SIGURNOST RAČUNALNIH SUSTAVA, ak. god. 2021./2022.

4. laboratorijska vježba: Sigurnost mrežnih protokola i vatrozid

Prije rješavanja zadataka logirajte sa na virtualni stroj i dohvatite najnoviju verziju:

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

Ako naredba "git pull" javi grešku tipa:

```
fatal: unable to access https://gitlab.tel.fer.hr/sigkom/sigkom-lab.git/:
server certificate verification failed. CAfile: none CRLfile: none
```

Pozovite:

```
$ sudo su
# echo $(echo -n | openssl s_client -showcerts -connect gitlab.tel.fer.hr:443 \
      2>/dev/null | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p') \
      >> /etc/ssl/certs/ca-certificates.crt
```

Nakon toga bi "git pull" trebao ispravno dohvatiti sve datoteke. Dohvatite najnoviju verziju zadatka:

```
$ git pull
```

U datoteci NETWORK.imn se nalazi primjer male mreže s demilitariziranom zonom. Računala `PC1` i `PC2` su u vanjskoj mreži (Internetu), `server` je u DMZ, a `host` i `admin` se nalaze u zaštićenoj lokalnoj mreži LAN.

Pokrenite IMUNES eksperiment:

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

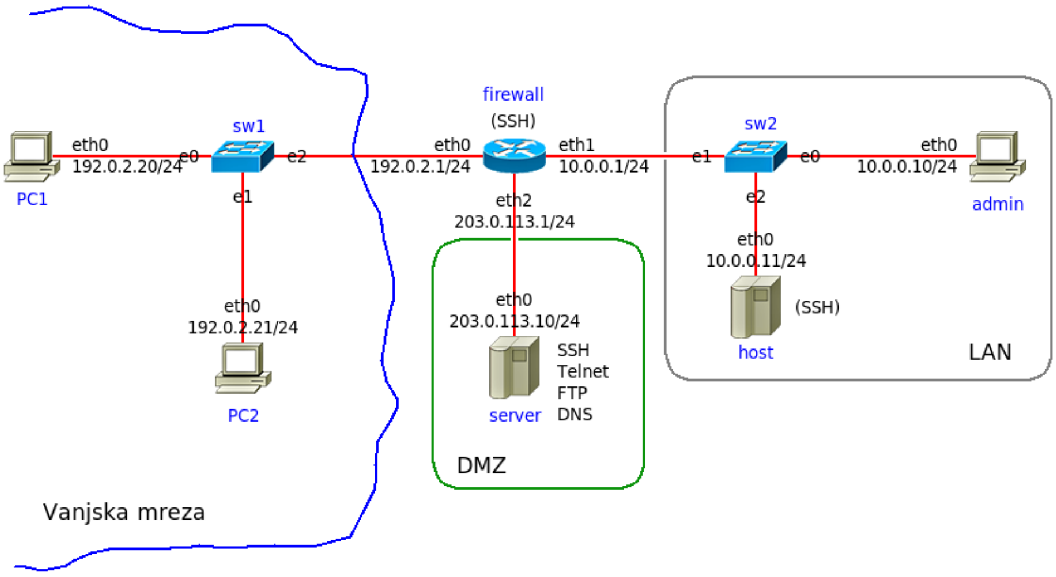
Pokretanjem eksperimenta, na svim čvorovima će se automatski pokrenuti mrežne usluge: Telnet, FTP i SSH.

Pokrenite Wireshark na sučelju eth0 čvora `firewall`.

Otvorite terminal na `PC1` (dvoklik na ikonu ili `sudo himage PC1` iz terminala na Ubuntu) i (sa čvora `PC1`) pozovite telnet i ssh na 203.0.113.10 (`server`).

```
$ sudo himage PC1
PC1# telnet 203.0.113.10
...
PC1# ssh 203.0.113.10
...
```

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



Slika mreže NETOWORK.imn

Konfiguracija vatrozida

Vaš je zadatak konfigurirati vatrozid (`firewall`) te provjeriti dostupnost usluga iz vanjske mreže (Interneta) i iz lokalne mreže.

Zahtjevi:

- računala iz lokalne mreže (LAN) imaju neograničeni pristup poslužiteljima u DMZ i Internetu,
- pristup iz vanjske mreže u lokalnu LAN mrežu je zabranjen,
- iz vanjske mreže (Interneta) dozvoljen je pristup poslužitelju `server` u DMZ korištenjem protokola SSH (tcp port 22) i DNS (udp i tcp port 53),
- s poslužitelja `server` je dozvoljen pristup DNS poslužiteljima u Internetu (UDP i TCP port 53),
- s poslužitelja `server` je dozvoljen pristup poslužitelju `host` (u LAN) korištenjem protokola SSH,
- SSH pristup vatrozidu `firewall` je dozvoljen samo s računala `admin` (LAN),
- dodajte "anti-spoofing" pravila.

Skripte za konfiguriranje vatrozida

U direktoriju se nalazi "shell skripta" za konfiguriranje vatrozida: `FW.sh`.

Svoja pravila upisujete na mjesta označena s:

```
# <--- Dodajte pravila
```

Skripta se mora kopirati na čvor `firewall` i na njemu izvesti:

```
$ sudo hcp FW.sh firewall:
$ sudo himage firewall sh ./FW.sh
```

Kopiranje se izvodi naredbom `hcp`, a naredbe se izvode na virtualnom čvoru pozivanjem `himage`.

Testiranje postavljenih pravila vatrozida spajanjem na poslužitelje

Provjerite dostupnost usluga spajanjem s virtualnih čvorova.

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

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

Na primjer, s `PC1` se pokušajte spojiti protokolima Telnet i SSH na `server` i `host`:

```
$ sudo himage PC1 telnet 203.0.113.10
$ sudo himage PC1 ssh 10.0.0.11
```

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

Provjerite dostupnost svih usluga prema zahtjevima iz zadatka.

Skeniranje alatom nmap

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

Primjer, provjera dostupnosti usluga u demilitariziranoj zoni (`server`) računalima iz Interneta (`PC1`):

```
$ himage PC1 nmap -n -Pn "-p20-25,53,80,443" 203.0.113.10
```

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

```
$ sudo himage admin nmap -n -Pn "-p20-25,53,80,443" 203.0.113.10
```

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 **trebate predati** sljedeće podatke kroz sustav Moodle nakon rješavanja vježbe:

- **izvještaj** o laboratorijskoj vježbi **u formular** na Moodlu (najviše **300 riječi**) koji sadrži postupak rješavanja zadatka
- **ZIP arhivu** koja sadrži konačnu verziju datoteke **FW.sh**

Alati korisni za izradu ove vježbe:

- `ping` - provjera mrežne povezivosti.
- `nmap` - skeniranje računala i servisa.
- `netstat` - pregled mrežnih servisa koji su trenutno pokrenuti na računalu.
- `service` - pokretanje i zaustavljanje servisa na operacijskom sustavu Linux.
- `iptables` - konfiguracija vatrozida na operacijskom sustavu Linux.
- `wireshark` - analiza mrežnog prometa.