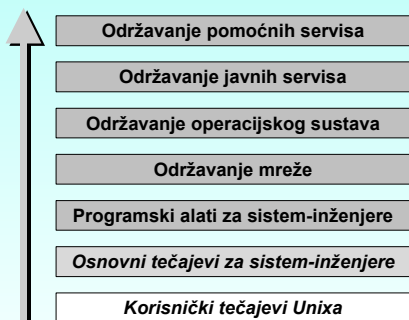


Održavanje operacijskog sustava

autor: Hrvoje Dogan (@carnet.hr)

mentor: Dobriša Dobrenić (@srce.hr)
recenzent: Vladimir Braus (@math.hr → @srce.hr)

(c) 2001-04 - 2001-10, CARNet & SRCE. Sva prava pridržana.
<http://sistemac.carnet.hr/nts/copyright.html>



Ciljevi tečaja

- Naučiti zašto i kako dokumentirati
- Objasniti konfiguriranje operacijskog sustava
- Objasniti tehnike i metode arhiviranja podataka
- Objasniti održavanje sustava
- Naučiti što činiti u slučaju incidenta
- Naučiti kako doći do pomoći

Potrebno predznanje

- Poznavanje i razumijevanje korisničkih koncepata UNIX-a
- Poznavanje osnovnih poslova operatera računalnog sustava

Sadržaj

Dokumenti - namjena poslužitelja, sigurnosna politika, dokumentiranje	60 min
Konfiguriranje OS-a - podizanje, rad sustava, izlaganje informacija, prava procesa, prava pristupa	210 min
Arhiviranje podataka - značaj arhiviranja, politika arhiviranja, strukture datotečnih sustava, tehnike arhiviranja, održavanje	60 min

Sadržaj (2)

Održavanje sustava - instalacija zakrpi, nadziranje sklopovlja, provjeravanje poruka, nadziranje procesa, nadziranje priključaka, nadziranje prometa, vremenska raspodjela poslova, ugađanje sustava	270 min
Incidenti - provjeravanje integriteta, provjeravanje ranjivosti, nadziranje incidenata, reagiranje na incidente	180 min
Pomoć - dokumentacija, službe pomoći	30 min

Dokumenti

Namjena poslužitelja

- Obavezne pretpostavke
 - lokalni backup
 - sigurno udaljeno održavanje
 - standardni sigurnosni zahtjevi



Dokumenti

Namjena poslužitelja (2)

- Obavezni servisi
 - E-mail poslužitelj svih radnika ustanove
 - E-mail poslužitelj svih studenata ustanove
 - imenički poslužitelj svih radnika ustanove
 - imenički poslužitelj svih studenata ustanove
 - WWW poslužitelj ustanove
 - domenski poslužitelj ustanove
 - poslužitelj točnog vremena ustanove



Dokumenti

Namjena poslužitelja (3)

- Poželjni servisi
 - caching poslužitelj ustanove
 - poslužitelj mailing lista ustanove
 - usluga sigurnog udaljenog terminala
 - FTP poslužitelj za korisnike sustava



Dokumenti

Namjena poslužitelja (4)

- Mogući javni servisi
 - anonimni FTP, NNTP (Usenet News), IRC
- Mogući pomoćni servisi
 - npr. DBMS, IP forwarding/filtering, backup server, NFS, SMB, aplikacijski/licencni poslužitelj za ustanovu ...

Dokumenti

Sigurnosna politika

- RFC1244, "Site security handbook"
 - tko smije koristiti resurse
 - što se podrazumijeva pod "pravilnom upotrebom"
 - tko je ovlašten dati pristup i odobravati korištenje
 - tko smije imati privilegije sistem-inženjera
 - koja su prava i obaveze korisnika
 - koja su prava i obaveze sistem-inženjera
 - što činiti s osjetljivim informacijama

Dokumenti

Drugi politički dokumenti

- Pravila za korisnike
- Pravila za sistem-inženjere
- Pravila i procedure za izvanredne situacije

Dokumenti

Dokumentiranje aktivnosti

- Čuvanje prethodnih verzija datoteka
 - unutar promijenjene datoteke
 - unutar istog direktorija
 - u drugom direktoriju
 - u sustavu za kontrolu revizija
- Dokumentiranje poduzetih aktivnosti
 - u posebnu datoteku
 - CARNetov paket "Intervencije"

Dokumenti

Dokumentiranje aktivnosti (2)

- Papirnatu dokumentiranje
 - za ključne akcije
 - okvir za pisanu proceduru
 - ne dokumentirajte za sebe!

Dokumenti

Dokumentiranje aktivnosti (3)

- Vježba
 - Solaris standardno dolazi sa sustavom za kontrolu revizija SCCS.
 - inicijalizirajte SCCS kontrolu nad direktorijem /etc
 - pohranite u SCCS bazu podataka /etc/services
 - napravite check-out, promjenu te check-in datoteke /etc/services
 - povratite originalnu verziju

Dokumenti Izveščivanje

- Interni izvještaji
 - sinteza papirnatu dokumentacije
- Izvještaji poslovodstvu
- Izvještaji korisnicima
- Izvještaji CARNetu

Konfiguriranje OS-a Podizanje sustava

- Boot loader
- Kernel
- Prvi procesi
- Sched: raspoređivanje procesa
- Update: diskovni cache
- Swapper: virtualna memorija
- Init: pokretanje procesa

Konfiguriranje OS-a Podizanje sustava (2)

- Runlevel: skup servisa koji se izvršavaju na sustavu u određenom periodu, stanje sustava
- 1: jednokorisnički rad
- 2: višekorisnički rad
- 3: višekorisnički mrežni poslužitelj
- 6: reboot
- 0: halt

Konfiguriranje OS-a Podizanje sustava (3)

- /etc/init.d
- /etc/rc[0-6].d
- Apsolutni ili simbolički linkovi
- Pokretanje/zaustavljanje servisa
- Uklanjanje servisa
- Označavanje lokalnih servisa

Konfiguriranje OS-a Podizanje sustava (4)

- Primjer init skripte

```
#!/bin/sh
test -f /usr/sbin/ntpd || exit 0
case "$1" in
  start)
    echo -n "Starting NTP server: ntpd"
    start-stop-daemon --start --quiet --exec /usr/sbin/ntpd
    echo "."
    ;;
  stop)
    echo -n "Stopping NTP server: ntpd"
    start-stop-daemon --stop --quiet --exec /usr/sbin/ntpd
    echo "."
    ;;
*)
    echo "Usage: /etc/init.d/ntp {start|stop}"
    exit 1
    ;;
esac
```

Konfiguriranje OS-a Podizanje sustava (5)

- /etc/inittab

```
# /etc/inittab: init(8) configuration.
# $Id: inittab,v 1.8 1998/05/10 10:37:50 miquels Exp $
# The default runlevel.
id:2:initdefault:
# Boot-time system configuration/initialization script.
# This is run first except when booting in emergency (-b) mode.
si::sysinit:/etc/init.d/rcS
# What to do in single-user mode.
--s:wait:/sbin/sulogin
# /etc/init.d executes the S and K scripts upon change
# of runlevel.
#
# Runlevel 0 is halt.
# Runlevel 1 is single-user.
# Runlevels 2-5 are multi-user.
# Runlevel 6 is reboot.
10:0:wait:/etc/init.d/rc 0
11:1:wait:/etc/init.d/rc 1
12:2:wait:/etc/init.d/rc 2
13:3:wait:/etc/init.d/rc 3
14:4:wait:/etc/init.d/rc 4
```

Konfiguriranje OS-a Podizanje sustava (6)

- Vježba
 - napravite shell skriptu `/usr/local/sbin/food`, koja će na standardni izlaz ispisati "bar!"
 - napravite init skriptu koja će pokretati FOO daemon (`/usr/local/sbin/food`)
 - kod ulaska sustava u runlevel 2, FOO daemon se mora dizati nakon što je dignut syslog, ali prije sendmaila



Konfiguriranje OS-a Podizanje sustava (7)

- Uklanjanje servisa
 - preimenujte odgovarajući link u `/etc/rc?.d` direktoriju tako da ne počinje sa S ili K
 - preporučeno
 - `.S00servis`
 - `MOVED_S00servis`
 - `_S00servis`



Konfiguriranje OS-a Podizanje sustava (8)

- Lokalne init skripte
 - imenujte skripte tako da je lako uočljivo koje ste vi dodavali, a koje su došle sa sustavom
 - sve skripte stavljajte u `/etc/init.d`, a linkajte u `/etc/rc?.d`
 - koristite simboličke linkove



Konfiguriranje OS-a Podizanje sustava (9)

- BSD init
 - /etc/rc
 - /etc/rc.local
 - /etc/rc.inet*
- Pazite na dokumentiranje promjena!

