

# Hardening GNU/Linux

---

Securing your environment

Alejandro Sánchez Acosta  
asanchez@gnu.org

# Agenda

- ✓ Introduction to security.
- ✓ Why GNU/Linux and Free Software?
- ✓ Securing methods.
- ✓ Workstation and Server security.
- ✓ Security tools.
- ✓ Best practices.
- ✓ Protecting your environment.
- ✓ Integrating security.

# Introduction to Security

- Security concept
  - Protect your self from common risks
  - Security is important in the live of a sysadmin
- Why?
  - Security attacks every day
  - Services are not secure and safe
- Apply it
  - We need to protect our systems

# ¿Libre Software?

- Why?
  - Four rights fundamental in software development or usage
  - Low TCO in companies
  - Good escalability and performance
  - Enhancing desktop with usability
  - Good practices and philosophy
  - Not security by obscurity.

# Hardening methods

# Installing methods

- Automatic
  - Kickstart in Fedora
  - Yast AutoInstall in Suse
  - Preseed with Debian or Ubuntu
  - SysInstall in FreeBSD and OpenBSD
- Manual
  - System imaging
  - Manual configuration

# Security in installation

- PostInstall distribution
  - Secure scripts via NFS
- PostInstall
  - Secure scripts via NFS

# Workstation Security

# Boot Settings

- Boot Loading
  - Boot method (diskette, CDROM)
  - System booting (BIOS/EFI)
  - Bootloader password
    - Prevent single mode without password
    - Access grub console
    - Dual boot
    - grub-md5-crypt and passwd
    - lock option
    - password per boot

# Password generation

- Password Security
  - Creation
    - Memory phrasal
      - One Day I was in the Kaslab Meeting
        - » odlwitKM
    - Change common chars (a and @, t and 7, etc)
    - Capitalize some words
  - Protection
    - Check dictionary words: pam\_cracklib
    - Strength checking: pam\_passwdqc
  - Password aging
    - chage -M 90 user
  - Check passwords
    - slurpie, john, crack.

# Root protection

- Disable root
  - /sbin/nologin shell
  - /etc/securetty vtys access
  - root SSH PermitRootLogin no
  - PAM
  - Su protection
    - wheel
    - /etc/pam.d/su
      - auth required /lib/security/\$ISA/pam\_wheel.so use\_uid
- sudo
  - user
  - %users localhost=/sbin/shutdown -h now

# Server Security

# Operating system adjusts (I)

- Inittab
  - Remove vtys
  - `sed -i 's/ca::ctrlaltdel:/#ca::ctrlaltdel:/g'`
  - Default runlevel: `id:3:initdefault:`
  - `init q`
- Default services
  - `alternatives --set mta /usr/sbin/sendmail.postfix`
- Check permissions
  - SUID: `find / -path /proc -prune -o -type f -perm +6000 -ls`
  - World writable: `find / -path /proc -prune -o -perm -2 ! -type l -ls`
- Login messages
  - `/etc/motd`: Monitoring message
  - `/etc/X11/gdm/PreSession/Default`
    - `if ! gdialog --yesno '\nThis system is classified...\n' 10 10; then sleep 10; exit 1; fi`

# Operating system Adjusts (II)

- /proc
  - sysctl -p
  - SYN flood: net.ipv4.tcp\_syncookies = 1
  - Source routing: net.ipv4.conf.all.accept\_source\_route = 0
  - Disable ICMP redirect: net.ipv4.conf.all.accept\_redirects = 0
  - IP Spoofing protection: net.ipv4.conf.all.rp\_filter = 1
  - Ignore ICMP requests: net.ipv4.icmp\_echo\_ignore\_all = 1
  - Ignore net.ipv4.icmp\_echo\_ignore\_broadcasts = 1
  - net.ipv4.icmp\_echo\_ignore\_broadcasts = 1
  - net.ipv4.conf.all.log\_martians = 1

# Network services

- Disable services
  - Inetd / Xinetd
- Secure common servers
  - OpenSSH
  - Bind
  - Apache
  - etc.
- Firewall

