Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu
Zavod za elektroničke sustave i obradbu informacija
Laboratorij za sustave i signale

Sustavi za praćenje i vođenje procesa

Vježba 4: **Internet**

O ČEMU JE RIJEČ?

U ovoj vježbi pažnja će se posvetiti osnovnim konceptima vezanim uz Internet. Naglasak je dan na prijenosni i aplikacijski sloj OSI referentnog modela odnosno promatranje paketnog prometa, mrežnih vrata i njihovih uloga, uspostave prijenosa, te konfiguriranja vatrozida.

ŠTO BI TREBALO ZNATI NAKON VjEŽBE

Nakon vježbe očekuje se razumijevanje funkcija prijenosnog sloja OSI referentnog modela koji se javlja na Internetu, koncepta mrežnih vrata te poznavanje osnova filtriranja mrežnih paketa.

DODATNA LITERATURA

Materijali s predavanja i skripta o temi: Internet

VJEŽBU PRIPREMILI

P. Pale, A. Sović, J. Petrović, K. Skračić

SADRŽAJ

1. 1. Uvod

Ova vježba radi se na dostupnoj Linux distribuciji koji se učitava izravno s DVD-a (*live boot*).

1.1. Zašto Linux?

Na računalima u labosu instaliran je Windows operacijski sustav, u kojem se također mogu izvoditi odgovarajuće naredbe (drugačije sintakse), odnosno u kojemu se također može odraditi vježba. Ipak, studenti na laboratorijskim računalima nemaju dovoljna prava da bi izvodili potrebne naredbe kako ne bi poremetili mrežne postavke u labosu. Budući da Windowse nije moguće koristiti kao *live-boot* operacijski sustav, u vježbi se koristi neka distribucija Linux operacijskog sustava u *live-boot* načinu rada, odnosno bez instaliranja na čvrsti disk.

1.2. Imajte na umu…

Ikona terminala

Sve naredbe koje se koriste u vježbi unose se u *terminal* prozor odnosno komandnu liniju, koju možete otvoriti klikom na odgovarajuću ikonu na radnoj površini (ili kraticom Alt+F2 i unosom naredbe *gnome-terminal*). Imajte na umu da:

- se pri ***live boot*** načinu rada **ne koristi čvrsti disk** nego se sve promjene pohranjuju u radnu memoriju i **kod ponovnog pokretanja gube**.
- se **tipkovnica** mijenja tako da odaberete Applications/Settings/Keyboards/Layouts, a potom **dodajte hrvatsku tipkovnicu i uklonite englesku iz popisa (vrijedi za Kali distribuciju)**.

1.3. Potrebni alati

Prije početka rada na vježbi dodajte odgovarajući repozitorij i instalirajte potrebne alate sljedećim naredbama:

```
echo "deb http://http.kali.org/kali kali-rolling main non-free contrib" > /etc/apt/sources.list
apt-get update
apt-get install zenmap apache2 wireshark dnsutils gedit
```

Potvrdno odgovorite na sve eventualne upite pri instalaciji.