Konfiguriranje OS-a Rad sustava

- Praćenje aktivnosti na sustavu
 - pazite na točno vrijeme
 - sigurno logiranje
 - sigurni mrežni superserver
 - BSD obračun procesa

Konfiguriranje OS-a Rad sustava (2)

- NTP klijent - *ntpd*

```
/usr/sbin/ntpd [ -bdosu ] [ -a key# ] [ -e authdelay ] [ -k  
keyfile ] [ -m ] [ -o version ] [ -p samples ] [ -t  
timeout ] [ -w ] server ...
```
- NTP poslužitelj - *ntpd*
 - CARNet paket
 - CARNetov sustav poslužitelja točnog vremena

Konfiguriranje OS-a Rad sustava (3)

- NTP poslužitelj - *ntpd*
 - konfiguracijska datoteka: */etc/ntp.conf*

```
server Stratum-1.ntp.carnet.hr key 1 version 3 prefer
peer zg1.ntp.carnet.hr key 2
peer zg2.ntp.carnet.hr key 3
keys /home/ntp/etc/ntp.key
trustedkey 1 2 3 10
requestkey 10
controlkey 10
statsdir /home/ntp/stats/
filegen loopstats file loopstats type day link enable
filegen peerstats file peerstats type day link enable
```

Konfiguriranje OS-a Rad sustava (4)

- Sigurno logiranje
 - logovi čitljivi samo root korisniku
 - udaljeno logiranje na bastionski host
 - enkripcija logova?
 - logiranje na linijski pisač?

Konfiguriranje OS-a Rad sustava (5)

- Udaljeno logiranje

```
auth,authpriv.* /var/log/auth.log
*.*;auth,authpriv.none -/var/log/syslog
#cron.* /var/log/cron.log
*.* @dekica
```

- Enkripcija logova
 - siguran prijenos preko mreže
 - ne kriptirati lokalno

Konfiguriranje OS-a Rad sustava (6)

- Logiranje na linijski pislač

```
* .debug /dev/lp0
```

- bučno
- nepouzđano
- osjećaj lađne sigurnosti

Konfiguriranje OS-a Rad sustava (7)

- Sigurni mređni superserver

- inetd + tcpd
 - /etc/inetd.conf
 - /etc/services
 - /etc/hosts.allow
 - /etc/hosts.deny
- xinetd
 - sigurna zamjena za inetd+tcpd

Konfiguriranje OS-a Rad sustava (8)

- Xinetd
 - bolje mogućnosti logiranja
 - ograničenja broja servera po servisu, ili globalno
 - vremensko ograničavanje pristupa
 - ograničavanje veličine logova
 - vezivanje servisa uz pojedino sučelje
 - alati za migraciju sa inetd+tcpd

Konfiguriranje OS-a Rad sustava (9)

- /etc/xinetd.conf

```
defaults {
instances = 15
log_type = FILE /var/log/service.log
log_on_success = HOST PID USERID DURATION EXIT
log_on_failure = HOST USERID RECORD
disabled = shell login exec comsat
disabled = finger systat netstat
}

service ftp {
socket_type = stream
wait = no
user = root
server = /usr/sbin/in.ftpd
server_args = -l
instances = 4
access_times = 7:00-12:30 13:30-21:00
nice = 10
only_from = 192.168.1.0/24
}
```

Konfiguriranje OS-a Rad sustava (10)

- BSD obračun procesa
 - za svaki pokrenut proces na sustavu bilježi se naziv programa, vrijeme pokretanja, vrijeme završavanja, korisnik koji ga je pokrenuo i podaci o potrošenom procesorskom vremenu
 - dobra mjera sigurnosti jer crackeri ne znaju za njega
 - osim za praćenje procesa na sustavu, služi i za izradu statistike korištenja sustava

Konfiguriranje OS-a Rad sustava (11)

- Pokretanje obračuna procesa
 - accton; acctoff
- Lokacija obračunske datoteke "pacct" ovisi o sustavu
- Pacct može zauzeti veliku količinu diska na jako upotrebljavanim sustavima, pa ga treba rotirati

Konfiguriranje OS-a Rad sustava (12)

- Vježba
 - isključite uslugu *finger* na svom računalu
 - dodajte uslugu *foo* na portu 9876, koja će se izvršavati kao *stream* usluga, s ovlastima korisnika *nobody*, bez čekanja, koristeći protokol TCP
 - *inetd* mora pokretati *FOO* daemon koji smo kreirali u prošloj vježbi

Konfiguriranje OS-a Izlaganje informacija

- Trebalo bi biti regulirano politikom
- Kritični servisi
 - SNMP
 - RPC
 - *finger*
 - *ident*
 - X

Konfiguriranje OS-a Izlaganje informacija (2)

- SNMP
 - *Simple Network Management Protocol*
 - namijenjen središnjem nadzoru i upravljanju mrežom
 - slab mehanizam autentikacije/autorizacije
 - dopušta **mijenjanje** određenih postavki na sustavu
 - struktura upravljanih informacija - **MIB** (Management Information Base)

Konfiguriranje OS-a Izlaganje informacija (3)

- MIB
 - stablasta hijerarhija objekata
 - pristup MIB-u regulira se preko mehanizma SNMP *community*
- SNMP *community*
 - "lozinka" za pristup SNMP poslužitelju
 - read ili write
 - community i svi podaci se prenose **bez enkripcije**



Konfiguriranje OS-a Izlaganje informacija (4)

- Sun RPC
 - *Remote Procedure Call*
 - definicija jednostavnih procedura za ostvarivanje komunikacije među procesima u mrežnom okruženju
 - XDR - Cross-platform Data Representation
 - RPC+XDR omogućuje NFS



Konfiguriranje OS-a Izlaganje informacija (5)

- RPC Portmapper
 - mapira RPC servise na TCP/IP portove
 - svaki program koji podržava RPC kod pokretanja javlja usluge koje nudi te portove koje koristi portmapperu
 - klijenti upućuju upite portmapperu kako da se povežu s poslužiteljem za pojedinu RPC uslugu



Konfiguriranje OS-a Izlaganje informacija (6)

- RPC usluge
 - nedovoljno poznavanje RPC usluga često dovodi do otkrivanja previše informacija
 - nedovoljno poznavanje funkcioniranja NFS-a često dovodi do neželjenog izlaganja diskova
 - RPC servisi mogu podržavati TCP wrapper!

Konfiguriranje OS-a Izlaganje informacija (7)

- Finger
 - "pristojna" usluga udaljenim korisnicima
 - potencijalni sigurnosni rizik
- Ident
 - klijent javlja serveru koji korisnik traži uslugu od servera
 - baziran na povjerenju, može biti lažan
 - dobro ga je imati zbog vlastite sigurnosti

Konfiguriranje OS-a Izlaganje informacija (8)

- X protokol
 - izuzetno nesiguran, nekriptiran prijenos
 - klasična metoda autentikacije je "xhost" kontrola bazirana na računalima koja se mogu povezivati na X server
 - ukoliko je korisnik neoprezan, moguće je kompromitirati korisnički račun
 - novija MIT Magic Cookie autentikacija je sigurnija

Konfiguriranje OS-a

Prava procesa

- Prava pristupa datotekama koja utječu na ponašanje procesa
 - SUID
 - SGID
- Mijenjanje korijenskog direktorija (chroot)
- Postavljanje i mijenjanje prioriteta procesa (nice, renice)



Konfiguriranje OS-a

Prava procesa (2)

- SetUID: Proces se izvršava s ovlastima vlasnika izvršne datoteke na disku
- SetGID: Proces se izvršava s ovlastima grupe izvršne datoteke na disku



Konfiguriranje OS-a

Prava procesa (3)

- Četiri ID-a za svaki proces
 - UID: korisnik koji je pokrenuo proces
 - EUID: efektivni UID - korisnik pod čijim ovlastima se proces izvršava
 - GID: grupa korisnika koji je pokrenuo proces
 - EGID: grupa pod čijim ovlastima se proces izvršava



Konfiguriranje OS-a

Prava procesa (4)

- Chroot: sistemski poziv kojim okolinu procesa smještamo u siguran prostor
- Nice/renice: postavljanje/promjena prioriteta procesa
 - od -20 (najviši) do +20 (najniži)
 - standardno 0
 - samo procesi koji se izvršavaju pod ovlastima korisnika *root* mogu "poboljšati" svoj prioritet
 - sva djeca nekog procesa nasljeđuju prioritet roditelja

Konfiguriranje OS-a

Prava procesa (5)

- Vježba
 - kao root napravite kopiju shella /bin/sh u /tmp
 - kao običan korisnik pokrenite tu datoteku, i otipkajte "id" u tom shellu
 - kao root pomoću naredbe chmod postavite setuid privilegiju toj datoteci
 - ponovo pokrenite datoteku kao običan korisnik, i otipkajte "id"

Konfiguriranje OS-a

Prava pristupa

- Pristup datotekama
- Sigurnije izvršavanje programa pod drugim EUID-om
- Sigurnost lozinki
- Siguran udaljeni pristup
- Jednokratne lozinke
- Ograničavanje pristupa mrežnim uslugama
- Ograničavanje korištenja resursa

Konfiguriranje OS-a Prava pristupa (2)

- Grupni pristup datotekama
 - ne smiju se zanemarivati podrazumijevane postavke
 - izbjegavati direktorije koji su svima otvoreni za pisanje
 - oni direktoriji koji jesu otvoreni za pisanje svima, moraju imati postavljen *sticky bit*
 - za podešavanje podrazumijevanih prava pristupa koristi se *umask*
 - *umask* ima obrnute vrijednosti od prava za *chmod*!

