SIGURNOST RAČUNALNIH SUSTAVA, ak. god. 2022./2023.
Četvrta laboratorijska vježba: Sigurnost mrežnih protokola i vatrozid

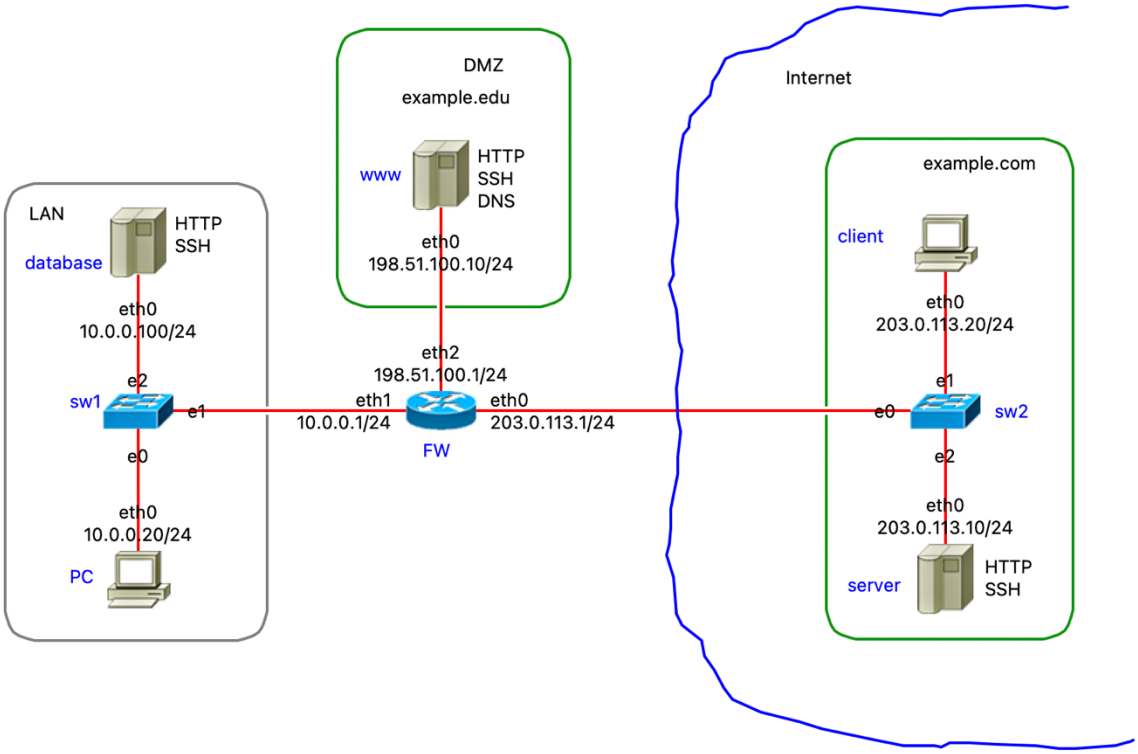
Logirajte se na virtualni stroj i dohvatite najnoviju verziju zadatka:

```
$ cd ~/srs-lab/Lab4
$ git pull
```

Ako direktorij `~/srs-lab` ne postoji, dohvatite ga naredbom:

```
$ git clone https://gitlab.tel.fer.hr/srs/srs-lab.git
$ cd srs-lab/Lab4
```

U datoteci `NETWORK.imn` se nalazi primjer male mreže s demilitariziranom zonom. Računala `client` i `server` su u vanjskoj mreži (Internetu), `www` je u DMZ, a `database` i `PC` se nalaze u zaštićenoj lokalnoj mreži LAN.



Kao korisnik `root` pozovite `imunes` s pripremljenom topologijom (`NETWORK.imn`) i pokrenite eksperiment, Experiment → Execute:

```
$ sudo imunes NETWORK.imn
```

Na svim čvorovima će se automatski pokrenuti mrežne usluge: Telnet, FTP i SSH.

Pokrenite Wireshark na sučelju `eth0` čvora `FW`.

Otvorite terminal na čvoru `client` (dvoklik na ikonu ili `sudo himage client` iz terminala na Ubuntu) i pokušajte se spojiti na 198.51.100.10 (`www`) korištenjem protokola TELNET i SSH. Za `login/password` upišite bilo što jer nas zanima samo početak prijave na sustav.

```
$ sudo himage client
client# telnet 198.51.100.10
client# ssh 198.51.100.10
```

Što se vidi u Wiresharku? (Možete koristiti "Follow TCP stream")

Pokretanje web poslužitelja i DNS poslužitelja

Pozovite shell skriptu `prepare.sh` koja će konfigurirati i pokrenuti DNS poslužitelj na čvoru `www` te WEB poslužitelje na čvorovima `www`, `server` i `database`:

```
$ sudo ./prepare.sh
```

Pokrenute usluge možete provjeriti na pojedinom čvoru (lokalno) naredbama `ps` (ispis pokrenutih procesa) i `netstat` (ispis *portova* / pristupa):

```
$ sudo himage www
www# ps -ax
www# netstat -anp4
```

Konfiguracija vatrozida

Vaš je zadatak konfigurirati vatrozid (engl. firewall) na `FW` te provjeriti dostupnost usluga iz vanjske mreže ("Interneta") i iz lokalne mreže ("LAN") u skladu sa sljedećim zahtjevima:

DMZ:

- Web poslužitelju i DNS poslužitelju na čvoru `www`, koji se nalazi u demilitariziranoj zoni, se može pristupiti s bilo koje adrese (iz Interneta i iz lokalne mreže).
- SSH poslužitelju na čvoru `www` se može pristupiti samo iz lokalne mreže LAN.
- S `www` je dozvoljen pristup poslužitelju `database` (LAN) na TCP portu 10000 te pristup DNS poslužiteljima u Internetu (UDP i TCP port 53), a sve ostalo je zabranjeno.
- Pristup svim ostalim adresama i poslužiteljima u DMZ je zabranjen.