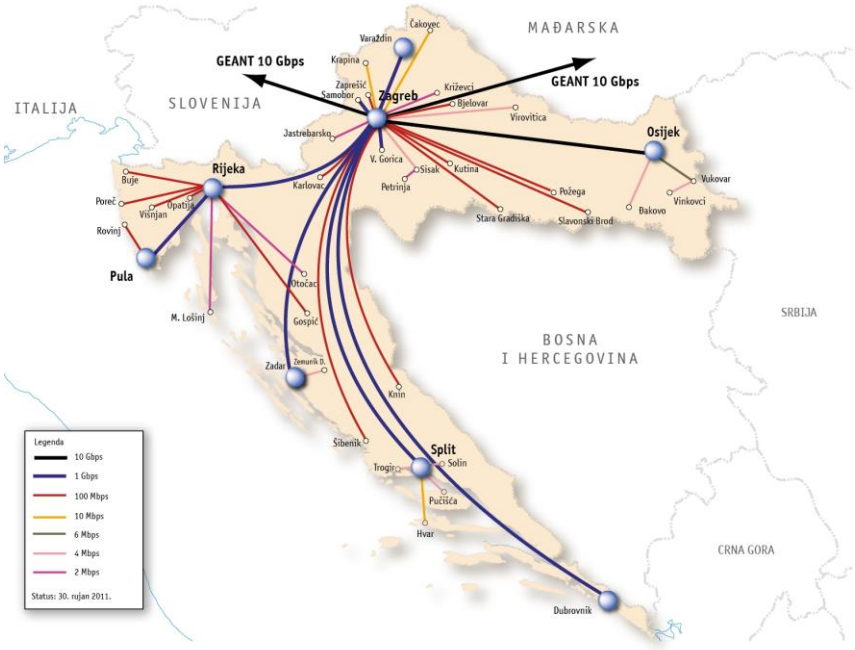
2. Mrežni sloj

2.1. Usmjeravanje IP paketa na Internetu

FER je spojen na CARNet-ovu računalnu mrežu i preko nje ostvaruje spoj prema Internetu.

Mreža CARNet privatna je WAN mreža hrvatske akademske i znanstveno-istraživačke zajednice. Mrežnu infrastrukturu posjeduje CARNet ustanova, a bakrene i optičke veze zakupljene su od Hrvatskih telekomunikacija. Ministarstvo znanosti i tehnologije Republike Hrvatske osnovalo je CARNet kao ustanovu kojoj je djelatnost razvoj, izgradnja i održavanje mreže.

Na usmjerniku (engl. router) u distribucijskom čvorištu SRCE, Zagreb ostvarena je veza prema europskoj istraživačkoj mreži GEANT brzinom 20Gbit/s od 2014. godine.



Slika 1. CARNet mreže u Hrvatskoj s prikazanim linkovima prema svijetu
(preuzeto sa http://www.carnet.hr/network/)

3. Transportni sloj: TCP i UDP - koncept portova

Kako je već rečeno, svako sučelje računala prema mreži ima svoju IP adresu. Korištenjem koncepta *portova* (mrežnih vrata) omogućeno je da se na jednom sučelju može ostvariti više istovremenih veza prema više različitih aplikacija. Zbog toga je moguće da se na računalu sa jednom IP adresom nalazi više mrežnih servisa (npr. *telnet*, *ftp* i *web* servis) jer svaki takav servis se javlja na drugom portu.

Većini je servisa dogovorom određen port na kojem se nalaze. Portovi <1024 su stoga rezervirani odnosno već je dogovoreno čemu služe. Niže su navedeni servisi vezani uz prvih 110 portova. Tako se primjerice *ftp* nalazi na portu 21, dok se *www* nalazi na portu 80.

Popis servisa i pripadajućih im portova:

```
tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
```

```
msp             18/tcp                          # message send protocol
msp             18/udp                          # message send protocol
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp                          # SSH Remote Login Protocol
telnet          23/tcp
# 24 - private
smtp            25/tcp          mail
# 26 - unassigned
time            37/tcp          timserver
time            37/udp          timserver
rlp             39/udp          resource        # resource location
nameserver      42/tcp          name            # IEN 116
whois           43/tcp          nicname
re-mail-ck      50/tcp                          # Remote Mail Checking Protocol
re-mail-ck      50/udp                          # Remote Mail Checking Protocol
domain          53/tcp          nameserver      # name-domain server
domain          53/udp          nameserver
mtp             57/tcp                          # deprecated
bootps          67/tcp                          # BOOTP server
bootps          67/udp
bootpc          68/tcp                          # BOOTP client
bootpc          68/udp
tftp            69/udp
gopher          70/tcp                          # Internet Gopher
gopher          70/udp
rje             77/tcp          netrjs
finger          79/tcp
www             80/tcp          http            # WorldWideWeb HTTP
www             80/udp                          # HyperText Transfer Protocol
link            87/tcp          ttylink
kerberos        88/tcp          kerberos5 krb5  # Kerberos v5
kerberos        88/udp          kerberos5 krb5  # Kerberos v5
supdup          95/tcp
# 100 - reserved
hostnames       101/tcp         hostname        # usually from sri-nic
iso-tsap        102/tcp         tsap            # part of ISODE.
csnet-ns        105/tcp         cso-ns          # also used by CSO name server
csnet-ns        105/udp         cso-ns
rtelnet         107/tcp                         # Remote Telnet
rtelnet         107/udp
pop-2           109/tcp         postoffice      # POP version 2
pop-2           109/udp
pop-3           110/tcp                         # POP version 3
pop-3           110/udp
```

Zadatak 1: Koji port koristi SMTP (Simple Mail Transport Protocol) protokol za slanje e-maila?