Konfiguriranje OS-a Prava pristupa (3)

- Sigurnije izvršavanje programa pod drugim EUID-om - *sudo*
 - mogućnost izvršavanja zadanih programa pod drugim EUID-om
 - raznolike opcije autorizacije: vlastita lozinka, lozinka korisnika pod kojim se program izvršava, bez lozinke
 - sigurnosni je rizik, i koristi samo zato da korisnici kojima **vjerujemo** ne bi slučajno napravili štetu na sustavu!!

Konfiguriranje OS-a Prava pristupa (4)

- Pokretanje:
`sudo <naredba>`
- Konfiguracijska datoteke: `/etc/sudoers`
- Konfiguriranje sa `visudo`!

```
# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
# See the sudoers man page for the details on how to write a sudoers file.
#
# User privilege specification
root    ALL=(ALL) ALL
ljerka  kvarner = (root) /usr/local/bin/admin/dodaj, /usr/local/bin/admin/produzi,
        /usr/local/bin/admin/brisi
```

Konfiguriranje OS-a Prava pristupa (5)

- Siguran udaljeni pristup
 - TCP/IP **nije** siguran skup protokola
 - UNIX **nije** dizajniran da bude siguran
 - SSL - *Secure sockets layer*
 - SSL-izirani telnet, rlogin, ftp i drugi servisi
 - SSH - secure shell
 - komercijalni ssh
 - openssh



Konfiguriranje OS-a Prava pristupa (6)

- SSH - konfiguracijske datoteke
 - /etc/sshd_config

```
Port 22
ListenAddress 0.0.0.0
HostKey /etc/ssh/ssh_host_key
ServerKeyBits 768
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin no
#
# Don't read ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
RhostsAuthentication no
#
RSAAuthentication yes
PermitEmptyPasswords no
# since these are likely to be being handled by PAM, switch them off here
PrintMotd no
PrintLastLog no
CheckMail no
```



Konfiguriranje OS-a Prava pristupa (7)

- SSH - klijenti
 - Windows: TeraTerm Pro + SSH ekstenzije
 - <http://www.zip.com.au/~roca/tssh.html>
 - UNIX: OpenSSH klijent

```
Host localhost
  ForwardAgent yes
  ForwardX11 yes
# Site-wide defaults for various options
Host *
# ForwardAgent no
# ForwardX11 no
# IdentityFile ~/.ssh/identity
# Port 22
# Cipher blowfish
# EscapeChar ~
```



Konfiguriranje OS-a Prava pristupa (8)

- Sigurnost lozinki
 - lozinke moraju biti što duže (do 8 znakova)
 - koristiti programe za generiranje lozinki
 - trebaju li lozinke isticati?
 - kako imati sigurne i lako pamtljive višestruke lozinke?
 - često mijenjati lozinke

Konfiguriranje OS-a Prava pristupa (9)

- Jednokratne lozinke: S/Key
 - challenge - response sustav
 - inicijalizacija sustava:
`keyinit -s`
 - generiranje ključeva:
`key -n <count> <seq_no> <seed>`
 - upotreba: pri logiranju, ili `keysu`
 - ključeve generirajte **samo u sigurnoj okolini!**

Konfiguriranje OS-a Prava pristupa (10)

- Ograničavanje pristupa mrežnim uslugama: TCP wrappers
- `/etc/hosts.{allow, deny}`
- Redoslijed obrade zahtjeva
 - pristup je dozvoljen ako se klijent nalazi u `hosts.allow`
 - u drugom slučaju, pristup neće biti dozvoljen ako se klijent nalazi u `hosts.deny`
 - inače, pristup će biti dozvoljen

Konfiguriranje OS-a Prava pristupa (11)

- Sintaksa hosts.allow i hosts.deny
 - ključne riječi: ALL, LOCAL, UNKNOWN, KNOWN, EXCEPT, PARANOID

```
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#
# See the manual pages hosts_access(5), hosts_options(5)
# and /usr/doc/netbase/portmapper.txt.gz
#
# Example:  ALL: some.host.name, .some.domain
#          ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#ALL: PARANOID
#profupd: ALL@ALL EXCEPT ALL@hr
#pc.rstamd : ALL@ALL EXCEPT ALL@localhost
```

Konfiguriranje OS-a Prava pristupa (12)

- Ograničavanje korištenja resursa: Limits PAM modul
 - Linux: /etc/security/limits.conf

```
# /etc/security/limits.conf
#
# Each line describes a limit for a user in the form:
#
# <domain> <type> <item> <value>
#
#*          soft   core    0
#*          hard   rps     10000
##student  hard   nproc   20
##faculty  soft   nproc   20
##faculty  hard   nproc   50
#ftp       hard   nproc   0
##student  -       maxlogins 4
# End of file
```

Konfiguriranje OS-a Prava pristupa (13)

- Ograničavanje pristupa mrežnim uslugama: BSD ipfilter
- Sučelje: *ipf*, *ipfstat*
- Konfiguracijska datoteka: /etc/ipf.conf

```
block in from any to any port < 6000
pass in from any to any port >= 6000
block in from any to port > 6003
block in from any to any proto icmp
```

Sažetak

- Dokumentiranje, dokumentiranje, dokumentiranje
- Init, /etc/init.d, runleveli
- Sigurni i pouzdani osnovni servisi
- Pokazujte što manje
- Pazite na prava pristupa!

Literatura

- <http://www.carnet.hr/clanice/mrezni-posluzitelji/zadace.html>
- RFC 1244, Site Security Handbook
- E. Nemeth et al.: "UNIX System Administration Handbook", 2nd Ed., Prentice-Hall Intl, 1995.
- <http://www.ntp.org>
- <http://www.xinetd.org>
- <http://wwwsnmp.cs.utwente.nl>

Literatura (2)

- <http://www.ri.carnet.hr/~hdogan/papers/hdogan-kom2000.doc>
- <http://www.openssl.org>
- <http://www.openssh.net>
- <http://www.csua.berkeley.edu/skey-howto.html>
- <http://coombs.anu.edu.au/ipfilter/>

Arhiviranje podataka

Značaj arhiviranja

- Pomoć u otklanjanju posljedica
 - grešaka u datotečnom sustavu
 - hardverskih pogrešaka
 - neovlaštene promjene podataka
 - ljudske pogreške!
- Čuvanje sigurnosnih kopija različitih stanja sustava

Arhiviranje podataka

Politika arhiviranja

- Dio dokumentacije sustava
- Propisuje načine, intervale i postupke arhiviranja, odabrane medije i načine iskorištavanja, lokaciju i trajanje čuvanja medija, te metode i tehnike verifikacije medija
- Preporuča se čuvanje kritičnih arhiva izvan matične zgrade [off-site]

Arhiviranje podataka

Strukture datotečnih sustava

- Dva značenja pojma datotečnog sustava
 - hijerarhija datoteka i direktorija
 - logička organizacija zapisa podataka na medij

Labela	Boot područje	Primarni superblok	Sumarni blok grupe cilindara	Tablica inode-ova	Područje podatkovnih blokova
Kopija superbloka	Sumarni blok grupe cilindara	Tablica inode-ova	Područje podatkovnih blokova		

Arhiviranje podataka

Strukture datotečnih sustava (2)

- Informacije o strukturi i izgledu datotečnog sustava: **superblok**
 - broj podatkovnih blokova
 - broj grupa cilindara
 - veličina podatkovnih blokova
 - opis hardvera (uređaja)
 - naziv točke montiranja

Arhiviranje podataka

Strukture datotečnih sustava (3)

- Informacije o grupi cilindara: sumarni blok grupe cilindara
 - broj **inodeova**
 - broj podatkovnih blokova u grupi
 - broj direktorija, slobodnih blokova i slobodnih inodeova
 - mapa slobodnih blokova
 - mapa korištenih inodeova

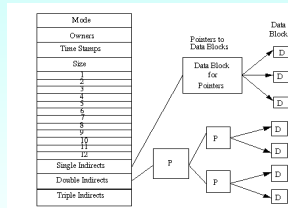
Arhiviranje podataka

Strukture datotečnih sustava (4)

- Informacije o objektima u datotečnom sustavu: **inode**
 - tip datoteke
 - prava pristupa
 - UID i GID vlasnika datoteke
 - veličina datoteke
 - vrijeme zadnjeg pristupa i promjene datoteke, te vrijeme zadnje promjene inodeova
 - broj podatkovnih blokova koje datoteka koristi, ili koji su joj alocirani

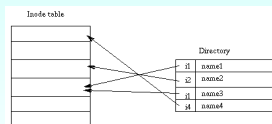
Arhiviranje podataka Strukture datotečnih sustava (5)

- Alokacija podatkovnih blokova



Arhiviranje podataka Strukture datotečnih sustava (6)

- Direktoriji
 - direktorij - poseban tip datoteke
 - sadržaj direktorija - uređeni parovi (broj inodea, naziv datoteke)



Arhiviranje podataka Tehnike arhiviranja

- Tehnike arhiviranja s obzirom na količinu podataka
 - potpuno arhiviranje
 - arhiva cijelog sadržaja ciljanih struktura datotečnog sustava
 - velike, nepraktične, ali potpune i neovisne arhive
 - inkrementalno arhiviranje
 - arhiviranje u više razina
 - nulta razina - potpuna arhiva
 - arhiva svake slijedeće razine (n) bilježi samo promjene na datotečnom sustavu od posljednjeg arhiviranja niže razine (n-1)