LAN:

- Pristup SSH poslužitelju na čvoru `database`, koji se nalazi u lokalnoj mreži LAN, dozvoljen je samo računalima iz mreže LAN.
- Pristup web poslužitelju na čvoru `database` (koji sluša na TCP *portu* 10000) dozvoljen je isključivo s računala `www` koje se nalazi u DMZ (i računalima iz mreže LAN).
- S računala `database` je zabranjen pristup svim uslugama u Internetu i u DMZ.
- S računala iz lokalne mreže (osim s `database`) se može pristupati svim računalima u Internetu ali samo korištenjem protokola HTTP (tcp/80) i DNS (udp/53 i tcp/53).
- Pristup iz vanjske mreže u lokalnu LAN mrežu je zabranjen.

`FW`:

- Na `FW` je pokrenut SSH poslužitelj kojem se može pristupiti samo iz lokalne mreže i to samo s čvora `PC`.
- Pristup svim ostalim uslugama (*portovima*) na čvoru `FW` je zabranjen.

Internet:

- Na čvoru `server` (u Internetu) su pokrenuti web poslužitelj i SSH poslužitelj kojima se može pristupiti s bilo koje adrese.

Skripta za konfiguriranje vatrozida

U direktoriju se nalazi *shell* skripta za konfiguriranje vatrozida, `FW.sh`, u koju trebate dodati svoja pravila u skladu s navedenim zahtjevima.

Skriptu kopirajte na čvor `FW` naredbom `hcp`:

```
$ sudo hcp FW.sh FW:
```

i izvedite na virtualnom čvoru `FW` pozivanjem naredbe `himage`:

```
$ sudo himage FW sh ./FW.sh
```

Upute za hcp i himage možete pronaći na stranici:
https://github.com/imunes/imunes/wiki/Making-scripts-for-IMUNES.

Provjerite dostupnost usluga prema zahtjevima iz zadatka. Dostupnost poslužitelja možete provjeriti skeniranjem naredbom `nmap` ili spajanjem na poslužitelj odgovarajućim klijentskim aplikacijama.

Testiranje postavljenih pravila vatrozida spajanjem na poslužitelje

Iz Ubuntu terminala možete pokrenuti izvođenje naredbe na virtualnom čvoru pozivom:

```
$ sudo himage naziv_čvora naredba arg1 arg2 ...
```

Na primjer, s `PC` se pokušajte spojiti protokolima Telnet i SSH na `server` i `www`:

```
$ sudo himage PC telnet 203.0.113.10
$ sudo himage PC ssh 198.51.100.10
```

Izvođenje naredbi na virtualnom čvoru možete izvesti i dvostrukim klikom na ikonu čvora što će otvoriti terminal i pokrenuti ljusku (*shell*) na tom čvoru.

Provjera dostupnosti web poslužitelja na računalu `www` s računala `client` i s računala `PC`:

Otvorite terminal i kao korisnik root (sudo su) pozovite:

```
# himage client
client# curl http://www.example.edu/index.html
client# curl http://198.51.100.10/index.html

# himage PC
PC# curl http://www.example.edu/index.html
PC# curl http://10.0.0.100/index.html
```

Provjera dostupnosti DNS poslužitelja na čvoru `www` s čvora `client`:

```
# himage client
client# host www.example.com
```

Skeniranje alatom nmap

Skeniranje dostupnih servisa može se provesti i alatom `nmap`. Korištenjem alata Wireshark možete vidjeti promet koji alat `nmap` generira.

Na primjer, provjera dostupnosti TCP usluga u demilitariziranoj zoni (`www`) računalima iz Interneta (`client`):

```
$ sudo himage client nmap -n -Pn "-p20-25,53,80,443" 198.51.100.10
```

Provjera dostupnosti usluga u demilitariziranoj zoni računalima iz privatne mreže (čvor `PC`):

```
$ sudo himage PC nmap -n -Pn "-p20-25,53,80,443" 198.51.100.10
```

Istražite i isprobajte sljedeće opcije u alatu `nmap`:

- skeniranje TCP i UDP portova
- TCP syn scan
- detekcija operacijskog sustava (-O)
- detekcija verzija servisa (-sV)
- općeniti scan (-A opcija)

Rezultati laboratorijske vježbe

Kao rezultat laboratorijske vježbe na `ferko` trebate predati **ZIP arhivu** koja će sadržavati:

- **opis.txt** - sažeti izvještaj o laboratorijskoj vježbi (u obliku txt datoteke) koji sadrži postupak rješavanja zadatka
- **FW.sh** - vaša verzija datoteke FW.sh