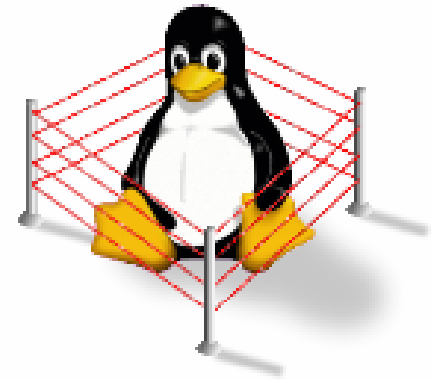


Sigurnost Linux operacijskog sustava



Verzija 1.0

Dinko Korunić, 2004.

O predavaču

- višegodišnji vanjski suradnik časopisa Mrež@, vlastita kolumna "Digitalna radionica - Linux", itd.
- vanjski suradnik SRCE-a: forenzike provaljenih sustava, izgradnja sistemskih paketa, helpdesk za sistemce, sigurnost Unix baziranih sustava, predavač, itd.
- sigurnosni ekspert pri InfoMAR d.o.o.
- Un*x/Linux sysadmin od 1996. :-)

Tijekom prezentacije

- **ako što nije jasno - pitajte i tražite objašnjenje!**
- **ako što nije točno - ispravite!**
- **diskusija** je poželjna i produktivna
- **ako je prebrzo - tražite da se uspori!**
- **ako je pak presporo i uspavljuje vas - lako se ubrza sa sadržajem**
- **podijelimo** zajedno vlastita iskustva, ideje, pitanja!

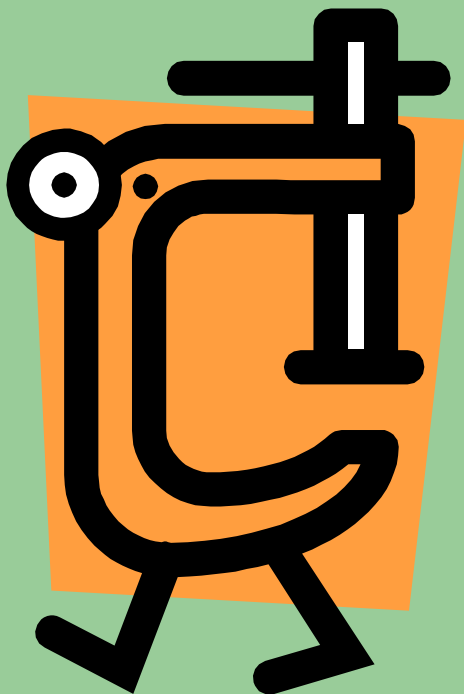
Konvencije

- popratni tekst i komentari
- **ključne riječi**
- naredbe i programi koje je moguće izvršavati u shellu
- *konfiguracijske datoteke i njihove lokacije*

Sadržaj

- računalna sigurnost općenito
- standardni problemi sa Linuxom:
 - dozvole, procesi, servisi, korisnici, lozinke, aplikacije, itd.
 - mrežni promet, firewall, pristupne liste, filtriranje prometa
- sigurnosne nadogradnje na Linux jezgru

Glede i u svezi



.. ili o svemu pomalo

Računalna sigurnost

- **što:** prevencija i detekcija nedozvoljenog korištenja računalnih i inih resursa
- **zašto:** nitko ne želi da mu "stranci" kopaju po privatnom sadržaju, a kamoli poslovnim tajnama
- **tko:** napadači (hackeri, crackeri, prolaznici) ne traže nužno vas kao osobu, već vaše računalo ili samo kakvu informaciju
- **kako:** kroz postojeće nesigurnosti (sigurnosne rupe) koje postoje u skoro svakom softveru bilo kao greška bilo kao zaboravljene postavke

Računalna sigurnost (2)

- interdisciplinarna:
 - sistemsko i aplikativno programiranje
 - telekomunikacija, mreže računala, itd.
 - kriptografija
 - sociološki problem:
 - sigurnosna politika
 - upravljanje korisnicima
 - podjela korisnika na tipove
 - procjena problematičnih korisnika

Internet - problem

- **dijeljenje** "podataka" preko Interneta
- virusi, trojanski konji, DoS napadi, socijalni inženjering = **zlonamjerni sadržaj**
- **milijuni** međusobno umreženih računala
- **"curenje"** informacija:
 - nedostatak obrazovanja
 - nedostatak predostrožnosti
 - nedostatak sigurnosnih mehanizama

Obrana!

