Zadatak 1)

Pinging 192.168.56.101 with 32 bytes of data: Reply from 192.168.56.101: bytes=32 time<1ms TTL=64 ...
Pinging mail.fer.hr [161.53.72.233] with 32 bytes of data: Reply from 161.53.72.233: bytes=32 time=3ms TTL=121 ...
Pinging 161.53.19.1 with 32 bytes of data: Reply from 161.53.19.1: bytes=32 time=4ms TTL=246 ...
Pinging imunes.net [161.53.19.8] with 32 bytes of data: Reply from 161.53.19.8: bytes=32 time=4ms TTL=57 ...

Početna vrijednost brojača TTL ovisi o operacijskom sustavu kojega pingamo. Pomoću TTL-a možemo samo pretpostaviti o kojem je operacijskom sustavu riječ (nismo nikada u potpunosti sigurni).

IP	TTL	TTL max	OS
192.168.56.101	64	64	Linux/Unix
mail.fer.hr	121	128	Windows
161.53.19.1	246	254	AIX/Solaris
imunes.net	57	64	Linux/Unix

Zadatak 2)

• Pomoću alata nmap možemo skenirati sve TCP i UDP portove pozivom naredbe " nmap -sU -sT 192.168.56.101 ".

```
Starting Nmap 7.91
...
Not shown: 1933 closed ports, 66 open|filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:23:FF:69 (Oracle VirtualBox virtual NIC)

... scanned in 1256.35 seconds
```

Pokrenuta naredba nije promijenila ispis watch naredbe na virtualnome stroju.

• Pomoću alata nmap možemo napraviti TCP syn scan pozivom naredbe " nmap -sS 192.168.56.101 "

```
Starting Nmap 7.91
...
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:23:FF:69 (Oracle VirtualBox virtual NIC)

... scanned in 1.29 seconds
```

Pokrenuta naredba promijenila je ispis watch naredbe na virtualnome stroju na taj način da se u listi aktivnih Internet konekcija pojavio redak:
" tcp 0 0 192.168.56.101:22 192.168.56.1:53031 SYN_RECV"

• Pomoću alata nmap možemo detektirati operacijski sustav pozivom naredbe " nmap -O 192.168.56.101 "

```
Starting Nmap 7.91
...
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:23:FF:69 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

... scanned in 4.12 seconds
```

Pokrenuta naredba promijenila je ispis watch naredbe na virtualnome stroju na taj način da su se u listi aktivnih Internet konekcija pojavili redci:

```
tcp      0     0 192.168.56.101:22      192.168.56.1:49134     SYN_RECV
tcp      0     0 192.168.56.101:22      192.168.56.1:49125     SYN_RECV
... (još 5 redaka) ...
tcp      0     0 192.168.56.101:22      192.168.56.1:51318     SYN_RECV
```

Promjene u ispisu watch naredbe se događaju jer radimo uspostavu tcp veze na različitim portovima kako bi prikupili podatke o virtualnom stroju i servisima.

• Pomoću alata nmap možemo detektirati verziju servisa pozivom naredbe " nmap -sV 192.168.56.101 "

```
Starting Nmap 7.91
...
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
MAC Address: 08:00:27:23:FF:69 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

... scanned in 2.64 seconds
```

Pokrenuta naredba promijenila je ispis watch naredbe na virtualnome stroju na taj način da se u listi aktivnih Internet konekcija pojavio redak:

"tcp 0 0 192.168.56.101:22 192.168.56.1:45185 SYN_RECV "

• Pomoću alata nmap možemo napraviti općeniti scan pozivom naredbe " nmap -A 192.168.56.101 "

Pokrenuta naredba promijenila je ispis watch naredbe na virtualnome stroju na taj način da su se u listi aktivnih Internet konekcija pojavilo 13 redaka s različitim portovima i stanjima (SYN_RECV ili TIME_WAIT).

Uspoređujemo li rezultate skeniranja izvana i iznutra jedina razlika je da skeniranje izvana dodatno ispisuje MAC adresu virtualnog stroja. Drugih razlika nema.

Zadatak 4)

Na računalu "pc" koje se nalazi u Internetu potrebno je kreirati SSH par ključeva. Poslužitelj "mail-relay" potrebno je konfigurirati tako da sluša na vratima 1111, a poslužitelj "mail" potrebno je konfigurirati tako da sluša na vratima 2222. Konfiguracije se rade u tekstualnim datotekama naziva sshd_config za svakog poslužitelja. Također, osim postavljanja novih portova, potrebno je i omogućiti " HostKey " polje.
Kako bi bolje zaštitili ssh poslužitelje možemo zabraniti direktno povezivanje root korisnika na njih " PermitRootLogin no" ili postaviti maksimalan broj mogućih pokušaja prijave " MaxAuthTries 3 " ili postaviti vremensko ograničenje prilikom autentifikacije korisnika " LoginGraceTime 20s "

Zadatak 5)

Pokretanjem "aircrack-ng SUI1_WEP.cap" i "aircrack-ng SUI2_WEP.cap" pokrećemo alat pomoću kojeg saznajemo lozinke kojima su datoteke šifrirane. Lozinke su prikazane u heksadekadskom formatu: "88:E2:F8:53:6E:99:27:35:BC:69:C8:4C:7E" i "D5:71:92:38:04:EE:50:FA:E2:D2:0D:F7:DC". Datoteku SUI1_WEP.cap učitavamo u Wireshark alat i dešifriramo ju pronađenim ključem. Odabiremo prvi TCP paket sa poslužitelja 161.53.19.80 i odabiremo opciju "Follow TCP stream". Možemo vidjeti da je HTTP zahtjev napisan u XML formatu, a datoteka koja se dohvaća je "SUI-disk1.vmdk". Protokol je HTTP preko TCP-a.

Razlika između navedenih .cap datoteka je da u prvoj datoteci su uhvaćeni TCP podaci između 2 računala. Druga datoteka sadrži mnogo ARP zahtjeva koji na početku nasumično pretražuju IP adrese s ciljem pronalaska IP adrese koja se koristi. Kada se takva adresa nađe onda se za nju zagušuje promet broadcastom "Who has 161.53.19.2? Tell 161.53.19.221". Riječ je o DoS napadu.