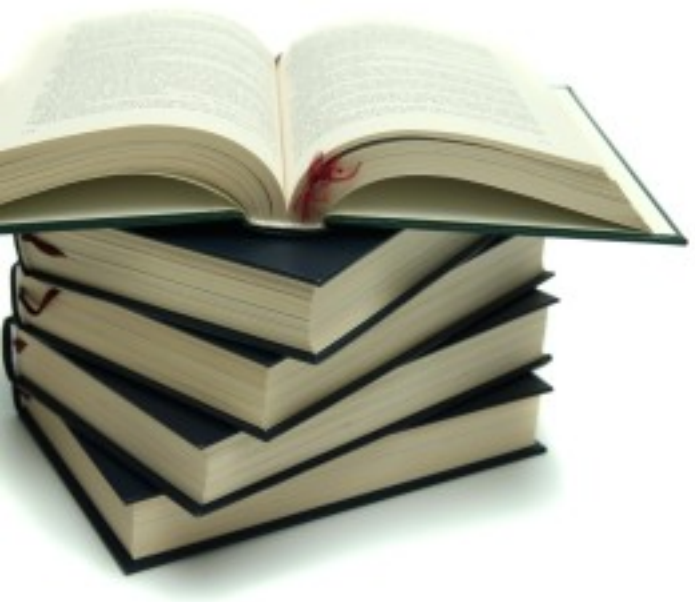

4

Drepturi. Limitarea drepturilor. Monitorizare

29 octombrie 2009

The user's going to pick dancing pigs over security every time.

Bruce Schneier

Cuprins

- Drepturi pe sistemul de fișiere
- Limitarea drepturilor utilizatorului
- sudo
- Cote
- Monitorizare
- Jurnalizare

Controlul accesului

- Acces control
- Subiecți/obiecte
  - matrice de control a accesului (access control matrix)

	obiect1	obiect2	fișier	dispozitiv
subiect1	citire, scriere, execuție, deținător	execuție	citire	scriere
subiect2	citire			

Controlul accesului (2)

- DAC – discretionary access control
  - decis de posesorul obiectului
  - posesor (owner) și drepturi de access (access rights)
  - ACL-based, capability-based
- MAC – mandatory access control
  - decis de sistem, nu de posesorul obiectului
  - subiectele și obiectele dispun de o etichetă
  - un subiect cu eticheta L1 poate accesa un obiect cu eticheta L2 dacă L1 > L2
- RBAC – role-based access control
  - decis de sistem
  - acces pe bază de roluri; un rol este un set de permisiuni

ACL vs. capabilități

- ACL
  - listă de permisiuni atașate unui obiect
  - specifică subiecții (utilizatori, procese) care pot accesa obiectul
  - specifică operațiile posibile asupra subiectului
  - (andrei, read), (bianca, read & write), (cosmin, execute)
  - ACE (access control entries) în sisteme de fișiere
  - POSIX.1e ACL pe sisteme Unix
  - forma standard de drepturi Unix sunt o formă simplificatăa ACL
- Capabilități
  - token de autoritate
  - referă un obiect și acțiunile posibile asupra acestuia
  - un proces/utilizator trebuie să posede token-ul pentru a putea accesa obiectul
  - se permite transferul token-ului de la un subiect la altul (neimplementat în majoritatea sistemelor de operare

Drepturi Unix

- DAC
  - există noțiunea de posesor (owner) (user, group)
  - chown, chgrp
- Formă simplificată de ACL
- Trei subiecți: utilizator (user), grup (group), ceilalți (others)
- chmod
  - deținătorul (user) poate schimba drepturile de access
  - read, write, execute
- umask
  - drepturile implicite pentru crearea unui fișier
  - ~umask & 666 pentru fișiere
  - ~umask & 777 pentru directoare

Bitul setuid

- Privilege escalation
- Programul se execută cu drepturile deținătorului
- chmod u+s exec
- chmod 4755 exec

```
ls -l /usr/bin/passwd

-rwsr-xr-x 1 root root 41296 Jul 24 07:29 /usr/bin/passwd
```

