

Univerzitet Crne Gore  
Elektrotehnički fakultet  
Studije primjenjenog računarstva  
Podgorica

# Projekat

## Linux firewall, web i ftp server - instalacija i konfigurisanje -

Predmet:  
Internet tehnologije  
Dr. Božo Krstajić

Student:  
Obradović Veselin, 154/03

## Sadržaj:

Projektni zadatak .....	3
1. Operativni sistem Linux .....	4
1.1. Istorija.....	4
1.2. Distribucija .....	5
1.3. Instalacija.....	5
2. Webmin .....	7
3. DHCP .....	9
4. Firewall.....	11
4.1. Uvod.....	11
4.2. Načini napada.....	11
4.3. Šta je firewall? .....	13
4.4. IP masquerading.....	14
4.5. Šta je IP filtriranje? .....	15
4.6. U našem slučaju.....	16
5. Web server.....	20
6. FTP server.....	22
7. Zaključak .....	23
8. Interesantni linkovi .....	25

## Projektni zadatak

Poštovani kolega,

Tvoj zadatak je da demonstriraš studentima i nama:

1. Instalaciju te distribucije (vrlo kratko) i administriranje
2. Instalaciju i podešavanje Web servera
3. Instalaciju i podešavanje ftp servera
4. Instalacija i podešavanje DHCP servera
5. Funkcije i podešavanje tog firewall-a .

Osim toga treba da napraviš pisani trag seminarskog rada koji će biti dostupan studentima (ja ću ga staviti na moj sajt). Dakle ono što ćeš da pokažeš opiši u tom materijalu. Sve mora biti gotovo do sredine decembra i očekuj prezentaciju krajem decembra.

Pozdrav

Božo

# 1. Operativni sistem Linux

## 1.1. Istorija

*Linux* je istovremeno i fenomen i operativni sistem. Da bi se shvatilo zašto je Linux postao toliko popularan, neophodno je znati ponešto od njegove istorije. Prva verzija *UNIX*-a je razvijena prije nekoliko decenija i koristila se uglavnom kao operativni sistem za istraživanja u univerzitetima. Veoma jake radne stanice su se pojavila u osamdesetim godinama prošlog vijeka od strane proizvođača kao što je *Sun* i sve su bile bazirane na *UNIX*-u. Mnoge druge kompanije su se upustile u takmičenje sa *Sun*-om, kao što su *HP*, *IBM*, *Silicon Graphics*, *Apollo*, i druge. Nažalost, svaka od njih je imala sopstvenu verziju *UNIX*-a što je činilo prodaju softvera teškom. *Windows NT* je bio *Microsoft*-ova ponuda tržištu. *NT* je nudio istu vrstu mogućnosti kao i *UNIX* operativni sistemi – sigurnost, podršku višeprocorskim mašinama, rad sa velikim kapacitetima diskova i memorije, itd., ali na način koji je bio kompatibilan sa većinom *Windows* aplikacija.

Pojavljivanje *Microsoft*-a na ovom tržištu je stvorilo čudna kretanja. Vlasnički operativni sistemi koji su posjedovale različite kompanije i nedostatak centralnog tijela za *UNIX* svijet su oslabile *UNIX*, ali se mnogim ljudima nije sviđao *Microsoft*. Tada je, 1991. godine, na scenu stupio *Linux* i privukao dosta pažnje.

*Linux* kernel, koga je napisao *Linus Torvalds*, je bio na raspolaganju besplatno. *Torvalds* je onda pozvao druge da unaprijeđuju njegov kernel, pod uslovom da su i te izmjene dostupne besplatno. Hiljade programera su počeli da rade na unaprijeđivanju *Linux*-a, i taj je operativni sistem rastao veoma brzo. Budući da je besplatan i da se izvršava na *PC* platformi, stekao je veliku popularnost među *hard-core* programerima veoma brzo. Njegovi korisnici su uglavnom ljudi koji:

- ... već poznaju *UNIX* i žele da ga izvršavaju na *PC* mašinama
- ... žele da eksperimentišu sa osnovama operativnih sistema
- ... trebaju ili žele veliku kontrolu nad operativnim sistemom
- ... ne vole *Microsoft*.

Generalno gledano, *Linux* je nešto teži za korišćenje od *Windows*-a, ali nudi daleko veću fleksibilnost i mogućnosti podešavanja.

## 1.2. Distribucija

U projektu je korišćena *Trustix Secure Linux*<sup>1</sup> (TSL) distribucija Linuxa. Zašto TSL? Kao što kažu autori ove distribucije na njihovom sajtu, "svrha TSL-a je da kreira visoko kvalitetni, open source operativni sistem namjenjen za serverski dio PC tržišta. Ovo je potignuto korišćenjem pažljivo izabranih komponenti iz dobro poznatih i pouzdanih izvora kao što su GNU projekat i Linux Kernel, kao dodatak softveru napravljenom posebno za TSL. Jedna od glavnih osobina Trustix-a je njegova mala veličina." U sledećem dijelu biće ukratko objašnjena step-by-step instalacija ove distribucije.



## 1.3. Instalacija

Instalacija TSL linuksa je prilično jednostavna. Sa nekoliko lokacija na Internetu moguće je download-ovati ISO image instalacionog CD-a koji se u svim standardnim programima veoma jednostavno nareže na CD. Instalacioni CD je butabilan (moguće je podići sistem sa njega), tako da osim njega i veze na Internet nije potrebno ništa drugo za realizaciju ovog projekta.

Proces otpočinje jednostavnim ubacivanjem CD medija sa instalacijom TSL-a u računar i podizanjem sistema sa njega. Program za instalaciju će postaviti određena pitanja kojima se određuje vrsta instalacije i podešavanja sistema. Korak po korak, to bi izgledalo na sledeći način:

- Na prvom ekranu imate pozdravnu poruku i sa pritiskom na <ENTER> taster otpočinje instalacija.
- Bira se vrsta tastature koja se koristi. Standardna vrijednost (ujedno i najčešća) je US.
- Install New System.