Zadatak 2: Korištenjem alata Zenmap (poziva se naredbom *zenmap* iz terminala) doznajte koji su portovi "otvoreni" na računalu `diana.zesoi.fer.hr` i koji operacijski sustav to računalo koristi. (Uputa: u polje *Target* unesite ime ciljnog računala a pod *Profil* odaberite *Intense scan*). Koji operacijski sustav koristi ciljno računalo? Koju inačicu SSH protokola i Apache web servera koristi ciljno računalo? Kako možete u praksi iskoristiti te informacije?

Ta se radnja naziva skeniranje portova i ne preporuča se raditi na drugim računalima. Naime, ovakvo ponašanje na mreži nije "pristojno" jer se može shvatiti kao traženje potencijalnih sigurnosnih rupa na računalu kojem se skeniraju portovi. Ponovite naredbu za skeniranje računala na adresi 161.53.64.4.

Koje TCP ili UDP konekcije vaše računalo očekuje (*listening*) ili je uspostavilo vezu (*established*) možete saznati naredbom (iz komandne linije):

```
netstat –tan | more
```

Ovom naredbom moguće je saznati koji portovi na vašem računalu su otvoreni. Inače je potrebno voditi računa da svaki otvoreni port može predstavljati određeni sigurnosni rizik. Naime pošto je aplikacija otvorena za konekcije i očekuje pakete moguće je da joj se «podvale» paketi koji će kompromitirati njeno uobičajeno djelovanje.

Zadatak 3: Zatvorite web preglednik i sve ostale prozore osim terminala i pričekajte dvije minute. Sada izvršite prethodnu naredbu. Potom otvorite web preglednik i otvorite proizvoljni *youtube* video. Pričekajte 30-ak sekundi te potom opet izvršite prethodnu naredbu. Sada ponovno zatvorite web preglednik, pričekajte jednu minutu i ponovno izvršite istu naredbu.

Komentirajte ispis prethodne naredbe. Što sve iz njega saznajete? U čemu se razlikuju ispisi koje ste dobili i kako to tumačite?

3.1. Transport Control Protocol (TCP)

IP koji je implementiran na mrežnom sloju je *bespojnog* (*connectionless*) tipa. Podaci se rastave na pakete koji se zatim šalju prema odredištu međutim IP ne vodi računa o tome da li su ti paketi uopće stigli i kada stignu da li su pravilno poredani onako kako su i poslani.

Za takve stvari se brine TCP sa sloja iznad tj. *prijenosnog sloja*. TCP je *connection-oriented* protokol i osim što uvodi koncept portova, TCP se brine za uspostavljanje i prekidanje veze te potvrđivanje primljenih paketa i njihov pravilan poredak. Veze se uspostavljaju *point-to-point* između dva računala tj. ne podržavaju se *broadcast* veze Ukratko, TCP je dizajniran da osigura pouzdanu vezu preko nepouzdane mreže.

Svaka TCP konekcija između dva računala je identificirana parom (izvorišni port, odredišni port). Moguće je imati više veza između dva računala koje imaju isti odredišni port ali će tada svaka od njih imati različiti izvorišni (primnerice dva *internet browsera* kontaktiraju isti *web server*).

Sve bitne stvari ovog protokola su vidljive iz zaglavlja paketa. Tamo se nalazi: izvorišni port, odredišni port, sequence broj (*seq*), acknowledgement broj (*ack*) i par zastavica (*flagova*). Od zastavica će nam biti bitne SYN, ACK i FIN. SYN se koristi za uspostavljanje veze. ACK označava da li je *ack* broj valjan (tj. da li se koristi).

