

Week 7: Security Audit and System Evaluation

Overview

In Week 7, I conducted a comprehensive security audit and system evaluation on my Linux server. The focus was on assessing security posture, verifying access controls, auditing services, and reviewing overall system configuration. This ensures the server is secure and properly configured.

1. Lynis Security Audit

I ran Lynis to evaluate system security and identify vulnerabilities.

Command:

```
sudo lynis audit system
```

```
=====
Lynis security scan details:
Hardening index : 63 [#####          ]
Tests performed : 260
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 3.0.9

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2021, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

=====

[TIP]: Enhance Lynis audits by adding your settings to custom.prfl (see /etc/lynis/default.prfl for all settings)
=====
ukouss@ubuntu215%
=====
```

=====

Lynis security scan details:

Hardening index : 63 [#####]
Tests performed : 260
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

```
vboxuser@ubuntuS:~$ sudo apt install nmap -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear4 liblua5.4-0 libssh2-1t64 nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 liblua5.4-0 libssh2-1t64 nmap nmap-common
0 upgraded, 6 newly installed, 0 to remove and 50 not upgraded.
Need to get 6,452 kB of archives.
After this operation, 28.0 MB of additional disk space will be used.
0% [Connecting to gh.archive.ubuntu.com]
```

```
vboxuser@ubuntuS:~$ sudo apt install unattended-upgrades -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package unattended-upgrades
vboxuser@ubuntuS:~$ sudo dpkg-reconfigure unattended-upgrades
dpkg-query: package 'unattended-upgrades' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files.
/usr/sbin/dpkg-reconfigure: unattended-upgrades is not installed
vboxuser@ubuntuS:~$
```

```
vboxuser@ubuntuS:~$ sudo apy update
Sanadsafwan2025
[sudo] password for vboxuser:
Sorry, try again.
[sudo] password for vboxuser:
sudo: apy: command not found
vboxuser@ubuntuS:~$ sudo apt install lynis -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
lynis is already the newest version (3.0.9-1).
0 upgraded, 0 newly installed, 0 to remove and 50 not upgraded.
vboxuser@ubuntuS:~$ sudo lynis audit system
```