Arhiviranje podataka Tehnike arhiviranja (2)

- inkrementalno arhiviranje (nastavak)
 - manje, jednostavnije arhive, ali teže vraćanje podataka (potrebno je koristiti arhive svih razina)
 - obično se rade kombinacije periodičkog izvršavanja arhiva različitih razina

Arhiviranje podataka Tehnike arhiviranja - mediji

- Magnetni mediji
 - diskete
 - ZIP diskete
 - hard diskovi
 - trake
- Optički mediji
 - CD-ROM
 - CD-RW

Arhiviranje podataka Tehnike arhiviranja - mediji (2)

- Problemi s medijima za arhiviranje
 - organizacija izmjene medija manjeg kapaciteta od veličine arhive
 - manipulacija jednokratno zapisljivim medijima
 - kontrolirani uvjeti pohrane medija s arhivama
 - cijena medija bitno većeg kapaciteta od veličine arhive
 - trošenje medija prilikom upotrebe

Arhiviranje podataka

Tehnike arhiviranja - mediji (3)

- Najčešće korišteni mediji: magnetne trake
 - velik kapacitet, relativno niska cijena
 - brzina može biti problem
- Standardni formati traka
 - DDS (1-4): 2 do 20 GB čisti kapacitet, 20 do 40 GB s kompresijom
 - DLT (Digital Linear Tape): 20 do 40 GB bez kompresije, 40 do 80 GB s kompresijom
 - DLT je pouzdaniji i trajniji

Arhiviranje podataka

Tehnike arhiviranja - alati

- Alati koji dolaze s operacijskim sustavom
 - dd
 - tar
 - dump (ufsdump)
 - inkrementalno arhiviranje
 - arhiviranje cijelih datotečnih sustava
- Sustavi za backup
 - Amanda
 - Legato Networker

Arhiviranje podataka

Tehnike arhiviranja - alati (2)

- Arhiviranje pomoću programa *tar*
 - *tape archiver*
- tar <akcija> [opcije] [naziv arhive] [datoteke]
- akcija: c, r, t, u ili x
 - opcije: b, B, e, E, f, F, h, i, k, l, n, o, p, P, q, v, w, X
 - opcija f: umjesto primarne trake, (de)arhivira u datoteku
 - opcija v: na standardni izlaz ispisuje imena datoteka kojima manipulira

Arhiviranje podataka

Tehnike arhiviranja - alati (3)

- Arhiviranje pomoću programa *dump/restore*
 - alat za inkrementalno arhiviranje
 - arhivira cijele datotečne sustave, ne pojedinačne datoteke
 - različita sintaksa na različitim sustavima

dump <razina> [opcije] [arhiva] <datoteke>

restore <akcija> [opcije] [arhiva] <datoteke>

- Solaris: ufsdump, ufsrestore
- Linux: dump, restore (ext2fsdump, ext2fsrestore)

Arhiviranje podataka

Održavanje arhiviranja

- Mediji imaju ograničeni vijek trajanja
- Čuvajte arhive u kontroliranim uvjetima
- Periodički provjeravajte valjanost pohranjenih medija
- Ukoliko je interval čuvanja arhiva vrlo velik, arhive treba povremeno presnimiti na drugi, novi medij, da ne bi došlo do uništenja medija i nemogućnosti čitanja arhive
- Backup je gnjavaža - sve dok ne zatreba

Arhiviranje podataka

Vježba

- Vježba
 - predložite plan inkrementalnog arhiviranja za datotečni sustav od 120 gigabajta na magnetni medij kapaciteta 20 gigabajta
 - trajanje jednog medija je 10 operacija (de)arhiviranja, a količina promjena sadržaja na sustavu je 9 GB tjedno
 - alatom po vašem izboru izvršite potpuno arhiviranje vašeg računala
 - s arhive restaurirajte direktorij /home.

Održavanje sustava

Instalacija zakrpi

- Zakrpe proizvođača OS-a
- Zakrpe proizvođača/autora drugog softvera
- Zakrpe krovnih organizacija
- Zakrpe drugih priznatih i poznatih izvora
- Pazite se lažnih autoriteta!



Održavanje sustava

Instalacija zakrpi (2)

- Pratite relevantne distribucijske liste
- Promptno reagirajte na izvještaje o objavi zakrpa
- Provjerite da li se zakrpa odnosi na vaš sustav
- Provjerite autentičnost izvora zakrpe (digitalni potpis)



Održavanje sustava

Instalacija zakrpi (3)

- Instalacija zakrpi na Solaris
 - skinite *patch cluster* ili pojedinačne zakrpe s jednog od službenih poslužitelja
 - raspakirajte *patch cluster* ili arhive s pojedinačnim zakrapama u privremeni direktorij
 - za instalaciju *patch cluster*a pokrenite datoteku "install_cluster"
 - za instalaciju pojedinačnih patcheva pokrenite "patchadd -d ."
- Instalacija zakrpi na Debian GNU/Linux
 - pokrenite "apt-get update; apt-get upgrade"



Održavanje sustava

Instalacija zakrpi (4)

- Vježba
 - na svoja računala instalirajte posljednji Recommended Patch Cluster za vašu verziju Solarisa

Održavanje sustava

Nadziranje sklopovskih resursa

- Nadzor sustava virtualne memorije - vmstat
 - vmstat [-S] [interval [broj]]
 - -S ispisuje aktivnosti *swappinga*, umjesto *paginga*
 - interval određuje frekvenciju ispisa, a broj određuje broj ponavljanja ispisa

```
$ vmstat
procs  memory      page          disk      faults      cpu
r  b  w  swap  free  re  mf  pi  po  fr  de  sr  s0  s1  s2  s3  in  sy  cs  us  sy  id
0  0  0  11456  4120  1  41  19  1  3  0  2  0  4  0  0  48  112  130  4  14  82
```

Održavanje sustava

Nadziranje sklopovskih resursa (2)

- Opis izlaza naredbe vmstat
 - procs: broj procesa u tri različita stanja:
 - r: u redu za izvršenje
 - b: blokiran zbog resursa
 - w: izvršljiv, ali spremljen u *swap*
 - memory: iskorištenje fizičke i virtualne memorije
 - swap: količina trenutno raspoloživog *swap* prostora
 - free: veličina liste slobodnih *swap* okvira

Održavanje sustava Nadziranje sklopovskih resursa (3)

- Opis izlaza naredbe vmstat (2)
 - page: informacije o pogreškama straničenja i straničenju
 - re: ponovno zatražene stranice
 - ukoliko se koristi opcija -S, ovo polje će se zvati si, i prikazivati koliko puta se desio swap-in
 - mf: *minor fault*
 - ukoliko se koristi opcija -S, ovo polje će se zvati po, i prikazivati koliko puta se desio swap-out
 - pi: kilobajta učitano s diska [paged in]
 - po: kilobajta spremjeno na disk [paged out]
 - disk: broj operacija s diskom
 - diskovi su obilježeni tipom i brojem

Održavanje sustava Nadziranje sklopovskih resursa (4)

- Opis izlaza naredbe vmstat (3)
 - faults: broj zamki/prekida
 - in: prekidi uređaja
 - sy: sistemski pozivi
 - cs: promjene konteksta CPU
 - cpu: postoci iskorištenja procesorskog vremena
 - us: korisničko vrijeme
 - sy: sistemsko vrijeme
 - id: vrijeme neaktivnosti [idle]

Održavanje sustava Nadziranje sklopovskih resursa (5)

- Statistika ulaza/izlaza: iostat
iostat [-xtcn] [interval [broj]]

```
# iostat -xn
extended device statistics
r/s  w/s  kr/s  kw/s  wait  actv  wsvc_t  asvc_t  %w  %b  device
0.5  0.0  40.1  1.4  0.0  0.0  0.4  8.9  0  0  c0t0d0
0.0  0.0  0.0  0.0  0.0  0.0  0.0  0.0  0  0  fd0
8.7  8.5  183.2  375.3  0.0  1.2  1.3  69.3  0  19  c1t1d0
2.5  0.4  37.8  0.8  0.0  0.1  0.0  20.3  0  3  c1t2d0
7.1  1.3  212.6  20.4  0.0  0.5  0.0  55.9  0  8  c1t3d0
0.0  0.0  0.0  0.0  0.0  0.0  0.0  0.0  0  0  c0t2d0
```

Održavanje sustava

Nadziranje sklopovskih resursa (6)

- Opis izlaza naredbe iostat
 - device: naziv diska
 - r/s: čitanja u sekundi
 - w/s: pisanja u sekundi
 - Kr/s: kilobajta čitano u sekundi
 - Kw/s: kilobajta pisano u sekundi
 - wait: prosječni broj transakcija koji čeka u redu
 - actv: prosječni broj transakcija u opsluživanju

Održavanje sustava

Nadziranje sklopovskih resursa (7)

- Opis izlaza naredbe iostat (2)
 - wsvc_t: prosječno trajanje usluge u redu čekanja, u milisekundama
 - swvc_t: prosječno trajanje aktivnih transakcija usluge, u milisekundama
 - %w: postotak vremena u kojem transakcije čekaju na izvršavanje
 - %b: postotak vremena u kojem se transakcije izvršavaju (disk je zaposlen)

Održavanje sustava

Nadziranje sklopovskih resursa (8)

- Interaktivno praćenje opterećenja sustava: top
 - prikazuje trenutni broj procesa, broj procesa po stanjima, opterećenje procesora, ukupne količine i zauzeće fizičke memorije i swap prostora
 - može sortirati ispis procesa prema zauzeću memorije, zauzeću procesora, ukupnom vremenu izvršavanja ...
 - pomoć u interaktivnom načinu rada: "?"

