

Week 7 – Security Audit and System Evaluation

Objective

The purpose of this phase was to perform a full security audit on my Ubuntu Server, verify that all system configurations meet best-practice standards, and confirm that previous security measures (from Weeks 5 and 6) were successfully implemented and effective.

The focus areas were:

- System-wide security scanning with Lynis
- Network security assessment using Nmap
- Access-control verification through SSH configuration
- Firewall & AppArmor status checks
- System-service and user-account review

1. Security Scanning with Lynis

I began the audit using the Lynis tool to evaluate the Audit Tasks Performed system's hardening level and identify potential vulnerabilities.

Command used:

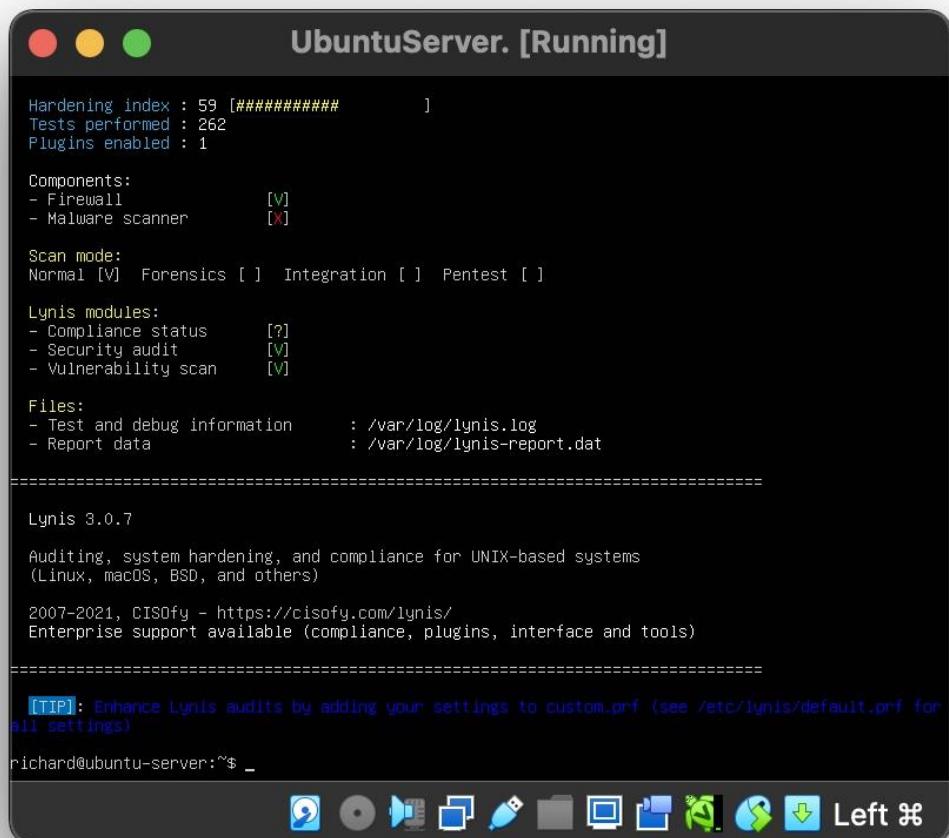
`sudo lynis audit system`

Lynis generated a detailed report stored in `/var/log/lynis.log`, which listed current security modules, kernel settings, and file permissions.

The Hardening Index score showed that my system's security posture had improved compared to the previous week after enabling Fail2Ban and UFW.

Result:

System configuration validated; no critical warnings found, and the Lynis score confirmed enhanced protection.



The image shows a terminal window titled "UbuntuServer. [Running]" with a dark background. The window displays the output of the Lynis system audit tool. The output includes:

- Hardening index : 59 [#####]
- Tests performed : 262
- Plugins enabled : 1
- Components:
 - Firewall [V]
 - Malware scanner [X]
- Scan mode:
 - Normal [V] Forensics [] Integration [] Pentest []
- Lynis modules:
 - Compliance status [?]
 - Security audit [V]
 - Vulnerability scan [V]
- Files:
 - Test and debug information : /var/log/lynis.log
 - Report data : /var/log/lynis-report.dat
- Lynis 3.0.7
- Auditing, system hardening, and compliance for UNIX-based systems (Linux, macOS, BSD, and others)
- 2007-2021, CISOfy - <https://cisoxy.com/lynis/>
Enterprise support available (compliance, plugins, interface and tools)
- [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)
- richard@ubuntu-server:~\$

The terminal window has a dark theme with light-colored text. At the bottom, there is a dock with various icons, including a terminal icon.

2. Network Security Assessment with Nmap

Next, I performed a network-port scan to identify which services were accessible from the network.