---

<sup>1</sup> Definišimo prvo šta distribucija nije! Distribucija nije Linux - Linux je operativni sistem. Distribucija nije grafički interfejs – to je prepušteno X window sistemu i GUI-u (*Graphical User Interface*) kao što su *Gnome, KDE, XFCE, Blackbox*, ili neki od mnogih drugih. Distribucija nije ono što se vidi u komandnoj liniji - Command Line Interface - cli – što se obično zove od strane Microsoft pobornika jednostavno DOS, gdje vidite prompt sa treperećim kursorom.

Šta je onda distribucija? Distribucija je upravo ono što njeno ime kaže – distribucija – tj. distribucija programa. Hiljade njih spakovanih zajedno u nekom logičnom formatu. Osnova svake Linux distribucije je kernel. Kernel okružuju raznorazni programi koji učitavaju Linux kernel u memoriju kada se kompjuter startuje, programi koji omogućavaju interakciju sa hardverom koji obavlja razne operacije kao što su kopiranje, premještanje fajlova i ostale manipulacije fajlovima. Većina, ako ne sve, distribucija koristi hiljade programa i rutina iz *open source* zajednice koji su na raspolaganju besplatno, na osnovu dozvole njihovih autora da se oni koriste na način koji to nama odgovara. Neki od njih pišu programe za novac, neki za slavu, neki da bi nešto naučili, a neki jednostavno zato što misle da oni to mogu najbolje da urade.

- Određivanje particija je najbolje prepustiti instalacionom programu, tj. opcija Autopartition.
  - Na pitanje ‘Remove all partitions on this sistem?’ odgovoriti sa Yes (taster F12).
  - Izabrati GRUB loader.
  - ‘Install boot loader to MBR’.
  - Pitanje o dodatnim argumentima pri dizanju sistema ostaviti bez odgovora.
  - Za dodatnu sigurnost postaviti Boot loader password. Inače nije neophodno.
  - Ovdje se vrše podešavanja NIC-ova (Network Interface Card). Uzeto je da je eth0 spoljna kartica (prema Internetu), a eth1 kartica sa strane lokalne mreže. Za eth1 je podešeno 10.0.0.1/255.255.255.0, a za eth0 je korišćena fiksna IP adresa dodjeljena od strane provajdera. Za ime servera nije bitno šta se stavlja, ako nije registrovano ime, a ako jeste treba staviti ime koje je registrovano.
  - Nakon osnovnih podešavanje mreže, podešava se časovna zona.
  - Unosi se veoma bitan *root* pasvord.
  - Pristup Linux sistemu zbog raznoraznih sitnica se ne preporučuje korišćenjem root naloga, već nekog običnog korisnika, koji ima daleko manje prava pristupa od root-a. Root se koristi samo kada je to neophodno. Zato se i pri samom procesu instalacije kreira običan korisnik sistema.
  - Sada se određuje šta će od paketa uključenih u TSL distribuciju zapravo biti instalirano na naš server. Ne garantujući da je to minimalna moguća konfiguracija u skladu sa projektnim zahtjevima, ja sam izabrao opcije:
    - o Minimal install with SSH
    - o Commonly used local utilities
    - o Commonly used network utilities
    - o Webserver with PHP
    - o FTP server (ProFTPD)
    - o Firewall
    - o LAN server
- Takođe se može izabrati i opcija ‘Select additional packages’ gdje se mogu izabrati dodatni paketi, po potrebi, kao što je npr. mod.php4-gd koji obezbjeđuje grafičku podršku za php.
- Za samo kopiranje fajlova sa CD-a na računar ni na Pentium II računaru nije trebalo više od 5 minuta, tako da je instalacija zaista brza. Log fajlovi instalacije su smješteni u /tmp/install.log

Ovo bi bio kratki (i sasvim dovoljni) opis instalacije TSL distribucije. Sledeći korak jeste skidanje Webmin programa sa Interneta i njegova instalacija. Većinu podešavanja ćemo obavljati korišćenjem ovog programa. O tome više u sledećem poglavlju.

## 2. Webmin

Webmin je program za udaljenu administraciju. Drugim riječima, on omogućava da upravljamo našim serverom sa nekog drugog računara, pod uslovom da oba kompjutera imaju pristup Internetu i da se ne nalaze iza nekog *firewall-a* koji onemogućava njihovu komunikaciju. Pomoću ovog softverskog rješenja je moguće startovati, podešavati, gasiti razne servise na našem serveru, pa čak i ugastiti ili restartovati sami server.

Kako je naš računar već konektovan na Internet, to ćemo instalacionu verziju softvera skinuti sa webmin web sajta. Kako TSL distribucija nema GUI, korišćićemo CLI web-browser *lynx*:

```
$> lynx www.webmin.com
```

Strelicama se krećemo do 'Downloading and Installing', sa <ENTER> vršimo selekciju, zatim biramo prvu verziju, u ovom slušaju 'webmin-1.170.tar.gz', određujemo lokaciju sa koje ćemo da skinemo program, kako lynx ne podržava napredne html tagove (tj. refresh tag), moraćemo selektovati link na vrhu stranice ručno, zatim opciju 'download'. Kada se čitav fajl skine sa Interneta (7649KB, u zavisnosti od brzine konekcije može da potraje i preko pola sata), treba pritisnuti <ENTER> da bi se izabrala opcija za snimanje fajla na disk, a onda opet <ENTER> da bi se prihvatilo ime fajla. Nakon što se završi snimanje, iz programa lynx se izlazi pritiskom na taster 'q'.

Sama instalacija Webmin-a je jednostavna. Potrebno je ukucati sledeće komande:

```
$> gunzip webmin-1.170.tar.gz
$> tar xf webmin-1.170.tar
$> cd webmin
$> ./setup.sh /usr/local/webmin
```

Na sva pitanja potvrditi default odgovor, kreirati administratora i to je to. Sada se može u bilo kom web-browseru poći na adresu <http://localhost:10000/> i ulogovati na program za udaljenu administraciju, gdje je *localhost* IP adresa našeg servera.

