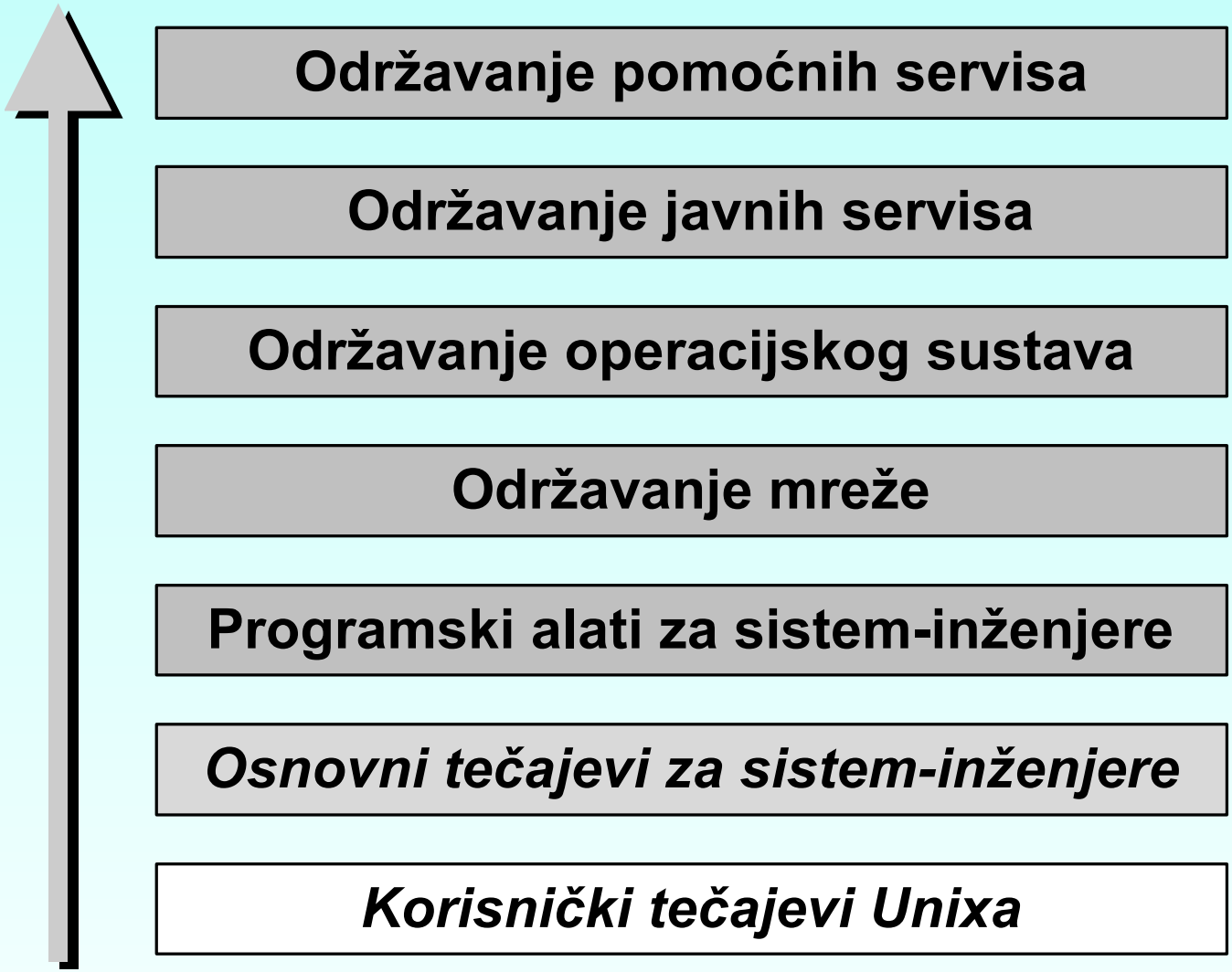
Održavanje pomoćnih servisa

autor: Aco Dmitrović (@fpzg.hr → @srce.hr)
©ilustracije: David Prajdić (@zg.hinet.hr)

mentor: Bojan Ždrnja (@fer.hr)
recenzent: Željko Boroš (@ptfos.hr)


Održavanje pomoćnih servisa
Održavanje javnih servisa
Održavanje operacijskog sustava
Održavanje mreže
Programski alati za sistem-inženjere
Osnovni tečajevi za sistem-inženjere
Korisnički tečajevi Unixa

Ciljevi tečaja

- Upoznavanje s dopunskim servisima koji se mogu ponuditi korisnicima LAN-a
- Poboljšanje sigurnosti CARNetovih čvorišta (firewall, antivirusna zaštita …)
- Praktično pokazati konfiguracije servisa, s naglaskom na sigurnost
- Razviti razumijevanje osnova i dati upute za kasnije samoobrazovanje

Potrebno predznanje

- Znanja sa Osnovnih tečajeva za sistem-inženjere
- Razumijevanje funkcioniranja TCP/IP mrežnih protokola
- Osnovna znanja o MS Windows OS i umreživanju Windows računala
- Osnovna znanja o relacijskim bazama podataka i SQL-u

Sadržaj

Firewall	150 min
NFS	15 min
Samba	30 min
Print servisi	15 min
Antivirusna zaštita	30 min
Baze podataka	30 min

Firewall

Svrha firewalla

- Primjena sigurnosne politike na mrežnoj razini
- Kontrola pristupa između dvije mreže
- Selektivno blokira/propušta određeni promet
- Zadržava uljeze, a istovremeno omogućava rad poželjnih servisa (E-mail, WWW ...)
- Restrikcijama smanjuje izloženost
- Nadzor i analiza – logovi su na jednom mjestu (*auditing*)

Firewall
Sigurnosna politika

- Prva i nezaobilazna faza rješavanja sigurnosnih problema
- Izvodi se iz pravila poslovanja
- Popis neophodnih/nepotrebnih servisa
- Svijest o ranjivosti otvorenih servisa
- Liste pristupa (*access list*)
- Sigurnost mreže zahtijeva specijalistička znanja i poseban tim

Firewall

Što firewall ne može?

- Ne može riješiti sve – samo je dio obrane!
- Ne može zamijeniti lošu fizičku sigurnost
- Ne brani od napada iznutra
- Propušta viruse, trojance...
- Ne pomaže ako iza firewalla imate PC s modemom
- Ne brani od socijalnog inženjeringa i korisnika koji daju svoje passworde prijateljima
- Ne štiti ništa ako ga je *cracker* već prošao

Firewall

Sigurnost po slojevima

Aplikacijska sigurnost
Mrežna sigurnost
Sigurnost operacijskog sustava
Fizička sigurnost

Firewall
Što firewall ne smije?

- Ometati redovno poslovanje
- Suviše ograničavati korisnike u LAN-u, jer će oni tada posegnuti za svojim rješenjima
  - modem + uključen routing
  - probijanje firewalla (*firewall piercing*)
- Zabrana jest najbrže rješenje, no sistemac treba tražiti složenije metode obrane

Firewall

Od čega se branimo?

Nekoliko metoda napada:

- Virusi, crvi (*worms*)
- DoS, DDoS (ping of death, WinNuke...)
- ICMP redirects, redirect bombs
- Session hijacking
- Source routing
- Greške u OS-u
- Greške u aplikacijama (npr. *buffer overflow*)

Firewall
Što čuvamo?

- Privatnost korisnika
- Povjerljivost podataka
- Integritet podataka
- Funkcioniranje sustava
- Ugled tvrtke/ustanove
- Ugled sysadmina
- Sigurnost Interneta kao cjeline

Firewall
Vrste firewalla

- Na mrežnoj razini (IP filteri)

  - odlučuje na osnovi IP adrese pošiljatelja/primatelja i broja porta

  - routeri znaju ponešto od toga (*access list*)

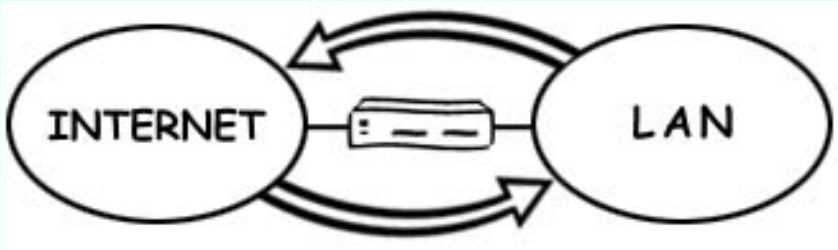
  - moderni firewall zna više: prati stanje otvorene veze, sadržaj data streamova, logira informacije

- Na aplikacijskoj razini (proxy servisi)