Održavanje sustava

Provjeravanje poruka sustava

- Redovito (periodičko) provjeravanje logova
- Razvrstavanje poruka prema prioritetima i izvorima
- Pazite i na druge poruke, osim onih od sysloga
- Programi za analizu log datoteka i prijavljivanje anomalija

Održavanje sustava

Provjeravanje poruka sustava (2)

- Logcheck - analizador log datoteka
 - izvršavanje *logcheck* skripte svaki sat
 - prikupljanje novih poruka u proteklih sat vremena
 - procesiranje novih poruka
 - pretraživanje poruka o aktivnim napadima
 - pretraživanje poruka o narušavanju sigurnosti
 - pretraživanje poruka koje se mogu ignorirati
 - slanje preostalih poruka mailom upravitelju sustava

Održavanje sustava

Provjeravanje poruka sustava (3)

- Logcheck - konfiguracija
 - editiranje *logcheck.sh* skripte
 - parametri koji se konfiguriraju:
 - varijabla SYSADMIN - kome se poruke šalju mailom
 - FILE CONFIGURATION SECTION dio - koje logove pregledavati
 - konfiguriranje zadatka za cron
 - učestalost pokretanja ovisi o važnosti računala - normalno svakih sat vremena, no na važnijim serverima ili *firewall* računalima i svakih 15 minuta
 - češće izvještavanje ne znači nužno i više mailova :-)

Održavanje sustava

Provjeravanje poruka sustava (4)

- Vježba
 - instalirajte i konfigurirajte logcheck na svojim računalima
 - konfigurirajte provjere svakih 10 minuta, i promatrajte pristigle E-mail poruke

Održavanje sustava

Nadziranje procesa sustava

- Ps: standardni UNIX alat za ispis podataka o procesu
 - ispisuje status i podatke o procesima, kao što su UID, GID, EUID, EGID, zauzeće memorije, prioritet izvršavanja, naziv i argumenti pokrenutog programa itd.
 - podržava specificiranje obima i formata specificiranih podataka

Održavanje sustava

Nadziranje procesa sustava (2)

- Proofs
 - virtualni datotečni sustav s podacima o procesima
 - svaki proces ima vlastiti direktorij s datotekama kojima se pristupa do struktura procesa
 - na Linuxu prikazuje i mnoge druge informacije o sustavu, i ima mogućnost postavljanja nekih sistemskih parametara
 - sučelje prema korisnicima preko pomoćnih programa

Održavanje sustava

Nadziranje procesa sustava (3)

- Solaris: /usr/proc/bin
 - pflags
 - ispisuje zastavice za praćenje u /proc, upućene i zadržane signale, i drugu statusnu informaciju za svaki LWP svakog procesa
 - pcred
 - ispisuje kredencijale (EUID, RUID, EGID, RGID ...) svakog procesa
 - pmap
 - ispisuje mapu adresnog prostora svakog procesa
 - psig
 - ispisuje signalne akcije svakog procesa



Održavanje sustava

Nadziranje procesa sustava (4)

- Solaris: /usr/proc/bin (2)
 - pstack
 - ispisuje hex i simbolički trag stoga [stack trace] LWP-ova svakog procesa
 - pldd
 - ispisuje dinamičke knjižnice vezane sa svakim procesom, uključujući dijeljene objekte koji su eksplicitno vezani koristeći *dlopen*
 - pfiles
 - ispisuje *fstat* i *fnctl* statistiku svih otvorenih datoteka svakog procesa
 - pwdx
 - ispisuje trenutni radni direktorij svakog procesa



Održavanje sustava

Nadziranje procesa sustava (5)

- Solaris: /usr/proc/bin (3)
 - pstop
 - zaustavlja procese
 - prun
 - pokreće procese (obrnuto od *pstop*)
 - pwait
 - čeka da svi navedeni procesi završe s izvršavanjem
 - ptree
 - ispisuje stabla procesa i njihove djece
 - ptime
 - mjeri vrijeme izvršavanja programa s vrlo velikom preciznošću



Održavanje sustava

Nadziranje procesa sustava (6)

- Ispis otvorenih datoteka: `lsdf`
 - ispisuje otvorene datoteke, procese koji ih drže otvorenima i parametre procesa
 - pokrenut s privilegijama običnog korisnika, ispisuje samo podatke o datotekama korisnika
 - ispisuje i druge otvorene *file descriptors*, kao što su TCP i UDP portovi, *pipeovi* i druge strukture

Održavanje sustava

Nadziranje procesa sustava (7)

- Identifikacija korisnika datoteke: `fuser`
 - kao argument prima lokaciju datoteke
 - ispisuje PID procesa koji drži otvorenom datoteku
 - ima mogućnost upućivanja *kill* signala procesima koji drže datoteku ili drugu strukturu (npr. *pipe*) otvorenom

Održavanje sustava

Nadziranje procesa sustava (8)

- Vježba
 - provjerite koje sve otvorene datoteke drži korisnik *nobody*.
 - provjerite koji od trenutnih procesa drži otvoren *libpam.so.1*.

Održavanje sustava

Nadziranje priključaka sustava

- Ispis mrežnih statistika: netstat
 - netstat -a
 - ispisuje otvorene portove svih adresnih familija
 - netstat -p
 - prikazuje ARP tablice
 - netstat -r
 - ispisuje usmjerivačke tablice
 - netstat -M
 - ispisuje *multicast* usmjerivačke tablice
 - netstat -d
 - ispisuje stanje svih uređaja kontroliranih preko DHCP

Održavanje sustava

Nadziranje priključaka sustava (2)

- Skeniranje otvorenih portova: nmap
 - nmap [tip skena] [opcije] <odredište>
 - tipovi skenova:
 - TCP povezivanje
 - TCP SYN
 - Ping sken
 - UDP sken
 - RPC sken
 - otkrivanje OS-a na ciljnom sustavu
 - velik dio funkcija dostupan je i običnim korisnicima
 - smatra se crackerskim alatom

Održavanje sustava

Nadziranje priključaka sustava (3)

- Nadzor pružanja servisa: mon
 - dvije osnovne komponente
 - mehanizam sonde za sintetičke transakcije
 - sučelje za prikupljanje i prikaz podataka
 - web sučelje
 - modularne sonde za nadzor usluga
 - modularni sustavi dojavljivanja
 - pregledno stanje sustava koristeći web
 - CARNet paket

Održavanje sustava Nadziranje priključaka sustava (4)

- Konfiguracija mon-a: mon.cf

```
watch routers
service ping
description routers which connect bd1 and bd2
interval 1m
monitor fping.monitor
period wd {Sun-Sat}
alert qpage.alert mis-pagers
alertevery 45m
period LOGFILE: wd {Sun-Sat}
alert file.alert -d /usr/lib/mon/log.d routers.log

# FTP server
#
watch ftp
service ftp
interval 5m
monitor ftp.monitor
period wd {Sun-Sat}
alert mail.alert mis@domain.com
alertevery 1h
```

Održavanje sustava Nadziranje priključaka sustava (5)

- Vježba
 - provjerite koji su svi portovi otvoreni na računalima u lokalnoj mreži
 - identifikirajte usluge koje se pokreću na tim portovima
 - na vašem računalu konfigurirajte mon tako da prati rad što više usluga na ostalim računalima u lokalnoj mreži

Održavanje sustava Nadziranje prometa

- Provjera aktivnih veza koristeći netstat
 - netstat -a ispisuje i trenutno uspostavljene veze
- Nadzor mrežnog prometa: tcpdump
 - tcpdump [opcije] [izraz]
 - opcije određuju način manipuliranja i prikaza podataka
 - izraz:
 - {src,dst} {host,net,port} <vrijednost>
 - {ether,ip,arp,rarp,tcp,udp...}
 - {gateway, broadcast} <vrijednost> {less, greater}
 - <vrijednost>

Održavanje sustava Nadziranje prometa (2)