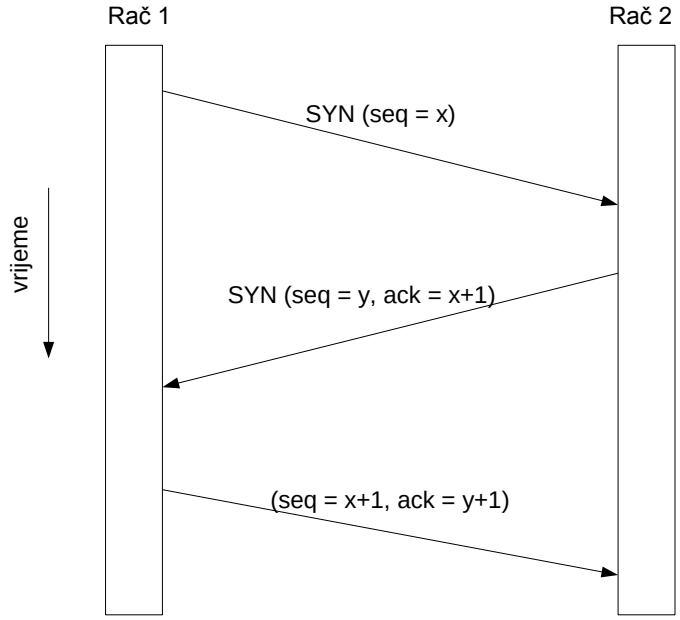
Da bi se osigurao siguran prijenos podataka prvo se mora uspostaviti veza između dva računala. Analogija postoji sa korištenjem telefona (prije početka razgovora mora se uspostaviti veza). Svi paketi koji se šalju sada imaju svoj redni broj (*seq*). Time se zna redoslijed koji ti paketi moraju imati. Isto tako ako stigne dva puta paket sa istim rednim brojem onda se zna da se jedan mora odbaciti. Kod slanja sljedećeg paketa *seq* se uveća za broj bajtova prethodno poslanih.

Za svaki poslani paket se traži da se potvrdi njegov primitak. Ako potvrda ne stigne paket se šalje ponovno. Potvrda dolazi u paketu kojem je zastavica ACK=1 a *ack* pokazuje na sljedeći *seq* broj koji se očekuje (time se potvrđuju svi prethodni *seq* brojevi). Nije potrebno za svaki primljeni paket slati posebni paket koji sadrži samo potvrdu. Moguće je poslati potvrdu da unutar paketa koji je inače trebao biti poslan na drugu stranu. Dakle računalo kada primi paket ne šalje odmah potvrdu nego čeka neko vrijeme da li će možda

dobiti zahtjev da paket mora poslati na drugu stranu i ako to dobije tada potvrdu prilijepi njemu. Ovaj postupak naziva se *piggybacking* i dosta pridonosi efikasnosti.

- **Uspostava veze**

  Prije nego krene razmjena podataka potrebno je uspostaviti vezu. Pri tome se razmijene početne vrijednosti *seq* polja tako da se zna od kuda kreće brojanje paketa. Šalje se SYN=1, ACK=0 te odgovarajući početni *seq* broj. Odgovor stiže u obliku SYN=1, ACK=1, *ack* polje potvrđuje *seq* broj i pri tom se šalje svoj početni *seq* broj čija se potvrda očekuje kao *piggyback* na prvom paketu s podacima.



Slika 2. Uspostava veze

- **Raskidanje veze**

  Šalje se paket s FIN=1 i znači da nema više podataka za slati. Ako ne stigne odgovor potvrde u određenom roku veza se raskida. Isto to radi i druga stana. Iako je TCP full-duplex prijenos, veza se prekida kao dva simplexa.

Zadatak 4: Na primjeru komuniciranja Internet preglednika sa nekim web serverom (npr. www.fer.hr) koristeći alat *Wireshark* (pokreće se naredbom *wireshark* iz terminala) uhvatite pakete kojima se uspostavlja veza, prenose podaci i prekida veza. Uočiti kako se paketi međusobno potvrđuju. Koji port je Internet preglednik otvorio da bi primao odgovore od web servera? Koliko je zasebnih konekcija bilo potrebno da se svi podaci (tekst, slike) prenesu?