U slučaju da pri instalaciji nisu izvršena mrežna podešavanja, ili da je iz određenih razloga neophodno naknadno izmijeniti ista, to je moguće uraditi korišćenjem Webmin programa. Ide se na stranu "*Networking*" (sl. 1.) i izabere se "*Network configuration*". Na "*Network Interfaces*" se podešavaju aktivni parametri



Slika 1. – Izgled *Networking* strane Webmin-a

svakog mrežnog interfejsa (IP adresa, sub-net maska, itd.), u "*Routing and Gateways*" se podešavaju adrese default gateways-a, u "*DNS client*" se podešavaju adrese DNS servera, a u "*Hosta addresses*" se određenim adresama hostova dodjeljuju IP adrese na kojima se oni nalaze.

Veoma detaljno uputstvo za korišćenje ovog paketa predstavlja knjiga "*The Book of Webmin, Or: How I Learned to Stop Worrying and Love UNIX*" od autora Džoa Kupera (*Joe Cooper*) na svojih 295 stranica. U njoj je opisan Webmin od A do Z tj. od same instalacije, do naprednih koncepata kao što su podešavanja boot loadera, mrežnih servisa, a obrađeno je i konfigurisanje programa *Usermin*, koji omogućava običnim korisnicima udaljeni pristup sistemu (čitanje elektronske pošte, promjena lozinke i sl.)

### 3. DHCP

**DHCP** (*Dynamic Host Configuration Protocol*) je Internet protokol za automatsko konfigurisanje kompjutera koji koriste TCP/IP. DHCP može da se koristi za automatsko dodjeljivanje IP adresa, ali i da isporuči ostale TCP/IP konfiguracione parametre kao što su *subnet mask*, *default router*<sup>2</sup>, adresa štampača, vrijeme, i sl. U ovom projektu smo koristili DHCP server da bi dinamički dodjeljivao IP adrese računarima u lokalnoj mreži, kao i da bi proslijedio informacije o default routeru, DNS<sup>3</sup> serveru, subnet maski.

Kao i za ostale servise, podešavanje DHCP servera korišćenjem Webmin alata je veoma jednostavno. Kada se administrator prijavi na Webmin, bira opciju Servers, a zatim DHCP Server. U prozoru za podešavanje DHCP servera se prvo bira 'Add a new subnet', gdje se unose osnovni podaci za mrežu. Za mrežnu adresu smo koristili 10.0.0.0, IP adresa privatne mreže klase A<sup>4</sup>. Za projekat bi bez sumnje više odgovarala IP adresa mreže klase C, ali je ova korišćena iz prostog razloga lakšeg pamćenja IP adrese.

Rang adresa koje DHCP server dodjeljuje dinamički je postavljen od 10.0.0.3 do 10.0.0.30 iako je subnet mask 255.255.255.0. To je urađeno tako da su ostale adrese rezervisane za računare koji imaju fiksnu IP adresu (kao što su razni serveri). Omogućen je i 'Dynamic BOOTP<sup>5</sup>', protokol koji omogućava da mrežne stanice koje nemaju sopstveni disk doznaju svoju IP adresu, IP adresu BOOTP servera i lokaciju fajla koji treba da se učita u njenu memoriju.

Ti podaci su dovoljni da mašine povezane u lokalnu mrežu mogu dinamički da dobijaju svoje IP adrese. Međutim, za pristup Internetu je pored sopstvene IP adrese i subnet maske potrebno još nekoliko podataka. Ti podaci se podešavaju korišćenjem opcije 'Edit client options'. Moguće je za svaku pojedinačnu lokalnu mrežu definisati posebna pravila, kao i pravila koja važe za sve mreže. Korišćena je ova druga mogućnost. Za default router (tj. default gateway) je uzet naš server, tj. IP

---

<sup>2</sup> Default router je posrednik koji koristi računar da pristupi hostovima na drugim mrežama. Zove se i samo default gateway.

<sup>3</sup> Skraćenica od *Domain Name System* (ili *Service* ili *Server*), je jedan Internet servis koji prevodi imena domena (*domain names*) u IP adrese. Kako su imena domena alfabetska, lakše se pamte. Ali, Internet je zapravo baziran na IP adresama. Svaki put kada se koristi ime nekog domena, DNS servis mora da prevede to ima u odgovarajuću IP adresu. DNS sistem je, zapravo, posebna hijerarhijska mreža. Ako jedan DNS server ne umije prevesti neko ime domena, on to traži od drugog DNS servera i tako dalje, sve dok ne dobiju odgovarajuću IP adresu.

<sup>4</sup> Klasa A – 10.0.0.0 do 10.255.255.255/8

Klasa B – 172.16.0.0 do 172.31.255.255/12

Klasa C – 192.168.0.0 do 192.68.255.255/16

<sup>5</sup> Skraćeno od: 'Bootstrap Protocol'

adresa njegove unutrašnje NIC (eth1) – 10.0.0.1, DNS server je DNS server ISP (*Internet Service Provider*), a subnet maska je kao i u prethodnom slučaju – 255.255.255.0.

The screenshot shows the 'Edit Subnet' configuration page. The 'Subnet description' field contains 'Projekat iz Internet Tehnologija - SPR'. The 'Network address' is '10.0.0.0' and the 'Netmask' is '255.255.255.0'. The 'Address ranges' are '10.0.0.3' to '10.0.0.30'. The 'Dynamic BOOTP?' checkbox is checked. The 'Default lease time' is set to 'Default'. The 'Boot filename' is 'None'. The 'Boot file server' is 'This server'. The 'Lease length for BOOTP clients' is 'Forever'. The 'Dynamic DNS enabled?' checkbox is checked. The 'Dynamic DNS reverse domain' is 'Default'. The 'Allow unknown clients?' checkbox is checked. The 'Server is authoritative for this subnet?' checkbox is checked. The 'Hosts directly in this subnet' is 'ns'. The 'Groups directly in this subnet' is empty. At the bottom, there are buttons for 'Save', 'Edit Client Options', 'List Leases', and 'Delete'. There are also links for 'Add a new host' and 'Add a new host group'.