- linije obrane:
 - **educirani korisnik/pojedinac**
 - **educirani sistem-inženjer** (Bugtraq, Securityfocus, CERT, itd.)
 - **hardver** (hw firewall, VPN, switchevi, VLAN, itd)
 - **softver** (system update, sw firewall, IPSec, IDS, antivirus, kriptografija: PGP, S/MIME, Kerberos, SSL, certifikati, tuneli, digitalni potpisi, CryptoAPI)
 - **security politika! backup!**

Internet danas

- broj računala:
 - **rapidno raste**, ne uvijek **poznat vlasnik** = akademske mreže, lažne adrese, lažni DNS
- opasnost:
 - od znatiželjnih prolaznika do dobro organiziranih, dobro tehnološki potkovanih "**terorista**"
 - razlog = novac, slava(?)
 - **opasnost rapidno raste**: broj napada i sofisticiranost rastu iz godine u godinu

Aksiomi

- **operacijski** sustavi imaju ranjivosti
 - **mrežni** uređaji imaju "slabe" točke
 - većina **protokola** ima "slabe" točke
 - **ljudski faktor!**
-
- svaki poslužitelj ili radna stanica - **provaljiva**
 - pitanje je koliko je **vremena** potrebno:
 - predzaštita, detekcija, logovi, zaštitni postupci

Provale

- činjenice:
 - ostvarivanje **nedozvoljenog pristupa** računalu
 - najčešće **repetitivno(!)**
 - služe za daljnje provale, trgovanje, ekstrakciju podataka, ucjenjivanje, poligone za DoS napade
 - **teško "očistiti" zarazu**
- **razlozi** da je došlo do provale:
 - nesavjesnost administratora i/ili korisnika
 - problem dozvola, opreme, OS-a ili pripadnih aplikacija

Curenje informacija

- **nesigurni** (cleartext) protokoli:
 - http, ftp, telnet, pop3, itd.
- rješenje? primjena moderne snažne **kriptografije!**
 - asimetrični algoritmi (pola + pola ključa)
 - šifriranje poruka, teksta, podataka, materijala!

Zanimljivosti

- što je **cracker/script-kiddie**?
 - koristi tuđe programe
 - slabo razumijevanje rada sistema
 - iskušava tuđe programe dok ne pogodi
- što je **hacker**?
 - piše vlastite programe za provalu i analizu
 - obično ne provaljuju
 - iznimno visok stupanj tehnološke potkovanosti
 - Whitehats, Grayhats, Blackhats

Zanimljivosti (2)

- Internet = sjecište različitih **grupacija**:
 - **systemci** - CERT, SANS, itd.
 - **systemci** i **hackeri** zajedno - Bugtraq, SecurityFocus, LinuxSecurity, itd.
 - **crackeri** i **script-kiddies** - EFNet, IRCNet, Undernet (Rumunjska i Poljska - žarišta)
 - obilje informacija i za sistem-inženjere i za provalnike
 - **DefCon**, SANS Institute, CERT, itd.
 - redoviti sastanci i hackera i sistemaca!

Linux i sigurnost

... ili što je sve dobro i loše, te što sve može poći krivo



Kako do zaštite?