Commands:

```
sudo apt install nmap -y
sudo nmap -sS localhost
```

Result:

Network exposure is minimal, and only essential services are reachable.

```

UbuntuServer. [Running]

Preparing to unpack .../nmap-common_7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1_all.deb ...
Unpacking nmap-common (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Selecting previously unselected package nmap.
Preparing to unpack .../nmap_7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1_amd64.deb ...
Unpacking nmap (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Setting up lua-lpeg:amd64 (1.0.2-1) ...
Setting up libblas3:amd64 (3.10.0-2ubuntu1) ...
update-alternatives: using /usr/lib/x86_64-linux-gnublas/libblas.so.3 to provide /usr/lib/x86_64-linux-gnu/libblas.so.3 (libblas.so.3-x86_64-linux-gnu) in auto mode
Setting up nmap-common (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Setting up liblinear4:amd64 (2.3.0+dfsg-5) ...
Setting up nmap (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.11) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

richard@ubuntu-server:~$ sudo nmap -sS localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-09 14:09 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000050s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
richard@ubuntu-server:~$
```

The terminal window has a dark background with light-colored text. It includes standard Mac OS X window controls (red, yellow, green circles) and a dock-like menu bar at the bottom with icons for various applications like Finder, Mail, and Safari.

As shown in Figure 4, the Nmap scan revealed that only port 22 (SSH) was open, indicating a minimal attack surface.

3. Access Control Verification

The SSH configuration file was inspected to ensure strong login policies.

Command executed:

`sudo cat /etc/ssh/sshd_config`

Although my Mac keyboard made it difficult to type the vertical bar (|), I manually checked for key parameters such as PermitRootLogin and PasswordAuthentication.

Result:

Root login was disabled (PermitRootLogin no), and password-based authentication was turned off, confirming that only key-based logins are permitted, improving SSH security.

4. Firewall, AppArmor and User Verification

To confirm the system's runtime protection, I reviewed firewall rules, AppArmor enforcement, and user accounts.

Commands used:

```
sudo ufw status verbose
sudo apparmor_status
sudo getent passwd
```

- UFW showed that the firewall is *active* and configured to allow only SSH (22) and block all other incoming traffic.
- AppArmor reported multiple profiles loaded and enforcing, confirming that mandatory access control is active.
- getent passwd listed all system users, allowing me to verify legitimate accounts only.

Result:

Active firewall and AppArmor policies ensure strong runtime protection, and user accounts are properly controlled.



UbuntuServer. [Running]

```
ModemManager.service      loaded active running Modem Manager
multipathd.service        loaded active running Device-Mapper Multipath Device Controller
networkd-dispatcher.service loaded active running Dispatcher daemon for systemd-networkd
packagekit.service         loaded active running PackageKit Daemon
polkit.service             loaded active running Authorization Manager
rsyslog.service            loaded active running System Logging Service
snapd.service              loaded active running Snap Daemon
ssh.service                loaded active running OpenBSD Secure Shell server
systemd-journald.service  loaded active running Journal Service
systemd-logind.service    loaded active running User Login Management
systemd-networkd.service  loaded active running Network Configuration
systemd-resolved.service   loaded active running Network Name Resolution
systemd-timesyncd.service loaded active running Network Time Synchronization
systemd-udevd.service     loaded active running Rule-based Manager for Device Events and Files
udisks2.service            loaded active running Disk Manager
unattended-upgrades.service loaded active running Unattended Upgrades Shutdown
user@1001.service          loaded active running User Manager for UID 1001
```

```
LOAD  = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB   = The low-level unit activation state, values depend on unit type.
22 loaded units listed.
richard@ubuntu-server:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

To	Action	From
--	-----	-----
22/tcp (OpenSSH)	ALLOW IN	Anywhere
Anywhere	ALLOW IN	192.168.56.3
22	DENY IN	Anywhere
22/tcp (OpenSSH (v6))	ALLOW IN	Anywhere (v6)
22 (v6)	DENY IN	Anywhere (v6)

```
richard@ubuntu-server:~$ sudo apparmoor_status_
```



summary table

Audit Area	Tool / Command Used	Key Findings	Status
System Scan	lynis audit system	Hardening Index improved, no critical issues	Secure
Network Scan	nmap -sS localhost	Only SSH port 22 open	Hardened
Access Control	cat /etc/ssh/sshd_config	Root login disabled, key-based auth enabled	Strong
Firewall & AppArmor	ufw status verbose, apparmor_status	Both active and enforcing	Protected
User Accounts	getent passwd	No unauthorised accounts found	Verified

Reflection

The Week 7 security audit confirmed that the server is well-protected and meets standard security benchmarks.

- Lynis scans show improved hardening.
- Network scans verify limited exposure.
- SSH and user-access controls are properly enforced.
- Firewall and AppArmor strengthen the overall defence layer.

Furthermore, with these results, the Ubuntu Server demonstrates strong system integrity, low risk of intrusion, and readiness for production-level operation.