  - http proxy, ftp proxy, telnet proxy …

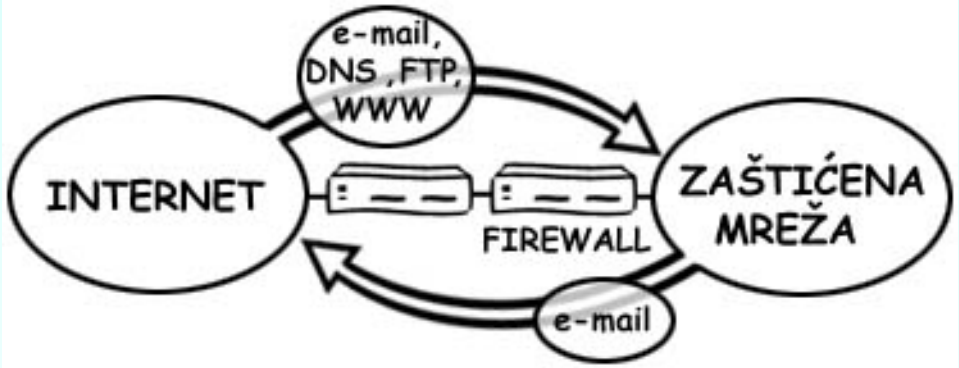
Firewall
LAN bez zaštite

- Svi paketi prolaze slobodno u oba smjera
- Obrana na razini hostova



Firewall
LAN sa zaštitom

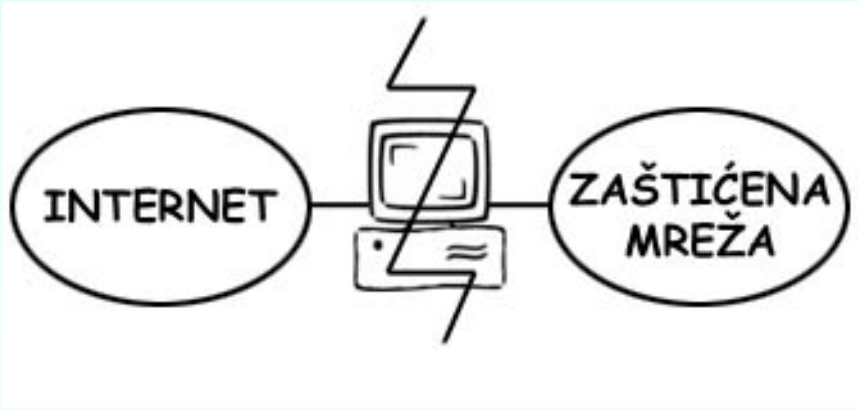
- Zaklonjena mreža (iza “vatrozida”)
- Ograničavanje prometa smanjuje rizik



Firewall

Osnovni pojmovi

- Vanjski svijet – Internet, mješavina sigurnih i nesigurnih mreža, *untrusted network*
- *Perimeter* – linija razdvajanja/obrane
- *Firewall* - zid između dvije mreže



Firewall
Bastion host

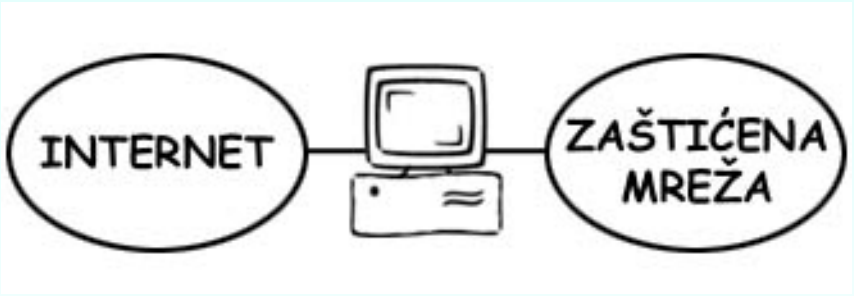
- Maksimalno utvrđeno računalo
- Obrana koncentrirana na jednom mjestu
- Jednostavna primjena
- Jeftino rješenje (jedan PC)
- Lakši nadzor (logovi su na jednom mjestu)
- Isključen `ip_forwarding`, nema rute izvana prema lokalnoj mreži
- Promet ide preko aplikacija (proxy)

Firewall

Arhetipovi

Dual homed gateway

- Računalo s dva mrežna sučelja
- *Bastion host* – utvrđeno računalo
- Jedini put između LAN-a i Interneta

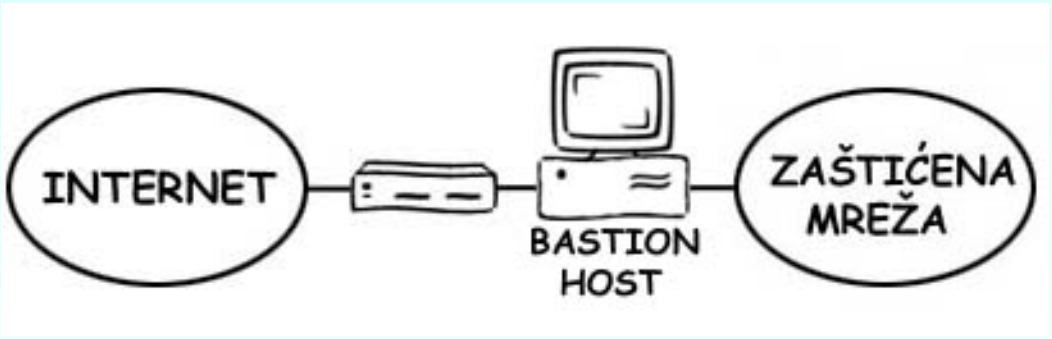


Firewall

Arhetipovi (2)

Screened host

- Ispred utvrđenog računala je router koji filtrira promet
- Dvije izložene točke

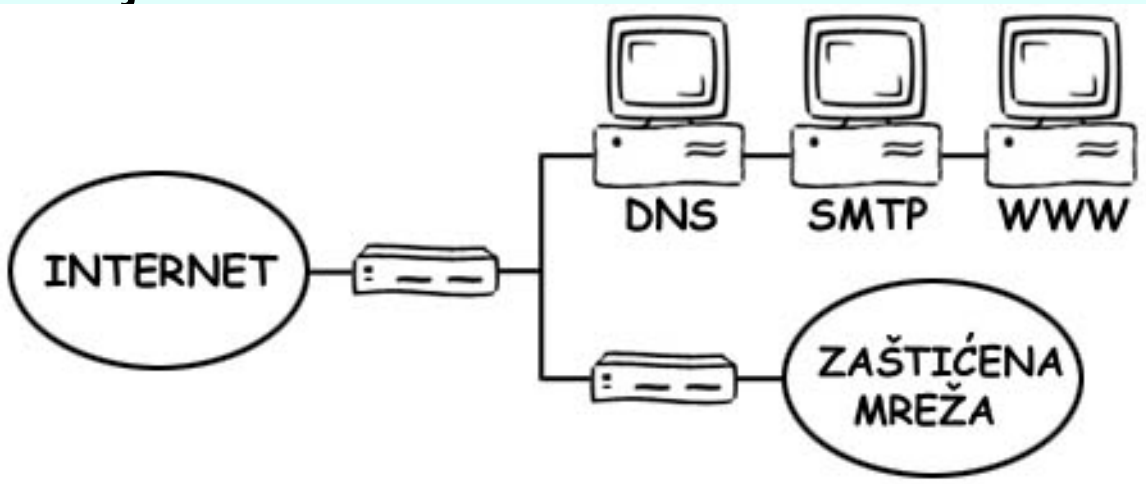


Firewall

Arhetipovi (3)

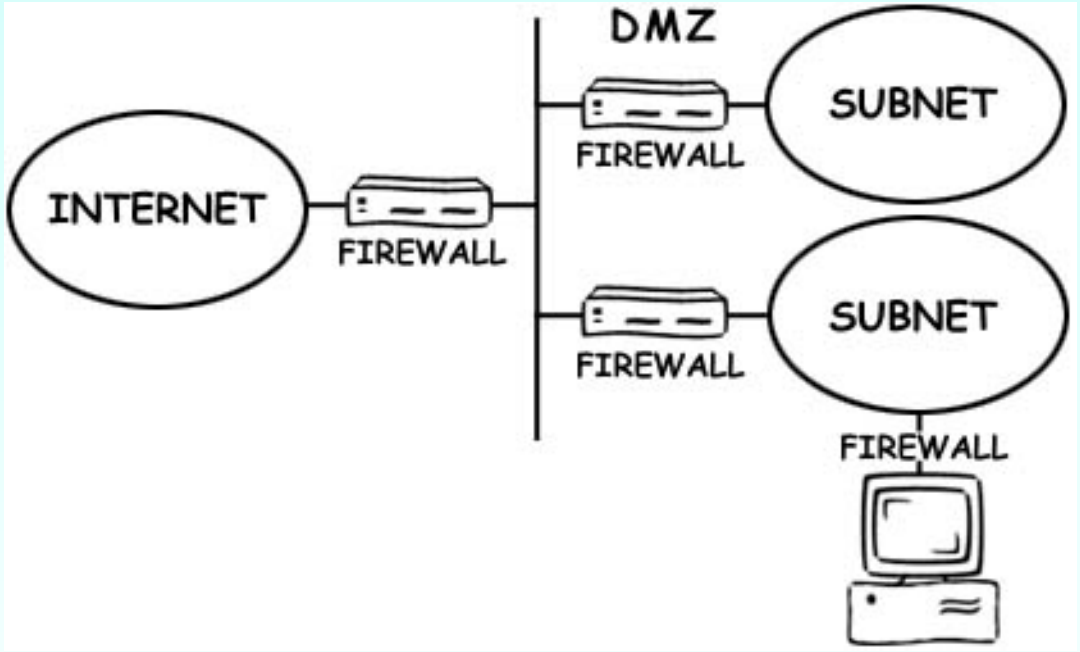
Screened subnet

- Farma servera na javnim adresama – DMZ (demilitarizirana zona)
- Zaklonjena mreža