- **nadogradnja** sustava na recentne inačice
- uklanjanje **nepotrebnih** servisa i aplikacija, standardno loših i sl.
- postavljanje **lozinki**, kontrola **dozvola** i **pristupa** (aplikacije, datotečni sustav, itd)
- postavljanje **nadglednih** sustava (provjera servisa, datoteka, logiranje, analiza logova)
- **analiza** mrežnog prometa i vatrozid
- sigurnosna **pojačanja** za jezgru sustava

Nadogradnja sustava

- vrlo **ovisna** o distribuciji:
 - npr. **apt-get dist-upgrade**, **emerge world**, itd.
- nužno **redovno** obavljati
- jednostavnije:
 - gotovi binarni paketi, security update, security
 - automatska nadogradnja konf. datoteka
 - npr. Debian, RedHat
- kompliciranije:
 - vlastito kompiliranje, patchiranje
 - ručno diffanje konf. datoteka, gnjavaža
 - npr. Gentoo, Slackware, itd.

Uklanjanje servisa (1)

- **servisi** nepotrebni za radne stanice:
 - **servis** - neinteraktivni proces poslužitelj; najčešće se pokreću kroz **SystemV init** skripte
 - NFS (nfsd, lockd, mountd, statd, portmapper), telnetd, sshd, bind/bind9, dhcpd, ftpd, sendmail
- **listeneri**
 - mrežni servisi koji čekaju na određenim portovima
 - `netstat -tlp`
 - `nmap eth0_ip`
 - `lsof -iTCP`

Uklanjanje servisa (2)

- gašenje daemona
 - odgovarajućim **signalom**
 - **killall daemon; pkill daemon**
 - **/etc/init.d/daemon stop**
- uklanjanje
 - iz **startup** (*init.d*, tj. System V) skripti:
 - **chkconfig daemon off**
 - **update-rc.d -f daemon remove**
 - **vi /etc/rc.d/rc.inet2**
 - sa sustava:
 - **dpkg --purge, emerge unmerge, itd**

Uklanjanje servisa (3)

- runleveli
 - stanja sustava, pri bootu izvršavaju se rc.?d
- primjer - inetd = zlo!
 - standardno zamijenjen sa xinetd
 - **nepotrebni** servisi - diže ih po zahtjevu
 - za svaku **konekciju** - novi proces-dijete
 - konfiguracija */etc/inetd.conf*
 - `/etc/init.d/inetd stop`
 - `mv /etc/inetd.conf \`
`/etc/inetd.conf-orig`
 - `update-rc.d -f inetd remove`

Zamjena servisa (1)

- problematični servisi/aplikacije:
 - sa **sigurnosnim rupama** kroz niz godina
 - sendmail vs. qmail/postfix
 - bind-bind9 vs. djbdns
 - qpopper-uwimap vs. dovecot/cyrus

 - dhcpd-dhcpd3, apache, samba, proftpd
 - php i razne izvedene aplikacije: postnuke, phpbb
 - rsh, rlogin, rexec

Zamjena servisa (2)

- cleartext protokoli:
 - http (apache) - alternativa **https** (apache-ssl)
 - ftp (proftpd, vsftpd, itd) - alternativa **sftp** (openssh)
 - telnet (telnetd) - alternativa **ssh** (openssh)
 - pop3 (...) - alternativa **pop3s** ili još bolje **imap/imap**s (dovecot)
 - smtp (...) - alternativa **smtp-tls** za server2server i **smtp-sasl** za klijent2server (sendmail, postfix)
 - sigurna komunikacija - **SSL biblioteke!**

Uklanjanje aplikacija

- "cum grano salis"
- moguće nepotrebne aplikacije:
 - Gnome, KDE, XOrg, XFree, OpenOffice :-)
- precizni odabir kod instalacije = minimum smeća
- zaostale biblioteke i headeri, itd.
 - **cruft**
 - **dpkg --purge paket**
 - **emerge unmerge paket**

Lozinke (1)

- **PAM sustav** - modularna autentifikacija i autorizacija - */etc/pam.d/**
- lozinke u */etc/shadow*, korisnici u */etc/passwd*, grupe u */etc/group*
- algoritam **enkripcije**
 - nekad samo DES, danas modularno (MD5)
 - **jednosmjerni** postupak
- loše lozinke - podložne provaljivanju (**bruteforce** = pogađanje lozinke)