- Riscuri de securitate
- Code demo
- man 7 credentials

Capabilități POSIX

- Folosite în Linux
- Procesele au un set de bitmap-uri
- Bitmapul E (effective) prezintă capabilitățile active
  - /usr/include/linux/capabilities.h
  - CAP_CHOWN (0), CAP_NET_BIND_SERVICE (10), CAP_NET_RAW (13), CAP_SYS_PTRACE (19), CAP_MKNOD (27)
- cap_set_proc, cap_get_proc
- man 7 capabilities

sudo

- Privilege escalation
- Execută o comandă cu drepturile altui utilizator
- Cu ce diferă „sudo command” de „su - -c command”?
  - sau „sudo -u user command” și „su - user -c command”
- Se folosește parola utilizatorului curent
  - se spune că utilizatorul are drept de sudo
- Comanda este rulată cu uid/euid al noului utilizator
- /etc/sudoers
- Are executabilul sudo bitul setuid activat?
- Are executabilul visudo bitul setuid activat?

/etc/sudoers

- Fișierul de configurare pentru sudo
- Alias-uri și specificații de utilizator
- Specificații:
  - cine? unde? = (în numele cui?) ce?
- %admin ALL = (ALL) ALL
- razvan ALL = (ALL) NOPASSWD: ALL
- WEBMASTERS www = (www) ALL, (root) /usr/bin/su www

```
ls -l /etc/sudoers
```

```
-r--r----- 1 root root 462 Jan  1  2009 /etc/sudoers
```

- visudo
- man sudoers

chroot

- Se rulează o comandă/proces într-un director rădăcină modificat
- Comanda chroot
- Apelul de sistem/bibliotecă chroot
- chroot jail
  - named -t /chroot/named
  - postfix, /var/spool/postfix

ulimit

- Comandă internă bash
- help ulimit
- Limitează resursele shell-ului și a proceselor create
- Limite soft și hard
  - resident set size
  - număr de descriptori de fișiere
  - dimensiunea stivei
  - dimensiunea memoriei virtuale
- Informații dinamice

/etc/security/limits.conf

- Modul PAM (Pluggable Authentication Modules) (pam_limits)
- Limitări pe utilizatori/grupuri
- <domain> <type> <item> <value>
- domain: utilizatori sau grupuri
- type: soft/hard
- Informații similare cu ulimit, dar la nivel de utilizator
  - număr maxim de procese create (anti fork bomb)
  - număr maxim de fișiere deschise
  - dimensiunea maximă a unui fișier
  - număr maxim de autentificări

/proc/sys/...

- net/ipv4/tcp_syncookies
- net/ipv4/icmp_echo_ignore_all
- /etc/sysctl.conf

Drepturi de montarea sistemului de fișiere

- Opțiuni pentru mount sau /etc/fstab
- nosuid – ignoră bitul setuid
- noexec – nu permite execuția fișierelor pe partiția montată
- nodev – fișierele dispozitiv sunt ignorate
- Util pentru montarea /tmp

Cote

- Limitări la nivelul sistemului de fișiere
- În Linux 4 valori de configurat la nivel de utilizator/grup
  - limitarea numărului de fișiere/inode-uri (soft/hard)
  - limitarea spațiului ocupat la nivel de blocuri (soft/hard)
- Necesită suportul sistemului de fișiere
  - usrquota, grpquota ca opțiune în /etc/fstab
- apt-get install quota quotatool
- touch /quota.user
- touch /quota.group
- quotacheck -vagum

Controlul cotelor

```
razvan@valhalla:~/code$ sudo repquota /home
*** Report for user quotas on device /dev/sda9
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used    soft    hard  grace    used  soft  hard  grace
----------------------------------------------------------------------
root      --  514608       0       0              689     0     0
razvan    -- 132106532       0       0          286722     0     0
# quotatool -u 0 -i -l 1000 /home
# edquota razvan
# setquota -u root 0 0 1000 1100 /home
# quotaon
# quotaoff
```

Limitarea accesului

- /etc/security/access.conf
- Modul PAM
- permite/interzice accesul utilizatorilor la sistem
- permission : users : origins
- + : @admins foo : ALL
- + : root : 192.168.201.0/24
- - : root : ALL
- Exemple în cadrul fișierului

Account locking

- Informații stocate în /etc/shadow
- usermod -L username
  - apare un semn ! în fața parolei criptate
  - contul va fi încuiat (locked)
  - usermod -U username (unlock)
- usermod -e 2009-10-31 razvan
  - contul va fi dezactivat după data 31 octombrie 2009
- usermod -f 10
  - după 10 zile de la expirarea parolei contul este dezactivat
- /etc/default/useradd