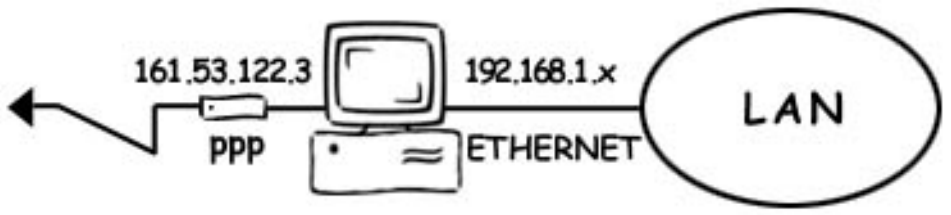
Firewall
Segmentiran LAN

- Promet se može ograničiti i unutar LAN-a



Firewall
NAT/IPMasq/Proxy

- Metode zaštite LAN-a
- Treba osigurati da poželjni servisi rade kroz gateway



Firewall
Network Address Translation

- RFC 1361
- One-to-one/one-to-many NAT (PAT)
- Ekonomičan pristup Internetu (SOHO)
- Minimalno trošenje javnih IP adresa
  (network, ISP router, vaš router, broadcast)
- LAN na privatnim adresama (npr.192.168.x.x)
- *Packet header rewrite*: gateway u zaglavlju paketa zamijeni privatnu adresu svojom
- Vanjski svijet vidi samo firewall

Firewall
IP Masquerade

- Izraz za NAT na Linuxu, ali i za crackerske trikove
- Uključen IP forwarding

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

- Dodatne mogućnosti:

  - port redirection (npr. port 80 na 8080)
  - port forwarding (npr. 161.53.22.3:80 na 192.168.1.5:80)

- Kernel moduli za pojedine servise/aplikacije

```
/sbin/modprobe ip_masq_ftp
/sbin/modprobe ip_masq_irc
/sbin/modprobe ip_masq_raudio
```

Firewall
Proxy

- Isključen IP forwarding!
- Jedini način prolaska paketa je pomoću aplikacije za određen servis - WWW/FTP/Telnet proxy
- Transparentan proxy je nevidljiv za korisnike
- Eksplicitan – traži podešavanje klijenta
- *Cache* – optimizira promet
- Pruža anonimnost korisnicima
- Može ograničavati promet (*access list*)

Firewall
Socks

- RFC 1928: SOCKS Protocol V5 – NAT+PT
- Veže port s aplikacijskim socketom – otud ime
- Prevođenje protokola: IPv4 u IPv6 i obratno
- Standardizacija komunikacije za različite aplikacije koje pristupaju serveru kroz proxy firewall
- SOCKS kompatibilni proxy serveri: Dante i DeleGate

Firewall
Linux

- Do kernela 2.0 – ipfwadm
- Od kernela 2.1 – ipchains
- Kernel 2.4 – netfilter (IPSec)
- TIS Firewall Toolkit
- Socks
- Squid
- Apache
- Phoenix Adaptive Firewall (ICSA certifikat)

Firewall
ipchains

- Blokira/propušta pakete ovisno o IP adresi izvora/cilja te /portu/interfaceu
- Maskiranje (zamjena adresa, NAT)
- Port redirection/forwarding
- Kreiranje vlastitih lanaca pravila
- QoS routing
- Inverzna specifikacija (! WWW)

Firewall
ipchains - alati

- `ipchains` - program za postavljanje pravila
- `ipchains-save` – snima pravila u file
- `ipchains-restore` – aktivira pravila iz filea
- `/etc/sysconfig/ipchains-rules`
- `/etc/init.d/ipchains {stop|start}`

Firewall
ipchains - alati (2)

- `ipchains-save > /etc/ipchains.rules`
-
```
#/bin/sh
case "$1" in
start)
  ipchains-restore < /etc/ipchains-rules
  echo "1" > /proc/sys/net/ipv4/ip_forward
stop)
  echo "0" > /proc/sys/net/ipv4/ip_forward
  /sbin/ipchains -F
  /sbin/ipchains -X
  /sbin/ipchains -P input ACCEPT
  /sbin/ipchains -P output ACCEPT
  /sbin/ipchains -P forward ACCEPT
```

Firewall

ipchains - podešavanje kernela

- Varijable koje treba podesiti pri kompiliranju

```
CONFIG_FIREWALL=y
CONFIG_IP_FIREWALL=y
CONFIG_IP_CHAINS=y
CONFIG_IP_MASQ=y
```

- Kako provjeriti?

```
/proc/net/ip_fwchains
/proc/net/ip_fwnames
/proc/net/ip_masquerade
```

Firewall
ipchains - lanci

- Tri ugrađena lanca sadrže liste pravila
  - `input` – pravila za ulazne pakete
  - `forward` – pravila prosljeđivanja
  - `output` – pravila za izlaz paketa

- Definiranje vlastitih lanaca

```
ipchains -N my_chain
```

Firewall

ipchains - kako paketi prolaze filtere?

Pri dolasku paketa kernel

1. provjeri pravila `input` lanca
2. ako paket preživi, odlučuje o ruti:
   - ako je namijenjen drugom računalu, provjerava `forward` pravila
   - u protivnom ide na slijedeći lanac
3. provjerava `output` pravila

Ako prođe sve lance, paket nastavlja put.

Firewall

ipchains - operacije s lancima

- Napravi novi lanac `ipchains -N`
- Briši korisnikov lanac `ipchains -X`
- Zadaj politiku `ipchains -P`
- Izlistaj pravila `ipchains -L`
- Isperi pravila (*flush*) `ipchains -F`
- Nuluj brojače (*zero*) `ipchains -Z`

Firewall

ipchains - operacije s pravilima

- Dodaj novo (*add*) `ipchains -A`
- Umetni novo (*insert*) `ipchains -I`
- Zamijeni (*replace*) `ipchains -R`
- Izbriši (*delete*) `ipchains -D`
- Provjeri (*check*) `ipchains -C`

Firewall

ipchains - argumenti pravila

- Protokol `-p {TCP|UDP|ICMP}`
- Interface `-i {ppp|eth+}`
- Adresa izvora `-s 192.168.0.1`
- Adresa odredišta `-d 192.168.0.1`
- Bidirectional `-b 192.168.0.1`
- Blokiraj SYN paket `-y`
- Detaljan ispis `-v`
- Logiraj paket `-l`

Firewall
ipchains - argumenti (2)

- Jump-to-Target – što uraditi s paketom?

`-j ACCEPT`	– propusti paket
`-j REJECT`	– blokiraj paket
`-j DENY`	– blokiraj paket kao da nije ni stigao
`-j MASQ`	– IP Masquerade
`-j REDIRECT`	– preusmjeri UDP/TCP paket
`-j RETURN`	– skok na kraj lanca (politika)

Firewall

ipchains - politika lanca

- Ako ponašanje filtera nije određeno pojedinim pravilom, primijeni opću politiku za taj lanac

  - `-P ACCEPT` prihvati paket
  - `-P DENY` odbaci paket
  - `-P REJECT` odbaci paket uz obavijest
  - `-P MASQ` samo za `forward` lanac

Firewall
ipchains - grananje

- Filtriranje se odigrava poput grananja u programu:

```
if [cond1] then -j ACCEPT
else if [cond2] then -j DENY
else if [cond3] then -j MOJ_LANAC
else if [cond4] then -j RETURN
…
else apply chain policy
```

- Filtriranje se nastavlja kroz slijedeći lanac pravila

Firewall
ipchains - primjeri

- Blokiraj ping
  - ping šalje ICMP tip 8 (echo request)
  - vraća se ICMP tip 0 (echo reply)

```
# ipchains -A input -s 127.0.0.1 -p icmp -j DENY
# ping -c 1 127.0.0.1
 --- 127.0.0.1 statistics ---
1 packets transmited,0 packets received,100% packets \
   lost
```

Firewall
ipchains - primjeri (2)

- Zabrani sve TCP servise osim WWW

```
# ipchains -A input -p tcp -d 0.0.0.0/0 -j DENY ! www
```

- Servis se može odrediti i brojem porta

```
# ipchains -A input -p tcp -d 0.0.0.0/0 -j DENY ! 80
```

Firewall
ipchains - primjeri (3)

- Dozvoli surfanje po Webu za svoje korisnike, zabrani pristup izvana na svoj Web server (Intranet)

  - problem: TCP traži da paketi idu u oba smjera
  - rješenje: zabrani SYN pakete za uspostavljenje veze

```
ipchains -A input -p tcp -s ! 161.53.122.0/24 -y www
```

- Posve zabrani surfanje!?

```
ipchains -A input -p tcp -s 0.0.0.0/0 -y www
```

ili

```
ipchains -A input -p tcp -j DENY www
```

Firewall
ipchains - primjeri (4)

- Logiraj sav promet s određene adrese

```
# ipchains -A input -s 161.53.2.130 -p any -l
```

kernel log:

```
Packet log: input DENY eth0 PROTO=17 161.53.2.130:53 \
161.53.2.100:1054 L=34 S=0X00 I=18 F=0x000 T=254 (#6)
```

....

