Linux hardening

Maak je systeem veiliger

Wat komt er allemaal bij kijken?

Alles ;-)

- Algemene opmerkingen
- Basis OS inrichting
- sudo
- Wachtwoorden
- Packet filtering
- ssh hardening
- Netwerk hardening
- Monitoring
- Auditing
- Remote logging
- Intrusion detection

Algemene opmerkingen

- verdiep je middels bekende benchmarks (CIS, STIG)!
- hanteer het principe van “least privileges”
  - permissies
  - gebruikers rechten
  - benodigde software
  - packet filtering
- werk altijd met “security in mind”
- maak zoveel mogelijk gebruik van configuration management (ansible, puppet) -> uniformiteit!
- schedule elke week een reboot (tenzij dat echt niet kan)
- reboot vanaf een console
- monitor (meten is weten)
- audit (ook voor “forensics”)
- log naar remote logserver
- signaleer!

Basis OS inrichting (1/3)

- Voorkom overbodige filesystemen in de kernel

  `rmmod *filesystem*`

  `echo "install *filesystem* /bin/true" >> /etc/modprobe.d/removed_filesystems.conf`

  filesystem is bv.: freevxfs, hfs, hfsplus, …

- mount-opties

  Bv. noexec op /tmp en /var/tmp (maar pas op met sommige software (bv. ansible))

  Denk ook aan nosuid en nodev

- Configureer mail (vooral root!). In /etc/aliases:

  postmaster: root

  root: oscar@kwalinux.nl

  Wel zorgen dat de mail afgeleverd kan worden.

Basis OS inrichting (2/3)

- Wachtwoord op BIOS/UEFI en op de bootloader

Voor de bootloader (grub)

```
grub-mkpasswd-pbkdf2

cat >> /etc/grub.d/40_custom <<EOF

set superusers="<username>"

password_pbkdf2 <username> <encrypted-password>

EOF
```

Boot zonder wachtwoord op te geven: in /etc/grub.d/10_linux (maar zoek uit voor jouw systeem):

```
CLASS="--class gnu-linux --class gnu --class os --unrestricted"
```

Basis OS inrichting (3/3)

- Enable Mandatory Access Control (MAC: Apparmor op Debian, Selinux op Red Hat systemen) **in de bootloader** (grub)

  Bv. voor apparmor (in /etc/default/grub):

  ```
  GRUB_CMDLINE_LINUX="... apparmor=1 security=apparmor"
  ```

- Check je repository config. Voor Debian systemen bijvoorbeeld:

  1) Check met `"apt policy"` en `"apt-key list"`

  ```
  -> wellicht expired keys?
  ```

  2) `# grep AllowUnauthenticated /etc/apt/apt.conf.d/*`

  3) Verwijder ongebruikte software:

  ```
  # grep -i remove-unused
  /etc/apt/apt.conf.d/50unattended-upgrades
  Unattended-Upgrade::Remove-Unused-Dependencies "true";
  Unattended-Upgrade::Remove-Unused-Kernel-Packages "true";
  ```

sudo

Gebruik `visudo` (niet `vi /etc/sudoers`)

Opties in /etc/sudoers:

```
Defaults requiretty

Defaults use_pty
```

Zorg voor “re-authenticate”: niet NOPASSWD (..)

Alleen specifieke commando’s:

```
Cmnd_Alias UPDATE_COMMANDS = /usr/bin/apt
Cmnd_Alias SHUTDOWN_CMDS = /usr/sbin/shutdown, /usr/sbin/reboot
bob ALL=(ALL:ALL) SHUTDOWN_CMDS, UPDATE_COMMANDS
```

Disable su (of alleen voor specifeke users)

Wachtwoorden

Indien wachtwoorden worden gebruikt (bv. voor sudo), forceer dan het gebruik van sterke wachtwoorden:

Lokaal:

- `apt install libpam-pwquality`
  - Edit `/etc/security/pwquality.conf`
- In `/etc/pam.d/common-password`:
  - Geen herhaling van wachtwoorden:
    - `password required pam_pwhistory.so remember=5`
  - Sterk hashing algoritme:
    - `password [success=1 default=ignore] pam_unix.so sha512`

Geef root altijd een sterk wachtwoord! (hoe log je anders in op het console?).

Op Debian/Ubuntu systemen heeft root standaard geen wachtwoord!

Enable console toegang:

```
GRUB_CMDLINE_LINUX="... console=tty1 console=ttyS0”
```

(en zet alleen die consoles in /etc/securetty)

En nog beter: multi-factor authenticatie (met bv. een authenticator app of met een sms).

packet filtering

Gebruik een packet filter (bv. ufw, of iptables)

Default policy voor INPUT en FORWARD -> DROP
(gratis bij gebruik van ufw)

ssh hardening

Werk met ssh keys, niet met wachtwoorden

- genereer key-pair met ssh-keygen
- zet je public key op de server in ~/.ssh/authorized_keys (mode 600)

Enkele server config (/etc/ssh/sshd_config) settings:

- AllowUsers/AllowGroups …
- PermitRootLogin no
- PasswordAuthentication no
- ListenAddress <IP adres>
- AllowTcpForwarding no (geen tunneling)
- X11Forwarding no
- Sterke key exchange (optie KexAlgorithms)
- Sterkte Ciphers (symmetrische encryptie -> shared secret)
- Sterke MACs (Message Authentication Codes): hashing algoritme voor de integriteit van de data
- Configureer connectie timeout:
    - ClientAliveInterval 300
    - ClientAliveCountMax 2

  -> timeout na 10 minuten (2 x 300 seconden).