Slika 2. – Podešavanje DHCP servera

Klikom na dugme 'Save' podešavanja se snimaju i vraćamo se u prethodni ekran. Tu treba da kliknemo na dugme 'Apply Changes' da bi se DHCP server startovao (ili ako je već startovan, restartovao sa novim parametrima koje smo upravo podesili).

Ovo su sva podešavanja koja je potrebno izvršiti na DHCP serveru da bi računari u lokalnoj mreži dinamički dobijali svoju IP adresu i podatke neophodne za pristup Internetu. Međutim, oni i dalje ne mogu da pristupaju resursima koji se nalaze sa spoljne strane našeg servera. O tom, drugom, koraku više u idućem poglavlju koji govori o IP masquerading-u i podešavanjima firewall-a.

## 4. Firewall

### 4.1. Uvod

Sigurnost je sve više bitna i za preduzeća i pojedince podjednako. Internet im je pružio moćnu alatku da distribuiraju podatke o sebi i da dobijaju podatke o drugima, ali ih je takođe izložio opasnostima od kojih su ranije bili izuzeti. Kompjuterski kriminal, krađa informacija i zlonamjerna šteta su potencijalne opasnosti.

Jedna neovlaštena i beskrupulozna osoba koja dobije pristup kompjuterskom sistemu može otkriti sistemsku lozinku ili iskoristiti greške i nepredviđena ponašanja određenih programa i na taj način da sebi omogući pristup štetnim informacijama, kao što su komercijalne informacije tipa marketinških planova, detalja o novim projektima, ili baza podataka klijenata. Oštećivanjem ili izmjenom ovakvih podataka mogu da se nanesu velike štete preduzeću.

Najbezbjedniji način da se onemogući ovako ozbiljna šteta je da se onemogući pristup neovlaštenim osobama računaru. Tu na scenu stupa firewall.

### 4.2. Načini napada

Da bi režni administrator bio efikasan, mora razumjeti prirodu potencijalnih napada na kompjutersku sigurnost. Slijedi kratak opis najbitnijih vrsta napada da bi se bolje shvatilo od čega nas naš Linux firewall štiti.

#### *Neovlašten pristup:*

Ovo jednostavno znači da ljudi koji nebi smjeli koristiti usluge vaših računara su u mogućnosti da se povežu na njih i koriste ih.

Postoji više načina na koji se ovo može spriječiti pažljivim specificiranjem ko može da pristupi računaru posredstvom raznih servisa. Moguće je spriječiti pristup mreži svim korisnicima osim onih kojima želimo to omogućiti.

#### *Iskorištavanje poznatih slabosti programa:*

Neki programi i mrežni servisi nisu originalno dizajnirani imajući u vidu visoki stepen sigurnosti i zbog toga su osjetljivi na napade. Dobar primjer su BSD remote servisi (rlogin, rexec, itd.).

Najbolji način da se sistem zaštiti od ovakvih napada je da se onemogući korištenje ranjivih servisa ili da se nađu alternative. Sa Open Source-om, ponekad je moguće i otkloniti ovakve slabosti u softveru.

### *Odbijanje servisa (Denial of service – DOS)*

DOS napadi prouzrokuju da servis ili program prestane funkcionisati ili onemogućavaju druge da koriste servis ili program. Ovo se može postići na mrežnom sloju šaljući pažljivo dizajnirane zlonamjerne datagrame koji prouzrokuju da mreža prestane da funkcioniše. Takođe se može postići u sloju aplikacije, gdje pažljivo izabrane komande su izdane programu zbog kojih on postaje izuzetno opterećen ili prestane da funkcioniše.

Spriječavanjem da sumnjivi mrežni saobraćaj signe do vaših hostova i onemogućavanjem sumnjivih komandi i zahtijeva programima su najbolji način minimizovanja rizika od DOS napada. Korisno je znati metode napada, tako da se treba stalno pratiti i čitati o novim vrstama DOS napada čim se njihovi podaci objave.

### *Obmana (Spoofing)*

Ova vrsta napada prouzrokuje da host ili aplikacija sakrije akcije drugog/druge. Tipično, napadač se pretvara da je bezopasan host praćenjem IP adresa u mrežnim paketima. Na primjer, dobro dokumentovana mana BSD rlogin servisa može da koristi ovu metodu da maskira TCP konekciju sa drugog hosta pogodaanjem TCP sekvence brojeva.

Da bi se zaštitili od ove vrste napada, treba da se verifikuje autentičnost datagrama i komandi. Onemogućiti rutiranje datagrama sa nepostojećim adresama porijekla.  
amic port addresses.

### *Eavesdropping*

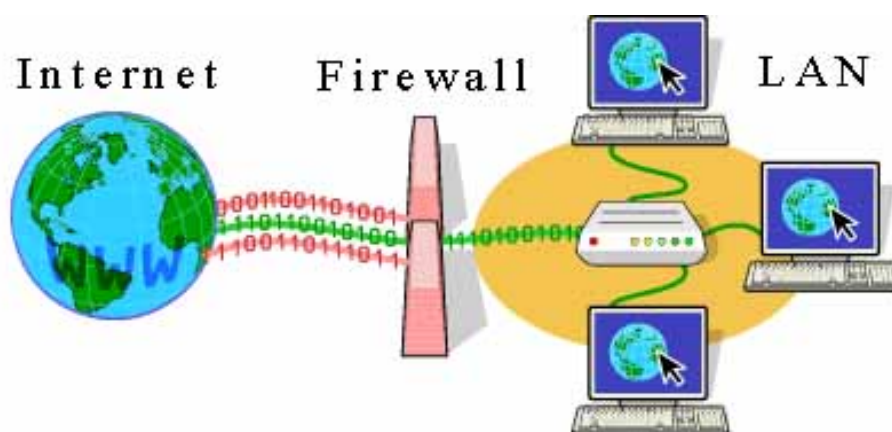
Ovo je najosnovnija vrsta napada. Neki računar je konfigurisan tako da “sluša” mrežni saobraćaj i hvata podatke koji nisu namjenjeni njemu. Pažljivo napisani programi ove namjene mogu doznati korisnička imena i lozinke korisnika koji se prijavljuju na mrežu. Broadcast mreže kao što je Ethernet su izrazito ranjive na ovu vrstu napada.

