlbackup
   CONFIG_do_monthly="01"
   CONFIG_do_weekly="5"
   CONFIG_rotation_daily=6
   CONFIG_rotation_weekly=35
   CONFIG_rotation_monthly=150
   ```

5. Objasnite svaku liniju prethodne konfiguracije.

_____

_____

6. Naredbom **automysqlbackup** pokrenite prvu sigurnosnu pohranu baza podataka.

```
# automysqlbackup
```

7. Nalaze li se pohranjene baze podataka u direktoriju **/var/lib/automysqlbackup/daily/**? Koji je datotečni nastavak pohranjenih baza podataka?

_____

_____

8. Uvezite jednu od pohranjenih baza podataka.

```
# mysql
MariaDB [(none)]> CREATE DATABASE uvoz_baze1;
MariaDB [(none)]> exit

# gzip -d /var/lib/automysqlbackup/daily/baza1/baza1_..sql*

# mysql -u root uvoz_baze1 <
/var/lib/automysqlbackup/daily/baza1/baza1_.*.sql
```

9. Instalirajte servise *bacula-server* i *bacula-client*. Tijekom instalacije odaberite **<yes>** na upit za konfiguraciju baze podataka.

```
# apt-get install bacula-server bacula-client
Configure database for bacula-director-sqlite3 with dbconfig-common?
<Yes>      <No>
```

10. Stvorite i dodijelite prava za sljedeće direktorije:

```
# mkdir -p /bacula/backup /bacula/restore
# chown -R bacula:bacula /bacula
# chmod -R 700 /bacula
```

11. U datoteku **/etc/bacula/bacula-dir.conf** servisa *bacula-director* unesite sljedeće konfiguracije za **Jobove** sigurnosne pohrane i oporavka:

```
# vim /etc/bacula/bacula-dir.conf

Job {
Name = "LokalnaPohrana"
Type = Backup
Level = Incremental
Client = debian-fd
FileSet = "PodaciZaPohranu"
Schedule = "DnevnaPohrana"
Storage = LokalnoSpremanjePodataka
Pool = File
JobDefs = "DefaultJob"
}

Job {
Name = "LokalniOporavak"
Type = Restore
Client=debian-fd
FileSet="PodaciZaPohranu"
Storage = LokalnoSpremanjePodataka
Pool = Default
Messages = Standard
Where = /bacula/restore
}
```

12. Objasnite svaku liniju prethodne konfiguracije.

13. U istu datoteku unesite podatke set datoteke koje će se pohranjivati:

```
FileSet {
  Name = "PodaciZaPohranu"
  Include {
    Options {
      signature = MD5
      compression = GZIP
     }
```

```
    File = /etc
    File = /home
    File = /var/lib/automysqlbackup
    }

    Exclude {
      File = /etc/UPower
     }
 }
```

14. U bloku **Schedule** definirajte koja će se vrsta sigurnosne pohrane izvršiti i u kojem terminu:

```
Schedule {
  Name = "DnevnaPohrana"
  Run = Full 1st sun at 00:04
  Run = Incremental mon-sun at 00:04
}
```

15. Objasnite svaku liniju prethodne konfiguracije.

_____

_____

_____

16. Dodajte konfiguraciju za blok Storage:

```
Storage {
  Name = LokalnoSpremanjePodataka
  Address = localhost
  SDPort = 9103
  Password = "sa$#5gfdas!~fasDSAF"
  Device = LokalniDirektorij
  Media Type = File1
  Maximum Concurrent Jobs = 10
}
```

17. Testirajte ispravnost konfiguracije sljedećom naredbom:

```
# bacula-dir -tc /etc/bacula/bacula-dir.conf
```

18. Za servis bacula-sd u konfiguracijsku datoteku **/etc/bacula/bacula-sd.conf** potrebno je dodati blok **Storage** i uskladiti lozinku u bloku **Director**:

```
Device {
  Name = LokalniDirektorij
  Media Type = File1
  Archive Device = /bacula/backup
  LabelMedia = yes
  Random Access = yes
  AutomaticMount = yes
  RemovableMedia = no
  AlwaysOpen = no
}

# ovaj dio se ne dodaje, vec se postojeca konfiguracija mijenja
Director {
  Name = debian-dir-1
  Password = "sa$#5gfdas!~fasDSAF"
}
```

19. Testirajte ispravnost konfiguracije sljedećom naredbom:

```
# bacula-sd -tc /etc/bacula/bacula-sd.conf
```

20. Za primjenu konfiguracije ponovno pokrenite servise *bacula- director* i *bacula-sd*:

```
# systemctl restart bacula-director
# systemctl restart bacula-sd
```

21. Provjerite kada će biti sljedeća sigurnosna pohrana kroz sučelje *Bacula Console*:

```
# bconsole
*

## izvršite naredbu label i odaberite LokalnoSpremanjePodataka:
* label
Automatically selected Catalog: MyCatalog
Using Catalog "MyCatalog"
The defined Storage resources are:
1: LokalnoSpremanjePodataka
2: File1
3: File2

## upišite proizvoljno ime Volumena i odaberite Pool File:
Enter new Volume name: l1
Defined Pools:
1: Default
2: File
3: Scratch
```

```
Select the Pool (1-3): 2

## sljedećom naredbom provjerite planirane sigurnosne pohrane
*     status director
```

22. Koje su sve sigurnosne pohrane nabrojane nakon izvršenja naredbe status director i kada će se izvršiti?

23. Testirajte ispravnost sigurnosne pohrane naredbom **run** i odabirom imena *Joba* LokalnaPohrana i potvrdom pomoću tipke **yes**:

```
*       run
Automatically selected Catalog: MyCatalog Using Catalog "MyCatalog"
A job name must be specified. The defined Job resources are:
1: LokalnaPohrana
2: LokalniOporavak
3: BackupClient1
4: BackupCatalog
5: RestoreFiles
Select Job resource (1-5): 1
Run Backup job
JobName: LokalnaPohrana
Level:  Incremental
Client: debian-fd
FileSet: PodaciZaPohranu
Pool:   File (From Job resource)
Storage: LokalnoSpremanjePodataka (From Job resource)
When:   2018-10-30 18:40:28
Priority: 10
OK to run? (yes/mod/no): yes
* m
```

24. Naredbom **m** otvorite poruku. Koji se sve detalji mogu saznati iz poruke?

25. Testirajte sigurnosni oporavak naredbom **restore** i odabirom točke 5 za oporavak zadnje pohrane. Nakon toga naredba **mark *** odabrat će sve datoteke i direktorije za oporavak, a naredba **done** potvrditi odabir:

```
* restore
```

```
Using Catalog "MyCatalog"

First you select one or more JobIds that contain files
to be restored. You will be presented several methods
of specifying the JobIds. Then you will be allowed to
select which files from those JobIds are to be restored.

To select the JobIds, you have the following choices:
1: List last 20 Jobs run
2: List Jobs where a given File is saved 3: Enter list of comma separated JobIds
to select
4: Enter SQL list command
5: Select the most recent backup for a client
6: Select backup for a client before a specified time
7: Enter a list of files to restore
8: Enter a list of files to restore before a specified time
9: Find the JobIds of the most recent backup for a client
10: Find the JobIds for a backup for a client before a specified time
11: Enter a list of directories to restore for found JobIds
12: Select full restore to a specified Job date
13: Cancel
Select item: (1-13): 5

$ mark *
2,391 files marked.
```

26. Potrebno je odabrati *Job* **LokalniOporavak** i potvrditi tipkom **yes**:

```
The defined Restore Job resources are:
1: LokalniOporavak
2: RestoreFiles
Select Restore Job (1-2): 1
Run Restore job
JobName:      LokalniOporavak
Bootstrap:    /var/lib/bacula/debian- dir.restore.1.bsr
Where: /bacula/restore
Replace:      Always
FileSet:      PodaciZaPohranu
Backup Client:       debian-fd
Restore Client: debian-fd
Storage:      LokalnoSpremanjePodataka
When:  2018-10-30 18:51:21
Catalog:      MyCatalog
Priority:     10
Plugin Options:
OK to run? (yes/mod/no): yes
```

27. Naredbom **status director** provjerite izvršenje oporavka. Je li se oporavak izvršio uspješno i koja je razlika u veličini sigurnosne pohrane i oporavka?

28. Naredbom **exit** izađite iz *Bacula Console*.

29. Nalaze li se oporavljene datoteke u direktoriju **/bacula/restore**?