Pomoć: *Wireshark* je alat koji omogućava snimanje svog paketnog prometa koji se odvija na računalu (odlaznih i dolaznih paketa). Po pokretanju alata potrebno je odabrati *Capture/Interfaces*, odabrati odgovarajuće aktivno mrežno sučelje (u slučaju rada u labosu to će biti ono vezano uz IP adresu 161.53.64.X), odabrati *Start*, potom u web pregledniku posjetiti stranicu www.fer.hr i nakon sto se stranica učita u *Wiresharku* zaustaviti praćenje prometa odabirom *Capture/Stop*. Među prikupljenim paketima potrebno je pronaći TCP pake koji prenose SYN, ACK i FIN zastavice odnosno uspostavljaju i raskidaju vezu. Iz

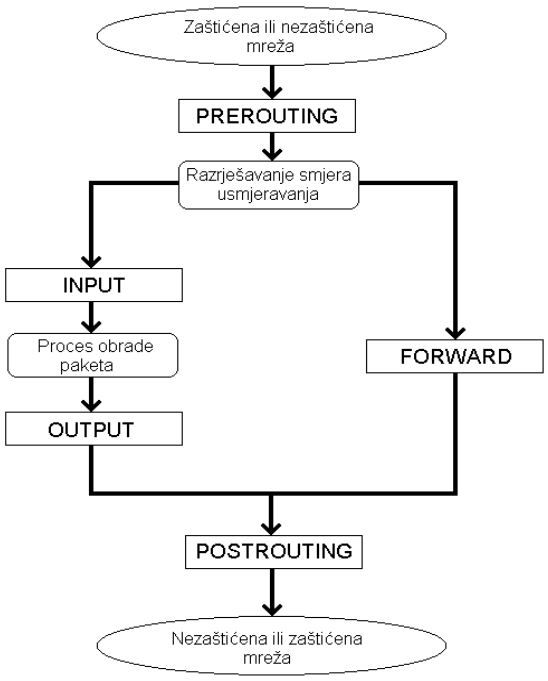
dobivenih paketa prepoznajte IP adresu koja odgovara adresi www.fer.hr. U danjem tekstu ta adresa označavati će se labelom „FER“.

4. Filtriranje mrežnog prometa (Firewall)

Cilj ove vježbe je upoznavanje s filtriranjem mrežnog prometa. Filtriranje mrežnog prometa najuobičajenije je na usmjerivačima koji se onda zbog takve svoje zaštitne uloge nazivaju vatrozidi (engl. *firewall*). Ipak, vatrozidi se nalaze i na osobnim računalima pri čemu služe najčešće za zaštitu od računalnih virusa i crva, trojanaca i sličnih malicioznih programa. Nažalost filtriranje mrežnog prometa na usmjerivačima nije moguće izvesti u sklopu ovih laboratorijskih vježbi pa je stoga naglasak stavljen na filtriranje prometa na osobnom računalu.

4.1. Faze obrade mrežnih paketa u vatrozidu

Kada mrežni paket dođe na mrežno sučelje vatrozida, on prelazi preko mrežnog sklopovlja na odgovarajući upravljački program u jezgri operacijskog sustava zadužen za obradu paketa. Paket nakon toga prolazi kroz određene faze prije nego bude proslijeđen na drugu mrežu ili na neku višu aplikaciju u vatrozidu. Glavne faze obrade nazivaju se još i karike (engl. *chains*) prikazane su na slici 3.



Slika 3. Usmjeravanje paketa unutar jezgre operacijskog sustava vatrozida

Ukoliko vatrozid dobije paket koji je namijenjen za sam vatrozid, paket će biti proslijeđen na INPUT (ulaznu) fazu. Tu je moguće definirati pravila u vezi s dolaznim paketom. Neka od tipičnih pravila bila bi da se paket proslijedi na neku drugu, na slici nespomenutu fazu koja je zadužena za obradu i provjeru paketa određenog tipa (npr. UDP ili TCP paketi). Nakon što paket uspješno prođe INPUT fazu paket odlazi na obradu određenom aplikacijskom procesu.

Ukoliko je riječ o slanju paketa od strane vatrozida, generirani paket prvo dolazi na OUTPUT fazu. Tu je moguće obaviti filtriranje paketa, tj. provesti zabranu prolaska neodgovarajućim paketima.

Ako paket treba samo proći s javne na internu, ili s interne na javnu mrežu, onda on mora proći preko FORWARD faze. U FORWARD fazi obavljaju se provjere prema pravilima koje određuju koji paketi smiju prolaziti na koju mrežu. Uobičajeni skup naredbi sadrži zabranu prosljeđivanju paketa s vanjske mreže prema zaštićenoj i dozvolu prosljeđivanja odgovora s vanjske mreže prema zaštićenoj mreži. Također, često se korisnicima

zaštićene mreže u FORWARD fazi zabranjuje pristup određenim ili vanjskim računalima (poslužitelji s Web igrama i sl.) ili određenim nesigurnim uslugama (ftp, tftp, itd...).