Da bi se zaštitili od ove vrste opasnosti, izbjegavati korišćenje broadcast mrežnih tehnologija i striktno sprovoditi enkripciju podataka.

IP firewall je veoma koristan u spriječavanju ili smanjivanju neovlaštenog pristupa, mrežnog nivoa DOS napada i IP spoofing napada. Nije posebno efikasan u izbjegavanju iskorištavanja slabosti mrežnih servisa ili programa i eavesdropping-u.

### 4.3. Šta je firewall?

Firewall je sigurna i povjerljiva mašina koja se nalazi između javne i privatne mreže (sl. 3.). To je uređaj konfigurisan sa setom pravila koja odlučuju koji će mrežni saobraćaj moći proći, a koji će biti blokiran ili odbijen. U nekim velikim organizacijama, mogu se naći firewall uređaji unutar korporacijske mreže kojim se odvajaju osjetljivi dijelovi organizacije od ostalih zaposlenih. Mnogi slučajevi kompjuterskog kriminala su se desili unutar organizacije, a ne samo spolja.



Slika 3. – Internet Firewall

Oni mogu biti konstruisani na veliki broj različitih načina. Najsofisticiraniji raspored uključuje veći broj različitih mašina i poznat je pod imenom *perimeter network*. Dvije mašine koje se ponašaju kao filteri koji dozvoljavaju samo određenoj vrsti saobraćaja da prođe, između kojih se nalaze serveri kao što su mail gateway ili www proxy server. Ovakva konfiguracija je veoma bezbjedna i lako omogućava veliku kontrolu u oba smjera, tj. ko se iznutra može konektovati spolja, i ko se spolja može konektovati iznutra. Ova vrsta podešavanja se koristi u velikim organizacijama.

Ipak, tipično je da je firewall jedna mašina koja služi svim ovim funkcijama. To je manje sigurno, jer ako postoji neka slabost u samom firewall-u koja omogućava ljudima pristup njemu, sigurnost čitave mreže može biti ugrožena. No, ova vrsta firewall-a je jeftinija i lakša za upravljanje nego ranije spomenute sofisticirane verzije.

Linux kernel obezbjeđuje široki spektar ugrađenih osobina koje mu omogućuju da veoma fino funkcioniše kao IP firewall. Mrežna implementacija uključuje kod za IP filtriranje na određen broj različitih načina kao što i obezbjeđuje mehanizam za veoma precizno konfigurisanje pravila koja želite da primjenite. On takođe omogućuje veoma korisnu osobinu koju ćemo koristiti u projektu: IP masquerade.

#### 4.4. IP masquerading

IP masquerading omogućava da se koristi privatna (rezervisana) IP mrežna adresa na našem LANu i da naš ruter, baziran na Linuxu, obavlja neke pametne translacije IP adresa i portova u realnom vremenu. Kada on primi datagram (IP paket) od kompjutera u LANu, on pamti o kakvoj vrsti datagrama se radi, TCP, UDP, ICMP, itd., pa modifikuje datagram tako da izgleda kao da je generisan od strane samog rutera (i pamti da je uradi to). Onda odašilje datagram na Internet sa samo jednom IP adresom kojom je on povezan na Internet. Kada odredišni računar primi datagram, on misli da je datagram stigao od samog rutera i šalje odgovor nazad na njegovu adresu. Kada Linux ruter koji obavlja IP maskiranje primi datagram sa Interneta, on gleda u svoju tabelu uspostavljenih maskirajućih konekcija da vidi da li zapravo datagram pripada nekom računaru u LANu i ako pripada, modifikuje reverzno onome što je uradio kada je taj računar iz LANa slao datagram na Internet i šalje ga njemu.

Mi imamo malu Ethernet mrežu koja koristi jednu od rezervisanih mrežnih adresa. Mreža ima Linux maskirajući ruter koji obezbjeđuje pristup Internetu. Jedna od radnih stanica u lokalnoj mreži (10.0.0.25) želi da uspostavi konekciju sa udaljenim hostom 216.239.37.99 (www.google.com) na portu 80. Radna stanica šalje njen datagram maskirajućem ruteru, koji identifikuje da ovaj zahtijev za konekciju treba maskirati. On prihvata datagram i dodjeljuje mu port (1035), zamjenjuje sopstvenu IP adresu i port onim od originalnog pošiljaoca, i šalje datagram primaocu. Odredišni host misli da je primio zahtijev za konekciju od našeg Linux maskirajućeg rutera i generiše povratni datagram. Maskirajući host, po prijemu ovog datagrama, pronalazi asocijaciju u svojoj tabeli maskiranja i sada u obrnutom smijeru mijenja svoju adresu i port adresom i portom radne stanice iz lokalne mreže. Tada šalje datagram tom računaru.

Lokalni računar misli da komunicira direktno sa udaljenim računarem. Udaljeni računar ne zna ništa o lokalnom računaru i misli da se sva komunikacija obavlja sa našim Linux ruterom. Linux maskirajući ruter zna da ova dva računara komuniciraju međusobno i na kojim portovima to rade i obavlja translaciju adresa i portova neophodnu da se omogući ta komunikacija.

Ova tehnika ima svoje sporedne pojave, od kojih su neke korisne, dok druge stvaraju probleme.

Ni jedan od računara u našoj lokalnoj mreži ne može da se direktno vidi sa interneta i kao posljedicu toga možemo da koristimo samo jednu validnu i rutabilnu

IP adresu da omogućimo svim tim računarima vezu sa Internetom. Mana ovoga je da ni na jedan od tih računara se ne može povezati direktno sa interneta; jedini računar vidljiv spolja je naš Linux maskirajući ruter. Zbog toga, ni jedan od računara u lokalnoj mreži ne može da bude server kome se pristupa spolja. Takođe, budući da se ti računari ne vide sa Interneta, oni su relativno zaštićeni od napada spolja; ovo može da umnogome uprošti ili čak i potpuno ukloni potrebu za konfigurisanjem firewall-a na maskirajućem ruteru. Kompletna mreža će biti onoliko sigurna koliko je siguran ruter, tako da je u tom slučaju potrebno koncentrisati se na sigurnost samog maskirajućeg rutera.