# Services security

- TCP wrappers
  - Hosts allow and deny
- Xinetd/Inetd services
  - Modify banners
  - Enable just useful services
- Modify banner access
  - Issue
  - Motd
  - /etc/service/banner

# Firewall

- Netfilter / Iptables
  - Filtering rules
  - NAT (SNAT/DNAT)
  - Port Knocking
    - Guessing?
  - Blocking Hosts

# Port Knocking

- Iptables (alias `k='telnet $IP'; k 100; k 200; ssh $IP'`)

```
/sbin/iptables -N INTO-PHASE2
```

```
/sbin/iptables -A INTO-PHASE2 -m recent --name PHASE1 --remove
```

```
/sbin/iptables -A INTO-PHASE2 -m recent --name PHASE2 --set
```

```
/sbin/iptables -A INTO-PHASE2 -j LOG --log-prefix "INTO PHASE2: "
```

```
/sbin/iptables -N INTO-PHASE3
```

```
/sbin/iptables -A INTO-PHASE3 -m recent --name PHASE2 --remove
```

```
/sbin/iptables -A INTO-PHASE3 -m recent --name PHASE3 --set
```

```
/sbin/iptables -A INTO-PHASE3 -j LOG --log-prefix "INTO PHASE3: "
```

```
/sbin/iptables -A INPUT -p tcp --dport 100 -m recent --set --name PHASE1
```

```
/sbin/iptables -A INPUT -p tcp --dport 200 -m recent --rcheck --name PHASE1 -j INTO-PHASE2
```

```
/sbin/iptables -A INPUT -p tcp -s $HOST_IP --dport 22 -m recent --rcheck --seconds 5 --name PHASE2 -j  
ACCEPT
```

# Port Knocking

- Knockd

[options]

logfile = /var/log/knockd.log

[openSSH]

sequence = 7000,8000,9000

seq\_timeout = 5

command = /sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j ACCEPT

tcpflags = syn

[closeSSH]

sequence = 9000,8000,7000

seq\_timeout = 5

command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT

tcpflags = syn

# Log checking

- Review logs
  - /var/log
  - syslog
  - utmp/wtmp
  - Cron tasks
- Useful tools
  - Logcheck
    - /etc/logcheck/logcheck.conf
    - /etc/logcheck/logcheck.[violations|hacking|ignore|violations.ignore]
  - Logrotate
    - /etc/logrotate.d/ services

# Monitorization

- Net-SNMP
  - Define agents and traps
  - Exec scripts to capture information
  - Represent the data with graphical stadistics
- RRD and SNMP tools
  - Cricket
  - MRTG
  - OpenNMS

# Securing applications

- SELinux example
  - policygentool googleearth /usr/local/google-earth/googleearth-bin
    - cat >> googleearth.te << \_\_EOF
    - gen\_require(`
      - type unconfined\_t;
    - `)
  - make -f /usr/share/selinux/devel/Makefile
  - semodule -i googleearth.pp
  - setenforce 0
- AppArmor

# Anonymous Browsing

- Anonymous networks
  - P2P model
  - Tor/socks
  - Torify applications

# Monitoring users

- Snoopy
  - Ttysnoop
  - ld.so hack with exec wrapper

# Intrusion Detection

- HIDS
  - Aide/Tripwire
    - Take care with database advices
    - aide init and update
- NIDS
  - Retrieve information data from network
  - Useful tools: tcpdump or snort as NIDS/NIPS
  - Review logs

# Backup

- Common backup tools
  - Tar
  - dd
  - Rsync
  - dump/restore
  - Amanda
  - Bacula
  - etc

# Security problems

- HIDS
  - Aide/Tripwire
    - Take care with database advices
    - aide init and update
- NIDS
  - Retrieve information data from network
  - Useful tools: tcpdump or snort as NIDS/NIPS
  - Review logs

Alejandro Sánchez Acosta  
asanchez@gnu.org

Muchas Gracias