PROTO=17 je UDP paket na port 53, znači DNS upit, source/destination adresa, L byte lenght,

#6 je broj pravila u lancu

Firewall
ipchains - primjeri (5)

- Dozvoli Ssh pristup samo s povjerljiva hosta

```
# ipchains -A input -s 161.53.2.100 -p TCP -j ALLOW 22
```

- Anti spoofing

```
# ipchains -A input -p all -j DENY -s 161.53.122.0/24 -i eth1
# ipchains -A input -p all -j DENY -s 127.0.0.0/8 -i eth1
# ipchains -A input -p all -j DENY -s 192.168.0.0/16 -i eth1
```

Firewall

TIS Firewall Toolkit

- Skup programa i konfiguracija
- Open source
- Ne nudi gotova rješenja, već alate
- Svaka mreža ima svoju topologiju, hardware, zahtjeve poslovanja, administrativne postupke – nema univerzalnih rješenja
- Verifikacija – zaštita od bugova u aplikaciji
- www.tis.com

Firewall

TIS Firewall Toolkit (2)

- Poboljšani standardni servisi (chroot, nepriviligirani korisnik, liste pristupa, ne mogu pokrenuti shell)
- Smap – dostava pošte
- Netacl: Telnet, Finger, Network Acess Control
- Ftp-Gw, Telnet-Gw, Rlogin-Gw, Plug-Gw

Za administriranje firewalla:

- Authd, Telnetd, Login, Syslogd (real time scanning, alarmi), Ftpd

Firewall

Apache kao HTTP proxy

- Jednostavan firewall za HTTP i FTP servise,

  - vanjski klijent kontaktira jedan port, unutarnji drugi

  - radi u oba smjera: *forward proxy/reverse proxy*
- *Cache* – efikasnije korištenje spore linije, rasterećuje i udaljene servere
- Kontrola pristupa (autentifikacija hosta/korisnika)

Firewall
Squid

- Apache zadovoljava za manje mreže (CARNetove članice), za velik promet efikasniji je Squid (proxy.carnet.hr)
- Podržava više protokola: HTTP, FTP, GOPHER, WAIS, SSL
- Sve vrste Unixa i MacOS, nema verzije za Windowse
- Troši dosta HW resursa
- squid.nlanr.net

Firewall
Solaris

- SunScreen
  - mrežna kontrola pristupa i logging
  - komercijalan proizvod
- SunScreen Lite
  - besplatan za Solaris 8
  - ograničenje na dva mrežna interfacea
- IP Filter
  - freeware alternativa koju preporučuje SUN

Firewall
ipfilter

- Razvijen na BSD Unixu
- Radi na Free/Net/OpenBSD verzijama
- Prenesen na SunOS 4.1.1-4.1.4,
  Solaris >2.3, IRIX 6.2, QNX, HP-UX 11.00
- coombs.anu.edu.au/ipfilter
- HOWTO, dobri primjeri s objašnjenjima
  www.obfuscation.org/ipf
- CARNet paket na ftp.carnet.hr

Firewall
ipfilter - alati

- ipf – umeće pravila u listu, briše ih (flush)
- ipfstat – pokazuje statistiku prometa
- ipftest – testira pravila slanjem paketa
- ipmon – pokazuje sadržaj buffera
- ipsend – generira IP paket za eth LAN
- ipresend – učita pakete (tcpdump) i vraća ih
- iptest – provjerava obranu (može srušiti OS)
- ipnat – uspostavlja/briše pravila za NAT

Firewall
ipfilter - pravila

- Konfiguracijska datoteka s pravilima
- Razumljiva sintaksa (block in from, pass out ...)
- Drugačije odlučuje nego ipchains:

  - provjerava sva pravila redom do kraja

  - kada nađe pravilo koje odgovara za paket, digne zastavicu (prolazi/ne prolazi)

  - provjerava ostala pravila te odluči na osnovu zadnje zastavice, odnosno zadnjeg pravila koje odgovara
- `block in all`

  `pass  in all #rezultat: prolazi sve!`

Firewall
ipfilter - primjeri

- Ključna riječ *quick* priječi provjeru preostalih pravila

```
block in quick all
pass  in all  #svi paketi blokirani!!!
```

- Blokiraj pakete s određene adrese (npr. cookies iz doubleclick.com)

```
block in quick form xxx.xxx.xxx.xxx/32
pass in all
```

Firewall
ipfilter - primjeri (2)

- Primjeri adresa koje bi trebalo blokirati:

```
# privatne adrese
block in quick on tun0 from 192.168.0.0/24 to any
block in quick on tun0 from 172.16.0.0/12 to any
block in quick on tun0 from 10.0.0.0/8 to any
# default gateway
block in quick on tun0 from 0.0.0.0/8 to any
# DHCP auto konfiguracija
block in quick on tun0 from 169.254.0.0/16 to any
# rezervirano za pisce dokumentacije
block in quick on tun0 from 192.0.2.0/24 to any
```

Firewall
ipfilter - primjeri (3)

- Blokiranje nesigurnih servisa (portova)

```
block in log quick proto tcp from any \
 to 161.53.122.0/24 port 513 #rlogin
block in log quick proto tcp from any \
 to 161.53.122.0/24 port 514 #rsh
block in log quick proto tcp from any \
 to 161.53.122.0/24 port 23 #telnet
block in log quick proto tcp/udp from \
 any to 161.53.122.0/24 111 #portmap
pass in all
```

Firewall
ipfilter - primjeri (4)

- Fragmentirani paketi mogu biti maliciozni

  - blokiraj ih sve

```
block in all with frag
```

  - ili barem najsumnjivije

```
block in proto tcp all with short
```

- Pravila za prolaz stavi prije blokade:

```
pass in quick on tun0 icmp-type 0
pass in quick on tun0 icmp-type 8
block in log quick on tun0 icmp from \
 any to any
```

Firewall

ipfilter - primjeri (5)

Keep state – prati stanje, flags S - SYN, keep frags

- Blokiraj sve osim Ssh

```
block out quick on tun0 all
pass in quick on tun0 proto tcp from any to \
  161.53.122.3/32 port = 22 flags S keep state keep \
  frags
```

- Zaštićena radna stanica

```
block in quick on tun0 all
pass out quick on tun0 proto tcp/udp from \
  161.53.122.13/32 to any keep state
pass out quick on tun0 proto icmp from \
  161.53.122.13/32 to any keep state
```

- UDP je *stateless* protokol! Ipf prati stanje 60 sekundi.

Firewall
ipfilter - primjeri (6)

- Pogled u neposrednu budućnost:

  IPSec bitovi u zaglavlju paketa

```
# blokiraj pakete bez IP sec opcije
block in all with no opt sec
# propusti pakete na le1 s najvišom sigurnosnom
   klasom
block out on le1 all
pass out on le1 all with opt sec-class topsecret
block in on le1 all
pass in on le1 all with opt sec-class topsecret
```

Firewall
ipfilter – skrivanje firewalla

- Ako blokiramo pakete bez odgovora, otkrivamo firewall. Bolje je simulirati standardne Unix odgovore na upite koji stižu na neaktivan port.
- TCP port - vrati RST (Reset) paket

```
# vraćamo poruku "connection refused" umjesto \
  "connection timed out"
block return-rst in log proto tcp from any \
 to 161.53.122.0/24 port = 23
```

- UDP port - vrati ICMP port unreachable

```
block return-icmp-as-dest(port-unr) in log \
 on tun0 proto udp from any to 161.53.122.0/24 \
  port = 111
```

Firewall

ipfilter – skrivanje firewalla (2)

- Kad firewall propušta paket, ponaša se kao router, umanjujući vrijednost TTL-a, te tako otkriva da je ovdje jedan “hop”. Traceroute će otkriti naš firewall!

```
block in quick on xl0 fastroute proto udp from any to
   any port 33434>< 33465
```

- *Fastroute* će spriječiti slanje paketa u Unix IP stack radi usmjeravanja, te se TTL ne mijenja. Ipf će sam usmjeriti paket na odgovarajući interface, koristeći sistemsku routing tabelu.
- Da smo umjesto `block quick` koristili `pass`, uz uključen IP forwarding, ipf bi se zbunio jer bi imao dvije moguće putanje za izlaz paketa.

Firewall
ipfilter - NAT

- Jednostavna sintaksa za uključivanje NAT-a

```
map tun0 192.168.1.0/24 -> 161.53.122.1/32
```

- Ako ne znamo vanjsku adresu (DHCP)

```
map tun0 192.168.1.0/24 -> 0/32
# nakon prekida veze treba osvježiti adresu:
ipf -y
```

- Da bi svaki host u LAN-u dobio svoj port

```
map tun0 192.168.1.0/24 -> 0/32 portmap tcp/udp
20000:30000
```

Firewall
ipfilter - podešavanje kernela

- Podešavanje varijabli kernela na Solarisu

```
ndd -set /dev/ip ip_forwarding 1

ndd -set /dev/tcp tcp_smallest_anon_port 25000

ndd -set /dev/ip ip_forward_directed_broadcasts 0

ndd -set /dev/ip ip_forward_src_routed 0

ndd -set /dev/ip ip_respond_to_echo_broadcast 0
```

Firewall

Vježba: dvije politike

- Otvorena: sve je dozvoljeno što nije izričito zabranjeno.

`Dozvoli sve osim NFS, Talk i Finger servisa.`

- Paranoična: sve je zabranjeno što nije izričito dozvoljeno

`Zabrani sve osim FTP, WWW, E-mail i DNS servisa.`

- Zadatak: napiši `input` pravila po gornjim obrascima za ipchains ili ipfilter (po izboru).

Firewall
VPN

- Prividna privatna mreža (*Virtual Private Network*)
- Simulacija privatne mreže preko javne mreže
- Prividna - privremena veza, neizvjesna ruta
- Privatna - skrivanje informacija, nevidljivost
- Ekonomičnost - umjesto skupe iznajmljene linije koristimo Internet
- Upitan QoS - Internet ponekad zapinje!

Firewall
VPN - privatnost

- Internet je nesiguran!
- Kako osigurati privatnost?