Faza PREROUTING omogućava manipulaciju paketima na razini promjene TOS (engl. *Type of Service*) varijabli i sl. Važnija primjena ove faze je DNAT (engl. *Destination Network Address Translation*) transformacija. DNAT transformacija koristi se za promjenu odredišne adrese.

Fazi POSTROUTING glavna je funkcija SNAT (engl. *Source Network Address Translation*) transformacija. SNAT transformacija koristi se za promjenu izvorišne adrese paketa. Umjesto SNAT-a u ovoj fazi moguće je koristiti i proces maskiranja (engl. *Masquerading*) privatnih adresa iz zaštićene mreže. Vatrozid mijenja IP adrese iz zaštićene mreže svojom adresom pridruženom vanjskom mrežnom sučelju i prosljeđuje tako modificirane pakete na vanjsku mrežu. Razlika između SNAT-a i maskiranja je u tome što SNAT zamjenjuje IP adrese s definiranom adresom, a maskiranje zamjenjuje IP adrese s adresom pridruženom određenom mrežnom sučelju. Ukoliko zaštićene mreže koriste privatne IP adrese nužno je koristiti jednu od spomenutih metoda jer se inače paketi nikad ne bi mogli vratiti na odgovarajuće računalo zbog toga što paketi s privatnim IP adresama nisu dozvoljeni na Internetu.

4.2. Konfiguracija vatrozida

4.3. Konfiguracija mrežnih postavki računala

Nakon podizanja operacijskog sustava potrebno je unutar grafičkog sučelja startati terminal prozor u kojem izvršavate sve daljnje naredbe.

- Najprije je potrebno definirati mrežno sučelje. Izlistavanje mrežnih sučelja postiže se pomoću naredbe:

```
ifconfig
```

Operacijski sustav obično sam definira potrebne mrežne postavke. Nakon prethodne naredbe trebalo bi biti prikazano sučelje `eth0` i `eth1`, jedno od kojih definira IP adresu i mrežne postavke. Provjerite otvaranjem web preglednika je li veza dobro podešena (u pregledniku otvorite neku web stranicu). Ukoliko to nije slučaj provjerite mrežni kabel i po potrebi resetirajte računalo.

Ukoliko je mreža ispravno podešena iz izlaza prethodne naredbe moći ćete saznati svoju IP adresu. Zapišite ju na papir. U danjem tekstu, labela „MyIP“ označava vašu IP adresu. Labela „FER“ odnosi se na IP adresu stranice *www.fer.hr*.

U ovom trenutku potrebno je još aktivirati Apache web poslužitelj na računalu naredbom:

```
/etc/init.d/apache2 start      - start Apachea
```

Nakon pokretanja Apache web poslužitelja na računalu je otvoren port 80 (HTTP port) i njemu možete pristupati tako da se u web pregledniku upiše http://localhost ili vlastitu IP adresu (MyIP) u prostor za adresu unutar web preglednika.

4.4. Definiranje pravila filtriranja i preusmjeravanja za mrežne pakete

Da bi se na računalu postavile određene naredbe za filtriranje mrežnih paketa potrebno je koristiti *IP Tables* programski alat. S njime se na jednostavan način definiraju pravila koja određene mrežne paket propuštaju, određene preusmjeruju na druga računala, a određene odbijaju i ne propuštaju.