Lozinke (2)

- PAM:
 - razni tipovi i načini AAA (autentifikacije, autorizacije i auditinga):
 - npr. OTP moduli, SmartCard, itd
 - kontrola pristupa po raznim kriterijima (dani, grupe, itd)
 - moguće pisati složene konfiguracije za AAA
- stalno neaktivni korisnik = nepotrebnik korisnik
 - **userdel -r korisnik**

Lozinke (3)

- lozinka
 - preporučljivo: niz (naizgled) nepovezanih znakova
 - npr. velika i mala slova i brojevi
- nužno ugasiti **nepotrebne** accounte
- promjena lozinke (ili zaključavanje) accounta:
 - `passwd korisnik; passwd -l korisnik`
- provjera **kvalitete** lozinki:
 - `PAM cracklib`
 - `john`

Kontrola dozvola (1)

- datotečni sustav
 - stroga Unixoidna hijerarhija
 - direktoriji: */bin, /sbin, /var, /share*
 - mogući prefiksi za podstabla: */, /usr, /usr/local*
- promjene r-w-x dozvola:
 - **chmod -R ugo=rwx direktorij**
- posebne oznake (s, S, t):
 - značenje ovisno o objektu (datoteka, direktorij)
 - **setuid, setgid, sticky**

Kontrola dozvola (2)

- **svi** mogu pisati:
 - */tmp, /var/tmp*
 - potencijalno **opasno** - izvršavanje provalničkih skripti/programa i sl.
 - mountaju se kao tmpfs: *nosuid, noexec, nodev*
 - fstab: *tmpfs /tmp tmpfs noexec,nosuid,nodev 0 0*
- **korisnički** direktoriji:
 - *nosuid, nodev*
 - često sami stavljaju **krive** dozvole
 - rješenje: **umask 022**

Kontrola dozvola (3)

- servisi - izvršavaju se pod nekim uid-gid:
 - provali se servis - provalnik ima ovlasti servisa
 - ako je servis pod rootom - dobiva root ovlasti!
 - rješenje - **chroot**:
 - promijeniti **tekući** direktorij (chdir())
 - promijeniti **root inode** za tekući proces (chroot())
 - odbaciti **root ovlasti** (setuid(), setgid() na nekog korisnika)
 - paziti na ovlasti takvog korisnika - najbolje da bude **izoliran** od ostalog sustava (**novi gid i uid**, bez ovlasti - npr. nobody/nogroup)

Kontrola vlasništva

- sistemske izvršne datoteke - moraju biti isključivo vlasništvo roota
- grupe:
 - prava korištenja (execute) binarnih datoteka
 - prava pisanja-brisanja
 - npr. cdrom, dialup i sl.
- upravljanje:
 - `chgrp root:adm direktorij`
 - `chown kreator:root datoteka`

Kontrola pristupa (1)

- TCP wrapper - za TCP i UDP (osim RPC):
 - */etc/hosts.allow* i */etc/hosts.deny*
 - za određeni servis definiraju se **dozvole** po IPjevima ili DNS labelama
 - **transparentno** rade za tcp wrapper linkane aplikacije, inače se koristi tcpd (za inetd)
 - *hosts.allow: leafnode: 127.0.0.1, .esa.fer.hr, .cmu.carnet.hr, .imu.carnet.hr*
 - *hosts.deny: statd: ALL EXCEPT 127.0.0.1, hpe50.esa.fer.hr*

Kontrola pristupa (2)

- moguće i specifično za **aplikacije**:
 - proftpd - */etc/proftpd.conf*
 - openssh (sshd) - */etc/ssh/sshd_config*
 - većina servisa logira u *auth.log* i *daemon.log*
- oboje je na **aplikativnom** nivou!
 - zahtjeve obrađuje potencijalno **ranjiva** aplikacija
 - tek jedan **nivo** sigurnosti
 - kvalitetnije je određivati na razini **paketa** i mreže!

