Week 5 – Assessment 2

Task 1 – Perfomance Testing Plan

The purpose of this performance testing plan is to monitor system performance and ensure the stability and reliability of an Ubuntu Linux system using remote monitoring techniques. Testing focuses on CPU usage, memory usage, disk space, network connectivity, and system uptime. Monitoring is performed remotely via SSH using tools such as top, free -h, df -h, uptime, and ping. System performance is compared against a baseline to identify potential performance issues.

Testing Scope

The performance testing will cover the following system components:

- CPU utilisation
- Memory (RAM) usage
- Disk space and disk I/O
- Network connectivity and traffic
- System uptime and running processes

Remote Monitoring Methodology

Remote monitoring is performed using secure SSH access. Standard Linux command-line tools are used to observe system performance without direct physical access.

Monitoring tools include:

- *top / htop* for CPU and memory usage
- *free -h* for memory status
- *df -h* for disk usage
- *uptime* for system load
- *ping* for network connectivity testing

Testing Approach

A baseline performance level is recorded during normal system operation. Performance is then periodically monitored and compared against this baseline to identify abnormal behaviour or resource bottlenecks.

Expected Outcomes

- Stable system performance

- Efficient resource usage
- Early detection of performance issues
- Improved system reliability

Task 2 - Security Configuration Checklist

Area	Configuration	Status
SSH Hardening	Disable root login	Planned
SSH Hardening	Use SSH key-based authentication	Planned
SSH Hardening	Disable password authentication	Planned
SSH Hardening	Change default SSH port	Planned
Firewall	UFW firewall configured	Enabled during setup
Firewall	Allow SSH traffic only	Enabled during setup
Firewall	Block all other incoming connections	Enabled during setup
Mandatory Access Control	AppArmor enabled	Default configuration
Mandatory Access Control	AppArmor profiles enforced	Default configuration
Automatic Updates	Automatic security updates	Planned
User Privilege Management	Least privilege principle	Applied
User Privilege Management	Sudo access restricted	Applied
Network Security	Network access restricted	Planned
Network Security	Network monitoring	Planned

Task 3 - Threat Model

Threat 1: Unauthorized SSH Access Attackers may attempt to gain access via SSH using weak credentials. Mitigation includes disabling root login, using SSH keys, and restricting access via firewall.

Threat 2: Network-based Attacks The system may be exposed to scanning or brute-force attacks. Mitigation includes limiting open ports and blocking unnecessary traffic.

Threat 3: Privilege Escalation A user may attempt to gain higher privileges. Mitigation includes applying the least privilege principle and monitoring user permissions.