  - firewall
  - enkripcija
  - autentifikacija računala/korisnika
  - skrivanje/maskiranje informacija o privatnoj mreži

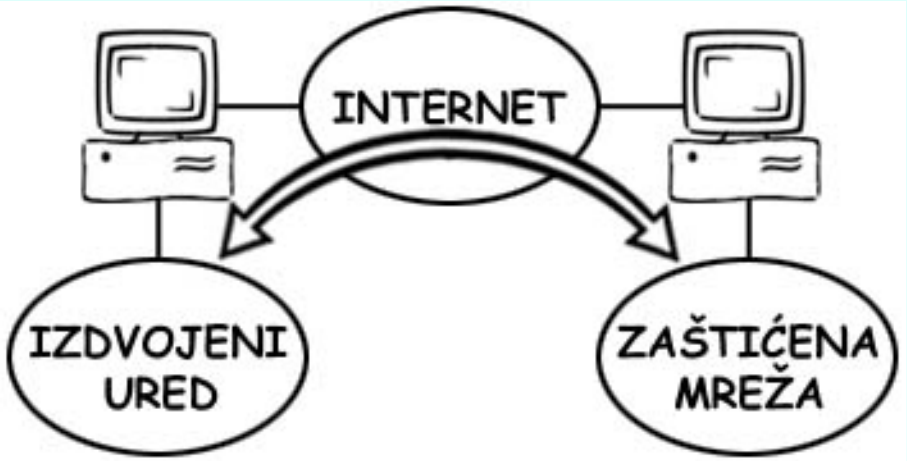
Firewall
VPN - metode

- Metode enkripcije:
  - secret key (DES)
  - public key (PGP, RSA)
  - IPSec (enkripcija na IP razini)
- Metode autentifikacije
  - CHAP (RFC 1994), RSA
  - obje strane izračunaju hash funkciju ključa
  - provjera na početku i u proizvoljnim razmacima
  - checksum podataka radi provjere integriteta

Firewall

VPN - tuneliranje

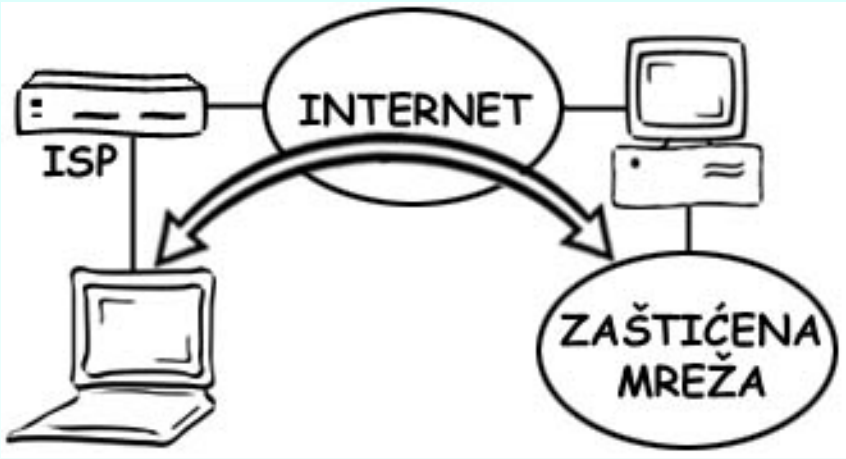
- Kriptiran paket putuje unutar običnog
- Enkapsulacija - unutarnji paket može biti različitog protokola (IPX)



Firewall

VPN - mobilni korisnici

- Tunel između privatne mreže i mobilnog računala s promjenjivom IP adresom



Firewall
Vrste VPN-a

- Zasnovan na HW
  - enkriptirajući router (poseban čip za enkripciju)
  - jednostavna konfiguracija, efikasnost, ali ograničena fleksibilnost
- Zasnovan na firewallu
  - sigurnosni mehanizmi (filtriranje, liste pristupa, NAT, opsežno logiranje, alarmi, autentifikacija, enkripcija ...)
  - troši HW resurse
- VPN aplikacije
  - tuneliranje na razini protokola ili IP adrese
  - primjenjivo u šarenilu opreme, OS-ova (npr. različite tvrtke)

Firewall
PPTP

- Protokol je razvio konzorcij nekoliko tvrtki, poznat je po Microsoftovoj implementaciji
- Zamišljen kao enkapsulacijski mehanizam za transport drugih protokola (IPX) preko TCP/IP-a, koristeći GRE (*generic routing encapsulation*)
- Dozvoljava različite mehanizme za autentifikaciju/enkripciju

Firewall
PPTP (2)

- PPTP server – Win NT 4.0 ili 2000
- Uključen IP forwarding i RAS
- Klijenti – WfW, Win95/98/NT, Macintosh
- Autentifikacija na razini MS domena
- Pristup preko interneta – Internet Authentication Services, RADIUS

Firewall
PPTP (3)

- Sigurnosni problemi:

  - slaba enkripcija (ključ je password, slab session ključ, 40 ili 128 bita - samo u USA)

  - lako je ukrasti passworde

  - nema autentifikacije na razini paketa, što omogućuje spoofing i DoS napade

  - MSCHAP je ranjiv (v. l0phtcrack)

Firewall
IPSec

- IP Security Protocol
- AH (Authentification Header) – štiti informacije u zaglavlju paketa – RFC 2402
- ESP (Encapsulating Security Payload) – štiti podatke u tijelu paketa – RFC 2406
  - povjerljivost
  - integritet podataka
  - autentifikacija – digitalni potpis
  - zaštita od ponavljanja

Firewall
IPSec i NAT

- NAT prepisuje zaglavlja paketa, što onemogućava AH
- Tuneliranjem se enkapsulira cijeli originalni paket, pa se kriptira. Na cilju se dekriptira prije autentifikacije. NAT je moguć u vanjskom “omotu”.
- Razmjena certifikata VPN gatewaya ne ide kroz NAT gatewaye!
- CISCO: IPSec over UDP, dopušta NAT

Firewall
Firewall piercing

- Firewall uobičajeno propušta E-mail
- Slanjem E-maila s PGP autentifikacijom aktivira se *procmail* skripta koja otvara *PPP* link enkapsulacijom kroz *SMTP*!
- Nakon toga *Telnet* ili *Ssh* prolaze kroz firewall
- Trik koristan za udaljeno administriranje kroz firewall, ali može poslužiti i korisnicima iza vrlo restriktivnog firewalla, odnosno crackerima.

Firewall
Komercijalni proizvodi

- Teže integraciji
  - Firewall
  - VPN
  - Antivirus
  - IDS
  - Centralni nadzor, upravljanje, praćenje opterećenja
- Događaji okidaju programirane akcije: slanje E-maila, rekonfiguraciju firewalla …
- www.checkpoint.com

Firewall
Zaključak

- Internet sve više postaje neprijateljska sredina
- Što je firewall? Raznovrsan software, može biti raspršen na više računala, ali i zatvoren u jednu kutiju.
- Osnovna namjena FW: ograničavanje i nadzor prometa, na različitim razinama TCP protokola (mrežni/aplikacijski, ali i transportni – interface)
- CARNet: jedan sistemac - Katica za sve!
- Prva briga je funkcionalnost, o sigurnosti se misli tek kada se pojave problemi
- Firewall traži sigurnosnu politiku (u protivnom - improvizacija, prepravljanje, nezadovoljstvo korisnika …)
- Nemojte se učiti na živom sistemu, jer ćete se “upucati u nogu”!

Firewall
Literatura

- *Building Internet Firewalls*
  Chapman & Zwicky, O'Reilly 1995
- *Professional Apache*
  Peter Wainwright, Wrox Press 1999
- www.interhack.net/pubs/fwfaq
- netfilter.kernelnotes.org
- www.linux-firewall-tools.com
- RFC 1918: adrese za nepovezane ili privatne mreže
- www.linuxdoc.org/HOWTO/IP-Masquerade-HOWTO.html … firewall-HOWTO …

NFS
Povijest

- SUN Microsystems 1985.
- Isprva se koristio za radne stanice bez diskova
- Ubrzo je postao popularan i doživio mnoge implementacije (U*X, DOS, Windows ...)
- Standard za file sharing u mrežama Unix računala
- U mješovitim mrežama prevladava Samba

NFS
Svojstva

- Dizajniran da se koristi u LAN-u i da bude brz
- Koristi UDP transportni protokol
- Klijent dobije `magic cookie`, koji preživi pad veze. Briše ga `umount` naredba.
- *Stateless*, ne prati stanje otvorene veze

  - nakon prekida klijent nastavlja raditi kao da se ništa nije dogodilo

  - klijent ne smije jednostavno pretpostaviti da će server obaviti svoj dio posla

  - neefikasno u WAN okruženju, kroz router, preko Interneta

NFS
Sigurnosni problemi

- Proizlaze iz korištenja UDP protokola:
  - nema dnevnika transakcija
  - nesigurne transakcije
  - slaba autentifikacija hosta
- Nema uvjerljive autentifikacije na razini korisnika (samo UID i GID)
- Opasnost od nemarne konfiguracije

  `access=lista, ro`

  Firewall neka brani NFS pristup preko Interneta

NFS
Klijent/poslužitelj

Poslužitelj

- `mountd` - dodavanje mrežnog diska
- `nfsd` - pristup datotekama na disku

Klijent

- Proširena mount naredba
  `hostname:direktorij`
- `biod` – cacheing daemon

NFS
Konfiguracija

- BSD verzije zovu dijeljenje diska `export`
- SYSV (ATT) verzije - `share`

Linux: `/etc/exports`

```
/home/prj access=orah:ljesnjak,root=orah
```

Solaris: `/etc/dfs/dfstab`

```
#!/bin/sh
share -F nfs -o rw=orah:ljesnjak,\
  root=orah  /home/prj
```