Nadgledni sustavi (1)

- sistemsko logiranje
 - klogd i syslogd: */etc/syslog.conf*
 - moguće definirati **različite datoteke** za spremanje
 - **rotiranje** logova - vremensko, količinsko
 - */var/log* direktorij najčešće
 - **provalnici** najčešće brišu logove
 - **analiza** i reporting logova: **logchecker**
 - syslog.conf: **.*;auth,authpriv.none,mail.none
-/var/log/syslog*

Nadgledni sustavi (2)

- nadgledanje sustava:
 - ponašanje **korisnika** - ponašajni sustavi, npr. **hostentry**
 - promjene **logova** i anomalije, npr. **logchecker**
 - promjene **datoteka**, dozvola i sl. - **tripwire**, **aide**
 - ponašanje **procesa** i servisa - **monit**, **daemontools**
 - mrežni promet i **statistika** - **ntop**, **darkstats**, **iptraf**
 - **analiza** mrežnog prometa i akcije - **snort**, **portsentry**

Mrežni promet (1)

- upitna vjerodostojnost, problematični paketi:
 - izvorišna, odredišna adresa, fragmentiranje; DoS i DDoS napadi (smurf, udpflood, synflood)
 - **portscanning** - **nmap**, **queso**
- nužna analiza i filtriranje
 - mrežne **pristupne** liste!
 - **vatrozid** - Netfilter (**iptables**)
 - **NIDS** - **snort** (i Acid) - prepoznavanje uzoraka
 - reporting - **netsaint**
 - statistike - **ntop**, **darkstats**, itd.

Linux vatrozid (1)

- Linux kernel - Netfilter (IPv4 i IPv6 promet)
- korisnički alat **iptables**
- paketni filter:
 - **statički** (stateless) i **dinamički** (stateful)
- mogućnosti:
 - analiza **zaglavlja** i **sadržaja**
 - **prepisivanje** adresa (SNAT, DNAT, MASQ), **zahvati** nad paketima (mangle)
 - praćenje **konekcija**, **QoS**, **shaping**, itd.

Linux vatrozid (2)

- moguća široka primjena
 - embedded uređaji - wireless i ini routeri i bridgevi
 - poslužitelji, ali i radne stanice
- omogućava preciznu kontrolu prometa:
 - **pristupne** liste
 - **filtriranje** potencijalno opasnog prometa
 - prepoznavanje **uzoraka**
 - prioritete i različite **zahvate** nad paketima
 - **ali nije rješenje za sve probleme!**

Linux kernel

- stabilne verzije - parne: 2.2, 2.4, 2.6
- aktualni kernel - 2.6.10-rc3
- sigurnosni propusti vezani uz jezgru:
 - DoS cijelog sustava ili aplikacije
 - prepisivanje kernel stoga (buffer overflow) i prepisivanje programskog stoga
 - nije sve dovoljno pseudoslučajno
 - root je svemoguć!
- djelomično rješenje
 - Linux kernel sigurnosne nadogradnje (patchevi)

Linux kernel nadogradnje (1)

- LIDS:
 - **granulacija** dozvola, ni root nije svemoguć
 - **zaštita** procesa, datoteka, IDS sustav
 - nužna sigurnosna **politika**
- Grsecurity:
 - Grsecurity projekt: **ojačanja** TCP/IP stoga, bolji RNG, različiti sigurnosni dodatci, složena politika **dozvola** procesa i datoteka
 - PaX: **randomizacija** svih stogova, random base mmap/malloc, **nonexec** stog!

Linux kernel nadogradnje (2)

- Grsecurity (nastavak)
 - onemogućuje **buffer overflow** i varijante
- SELinux
 - NSA projekt
 - ušao u **2.6 jezgru** :-)
 - obavezna sigurnosna politika pristupa nad objektima (procesi, datoteke i sl), međuodnosi (nasljeđivanja, posuđivanja, iznimke, itd)
 - sve u svemu: iznimno **komplicirano** konfiguriranje, **manje** mogućnosti od Grsecurity

Kraj!



... na opće veselje,
došao je napokon kraj