Linux Server Hardening Checklist

Checklist :

☐ 1. Encrypt Data Communication for Linux Server

- All data transmitted over a network is open to monitoring. Encrypt transmitted data whenever possible with password or using keys / certificates.
- GnuPG allows to encrypt and sign your data and communication, features a versatile key management system as well as access modules for all kind of public key directories.
- SSH / RSYNC / SFTP for file transfer
- SSL whenever it's possible

☐ 2. Avoid Using FTP, Telnet, and Rlogin / Rsh Services

- Commands and transferred files can be captured by anyone on the same network using a packet sniffer.
- Use instead OpenSSH , SFTP, or FTPS (FTP over SSL)

☐ 3. Minimize Software to Minimize Vulnerability

```
yum list installed
yum list packageName
```

or

```
dpkg --list
dpkg --info packageName
```

☐ 4. One Network Service Per System, VM or Container

Run each exposed service isolated via VM, Docker, LXC..

☐ 5. Keep Linux Kernel and Software Up to Date

```
yum update
```

or

```
apt update && apt upgrade
```

☐ 6. Use Linux Security Extensions

Use SELinux, Apparmor, Grsecurity when possible.

Feature	SELinux	AppArmor	grsecurity
Automated	No (audit2allow and system-config-selinux)	Yes (Yast wizard)	Yes (auto training / gradm)
Powerful policy setup	Yes (very complex)	Yes	Yes
Default and recommended integration	CentOS / RedHat / Debian	Suse / OpenSuse / Ubuntu based	Any Linux distribution
Training and vendor support	Yes (Redhat)	Yes (Novell)	No (community forum and lists)
Recommend for	Advanced user	New / advanced user	New users
Feature	Attaches labels to all files, processes and objects	Pathname based system does not require labeling or relabeling filesystem	ACLs

---

☐ 7. Linux User Accounts must respect a strong password policy

- Lockout/Error after X retry

```
passwd -l username
```

- Minimum length
- Force to change similar characters
- Force no null passwords
- Setup password aging For ex, you can directly edit the /etc/shadow file :

```
{userName}:{password}:{lastpasswdchanged}:{Minimum_days}:{Maximum_days}:{Warn}:{Inactive}:{Exp
ire}:
```

Where,

- Minimum_days: The minimum number of days required between password changes.
- Maximum_days: The maximum number of days the password is valid (after that user is forced to change his/her password).
- Warn : The number of days before password is to expire that user is warned that his/her password must be changed.
- Expire : Absolute date specifying when the login may no longer be used.

☐ 8. Ensure No Non-Root Accounts Have UID Set to 0 Only root account have UID 0 with full permissions to access the system. Check with :

```
awk -F: '($3 == "0") {print}' /etc/passwd
```

☐ 9. Disable Root Login Never ever login as root user. You should use sudo to execute root level commands as and when required.

☐ 10. Physical Server Security

- BIOS & Grub password w or w/o MFA

☐ 11. Disable Unwanted Linux Services

Check with :

```
systemctl list-unit-files
```

This command will list all services installed/deployed.

Print a list of services that lists which runlevels each is configured on or off

```
systemctl list-unit-files --type=service
systemctl list-dependencies graphical.target
```

☐ 12. Find Listening Network Ports

```
ss -tulpn
netstat -plntu
```

☐ 13. Delete X Window Systems (X11) X Window systems on server is not required.

```
yum groupremove "X Window System"
yum group remove "$DE_NAME Desktop"
```

☐ 14. Configure Iptable Firewall

☐ 15. Harden Linux Kernel with /etc/sysctl.conf

/etc/sysctl.conf file is used to configure kernel parameters at runtime. Linux reads and applies settings from */etc/sysctl.conf* at boot time.

☐ 16. Separate Disk Partitions for Linux System

Partition	Purpose
/usr	This is where most executable binaries, the kernel source tree and much documentation go.
/var	This is where spool directories such as those for mail and printing go. It also contains the error log directory.
/tmp	This is where most temporary data files are stored by apps.
/boot	This is where your kernel images and boot loader configuration go.
/home	This is where users' home directories go.

If the partitions are in one, a script like this one :

```
#!/bin/sh
man bash > $(mktemp)
$0
```

runned with cron or nohup can crash your entire system.

A good way of hardening could be , depending on your IS, to add the following option to /etc/fstab file:

- nosuid – Do not set SUID/SGID access on this partition
- nodev – Do not character or special devices on this partition
- noexec – Do not set execution of any binaries on this partition
- ro – Mount file system as readonly
- quota – Enable disk quota

Above options can be set only, if you have a separate partition.

Make sure you create a partition as above with special option set on each partition:

- /home – Set option nosuid, and nodev with diskquota option
- /usr – Set option nodev
- /tmp – Set option nodev, nosuid, noexec option must be enabled

---

☐ 17. Disable IPv6 if Not Using It

☐ 18. Disable Unwanted SUID and SGID Binaries

All SUID/SGID bits enabled file can be misused : https://gtfobins.github.io/

- [ ] 19. Check for World-Writable Files

If you find a script that is owned by root but is writable by anyone you can add your own malicious code in that script that will escalate your privileges when the script is run as root

```
# World writable files directories
find / -writable -type d 2>/dev/null
find / -perm -222 -type d 2>/dev/null
find / -perm -o w -type d 2>/dev/null

# World executable folder
find / -perm -o x -type d 2>/dev/null

# World writable and executable folders
find / \( -perm -o w -perm -o x \) -type d 2>/dev/null
```

- [ ] 20. Remove Noowner Files

Files not owned by any user or group can pose a security problem. Just find them with the following command :

```
find /dir -xdev \( -nouser -o -nogroup \) -print
```

- [ ] 21. Use Centralized Authentication Service

IAM / LDAP / SSO ....

- [ ] 22. Implement Kerberos for Authentication

Use Kerberos if available : https://docs.redhat.com/en/documentation/red_hat_ansible_automation_platform/2.4/html/automation_controller_administration_guide/assembly-controller-kerberos-authentication

---

- [ ] 22. Configure Logging and Auditing

- [ ] 23. Monitor Suspicious Logs with Logwatch / Logcheck

Read your logs using logwatch command (logcheck). You get detailed reporting on unusual items in syslog via email.

☐ 24. Use System Accounting with auditd

☐ 25. Secure OpenSSH Server

☐ 26. Install and Use Intrusion Detection Systems (IDS)

- Install a NIDS
- Use AIDE, a HIDS
- rkhunter to detect rootkit

☐ 27. Disable USB/Firewire/Thunderbolt Devices

Type the following command to disable USB devices on Linux system:

```
echo 'install usb-storage /bin/true' >> /etc/modprobe.d/disable-usb-storage.conf
```

You can use same method to disable firewire and thunderbolt modules:

```
echo "blacklist firewire-core" >> /etc/modprobe.d/firewire.conf
echo "blacklist thunderbolt" >> /etc/modprobe.d/thunderbolt.conf
```

Once done, users can not quickly copy sensitive data to USB devices or install malware/viruses or backdoor on your Linux based system.

☐ 28. Use fail2ban/denyhost/portsentry for IDS

Revision #13
Created 4 September 2024 20:49:55 by Alek
Updated 13 December 2024 09:40:26 by Kaiju