Expirarea parolelor

- Informații stocate în /etc/shadow
- chage
  - -E (similar cu usermod -e)
  - -I (similar cu usermod -f)
  - -m, -M (min/max zile de la o schimbare a parolei; dupa -M zile parola expiră)
  - -W n (înainte cu n zile de exprirarea parolei utilizatorul primește un avertisment)
- /etc/login.defs
  - PASS_MIN_DAYS
  - PASS_MAX_DAYS
  - PASS_WARN_DAYS

Monitorizare

- Activitatea de verificare a parametrilor de funcționare a sistemului
- Sisteme de fișiere
- Utilizatori
- Procese
- Resurse hardware
- Rețea

Monitorizarea sistemului

- Timp de rulare, încărcare, resurse folosite, mesaje de la nucleu
- uptime
- free
- top/htop
- dmesg, /var/log/messages, /var/log/debug, /var/log/kern.log
- sar, vmstat, iostat, pidstat, mpstat (sysstat)

Monitorizarea utilizatorilor

- apt-get install acct
  - jurnalizează (binar) acțiunile în /var/log/account/pacct
  - ac, lastcomm, sa
- w, who
  - utilizatorii autentificați curent
- last
  - ultimele autentificări în sistem
- /var/log/auth

Monitorizarea pachetelor software

- dpkg -l ‘*’
  - afișarea tuturor pachetelor instalate în sistem
- debsums
  - verifică MD5 pentru fișierele pachetelor instalate

Monitorizarea proceselor

- ps
- htop/top
  - monitorizarea dinamică a proceselor
  - interacțiunea cu procesele (semnale, nice)
- lsof
  - afișarea fișierelor deschise în sistem
  - lsof -p pid

Monitorizarea sistemului de fișiere

- df
  - spațiul ocupat de sistemele de fișiere
- quota -v username
- du
  - spațiul ocupat de un director
- find
  - find / -type f \(-perm -4000 -o -perm -2000 \) -exec ls -l {} \;

Monitorizarea serviciilor

- netstat
  - conexiunile de rețea
  - netstat -tlpn
  - netstat -ulpn
- nmap -sS -O -sV localhost
- Jurnalizare
  - /va/log/daemon.log
  - fișiere de tip jurnal specifice

Jurnalizare

- Fișiere jurnal (log files)
- Dată, rezultat (200OK, 404Error), mesaj specific
- În Unix stocate în /var/log
- Atât pentru servicii cât și pentru sistem
- Niveluri de jurnalizare (emerg, crit, error, warn, debug, info)
- Modul append
- Logrotate, arhivare
- tail -f log_file

syslogd

- apt-get install sysklogd
- Daemon de jurnalizare
  - /etc/init.d/sysklogd
- Logrotate
- /etc/syslog.conf
- facility.priority, action (log file, pipe, remote machine)

```
kern.*                          -/var/log/kern.log
lpr.*                           -/var/log/lpr.log
mail.*                          /var/log/mail.log
mail.info                       -/var/log/mail.info
mail.warn                       -/var/log/mail.warn
mail.err                        /var/log/mail.err
```

Exemple de jurnale

- /var/log/kern.log
- /var/log/messages, /var/log/debug
- /var/log/daemon.log
- /var/log/syslog
- /var/log/auth.log
- /var/log/wtmp, /var/log/btmp (last)
- /var/log/mail.*
- /var/log/dpkg.log

logger

- Comandă de interfațare cu daemonul syslog
- logger -p mail.info „mesaj”

Cuvinte cheie

- drept de acces
- chmod, umask
- setuid
- capabilities
- chroot
- ulimit
- /etc/security/limits.conf
- cote
- quota, edquota, quotaon
- sudo, /etc/sudoers
- password aging
- /etc/login.defs
- usermod, chage
- uptime, dmesg, sar
- last, ac, sa, w
- top, htop
- lsof
- find
- netstat
- jurnalizare
- syslogd
- logger

Bibliografie

- http://www.gentoo.org/doc/en/security/security-handbook.xml
- http://www.puschitz.com/SecuringLinux.shtml

Întrebări

?