Dalje, IP maskiranje ima nekog uticaja na performanse mreže. U tipičnim slučajevima, to će biti jedva mjerljivo, ali ako imamo veliki broj aktivnih maskirajućih sesija, može se desiti da procesiranje koje ruter mora da obavi pri maskiranju utiče na propusnu moć naše mreže. IP maskiranje mora da radi mnogo više posla u odnosu na klasično rutiranje.

Na kraju, neki mrežni servisi jednostavno neće raditi preko maskiranja, ili bar ne bez velike pomoći. Tipično, to su servisi koji se oslanjaju na to da dolazne sesije funkcionišu, kao što su neke vrste Direct Communications Channels (DCC), jedne od osobina IRC-a, ili neke vrste video i audio multicasting servisa.

#### *4.5. Šta je IP filtriranje?*

IP filtriranje je jednostavno mehanizam koji odlučuje koji će tipovi IP datagrama biti normalno obrađivani, a koji jednostavno zanemareni. Pod ‘zanemarenim’ podrazumjeva se da će datagram biti izbrisan i potpuno ignorisan, kao da nikad nije ni bio primljen. Mogu se primjeniti veliki broj različitih kriterijuma na osnovu kojih se određuje koje datagrame želimo filtrirati. Neki od primjera su:

- Vrsta protokola: TCP, UDP, ICMP, itd.
- Broj socket-a (za TCP/UDP)
- Vrsta datagrama: SYN/ACK, podaci, ICMP Echo Request, itd.
- Adresa pošiljaoca datagrama
- Adresa primaoca datagrama

Bitno je shvatiti da IP filtering funkcioniše na nivou mreže. To znači da ono ne razumije ništa o tome koje aplikacije koriste mrežne konekcije, već samo razumije same mrežne konekcije. Na primjer, možemo onemogućiti pristup našoj internoj mreži na standardnom telnet portu, ali ako se oslonimo isključivo na IP filtriranje, ne možemo spriječiti korišćenje telnet na neki drugi port koji firewall dozvoljava. Ovo se može spriječiti korišćenjem proxy servera za svaki servis koji omogućavamo preko firewall-a. Proxy serveri razumiju aplikacije za koje su dizajnirani i shodno

tome mogu da spriječe zloupotrebe , kao što je korišćenje telnet-a da zaobidje firewall koristeći adresu www porta.

#### 4.6. U našem slučaju...

...smo koristili IP masquerading (IP maskiranje) budući da imamo na raspolaganju samo jednu javnu IP adresu. Za aktiviranje IP maskiranja je potrebno izdati par komandi u CLI. Kako je u našem slučaju spoljni NIC eth0 i ako nam je rutabilna IP adresa 195.66.171.29, to će izgledati:

```
$> modprobe ipt_MASQUERADE
$> iptables -F
$> iptables -t nat -F
$> iptables -t mangle -F
$> iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to
195.66.171.29
$> echo "1" > /proc/sys/net/ipv4/ip_forward
```

Objašnjenje gornjih komandi:

- Komanda `modprobe` dodaje i uklanja module iz Linux kernela. Sa ovom komandom smo dodali modul neophodan za IP maskiranje u slučaju da on nije već ukompajliran u kernel.
- Sva podešavanja Linux firewall-a se obavljaju pomoću komande `iptables`. U ovom slučaju je korišćen prekidač `-F` (flush) čime se brišu sva eventualno već postojeća podešavanja filtera firewalla.
- U ovom redu se brišu sva podešavanja u NAT<sup>6</sup> tabeli koja eventualno već postoje.
- Slično kao i u prethodnom slučaju, brišu se sva već postojeća podešavanja, ali u MANGLE<sup>7</sup> tabeli.
- U ovom redu se zapravo podešava firewall da radi IP maskiranje. `-t nat` ga upućuje na NAT tabelu, `-A POSTROUTING` dodaje pravilo u postrouting<sup>8</sup> lanac, `-o eth0` označava da je izlazni NIC eth0, tj da se preko njega paket šalje dalje, `-j SNAT --to 195.66.171.29` znači da se izvorišna adresa paketa treba promjeniti u 195.66.171.29
- U zadnjem redu zapravo upisujemo broj 1 u konfiguracioni fajl `ip_forward` koji se nalazi u direktorijumu `/proc/sys/net/ipv4`, čime omogućavamo da se radi IP prosljeđivanje sa eth1 na eth0 NIC.

---

<sup>6</sup> Network Address Translation

<sup>7</sup> Ova tabela se koristi za specijalizovane izmjene paketa.

<sup>8</sup> Lanac za izmjenu paketa prije nego što pođu iz rutera.

To bi bilo kratko objašnjenje podešavanja IP maskiranja. Veoma detaljno objašnjenje iptables komande možete naći u `man`<sup>9</sup> stranicama samog Linuxa.

Kao što je napomenuto ranije, IP maskiranje samo po sebi predstavlja zaštitu naše mreže od spoljnih napada, samom činjenicom da se sa interneta ne mogu vidjeti ni jedna mašina iz mreže, već samo naš server. Ipak, ako želimo da ograničimo pristup Internetu korisnicima naše mreže, koristićemo razne filtere koje nam omogućuje IP filtriranje.

Svi paketi koje naš server obrađuje se procesiraju u tri tzv. lanca. INPUT je lanac u kojem se obrađuju paketi koji su upućeni serveru, bilo od strane nekog hosta lokalne mreže ili sa interneta, OUTPUT lanac je lanac u kome se obrađuju paketi koje naš server šalje nekom drugom računaru, a FORWARD lanac je lanac u kome se obrađuju paketi koje naš server prosljeđuje sa Interneta u našu mrežu, ili u suprotnom smijeru.