NFS
Konfiguracija (2)

atributi pristupa	mount flags
-access=lista	-ro, rw
-ro	-bg
-rw	-hard,soft,spongy
-ro=lista	-retrans=n
-rw=lista	-timeo=n
-root=lista	-intr
-anon=n	-rsize=n, wsize=n

NFS
Dodavanje NFS particija

- Ručno

```
mount host:share /mnt/nfs
```

- Pri podizanju sustava

```
#/etc/fstab
as:/opt  /mnt/opt nfs rw,bg,intr,hard 0 0
```

- Automatski

  SUNov `automount`

  freeware `amd`

NFS
NFS daemon

- `Nfsd` posreduje pri U/I operacijama na disku
- Pri pokretanju prima argument, broj procesa

  `nfsd -n`

  - minimalan 4
  - maksimalan 8 (Linux) ili 10 (Solaris)
  - optimalan utvrdite eksperimentalno

  `netstat -s`

  eliminirati UDP socket overflow

NFS
Administativne zavrzlame

- Ne dozvolite anoniman pristup, popunite access liste
- Korisnici neka na NFS serveru imaju otvoren račun
- UID i GID moraju biti isti na svim računalima!

  (replicirajte korisnike i grupe – NFS je zamišljen da radi uz NIS)
- Shell može biti `/bin/false`
- Mount direktorij kod klijenta neka se zove jednako kao i NFS server

  `(bor:/projekt na /bor/projekt)`

NFS
Literatura

- *Unix System Administration Handbook*
  Nemeth, Snyder, Seebass, Hein
  Prentice Hall, 1995

- www.linuxdoc.org/LDP/nag/node141.html

Samba

- Unix file i print server za Windows klijente
- GPL licenca
- Open Source
- Pouzdanost Unixovih servisa dostupna desktop računalima
- Slogan razvojnog tima:

  “Samba – opening Windows to a wider world!”

Samba
Povijest

- BIOS (Basic Input Output System) dio DOS-a, definira kako aplikacije traže U/I operacije od OS-a
- NetBIOS proširenja za U/I operacije preko mreže
- NetBEUI (NetBIOS Extendeded User Interface)
  - NetBIOS API
  - SMB (Session Message Block)
  - NBF (NetBIOS Frame protokol)
- CIFS (Common Internet File System) koristi TCP/IP i NetBIOS over TCP/IP name service (NBT)
- Od jednokorisničkog sistema, preko LAN protokola do WAN protokola

Samba
Instalacija

- Binarni paketi

```
dpkg -i samba-2.2.2.pkg
dpkg -i samba-docs.2.2.2.pkg
dpkg -i smbfs-2.2.2.pkg #samo za Linux
```

- Izvorni kod raspakira se u /usr/local/src

```
# tar xzvf samba-2.2.2.tgz
# cd samba-2.2.2
# ./configure; make; make install
```

- /etc/profiles

```
PATH="$PATH:/usr/local/samba/bin"
MANPATH="$MANPATH:/usr/local/samba/man"
```

Samba

Osnovni dijelovi

- `smbd` samba daemon
- `nmbd` NetBIOS name server
- `testparm` provjera konfiguracije
- `testprns` provjera tiskača
- `smbstatus` provjera statusa Sambe
- `nmblookup` traženje Windows računala sa Unixa
- `smbclient` klijent za pristup dijeljenom resursu
- `smbprint` klijent za pristup SMB print serveru
- `/etc/smb.conf` `/etc/smbpasswd` `/etc/smbusers`
- `swat` alat koji olakšava konfiguraciju

Samba
Inetd

- #/etc/services

```
netbios-ns      137/tcp  nbns
netbios-ns      137/udp  nbns
netbios-dgm     138/tcp  nbdg
netbios-dgm     138/udp  nbdg
netbios-ssn     139/tcp  nbssn
```

- #/etc/inetd.conf

```
netbios-ssn stream tcp nowait root \
   /usr/sbin/tcpd /usr/sbin/smbd
netbios-ns dgram udp wait root \
   /usr/sbin/tcpd /usr/sbin/nmbd -a
```

- **/etc/init.d/samba start|stop|restart**

Samba
rc.samba

- `/etc/rc.d/rc.samba`
  koji se pokreće iz `/etc/rc.d/rc.local`

```
#!/bin/sh
/sbin/smbd -D
/sbin/nmbd -D
```

Samba

Jednostavan test

Unix

```
$ testparm
$ smbclient '//server/homes' -Uusername
$ ls -l
```

Windows

- `Network_Neighbourhood\Entire_Network\`
  `\Workgroupname\servername\homes`
- `C:> net view \\moj_server`
  `C:> net view /workgroup:workgroupname`
  `C:> net use * \\moj_server\homes`
- `Start,Find,Computer`

Samba

Windows name resolution

Metode nalaženja računala u mreži:

- `/etc/smb.conf`

```
name resolve order=lmhosts host wins bcast
```

- `/etc/lmhosts` ili `C:\WINNT\System32\Drivers\Etc\lmhosts`

```
127.0.0.1 localhost
192.168.1.1 moj_server
```

- host – NIS, DNS, `/etc/hosts`
- Windows Internet Name Service
- Broadcast – NetBIOS name resolution, portovi 137-139

Samba

Mapiranje atributa

DOS	UNIX	`smb.conf`	`default`
+r	u-w		
+a	u+x	`archive=yes`	+
+s	g+x	`system=yes`	-
+h	o+x	`hidden=yes`	-

- `attrib +r file -> chmod u-w file`
- Dotfiles `.bashrc`?

  Skriveni, atribut ne može mijenjati s DOS-a.

Samba
Unix dozvole

Unix dozvole za datoteke preko Sambe podliježu logičkim operacijama nad bitovima

- Za datoteke: logička operacija
  - `create mask=` AND
  - `force create mode=` OR
- Za direktorije:
  - `directory mask=` AND
  - `force directory mode=` OR
- U slučaju konflikta, `force` ima prednost.
- AND umanjuje, OR uvećava Unix dozvole

Samba
Podrazumijevane dozvole

- Podrazumijevane dozvole za nove datoteke
- `create mask=744 #default`

  Unix: `-rwxr--r-` Win: `rash?`
- Samba napravi “bitwise AND”, stavite neparni broj!

```
create mask=755          # OK
create mask=700 -> 711 # za home dir.
create mask=770 -> 771 # za radne grupe
create mask=777    # svi Unix korisnici
mogu raditi što hoće na Samba shareu!?
```

Samba

smb.conf

```
[global]
   netbios name=moj_server
   workgroup=moja_grupa
   printcap name=/etc/printcap
   printing=bsd
[homes]
   browsable=no
   read only=no
[printers]
   print ok=yes
   path=/var/spool/samba
   browsable=no
   writable=no
   printable=yes
```

Samba
Share na Unixu

- Grupa za izradu web stranica dijeli direktorij:

```
mkdir /projects/web
chown root.web /projects/web
chmod 770 /projects/web
```

- Napravi share u `/etc/smb.conf`

```
[web]
   path=/projects/web
   read only=no
   valid users=@web
   create mask=770
   directory mask=770
   force group=web
```

Samba

Share za dvije grupe

- Dvije grupe pristupaju direktoriju, recenzenti mogu samo čitati.

```
[web]
   path=/projects/web
   read only=yes
   valid users=@web,@recenzenti
   write list=@web
   create mask=770
   directory mask=770
   force group=web
```

Samba
Kriptirana zaporka

Podrazumijeva se u NT/2000, Win98, Win95 OSR3

- `/etc/smb.conf:`

  `encrypt passwords = yes`
- `$ smbpasswd -a username`
- Win 95/98 Registry:

  `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VNETSUP\EnablePlainTextPassword=1`
- NT Registry

  `HKEY LOCAL_MACHINE\system\CurrentControlSet\Services\Rdr\Parameters\EnablePlainTextPassword=1`

Samba
Konfiguracija

```
[global]
log file=/var/log/samba/log.%m
max log size=50
security=user                    # ili share
password server=NTServerName # MDC
password level=8
username level=8
smb passwd file=/etc/smbpasswd
username map=/etc/smbusers    # razl.imena
```

Samba
Emulacija liste pristupa

```
[public]
  path=/home/projectX
  workgroup=grupaX
  valid users=<lista>
  admin users=marko
  write list=marko, pero
  invalid users=mrgud
  hosts allow=192.168.1. EXCEPT 192.168.1.111
  hosts deny=192.168.1.12
  guest ok=no
  guest only=no
```

Samba

Sinkronizacija zaporki

Istovremena promjena Unix i SAMBA zaporke s Windows klijenta

```
[global]
unix password sync=yes
password program=/usr/bin/passwd %n
passwd chat=*New*UNIX*password*%n\n \
            *Retype*password* %n\n \
            *passwd:*update*successful*
```

Samba
Dijeljeni pisač

- Na Unixu mora biti prijavljen kao jednostavan tekstualni pisač!
- Provjera da li /dev/lp radi dobro:

Na Unix prenesite FTP-om binarno c:\autoexec.bat

```
$ lpr -P lp autoexec.bat
```

S Windowsa:

```
C:> net use lpt9: \\moj_server\lp
C:> copy c:\autoexec.bat lpt9:
C:> echo ^L > lpt9:
```

- Nakon toga na Windowsima normalno prijavite pisač i instalirajte driver

Samba
Zaključak

- Nastoji pružiti najbolje iz dva svijeta
- Na slabijem računalu pruža pouzdane servise
- Nepotpuna funkcionalnost NT servera
  - Razlike OS
  - Microsoftovi standardi nisu otvoreni
- Samba može biti PDC, ali ako želite biti 100% sigurni, neka NT server bude Domain kontroler!
- Pazite na odnose vlasništva i Unix/Samba dozvola za direktorije i datoteke!
- Ne zaboravite: vidljivost nije isto što i pristup!