Filtriranje mrežnih paketa odvija se u različitim grupacijama. Dolazni paketi namijenjeni samom računalu pregledavaju se u INPUT fazi, odlazni u OUTPUT, a paketi koji se prosljeđuju na druga računala u FORWARD fazi. Ispis svih naredbi u pojedinim od spomenutih grupacija dobiva se unosom sljedeće naredbe:

```
iptables -L
```

Uz svaku grupu (tzv. lanac ili karika – engl. *chain*) definirana je i globalna politika lanca: ACCEPT, REJECT ili DROP. Globalni ACCEPT označava da se sve prihvaća osim naredbi koje su navedene kao DROP ili REJECT u tom lancu. Globalni DROP ili REJECT označava da se ništa ne prihvaća osim naredbi koje su navedene kao ACCEPT u tom lancu. Na početku vježbe sve globalne politike trebaju biti ACCEPT. Što se postiže sljedećim naredbama:

```
iptables –P INPUT ACCEPT
iptables –P OUTPUT ACCEPT
iptables –P FORWARD ACCEPT
```

Osim što se s IP Tables-om mogu filtrirati mrežni paketi, oni se mogu i preusmjeravati. To se postiže u POSTROUTING i PREROUTING fazama. PREROUTING faza namijenjena je promijeni odredišnih postavki (odredišna IP adresa i port) dok je POSTROUTING faza namijenjena promijeni izvorišnih postavki (izvorišna IP adresa i port). Ispis svih naredbi u pojedinim od spomenutih faza dobiva se unosom sljedeće naredbe:

```
iptables –t nat -L
```

Globalne politike ovih lanaca postavljaju se sljedećim naredbama:

```
iptables –t nat –P PREROUTING ACCEPT
iptables –t nat –P POSTROUTING ACCEPT
```

4.5. Filtriranje dolaznih mrežnih paketa

Pravila koja služe za definiranje prihvaćanja tj. odbacivanja mrežnih paketa namijenjenih vašem računalu definiraju se u INPUT fazi. Prvi zadatak vezan uz filtriranje dolaznih paketa je omogućavanje, tj. onemogućavanje pristupa podignutom lokalnom HTTP poslužitelju. Vježba se obavlja samostalno te u kombinaciji s drugim računalom.

Između svake naredbe potrebno je unijeti sljedeću naredbu da se ukloni efekt svih prethodnih naredbi:

```
iptables –F INPUT
```

- Prva naredba koju je potrebno definirati zabranjuje pristup lokalnom HTTP poslužitelju. Prije unosa naredbe za onemogućavanje pristupa HTTP servisu prisutnom na portu 80, potrebno je provjeriti da li je isti podignut otvaranjem stranice http://localhost sa lokalnog računala te vlastite IP adrese sa susjednog računala. Naredba koju je potom potrebno upisati je sljedeća:

```
iptables –A INPUT –p TCP –i eth1 --destination-port 80 –j DROP
```

- Navedena naredba unosi (–A : *append*) se na kraj INPUT lanca te definira da se sav TCP promet (-p TCP) usmjeren na mrežno sučelje eth1 (-i eth1) i na odredišni port 80 (–destination-port 80) odbaci. Nakon unošenja spomenute naredbe s drugog računala provjerite da li se može pristupiti vašem HTTP poslužitelju. Isti efekt ostvario bi se i sa sljedećom naredbom koju trebate unijeti nakon što ispraznite sadržaj INPUT lanca:

```
iptables –A INPUT –p TCP –d MyIP --destination-port 80 –j DROP
```

- Testirajte i prethodnu naredbu, ali prije nje ispraznite sadržaj INPUT lanca sa već navedenom naredbom:

```
iptables –F
```

- Druga funkcionalnost koju je potrebno testirati je zabrana ICMP protokola tj. *ping*-anja. Nakon što je ispražnjen INPUT lanac potrebno je prvo testirati sa susjednog računala da li se može računalo *ping*-ati. Nakon toga potrebno je unijeti novu naredbu koja zabranjuje ping na lokalno računalo:

```
iptables –A INPUT –p ICMP –d MyIP –j DROP
```

Testiranje navedene naredbe provedite sa susjednog računala korištenjem:

```
ping MyIP
```

Na kraju je potrebno isprazniti INPUT lanac. Navedeni način filtriranja primjenjuje se kad administrator računala želi zabraniti udaljenim korisnicima pristup određenim resursima lokalnog računala. Takav sustav naredbi naziva se *Black list*. Ukoliko bi sve bilo zabranjeno (globalna politika je DROP), osim definiranih naredbi, to bi bio slučaj *White list* sustava naredbi.