  Doe dit ook voor de shell (voor bv. het console) met de TMOUT variabele (maak readonly)

- Configureer een login *banner* (bv. met: `Banner /etc/ssh_banner.txt`)

Netwerk hardening

Disable IPv6 als dit niet wordt gebruikt, in `/etc/default/grub`:

```
GRUB_CMDLINE_LINUX="... ipv6.disable=1"
```

Met `sysctl` heb je invloed op kernel netwerk parameters. Maak een file /etc/sysctl.d/hardening.conf met bv.:

- `net.ipv4.conf.all.send_redirects = 0 (als geen router)`
- `net.ipv4.conf.default.send_redirects = 0 (als geen router)`
- `net.ipv4.conf.all.accept_redirects = 0`
- `net.ipv4.conf.default.accept_redirects = 0`
- `net.ipv4.ip_forward = 0 (als geen router)`
- `net.ipv4.conf.all.log_martians = 1`
- `net.ipv4.conf.default.log_martians = 1`
- `net.ipv4.tcp_syncookies = 1`

```
# sysctl --system
```

Monitoring

Onderscheid “metrics” en “alerting”

- metrics: bv. met observium -> trends!
- alerting: bv. met nagios (en nrpe op de clients)

Kracht van nrpe:

Lokaal: `command[check_firewall]=/usr/local/sbin/check_firewall.sh`

```
nlines=$(sudo iptables -L -n | grep ACCEPT | wc -l)

if [ $nlines -lt 10 ];then

  echo “Active rules < 10"

  exit 2

else

  echo “OK - running and configured”

  exit 0

fi
```

Auditing

Met auditing log je wie wat doet op je systeem.

```
apt install auditd
```

Edit /etc/default/grub met:

```
GRUB_CMDLINE_LINUX="... audit=1 audit_backlog_limit=8192"
```

In /etc/audit/auditd.conf:

```
max_log_file = 100  # (Megabytes)

space_left_action = email

action_mail_acct = root

disk_full_action = HALT
```

Auditing - remote logging

1) Stuur audit logging naar een remote server:

   In `/etc/audisp/plugins.d/au-remote.conf`

   ```
   active = yes
   ```

   In `/etc/audisp/audisp-remote.conf`

   ```
   remote_server = <IP-adres>
   ```

   ```
   systemctl restart auditd.service
   ```

2) Via syslog:

   In `/etc/audit/plugins.d/syslog.conf`

   ```
   active = yes
   ```

   ```
   systemctl restart auditd.service
   ```

   ```
   En dan zorgen dat syslog naar een remote (syslog) server logt.
   ```

   ```
   Wel extra syslog-data in logregel met:
   ```

   ```
   Feb 12 16:31:00 cws-003 audisp-syslog:
   ```

   (snapt `aureport` niet dus daartoe weer weghalen)

Auditing - audit rules

Maak je audit rules (wat wil je in de gaten houden?) in `/etc/auditd/rules.d/*.rules`

Enkele voorbeelden:

```
-w /etc/shadow -p wa -k shadow-change

-w /var/www -p wa -k www-change

-w /usr/bin/wireshark -p x -k susp_activity

-a exit,always -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change

-a exit,always -F arch=b64 -S clock_settime -k time-change

-a exit,always -F arch=b32 -F euid=0 -S execve -k rootcmd

-a exit,always -F arch=b64 -F euid=0 -S execve -k rootcmd

-e 2
```

Monitor audit rules! (gebruik bv. `aureport` om audit-logging te parsen en mail een rapport)

(Remote) logging

Zorg dat logging op een *remote logserver* komt.

Local compromise heeft dan geen effect op de logging: nuttig voor bv. *forensics*

Tool: rsyslog

Lokaal in rsyslog config: config de *remote* logserver

```
*.* @@192.0.2.1:10514 # do NOT use this any longer!
```

Zie op rsyslog.com

De logserver (die bv. rsyslog gebruikt) luistert standaard op poort 514: gebruik firewalling!

Ook nuttig: remote logserver met een ELK stack.

Zorg dat journald logging ook, via rsyslog, op de remote logserver terecht komt.

In /etc/systemd/journald.conf:

```
ForwardToSyslog=yes
```

Intrusion detection

Wel auditen maar geen signalering: alleen nut voor *forensics*

Intrusion detection: ook signalering

Hoe:

- uitbreiden auditing met signalering (..)
- gebruik “dedicated” ids tools als AIDE
- schrijf het zelf (met de “database” readonly en remote..)

Op een actief systeem lastig “false positives” zo laag mogelijk te houden.

Bewaak ook je signalering (bv. email)

Netwerk ids: snort

Bier?