Samba
Literatura

- Steve Litt "*Samba Unleashed*"
  SAMS 2000
- NetBIOS – RFC 1001, 1002
- Dokumentacija u /usr/doc/samba-x.x.x
- www.samba.org

Print servisi
Unix

Dvije inačice:

- BSD koristi *lpd*
  - podržava mrežni rad
  - BSD, Linux, SunOS, Digital Unix
- SVR4 koristi *lpshed*
  - isprva namijenjen lokalnom tiskanju
  - Solaris, HP-UX

Print servisi
BSD

- *lpd* line printing daemon
- *lpr* stavlja datoteku u red za ispis
- *lpq* izlista queue
- *lprm* uklanja datoteke iz liste
- *lpc* interaktivno upravljanje
  pokreće/zaustavlja lpd, status, kontrola liste
- *lptest* ispiše standardni test

Print servisi
/etc/printcap

- Definicije podržanih pisača nizom varijabli
  : graničnik
  = pridružuje string
  ```
  lp=/dev/ttyXX    lf=log-file
  sd=spool-direktorij
  ```
  # pridružuje numeričku vrijednost
  ```
  pw#page-width:pl=page-length (chars)
  py#page-width:px#page-length (pixels)
  ```
  true/false logička varijabla
  ```
  ff:true:
  ```

Print servisi

Vrste pisača

- ASCII
- PS - PostScript
- PCL – Printer Control Language
- GDI – Windows Printing System

  izbjegavati na Unixu, oslanja se na OS i pogonske programe za MS Windows
- Da bismo mogli ispisivati ASCII na PS ili PCL itd. potrebni su nam filteri koji rade konverzije

Print servisi
Filteri

- `if=input-filter-name`
- Paket s filterima za različite pisače:

  APS Print Filters

`ftp://metalab.unc.edu/pub/Linux/system/\`
`printing/aps-499.tgz`

- Napravite direktorij /usr/local/apsfilter

```
# tar xzvf aps-499.tgz
./SETUP
```

Print servisi

Lokalni pisač

```
cert | Cert-Pr | Unix Cert Lab:\
  :lp=dev/edc:sd=/var/spool/cert:\
  :lf=/usr/adm/lpd_errs:\
  :af=/usr/adm/edcert.acct:\
  :if=/usr/local/bin/cert:\
  :pl#64:pw#80:px#300:py#300:\
  :br#9600:fc#0000010:fs#0000301
```

Print servisi

Mrežni pisač

```
wcps | WC-PostScript | WC Machine
Room:\
:lp=:\
:sd=/var/spool/wcps:\
:lf=/usr/adm/lpd-errs:\
:mx#0:\
:rm=wclaser.srce.hr:\
:rp=wclaser:
```

Print servisi
SVR4

- *lpsched / lpshut* - pokreće/zaustavlja daemona
- *lp / cancel* - ispis/zaustavljanje
- *lpstat* - status poslova
- *lpmove* - preusmjeri ispis na drugi uređaj
- *accept / reject* - prihvaćanje/odbijanje poslova
- *enable / disable* - omogući/zabrani rad pisača
- *lpadmin* - dodavanje i konfiguracija pisača

Print servisi
Solaris

Lp naredba ima dva oblika

- Zahtjev za ispis

```
lp -d dest -t title moj_rad.txt
```

- Zahtjev za promjenu opcija ispisa

```
lp -i reqId hold
```

Print servisi
Solaris (2)

- Opcije lp naredbe

```
-d      destination, uređaj
-n      number – broj kopija
-m      mail – posao obavljen
-o      opcije - nobanner,nofilebreak,
                 length, width
-H      special handling
        hold, resume, immediate
-P      page list
-lpi    lines per inch
-cpi    characters per inch
```

Print servisi
Literatura

- www.uwsg.indiana.edu/edcert/session2/peripheral/printer.html#svr4
- Linux Documentation Project

  www.linuxdoc.org/HOWTO/Printing-HOWTO/index.html

Antivirusna zaštita
Obrana

- Priprema (backup i boot diskete)
- Prevencija (korištenje licenciranog softvera, “prljavi PC”, obuka korisnika, GW/firewall)
- Otkrivanje (antivirusni programi)
- Izolacija (karantena)
- Oporavak

  - dezinfekcija (ako je moguća)

  - vraćanje izgubljenih podataka

Antivirusna zaštita

Antivirusne mjere

Priprema boot disketa za Win95/98

- `FORMAT A: /S`
- `HIMEM.SYS,EMM386.EXE,FDISK.EXE,SYS.COM,`
  `DEBUG.EXE,SMARTDRV.EXE,SCANDISK.EXE,FORMAT.COM`

REM CONFIG.SYS	REM AUTOEXEC.BAT
DEVICE=A:\HIMEM.SYS	A:\SMARTDRV.EXE
DEVICE=A:\EMM386.EXE	SET TEMP=C:\
DOS=HIGH,UMB	SET TMP=C:\
FILES=15	
BUFFERS=4	

Antivirusna zaštita
Antivirusne mjere (2)

- NT 4.0 - Emergency Repair Disk u kombinaciji s instalacijskim disketama
- NTFSDOS - pristup NTFS filesistemu iz DOS-a, odnosno DOS boot diskete
- NTFS for Windows 98
- Freeware verzije daju read-only pristup
- Komercijalne verzije s punim pristupom

Antivirusna zaštita
S|O|P|H|O|S

- MZT koristi antivirusni software tvrtke Sophos
- sav.srce.hr
- www.qubis.hr
- www.sophos.com

Antivirusna zaštita
Instalacija

- Pojedinačno na Windows klijente
- Peer-to-Peer Win95/98 mreža
- WinNT/2000 server
- Unix poslužitelj (Solaris/Linux)
- Dokumentacija o instalaciji u .pdf formatu na sav.srce.hr/Docs/doc.html

Antivirusna zaštita

Ključne riječi

- **IDE** datoteka s identifikacijom virusa
- **CID** Central Instalation Directory
- **SAVAdmin** alat za administriranje instalacije i dogradnje u LAN-u
- **Rollout number** redni broj instalacije, služi za sinkronizaciju CID i radnih stanica
- **SFG file** konfiguracijska datoteka
- **Template installation** centralno instaliranje na radne stanice

Antivirusna zaštita

Razdioba posla

- **InterCheck** - otkrivanje kod pristupa datoteci
  - usporava rad
- **Sweep** - na zahtjev ili periodički
- Dezinfekcija – opcija koju tek treba uključiti!

  disinfect boot sector

  disinfect documents

  infected files: delete, move ...

  - za uklanjanje nekih virusa treba skinuti s weba zaseban program i upute

Antivirusna zaštita
Skeniranje

- Brzo (*quick*) – pregledava samo dijelove datoteka koji su vjerojatno zaraženi
- Puno (*full*) – pregledava cijeli sadržaj datoteka - dobitak je mali, opterećenje veliko
- Provjera arhiviranih/komprimiranih datoteka

  ZIP, GZIP, RAR, ARJ, CMZ, TAR

  Pklite, LZEXE, Diet

Antivirusna zaštita
Unix

- Unix može biti prijenosnik virusa
  - ako je datotečni poslužitelj
  - ako je poslužitelj E-pošte
- Unix na PC platformi može se inficirati virusom koji se naseli u boot sektor!
  - primjer: Virus Michelangelo
  - 6.4. (Michelangelov rođendan) pobriše početne sektore diska, gdje su vitalni podaci (boot sektor, tabela particija, FAT tablice, direktoriji …)
  - disk ostaje neupotrebljiv bez obzira na OS

Antivirusna zaštita
Autorizacija datoteka

- InterCheck vodi listu autoriziranih datoteka
- U trenutku pristupa provjerava listu, po potrebi šalje datoteku na skeniranje
- Ukoliko je čista, stavlja je u listu
- Ukoliko je inficirana, izvještava o virusu i brani pristup
- Ako je uključena dezinfekcija, dokument ili boot sektor bit će očišćeni, datoteka se zatim ponovo skenira i stavlja na listu

Antivirusna zaštita
Instalacija

- Dodajte korisnika/grupu `sweep`, ljuska `/bin/false`
- `dist.tar` raspakirajte u `/tmp/sweep`

```
# tar xvf dist.tar
```

- Sadržaj `sav-install` poddirektorija

```
install.sh
sweep, icheckd
libsavi.so.2.2.03.???
Readunix.txt, Install.txt
icheckd.1, icheck.conf.5, sweep.1
vd1.dat
```

- Sačuvajte originalni `/etc/sav.conf`!