4.6. Filtriranje odlaznih mrežnih paketa

Pravila koja služe za definiranje prihvaćanja tj. odbacivanja mrežnih paketa generiranih od strane vašeg računala definiraju se u OUTPUT fazi. Prvi zadatak vezan uz filtriranje odlaznih paketa je omogućavanje, tj. onemogućavanje pristupa udaljenom HTTP http://www.fer.hr poslužitelju. Vježba se obavlja samostalno.

- Prva naredba koju je potrebno definirati zabranjuje pristup udaljenom HTTP poslužitelju preko porta 80. Prije unosa naredbe, potrebno je provjeriti da li je isti podignut otvaranjem stranice http://www.fer.hr. Naredba koju je potom potrebno upisati je sljedeća:

```
iptables –A OUTPUT –p TCP –d FER --destination-port 80 –j DROP
```

Uspješnost navedene naredbe možete provjeriti otvaranjem FER-ove stranice putem adrese (FER). Također, provjerite da li možete `ping`-ati navedenu adresu. Primjetite da:

- FER koristi više mrežnih adresa (161.53.72.119 i 161.53.72.120). U ovisnosti o tome koju adresu ste blokirali u prethodnoj naredbi, još uvijek možete pristupiti FER-ovoj stranici.
- Čak i ako blokirate obije ove adrese, FER-ovoj stranici još uvijek možete pristupiti preko adrese https://www.fer.hr. Objasnite zašto i kako to možete spriječiti?

- Sljedeću naredbu za onemogućavanje slanja *ICMP* zahtjeva unesite bez da ste ispraznili OUTPUT lanac. Na taj način će istodobno biti zabranjeno pristupanje FER-ovoj glavnoj web stranici te ping-anje samog računala:

```
iptables –A OUTPUT –p ICMP –d FER –j DROP
```

Testiranje navedene naredbe provedite s lokalnog računala korištenjem naredbe ping:

```
ping FER
```

Izlistajte naredbe kako biste vidjeli način zapisa iptables naredbi u OUTPUT karici te potom uklonite sadržaj OUTPUT lanca:

```
iptables –L
iptables –F OUTPUT
```

- Zadnja naredba obuhvaća prve dvije, ali i više jer zabranjuje sav promet prema definiranoj IP adresi:

```
iptables –A OUTPUT –p ALL –d FER –j DROP
```

Na kraju je potrebno isprazniti OUTPUT lanac. Navedeni način filtriranja primjenjuje se kad administrator računala želi zabraniti lokalnim korisnicima pristup određenim resursima, IP adresama i slično (engl. *Black list*).

4.7. Preusmjeravanje dolaznih mrežnih paketa

Pravila koja služe za preusmjeravanje mrežnih paketa generiranih od strane računala definiraju se u PREROUTING fazi. Prvi zadatak vezan uz preusmjeravanje mrežnih paketa odnosi se na preusmjeravanje ICMP dolaznih paketa na drugo računalo. Vježba se obavlja u kombinaciji sa susjednim računalom s kojeg se obavlja testiranje.

- Prvi preduvjet koji je potreban da bi se paket mogao preusmjeravati na neko drugo računalo je uključeno prosljeđivanje (*ip_forward*). Stoga je potrebno unijeti sljedeću naredbu:

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

- Drugi preduvjet koji je potreban da bi se paket mogao preusmjeravati na neko drugo računalo su naredbe u FORWARD lancu koje to dozvoljavaju. Za svaku naredbu redirekcije potrebno je unijeti pripadnu naredbu u FORWARD fazi koja će to preusmjeravanje ACCEPT-ati. Ipak, jednostavnije je prvo odrediti da je globalna politika FORWARD faze ACCEPT sljedećom naredbom:

```
iptables –P FORWARD ACCEPT
```

- Prva naredba služi za preusmjeravanje *ICMP* zahtjeva koji će se preusmjeravati na FER-ov web poslužitelj:

```
iptables –t nat –A PREROUTING –p ICMP –d MyIP –j DNAT --to-destination FER
```

Testiranje navedene naredbe provedite sa susjednog računala korištenjem naredbe:

```
ping MyIP
```

Koje računalo vam vraća poslane pakete?

Preusmjeravanje mrežnih paketa koristi se najčešće ukoliko je poslužitelj skriven. U tom slučaju adresirano računalo (najčešće vatrozid ili usmjerivač) prima pripadne mrežne pakete i prosljeđuje ih na skriveni poslužitelj.