- tcpdump src or dst jagor.srce.hr

```
10:20:15.073284 vc.RDLab.CARNet.hr.2719 > jagor.srce.hr.finger: S 987952805:9879
52805(0) win 32120 <msg 1460,sackOK,timestamp 646533367 0,nop,wscale 0> (DF)
10:20:15.074589 jagor.srce.hr.finger > vc.RDLab.CARNet.hr.2719: S 1454711749:145
4711749(0) ack 987952806 win 10136 <nop,nop,timestamp 58878872 646533367,nop,wsc
ale 0,msg 1460> (DF)
10:20:15.074617 vc.RDLab.CARNet.hr.2719 > jagor.srce.hr.finger: . ack 1 win 3212
0 <nop,nop,timestamp 646533367 58878872> (DF)
10:20:15.074667 vc.RDLab.CARNet.hr.2719 > jagor.srce.hr.finger: P 1:3(2) ack 1 w
in 32120 <nop,nop,timestamp 646533367 58878872> (DF)
10:20:15.075859 jagor.srce.hr.finger > vc.RDLab.CARNet.hr.2719: . ack 3 win 1013
4 <nop,nop,timestamp 58878872 646533367> (DF)
10:20:15.131531 jagor.srce.hr.38047 > vc.RDLab.CARNet.hr.auth: S 760915871:76091
5871(0) win 8760 <msg 1460> (DF)
10:20:15.131555 vc.RDLab.CARNet.hr.auth > jagor.srce.hr.38047: S 994136336:99413
6336(0) ack 760915872 win 30660 <msg 1460> (DF)
10:20:15.132944 jagor.srce.hr.38047 > vc.RDLab.CARNet.hr.auth: . ack 1 win 8760
(DF)
```

Održavanje sustava Nadziranje prometa (3)

- tcpdump -X src or dst armada.ri.carnet.hr

```
10:36:02.792304 vc.RDLab.CARNet.hr > armada.RI.CARNet.hr: icmp: echo request
0x0000 4500 0054 9afd 0000 4001 c317 a135 b21d E..T....8...3..
0x0010 a135 280c 0800 307c 6771 0000 72bd 2d3b .5[....8]gq..r.-?
0x0020 c916 0e00 0809 0a0b 0c0d 0e0f 1011 1213 .....
0x0030 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!*#
0x0040 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
0x0050 3435 45
10:36:02.796686 armada.RI.CARNet.hr > vc.RDLab.CARNet.hr: icmp: echo reply
0x0000 4500 0054 c5d6 0000 7d01 3b3e a135 280c E..T....[.D>S(.
0x0010 a135 b21d 0000 387c 6771 0000 72bd 2d3b .5....8]gq..r.-?
0x0020 c916 0e00 0809 0a0b 0c0d 0e0f 1011 1213 .....
0x0030 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!*#
0x0040 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
0x0050 3435 45
10:36:03.790829 vc.RDLab.CARNet.hr > armada.RI.CARNet.hr: icmp: echo request
0x0000 4500 0054 9b00 0000 4001 c314 a135 b21d E..T....8...3..
0x0010 a135 280c 0800 e081 6771 0100 72bd 2d3b .5[....8]gq..r.-?
0x0020 1711 0e00 0809 0a0b 0c0d 0e0f 1011 1213 .....
0x0030 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!*#
0x0040 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
0x0050 3435 45
10:36:03.795101 armada.RI.CARNet.hr > vc.RDLab.CARNet.hr: icmp: echo reply
0x0000 4500 0054 c5d6 0000 7d01 3b3e a135 280c E..T....[.D>S(.
0x0010 a135 b21d 0000 387c 6771 0000 72bd 2d3b .5....8]gq..r.-?
0x0020 c916 0e00 0809 0a0b 0c0d 0e0f 1011 1213 .....
0x0030 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!*#
0x0040 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
0x0050 3435 45
```

Sažetak

- Arhiviranje je nužno
- Arhiviranje nije trivijalno
- Obratiti pažnju na izbor medija
- Sustav treba držati *up-to-date*
- Redovito provjeravati poruke sustava, procese, rad sklopovskih komponenti i rad mreže i mrežnih usluga. Posao sistem-inženjera je u tome da sustav funkcionira optimalno.

Literatura

- http://wks.uts.ohio-state.edu/sysadm_course/html/sysadm-39.html
- <http://web.mit.edu/tytso/www/linux/ext2intro.html>
- J. Mauro, R. McDougall: "Solaris Internals: Core Kernel Architecture", Sun Microsystems Press, 2001.
- A. S. Tannenbaum: "Operating Systems Design and Implementation", 2nd Ed., Prentice-Hall, 1997.

Održavanje sustava (2) Vremenska raspodjela poslova

- Politika periodičkih poslova održavanja
 - arhiviranje podataka sustava
 - provjera sklopovskih resursa
 - provjera integriteta sustava
 - instalacija zakrpa
 - instalacija novih verzija programskih paketa
 - izrada statistika i izvještaja
- Automatizirati što više periodičkih poslova!

Održavanje sustava (2) Vremenska raspodjela poslova (2)

- Cron
 - /etc/crontab
 - /etc/cron.d
 - /etc/cron.{daily, weekly, monthly}
 - /var/spool/cron/crontabs/*
 - crontab [-l | -e | -r] <username>

```
morcic:/home/hdogan# crontab -u hdogan -l
0 * * * * mailx -s "Ispravi VLASTITI bug u qpopperu" irako@carnet.hr <
/home/hdogan/ico
```

Održavanje sustava (2)

Vremenska raspodjela poslova (3)

- Vježba
 - napravite cron job koji će svakog petka 13. u ponoć svim korisnicima na sustavu poslati poruku "Be afraid. Be very afraid."
 - napravite cron job koji će vam svakih pola sata slati mailom novi sadržaj log datoteke /var/log/authlog

Održavanje sustava (2)

Ugađanje sustava

- Solaris
 - /etc/system: konfiguracijska datoteka kernela
 - nakon promjena potrebno napraviti boot -r
 - podešavanje parametara drivera u kernelu: ndd
- Linux
 - sysctl sučelje
 - naredbena linija: sysctl
 - sučelje preko /proc datotečnog sustava: /proc/sys/
 - konfiguracijska datoteka: /etc/sysctl.conf

Održavanje sustava (2)

Ugađanje sustava (2)

- Podešavanje parametara Solarisa
 - podešavanje broja korisnika na sustavu
 - u /etc/system dodati
 - set maxusers = <broj>
 - podešavanje broja BSD pseudoterminala
 - u /etc/system dodati
 - set pt_cnt = <broj>
 - set npty = <broj>
 - podešavanje neizvršljivog stoga
 - u /etc/system dodati
 - set noexec_user_stack=1
 - set noexec_user_stack_log=1

Održavanje sustava (2)

Ugađanje sustava (3)

- Podešavanje parametara Solarisa (2)

- podešavanje parametara IP drivera

```
ndd -set /dev/ip <atribut> <vrijednost>
```

- ip_forwarding 1
- ip_forward_src_routed 0
- ip_respond_to_echo_broadcast 0
- ip_forward_directed_broadcasts 0
- ip_ignore_redirect 1
- ip_respond_to_timestamp_broadcast 0

Održavanje sustava (2)

Ugađanje sustava (4)

- Podešavanje parametara Solarisa (3)

- podešavanje parametara TCP-a

- u /etc/default/inetinit promijenite vrijednost varijable TCP_STRONG_ISS u 2
- ndd -set /dev/tcp tcp_smallest_nonpriv_port 2050

- nddconfig init skripta:

<http://www.sun.com/blueprints/tools/nddconfig.tar>

- podešavanje veličine tmpfs datotečnog sustava

- u /etc/vfstab u opcijama za točku montiranja tmpfs datotečnog sustava (npr. /tmp) dodati
size=<veličina>

Održavanje sustava (2)

Ugađanje sustava (5)

- Vježba

- skinite i instalirajte nddconfig skriptu na svojim računalima
 - ne zaboravite je editirati i podesiti prema svojim potrebama

Incidenti

- Provjeravanje integriteta sustava
- Provjeravanje ranjivosti sustava
- Nadziranje incidenata
- Reagiranje na incidente

Incidenti

Provjeravanje integriteta sustava

- Tripwire: otkrivanje mijenjanih datoteka
 - kod pokretanja kreira bazu podataka s kontrolnim sumama datoteka
 - kod slijedećeg pokretanja omogućuje usporedbu novih kontrolnih suma sa starima, i time pregled datoteka koje su mijenjane
 - inicijalnu bazu treba kreirati kada ste sigurni u integritet sustava

Incidenti

Provjeravanje integriteta sustava (2)

- Tripwire (2)
 - kod mijenjanja nadgledanih datoteka, potrebno je prvo napraviti usporedbu s originalnom bazom (da se uvjerimo u trenutni integritet sustava), promijeniti datoteke, i onda generirati novu bazu
 - tripwire je počeo kao slobodni projekt, međutim 1994. je postao komercijalni proizvod, besplatan samo za Linux. Ovo je potaknulo razvoj slobodnih klonova tripwire-a.