Ako želimo da vršimo filtriranje na osnovu protokola koji se koristi, komanda može da ima sledeći oblik:

```
$> iptables -A INPUT -s 10.0.0.0/255.255.255.0 -p icmp
-j DROP
```

Na ovaj način smo onemogućili komunikaciju ICMP<sup>10</sup> protokolom sa računara u našoj lokalnoj mreži. Dobra demonstracija je ako sa nekog računara iz naše mreže pokušamo da pingujemo server (`ping 10.0.0.1`). Neće stići odgovor ni na jedan paket. Šta ako želimo da zabranimo sve icmp pakete koji ne dolaze sa naše mreže? U tom slučaju koristimo znak za negaciju '!'. U primjeru:

```
$> iptables -A INPUT -s ! 10.0.0.0/255.255.255.0 -p icmp
-j DROP
```

Objašnjenje:

- A dodaje se pravilo u INPUT lanac
- s source adresa
- p vrsta protokola koji se filtrira
- j akcija (jump), u našem slučaju DROP

Neki drugi interesantni prekidači:

---

<sup>9</sup> `$> man iptables`

<sup>10</sup> Internet Control Message Protocol, detaljnije u RFC 792

-d	adresa odredišta
-i	ulazni (IN) NIC
-o	izlazni (OUT) NIC
--sport	izvorišni port
--dport	odredišni port
--mac-source	filtriranje po MAC <sup>11</sup> adresi

Još par primjera. Ako bi smo željeli da našim korisnicima onemogućimo korišćenje WWW servisa, sve što treba da uradimo jeste da zabranimo tcp pakete na portu 80 u FORWARD lancu:

```
$> iptables -A FORWARD -p tcp --dport 80 -j DROP
```

A ako želimo da onemogućimo korišćenje FTP servisa, treba da se zabrane FTP portovi:

```
$> iptables -A FORWARD -p tcp --dport 21 -j DROP
$> iptables -A FORWARD -p tcp --dport 20 -j DROP
```

Ako želimo da vidimo koja su pravila filtriranja podešena koristićemo:

```
$> iptables -L
```

a za brisanje postojećih pravila se koristi komanda:

```
$> iptables -D FORWARD 1
```

sa kojom se briše prvo pravilo u lancu FORWARD.

Svaki lanac ima default akciju. Standardno, one su ACCEPT, tj. lanci prihvataju datagram u slučaju da ih neko od pravila koje smo definisali nije odbacilo. Ako želimo da pravimo siguran firewall, lanci bi trebalo da odbacuju sve datagrame koji nisu prihvaćeni pravilima koje smo mi definisali. Primjer za to bi bio:

```
$> iptables -P FORWARD DROP
$> iptables -A FORWARD -p tcp --dport 80 -j ACCEPT
$> iptables -A FORWARD -p tcp --sport 80 -j ACCEPT
```

Na ovaj način smo onemogućili korišćenje svih portova osim porta 80 (WWW port). Spisak svih dodjeljenih portova može se naći na web sajtu IANA<sup>12</sup> organizacije.

---

<sup>11</sup> Media Access Control address, hardverska adresa mrežne kartice. Jedinствena za svaki NIC.

Ovo bi bio kratak pregled mogućnosti Linux firewall-a. Jako mnogo informacija se može naći širom Interneta. Neke od najinteresantnijih lokacija su svakako ‘The Linux Documentation Project’ i ‘The netfilter/iptables project’. Sve interesantne linkove možete naći na kraju dokumentacije.

---

<sup>12</sup> Pogledati linkove.

## 5. Web server

Sigurno najpopularniji Internet servis je WWW<sup>13</sup>. Mnogim korisnicima Internet je zapravo sinonim za WWW. Osnova web servisa jesu http<sup>14</sup> serveri. Jedan od najpoznatijih web servera, a svakako najpoznatiji i najpopularniji Open Source http server jeste Apache http server. Najnovija verzija ovog servera je 2.0.52. Ogromna većina Linux distribucija, ako ne i sve, dolaze sa paketom za instalaciju ovog servera u nekoj od stabilnih verzija.

U projektu je korišćena verzija 2.0.51, jer ona dolazi uz TSL 2.1. Sama instalacija ovog servera je veoma jednostavna. U samom procesu instalacije Linuxa se navede da želimo da instaliramo i čitav proces instalacije će biti odrađen sam.

Startovanje servera, kao i većina njegovog podešavanja se može uraditi u Webmin-u dosta jednostavno. Čak je moguće i ručno podešavanje konfiguracionog fajla za one koji više vole da tako obavljaju podešavanja.

Jedna stvar na koju ćemo obratiti više pažnje u sklopu ovog projekta jeste kako se podešava server tako da je za neke stranice neophodna autorizacija korisnika prije nego pristupi njenom sadržaju. Proces pravljenja same prezentacije nije u sastavu teme ovog projekta, kao ni ispita iz Internet Tehnologija. O toj tematici može se naći veliki broj manje ili više kvalitetnih uputstava na Internetu.

Podatke koje želimo da zaštitimo od neovlaštenog pristupa (html stranice i ostale fajlove) smještamo u jedan direktorijum unutar web direktorijuma. U glavnom konfiguracionom fajlu (httpd.conf) treba podesiti AllowOverride direktivu na sledeći način:

```
AllowOverride AuthConfig
```

Time smo omogućili da regulišemo prava pristupa svakom pojedinačnom direktorijumu u kome se nalaze fajlovi naše prezentacije. U direktorijumu u kome je instaliran apache server kreiramo još jedan direktorijum koji ćemo nazvati passwd i u njemu kreiramo fajl sa lozinkama koristeći alat htpasswd koji dolazi uz apache server na sledeći način:

```
htpasswd -c /usr/local/apache/passwd/passwords guest
```

---

<sup>13</sup> World Wide Web

<sup>14</sup> Hypertext Transfer Protokol – protokol koji omogućava da WWW funkcioniše.

Sa -c je označeno da se kreira novi fajl sa lozinkama. Ako želimo da dodamo novog korisnika, ne koristimo prekidač -c. Lozinka se kreira za korisnika guest. Nakon ove komande, bićemo upitani za lozinku dva puta.

