Week 10 – Assessment week 7

In this phase, a security audit was conducted to evaluate the overall system configuration and security posture of the Ubuntu server. The audit focused on system hardening, SSH security, firewall status, and running services. Industry-standard tools and configuration checks were used to assess the server.

Security Audit Using Lynis

The primary security assessment was performed using Lynis, a Linux security auditing tool.

Command used: *sudo lynis audit system*

The initial audit reported a hardening index of 66, indicating a moderate security baseline.

Based on Lynis recommendations, additional SSH hardening was applied to reduce attack surface and improve authentication security.

SSH Configuration Hardening

SSH security settings were reviewed and updated by editing the SSH daemon configuration file: *sudo nano /etc/ssh/sshd_config*

The following parameters were added to improve security:

- Reduced number of authentication attempts and sessions
- Disabled TCP, agent, and X11 forwarding
- Limited idle session tolerance

These measures help protect against brute-force attacks and unauthorised SSH usage.

```
================================================================================

  Lynis security scan details:

  Hardening index : 66 [#############       ]
  Tests performed : 266
  Plugins enabled : 1

  Components:
  - Firewall               [V]
  - Malware scanner        [V]

  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

================================================================================
```

Post-Hardening Security Scan

After applying the SSH hardening measures, the Lynis audit was executed again. The updated scan reported a hardening index of 71, confirming an improvement in overall system security.

```
================================================================================

  Lynis security scan details:

  Hardening index : 71 [##############      ]
  Tests performed : 266
  Plugins enabled : 1

  Components:
  - Firewall               [V]
  - Malware scanner        [V]

  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

================================================================================
```

This increase demonstrates that the applied security controls positively impacted the system's security posture.

Firewall and Service Assessment

The security audit confirmed that:

- A firewall is active and detected by Lynis
- Only required services are running on the system
- SSH is the primary remote access method

All running services were reviewed and justified as necessary for system operation and administration.

Remaining Risks and Evaluation

Although the server follows recommended security practices, some residual risk remains due to external network connectivity and essential services. These risks are considered acceptable for the scope of this project and can be mitigated further with continuous monitoring and periodic audits.