Incidenti

Provjeravanje integriteta sustava (3)

- Klon tripwire-a: AIDE
 - *Advanced Intrusion Detection Environment*
 - konfiguracijska datoteka: Aide.conf
 - osim kontrolne sume, baza sadržava i ostale podatke o datotekama: dozvole, broj inodea, korisnika, grupu, veličinu, mtime, ctime, atime, mjesto za rast i broj linkova
 - sučelje za spremanje podataka prema Postgresql bazi

Incidenti

Provjeravanje integriteta sustava (4)

```
#AIDE.conf
#i: permissions
#i: inode
#n: number of links
#u: user
#g: group
#s: size
#b: block count
#a: atime
#c: ctime
#S: check for growing size
#md5: md5 checksum
#shal: shal checksum
MyRule = p+i+n+u+g+s+b+m+c+md5+shal
# Next decide what directories/files you want in the database
/etc p+i+u+g #check only permissions, inode, user and group for etc
/bin MyRule # apply the custom rule to the files in bin
/sbin MyRule # apply the same custom rule to the files in sbin
/var MyRule
!/var/log/* # ignore the log dir it changes too often
!/var/spool/* # ignore spool dirs as they change too often
!/var/adm/utmp$ # ignore the file /var/adm/utmp
```

Incidenti

Provjeravanje integriteta sustava (5)

- Upotreba AIDE
 - početno generiranje baze:
 - aide --init
 - nakon generiranja, potrebno je bazu (a poželjno i AIDE programe i konfiguracijsku datoteku) snimiti na read-only medij, i pohraniti na sigurno mjesto. Ukoliko na medij snimate i AIDE konfiguraciju, potrebno je promijeniti konfiguracijsku datoteku da čita inicijalnu bazu sa drugog mjesta
 - usporedba sadržaja
 - aide --check

Incidenti

Provjeravanje integriteta sustava (6)

- Uпотреba AIDE (2)
 - obnavljanje baze:
 - aide --update
 - treba se izvršiti nakon promjene konfiguracije AIDE, ili nakon bitnih promjena u konfiguraciji sustava.
 - također je uputno maknuti AIDE program i konfiguraciju sa sustava na medij koji se ne može brisati.

Incidenti

Provjeravanje integriteta sustava (7)

- Pregled izvršavanja programa: truss/strace
 - Solaris: truss, Linux: strace
 - ispisuje sistemske pozive i funkcije koje program poziva

Incidenti

Provjeravanje integriteta sustava (8)

- Solaris: truss

```
exeve("/usr/bin/cat", 0x00000000, 0x00000000) argc = 2
open("/dev/zero", 0_RDONLY) = 3
mmap(0x00000000, 4096, PROT_READ|PROT_WRITE|PROT_EXEC, MAP_PRIVATE, 3, 0) = 0xEF7C0000
stat("/usr/bin/cat", 0x00000000) = 0
open("/usr/lib/libc.so.1", 0_RDONLY) = 4
open("/usr/lib/libdl.so.1", 0_RDONLY) = 4
open("/usr/platform/SUNW_SPARC64/lib/libc_pr.so.1", 0_RDONLY) Err#2 ENOENT
close(3) = 0
fcntl(4, 0x00000000) = 0
open(4, "proba", 0_RDONLY) = 3
fcntl(4, 0x00000000) = 0
lseek(3, 0, SEEK_CUR) = 0
mmap(0x00000000, 33, PROT_READ, MAP_SHARED, 3, 0) = 0xEF7A0000
read(3, "0", 1) = 1
munmap(0xEF7A0000, 33, MC_ADVISE, 0x0002, 0, 0) = 0
Ovo je probna datoteka za Eruss.
write(1, "0 v o j e p r o b n a . . .", 33) = 33
lseek(1, 33, SEEK_SET) = 33
munmap(0xEF7A0000, 33) = 0
lseek(1, 0, SEEK_CUR) = 33
close(3) = 0
close(1) = 0
lseek(0, 0, SEEK_CUR) = 13850
_exit(0)
```

Incidenti

Provjeravanje integriteta sustava (9)

- Linux: strace

```
execve("/bin/cat", ["cat", "proba"], [/* 23 vara */]) = 0
brk(0)                                     = 0x239fc
open("/etc/ld.so.cache", O_RDONLY)        = 3
fcntl(3, {at_mode=SFREGIO664, st_size=12324, ...}) = 0
mmap(NULL, 12324, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7001a000
close(3)                                   = 0
open("/lib/libc.so.6", O_RDONLY)         = 3
mmap(NULL, 1050672, PROT_READ|PROT_EXEC, MAP_PRIVATE, 3, 0) = 0x7002c000
mprotect(0x70114000, 100800, PROT_NONE) = 0
mmap(0x7012a000, 10288, PROT_READ|PROT_WRITE|PROT_EXEC, MAP_PRIVATE|MAP_FIXED|MA
P_ANONYMOUS, -1, 0) = 0x70128000
close(3)                                   = 0
getpid()                                  = 28400
getpagesize()                             = 0x2000
fcntl(1, {at_mode=SFIFO0600, st_size=457, ...}) = 0
open("proba", O_RDONLY|0x4000)           = 3
fcntl(3, {at_mode=SFREGIO664, st_size=34, ...}) = 0
read(3, "Ovo je probna datoteka za strace"... 8192) = 34
write(1, "Ovo je probna datoteka za strace"... 34) = 34
read(3, "", 8192)                        = 0
close(3)                                   = 0
close(1)                                   = 0
exit(0)                                    = ?
```

Incidenti

Provjeravanje integriteta sustava (10)

- Pregled programa: strings

- ispisuje sve nizove znakova u datoteci
- moгуće otkrivanje kompromitiranih računala

```
SUNW_OST_OSCMD
Invalid Command name (%s); expecting mv, cp, or ln.
strings
%s: insufficient arguments (%d)
%s: %s not found
%s: Target %s must be a directory
%s: Target %s file name length exceeds MAXPATHLEN %d
%s: insufficient memory to %s %s
%s/%s
%s: cannot create %s:
%s: %s is a directory
%s: %s is on a different file system
%s: %s is a directory
%s: cannot rename %s:
%s: cannot mkdir %s:
%s: cannot open %s:
%s: cannot create %s:
%s: failed to set acl entries on %s
```

Incidenti

Provjeravanje ranjivosti sustava

- Provjera loših lozinki: crack
 - program za razbijanje UNIX lozinki
 - bazira se na rječnicima
 - računski vrlo intenzivan
 - kompleksno pokretanje
 - moгуćnost dodavanja vlastitih rječnika

Incidenti

Provjeravanje ranjivosti sustava (2)

- Lokalno nadgledanje sigurnosti sustava: cops
 - *Computer Oracle and Password System*
 - E-mailom izvještava o potencijalnim problemima
 - praćeni parametri su:
 - dozvole pristupa datotekama, direktorijima i uređajima
 - sadržaj /etc/passwd i /etc/group
 - sadržaj sistemskog crontaba i rc skripti
 - da li svi mogu pisati u neki korisnički direktorij

Incidenti

Provjeravanje ranjivosti sustava (3)

- Provjera ranjivosti preko mreže: nessus
 - klijent-server arhitektura
 - plug-inovi i skriptni jezik za njihov razvoj
 - fokusiranje na rješavanje **trenutnih** sigurnosnih problema
 - "pametno" otkrivanje usluga - nevezano uz brojeve portova
 - potpuni izvještaji, s prioritetima ispravljanja rupe, i ukoliko je moguće, recept za popravak

Incidenti

Provjeravanje ranjivosti sustava (4)

- Plug-inovi za nessus
 - nekoliko stotina plugina razvrstano u kategorije
 - backdoors
 - zloupotreba CGI-a
 - uskraćivanje usluge
 - zloupotreba fingera
 - vatrozidovi
 - FTP
 - dobivanje udaljene ljuške
 - dobivanje udaljenog root pristupa
 - opći

Incidenti

Provjeravanje ranjivosti sustava (5)

- Plug-inovi za nessus (2)
 - razno
 - NIS
 - skeniranje portova
 - udaljeni pristup datotekama
 - RPC
 - SMTP
 - SNMP
 - beskorisni servisi
 - Windows

Incidenti

Provjeravanje ranjivosti sustava (6)

- Nadgledanje stanja mrežnih sučelja: ifstatus
 - dodatni program za Solaris koji prijavljuje Ethernet uređaje koji su u promiskuitetnom modu
 - <http://www.enteract.com/~robt/Tools/>
 - Ethernet uređaj u promiskuitetnom modu predaje višim slojevima sve pakete, a ne samo one namijenjene njemu
- Linux: ifconfig
 - uz druge podatke o uređaju, naredba ifconfig prijavljuje ukoliko je uređaj u promiskuitetnom modu

Incidenti

Provjeravanje ranjivosti sustava (7)

- Vježba
 - konfigurirajte COPS na svojim računalima
 - postavite interval slanja izvještaja na 10 minuta, i promatrajte izvještaje

Incidenti

Nadziranje incidenata

- IDS - *Intrusion Detection System*: snort
 - sniffer i logger paketa
 - prepoznavanjem uzoraka u mrežnom prometu ima mogućnost otkrivanja
 - napada s prekoračenjem spremnika
 - nevidljivog pregledavanja portova
 - CGI napada
 - SMB sonde ...
 - mehanizam za razvoj novih pravila za otkrivanje

Incidenti

Nadziranje incidenata (2)

- IDS - *Intrusion Detection System*: snort (2)
 - razne mogućnosti dojave
 - bilježenje preko sysloga
 - posebna datoteka s uzbunama
 - slanje SMB "WinPopUp" poruka ...
 - integracija s BSD ipfilterom
 - konfiguracija preko opcija zadanih u komandnoj liniji i skupa pravila za detekciju i uzbunjivanje

```
Alert tcp any any -> 10.1.1.0/24 100:600 (flags: S; msg: "SCAN!");
```

Incidenti

Nadziranje incidenata (3)

- Praćenje rada korisnika: ttysnoop
 - nadgleda rad korisnika na sustavu
 - upotrebljava se kada smo sigurni da je na određenom terminalu na sustav prijavljen uljez sa zlim namjerama
 - paziti na poštivanje privatnosti korisnika

Incidenti

Reagiranje na incidente

- Reagiranje na incidente mora biti regulirano politikom
- Sve akcije i incidenti moraju biti dokumentirani
- Odredite akcije koje ćete poduzeti
 - gotovo ništa, skrpiti stroj da radi
 - reinstalirati OS s najnovijim zakrpama
 - analizirati uzroke i povećati razinu sigurnosti stroja
 - okomiti se na počinitelje i progoniti ih svim sredstvima
- Bilježite tijek akcija

Incidenti

Reagiranje na incidente (2)

- IRT
 - *Incident Response Team*
 - pojam se odnosi i na sve akcije reagiranja na sigurnosne incidente
 - istraživanje podataka na kompromitiranom računalu se naziva *forenzičko računarstvo*
 - incidenti se moraju riješavati planirano i koordinirano

Incidenti

Reagiranje na incidente (3)

- Osnovni postupci forenzike:
 - osigurajte i izolirajte mjesto zločina
 - snimite mjesto zločina
 - izvršite sistematičnu potragu za dokazima
- Brzina je važna, ali budite smireni i ne dižite paniku
- **Ne dirajte** tipkovnicu ukoliko baš ne morate!