Sada možemo kreirati fajl .htaccess u direktorijumu sa podacima u kome ćemo podesiti pravila pristupa. Karakteristično, fajl izgleda ovako:

```
AuthType Basic
AuthName "Restricted Files"
AuthUserFile /usr/local/apache/passwd/passwords
Require user guest
```

Ako želimo da omogućimo pristup direktorijumu svim korisnicima koje smo kreirali u fajlu sa lozinkama, umjesto zadnjeg reda kucamo:

```
Require valid-user
```

Sa ovim smo završili podešavanja neophodna za autorizaciju pristupa našim fajlovima. Na kraju je bitno da svim direktorijumima i fajlovima damo odgovarajuća prava pristupa.

## 6. FTP server

Kao i u slučaju http servera, ftp server se instalira prilikom instalacije samog operativnog sistema. Iz programa Webmin možemo startovati i podešavati taj servis. U projektu je korišćen ProFTPD server.

Sva podešavanja iz Webmin-a su jednostavna. Moguće je odrediti u koje će se direktorijume korisnici prijavljivati, ograničavati im kretanje, konfigurisati log fajlove, zabranjivati određene korisnike i sl.

Jedna od interesantnijih stvari je kako omogućiti anonymous ftp. To se postiže tako što se iz spiska korisnika (/etc/ftpusers) obrišemo korisnika ftp, što je veoma jednostavna operacija korištenjem nekog od Linux editora (npr. vi).

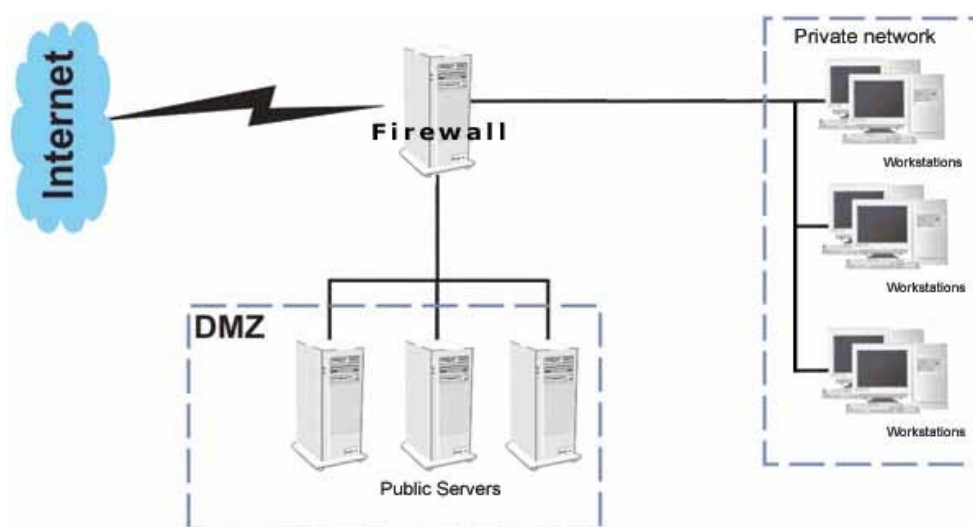
Slika 4. – Konfiguracioni ekran ProFTPD servera

## 7. Zaključak

Linux predstavlja veliki bauk iz prostog razloga što mnogi potencijalni korisnici, naviknuti na Microsoft operativne sisteme, misle da je korišćenje, podešavanje i administracija Linux servera komplikovana. Ovdje smo demonstrirali jedan alat koji tu administraciju čini veoma jednostavnom, pa čak i omogućava udaljeno administriranje našeg servera. Takođe, pokazano je da je instalacija i korišćenje Linux servera kao firewall uređaja veoma jednostavno, kao i na koji način pomoću njega postići maskiranje IP adresa računara u lokalnoj mreži na samo jednu rutabilnu IP adresu dodjeljenu od strane našeg ISP-a.

Sa strane pružanja Internet servisa, Linux je zaokružen sistem. Svi serveri (http, ftp, dhcp, dns, proxy, itd.) se već duže vremena razvijaju na Linux platformi, tako da su postigli veliku stabilnost, mogućnosti i kapacitete. Većina njih se instalira po potrebi pri samoj instalaciji operativnog sistema, a i njihovo podešavanje je moguće kroz Webmin.

Sa stanovišta sigurnosti, instalacija ovih servera na računaru koji se koristi kao firewall svakako nije preporučljiva, jer na taj način činimo naš server ranjivijim na zlonamjerne napade sa Interneta. Svakako bolje rješenje bi bilo ubacivanje treće mrežne kartice u naš firewall, na koju bi se povezali svi serveri. Mreža na trećoj mrežnoj kartici se popularno zove DMZ<sup>15</sup> (sl. 5.). Korišćenjem Linux firewall-a je moguće veoma efikasno i jednostavno omogućiti razmjenu podataka između ta tri NIC-a na način koji nama to odgovara, a svakako održavajući veoma visok nivo sigurnosti naše lokalne mreže.



Slika 5 – Firewall sa tri mrežna adaptera

<sup>15</sup> Demilitarizovana Zona

Rješenje predloženo u ovom projektu svakako predstavlja finansijski veoma isplativu soluciju. Kompletan softver servera je iz Open Source zajednice, što će reći potpuno besplatan za korišćenje. Takođe, za relativno male mreže (reda veličine nekoliko desetina radnih stanica) kao server može da služi neki Pentium II ili čak i Pentium I računar. Naravno, povećanjem saobraćaja (i eventualnim instaliranjem proxy servera) se povećavaju i zahtjevi za procesorskom snagom tog računara.

## 8. Interesantni linkovi

- Trustix Secure Linux <http://www.trustix.org/>
- Apache Web Server <http://www.apache.org/>
- ProFTPD FTP server <http://www.proftpd.org/>
- PHP project <http://www.php.net/>
- Webmin <http://www.webmin.com/>
- The Linux Documentation Project <http://www.tldp.org/>
- The netfilter/iptables project <http://www.netfilter.org/>
- Internet Assigned Numbers Authority <http://www.iana.org/>

Takođe, moguće je naći jako puno korisnih linkova pomoću poznatih pretraživača:

- Google <http://www.google.com/>
- Altavista <http://www.altavista.com/>

i dosta informacija na:

- How Stuff Works <http://www.howstuffworks.com/>