Antivirusna zaštita
Instalacija (2)

- `# cd sav-install`

  `# ./install.sh`
- Instalira u `/usr/local (bin,man,lib)`
- Dijeljeni direktorij (Samba)

  `/var/spool/intercheck`
- U njemu su dva poddirektorija

  `chmod 0700 infected`

  `chmod 1777 comms`

Antivirusna zaštita
Instalacija (3)

- Time je instaliran InterCheck Server za centralno skeniranje i izvještavanje u mreži klijenata koji nisu Unix radne stanice.
- Opcije pri instalaciji:
  `-ni` instaliraj samo Sweep
  `-idc` instaliraj IC za klijente bez diska
- Provjerite:
  je li `/usr/local/bin` uključen u `PATH`
  je li `/usr/local/man` uključen u `MANPATH`
  je li `/usr/local/lib` uključen u `LIBPATH`

Antivirusna zaštita
InterCheck poslužitelj

- Pokretanje:

```
# /usr/local/bin/icheckd
```

- Opcije:

```
-d              radi kao daemon
-nd             ne radi kao daemon
-c <file>       konfiguracijska datoteka
-h              upute
```

- Zaustavljanje:

```
# icheckd -stop
```

- Konfiguracija u `/etc/icheckd.conf`

Antivirusna zaštita
Centralno izvještavanje

- Na Windows klijente instalirajte SAV: skeniranje se obavlja lokalno, ali izvještaji se šalju InterCheck poslužitelju
- Pri instalaciji odaberite:
  - Central Installation
  - Enable InterCheck Client

Antivirusna zaštita
Konfiguracijski program

- DOS – ICONTROL.EXE
- Windows – ICW.EXE
- Unix – član grupe `sweep` može pokrenuti ICONTROL

Antivirusna zaštita
Mrežna instalacija

S Windows klijenata

- pomoću programa Setup:

```
\\Server\INTERCHK\W95inst\Setup -INL -A
```

- pomoću programa ICLOGIN:

```
NET USE I:   \\Server\INTERCHK
I:\ICLOGIN -A
```

umjesto `\\Server` upišite ime vašeg poslužitelja

umjesto `\INTERCHK` upišite ime dijeljene mape

Antivirusna zaštita
Dogradnja

- Sophos:

(izbrišite sve definicije virusa iz CID direktorija)

```
SGET http://www.sophos.com/downloads/ide/ides.zip
```

Ili napišite skriptu koju će aktvirati E-mail s naslovom:

```
Sophos Anti-Virus IDE alert: <virusname>
```

- SRCE:

```
wget -m -np -nH --cut-dirs=1 \
  http://korisnik:lozinka@sav.srce.hr/Sophos.CD/
```

(uzima samo promijenjene datoteke)

Antivirusna zaštita
Amavis

- A Mail Virus Scanner
- Da bi radio zahtijeva AV software (npr. Sophos), arhivere (zoo, arc...), GNU file naredbu, dodatne Perl module
- /var/spool/mqamavis, dozvole kao za /var/spool/mqueue
- Restartajte Sendmail
- Konfiguracija CARNetova paketa pregledava dolazeću i odlazeću poštu
- Podešavanje prioriteta (*nice*)

Antivirusna zaštita
Literatura

- Informacije o virusima:

  www.sophos.com

  www.datafellows.com/virus-info/

  www.securityfocus.com

  www.antivirus.com
- Popularne zablude o virusima:

  www.vmyths.com

Baze podatka
Raspoloživi programi

- Kriteriji za odabir:
  - Open source, freeware
  - Podrška (online dokumentacija, mailing liste, newsgrupe)
  - Vitalnost (kontinuiran razvoj, ispravke, dogradnje ...)
  - Široka baza korisnika
  - Raspoloživost dodatnih alata i aplikacija
  - Integracija s Apache web serverom

Baze podataka
MySQL

- Licenca: GPL
- OS: MacOS, Windows 95/98/NT/2000, OS/2, AIX, HP-UX, IRIX, SCO, BSD, Solaris, Linux
- www.mysql.com

Baze podataka
Postgres

- Objektna relacijska baza podataka
- Istraživački projekt sveučilišta Berkeley
- Licenca: BSD
- OS: MacOS, Win NT/2000, BeOS, BSD, Linux, AIX, Solaris, SCO, IRIX, HP-UX, Tru64
- www.postgresql.org

Baze podataka
Sybase

- Licenca: komercijalan proizvod
  besplatna Linux verzija
- OS: MacOS, Win NT/2000, BSD, Linux, AIX, Solaris, SCO, IRIX, HP-UX,Tru64
- www.sybase.com

Baze podataka
IBM DB/2

- Licenca: komercijalan proizvod, ali na Linuxu besplatan za nekomercijalu uporabu
- OS: Windows, Linux, Solaris, HP-UX, AIX, OS/2, AS/400, OS/390, Windows CE, Palm
- www.ibm.com/linux (slijedite link) ili ww.ibm.com/db2/linux

Baze podataka
PHP

- Programski jezik integriran u HTML (*embedded*)
- Specijaliziran za rad s bazama podataka
- Apache modul (*mod_php*)
- Dinamičke web stranice, korisnik unese podatke od kojih se generira database querry
- www.php.org

Baze podataka
MySQL

- Zamišljen kao brza baza za male korisnike
- Podskup SQL standarda
- Locking na razini tablice (ovisno o OS)
- Brži pri čitanju nego pisanju
- Brzo i jeftino rješenje ako:
  - nema previše podataka
  - mali broj korisnika istovremeno pristupa podacima

Baze podataka
MySQL - instalacija

```
# tar xzvf mysql-x.xx.x.tgz
# cd /usr/local/src/mysql-x.xx.x
# ./configure prefix=/usr/local/mysql –with-mysqld-
  ldflags=-all-static –enble-large-files –with-charset-
  croat –with-thread-safe-client –with-berkeley-db
# make; make install
# echo “/usr/local/mysql/lib/mysql” >> /etc/ld.so.conf
# ldconfig
# echo “/usr/local/mysql/bin/safe_mysqld > /dev/null &”
  >> /etc/rc.d/rc.local
# ln -s /usr/local/mysql/bin/mysql /usr/bin/mysql
# ln -s usr/local/mysql/bin/mysqlshow /usr/bin/mysqlshow
ili
# PATH=“$PATH:/usr/local/mysql/bin”; export PATH
```

Baze podataka
MySQL - post-instalacija

- ```
  ./scripts/mysql_install_db
  cd mysql_installation_directory
  ./bin/safe_mysqld -user=mysql &
  ```
- Time smo kreirali MySQL bazu koja će sadržavati korisničke privilegije i testnu bazu, te pokrenuli `mysql` daemona
- Testnu bazu možete kasnije izbrisati:

  ```
  mysqladmin -u root drop test
  ```


  ```

Baze podataka
MySQL - post-instalacija (2)

- Ako niste kreirali *grant table,* pri pokretanju dobijete poruku:

```
# mysqld: Can't find file: 'host.frm'
```

- `# BINDIR/mysqladmin version`

```
Mysqladmin Ver. 8.14 Distrib 3.23.32, for
  Linux i586
Server version    3.23.32
Protocol version 10
Connection        Localhost via Unix socket
TCP port          3306
UNIX socket       /tmp/mysql.sock
Uptime            20 sec
```

Baze podataka
MySQL - proba

- Spuštanje daemona

```
# mysqladmin -u root shutdown
```

- Pokretanje

```
# safe_mysqld -log &
```

-

```
# mysqlshow
+------------+
| Databases  |
+------------+
| mysql      |
+------------+
```

Baze podataka
MySQL - prvi koraci

- ```
  # mysqlshow mysql
  Database: mysql
  +--------------+
  | Tables       |
  +--------------+
  | columns_priv |
  | db           |
  | func         |
  | host         |
  | tables.priv  |
  | user         |
  +--------------+
  ```
  ```

Baze podataka
MySQL - vježba

```
# mysql -h localhost -u <user> -p <pass>
# create database CARNET
# use CARNET
# create table sistemci (
  id          longint      autoincrement,
  ime         varchar(30)  not null,
  prezime     varchar(30)  not null,
  ustanova    varchar(60)  ,
  adresa      varchar(69)  ,
  telefon     varchar(20)  ,
  email       varchar(40) )
```

Baze podataka
MySQL - vježba (2)

```
# show tables
# describe sistemci
# insert into table sistemci
  (ime,prezime,ustanova,adresa,telefon,
  email) values (“Pero”, ”Perić”,
  ”Fakultet za prometne znanosti”, ”Ilica
  333”, “+385 1 3334444”,
  “Pero.Peric@fpz.hr” )
# select * from sistemci
# quit
```

Baze podataka

MySQL - administriranje korisnika

- Dodavanje korisnika

```
> INSERT INTO user VALUES
  ('localhost','admin',PASSWORD('h0moL2'),
  'Y','Y','Y','Y','Y','Y','Y','Y','Y','Y',
  'Y','Y','Y');
> FLUSH PRIVILEGES
```

- Dodjela prava

```
> GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP
  on sistemci.* to admin@localhost IDENTIFIED BY
  'h0moL2');
```

- Promjena lozinke

```
> INSERT INTO user (Host,User,Password) VALUES
  ('localhost','admin',PASSWORD('h0moL2'));
```

Baze podataka
Literatura

- www.php.net
- www.mysql.com
- www.linuxplanet.com/linuxplanet/tutorials/1046/1/
  (kako napraviti Web site zasnovan na MySQL-u)
- www.weberdev.com (primjeri koda)
- www.wernhart.priv.at/php (primjeri MySQL+PHP)
- www.ca.postgresql.org/idocs/
- www.sqlcourse.com (online priručnik)