Incidenti

Reagiranje na incidente (4)

- Osigurajte i izolirajte
 - ukoliko je moguće, isključite računalo iz mreže
 - loša zamjena za isključivanje računala iz mreže može biti i isključivanje što je više moguće mrežnih usluga

Incidenti

Reagiranje na incidente (5)

- Snimite situaciju
 - zapisujte sve važne podatke **na papir** (da, olovkom!)
 - ime računala
 - vrijeme otkrivanja napada
 - tko je otkrio problem, na koji način
 - kako ste vi bili obaviješteni o problemu
- **ne dirajte** ništa na računalo. Idealno bi bilo da računalo u ovoj fazi stoji ugašeno.

Incidenti

Reagiranje na incidente (6)

- Prikupljanje dokaza: TCT
 - *The Coroner's Toolkit*
 - skupina alata za analizu i prikupljanje podataka o provali na sustav
 - instaliran i spreman za rad na CDROM-u, ili na identičnom računalo spremnom za montiranje diskova preko NFS-a, ili na pomoćnom disku **nepovezanom uz provaljeno računalo**
 - ukoliko je počinitelj kompromitirao sustav, mogao je promijeniti i lokalno instalirani TCT!

Incidenti

Reagiranje na incidente (7)

- TCT: rad
 - tokom rada na kompromitiranom računalu, bilježite sve svoje akcije koristeći naredbu *script*
 - pokrenite glavni modul TCT-a:
grave-robber -v <direktorij>
 - budite sigurni da je na računalu raspoloživa veća količina slobodnog prostora na diskovima
 - pratite izlaz grave-robbera, i čekajte završetak

Incidenti

Reagiranje na incidente (8)

- TCT: rad (2)
 - dok čekate završetak analize TCT-a, pročitajte još jednom svu dokumentaciju
 - analiza traje vrlo dugo - od 30-ak minuta do nekoliko sati
- nakon završetka prikupljanja i analize podataka, potrebno je izvršiti dodatnu analizu i korelaciju događaja

Incidenti

Reagiranje na incidente (9)

- Smisao forenzičkog računarstva je pokušati staviti u vremenski okvir događaje oko incidenta
- Vješti **crackeri** mogu glumiti početnike, da bi vas odvratili od pravog cilja napada
- Bez obzira na vrijeme uloženo u analizu podataka, nikada ne možete biti potpuno sigurni da ste utvrdili sve relevantne činjenice

Incidenti

Reagirane na incidente (10)

- Prijavljivanje i koordiniranje incidenata
 - prijave incidenata preko weba ili E-maila CARNet CERT-u
 - CARNet CERT preuzima koordinaciju i obavještanje drugih CERT-ova
 - digitalno potpisujte sve izvještaje CERT-u i izvatke iz logova
 - vrlo je važno da prijavljujete sve incidente, jer su možda dio većeg incidenta u regiji



Incidenti

Reagirane na incidente (11)

- Kontakti CARNet CERT-a:
CARNet CERT
CARNet
c/o SRCE - Sveučilišni računski centar
Marohničeva ulica bb
10000 Zagreb
Telefon: 01-6164-194
Telefax: 01-6164-395
E-mail: ccert@cert.hr
- Web za prijavu incidenata:
<http://www.cert.hr/prijava.php>



Incidenti

Reagirane na incidente (12)

- Važeći dokazi u računalnom kriminalu
 - vrlo kontroverzna tema
 - kako dokazati autentičnost log datoteka?
 - kako dokazati identitet počinitelja?
 - kako dokazati autentičnost počinitelja?
 - kako dobiti dokaze sa sustava posredno uključenih u incident?
 - Kazneni zakon RH: kao dokazni materijal može se upotrijebiti samo sadržaj pronađen u posjedu počinitelja (npr. na tvrdom disku računala)



Incidenti

Reagiranje na incidente (13)

- Zakonska regulativa u USA:
 - 14 različitih zakona na saveznoj razini
 - posebna regulativa pojedinih država
 - specijalistički timovi za računalni kriminal postoje samo u nekim područjima
 - iskusno sudstvo i timovi vještaka na višim razinama
 - velik broj riješenih slučajeva

Incidenti

Reagiranje na incidente (14)

- Kazneni zakon RH, čl. 223:
 - “(1) Tko ošteti, izmijeni, izbriše, uništi ili učini neuporabljivim tuđe automatski obrađene podatke ili računalne programe, kaznit će se novčanom kaznom ili kaznom zatvora do jedne godine.
 - (2) Tko unatoč zaštitnim mjerama neovlašteno pristupi automatski obrađenim podacima ili računalnom programu, kaznit će se novčanom kaznom do stopedeset dnevnih dohodaka ili kaznom zatvora do šest mjeseci.
 - (3) Kazneni postupak za kazneno djelo iz stavka 1. ovoga članka, ako se ne radi o obrađenim podacima ili računalnim programima državnog tijela, pokreće se povodom prijedloga.
 - (4) Posebne naprave i sredstva kojima je počinjeno kazneno djelo iz stavka 1. i 2. ovoga članka oduzet će se.”

Incidenti

Reagiranje na incidente (15)

- Prema KZ, državne ustanove su dužne prijaviti incidente, a državno tužiteljstvo podići tužbu
- Inače je moguće podići samo građansku parnicu
- Problem MUP-a je nedostatak obrazovanih inspektora
- Nepostojanje odjela za računalni kriminal, već grupe unutar odjela za gospodarski kriminal

Pomoć Dokumentacija

- Lokalna dokumentacija:
 - man
 - info
 - /usr/doc



Pomoć Dokumentacija (2)

- Web:
 - <http://www.sun.com>
 - <http://docs.sun.com>
 - <http://www.sunhelp.org>
 - <http://www.linux.org>
 - <http://www.linux.com>
 - <http://www.linux.hr>
 - <http://dokumentacija.linux.hr>
 - <http://www.ugu.com>



Pomoć Dokumentacija (3)

- News:
 - hr.comp.os.linux
 - hr.comp.os.unix
 - comp.os.unix.admin
 - comp.sys.sun.managers



Pomoć Dokumentacija (4)

- Mailing liste:
 - linux@linux.hr - upute na <http://www.linux.hr>
 - sun-managers - upute na <http://sunmanagers.org>
 - Debian GNU/Linux mailing liste - <http://www.debian.org/MailingLists/>

Pomoć Dokumentacija (5)

- Knjige:
 - E. Nemeth et al.: "UNIX System Administration Handbook", 3rd ed., Prentice-Hall Intl, 2000.
 - S. Garfinkel, G. Spafford: "Practical UNIX and Internet Security", O'Reilly, 1996.
 - A. Firsich: "Essential System Administration", 2nd ed., O'Reilly, 1995.
 - W. C. Preston: "UNIX Backup and Recovery", O'Reilly, 1999.
 - P. Albitz and C. Liu: "DNS and BIND", 4th ed., O'Reilly, 2001.

Pomoć Službe pomoći

- CARNetov helpdesk za sistemce
 - <http://sistemac.carnet.hr>
 - troubleticketing sustav (WREQ)
 - traži vašu povratnu informaciju za zatvaranje problema!
- Službe pomoći proizvođača
- Pomoć vanjskih konzultanata

Sažetak

- Odredite cikluse periodičkih poslova
- Razvijte pisani plan reakcije na incidente
- Provjeravajte integritet sustava
- U slučaju incidenta ostanite mirni, i djelujte staloženo i planirano
- Dokumentirajte akcije o incidentima i prijavljujte koordinacijskim tijelima
- Služite se službenom dokumentacijom i službama pomoći

Literatura

- E. Nemeth et al.: "UNIX System Administration Handbook", 2nd ed., Prentice-Hall Intl, 1995.
- S. Garfinkel, G. Spafford: "Practical UNIX and Internet Security", O'Reilly, 1996.
- <http://www.insecure.org>
