ASSESSMENT WEEK2
Phase 2: security planning and testing methodology

Performance Testing Plan

For this phase, my goal was to design a security baseline and a performance-testing methodology for my two virtual machines: Ubuntu Server and Linux Mint. Both are running on Oracle VirtualBox on my MacBook Pro.

I set up Ubuntu Server (192.168.56.2) as the remote server and Linux Mint (192.168.56.3) as the workstation for remote monitoring and configuration. The plan was to connect both systems securely using SSH while ensuring stable network performance.

Testing Procedure

To start, I configured both virtual machines using the Host-Only Adapter network mode in VirtualBox, enabling the Ubuntu Server and Linux Mint workstation to communicate locally within a secure, isolated environment. Once the configuration was complete, I verified network connectivity by running ping 192.168.56.2 in the Linux Mint terminal. The results showed 0% packet loss and an average latency of approximately 1 millisecond, confirming a stable, reliable connection between the systems.

After confirming the network connection, I established a secure shell (SSH) connection from Linux Mint to Ubuntu using the command ssh admin@192.168.56.2. Although the initial attempts failed due to configuration issues, I ultimately succeeded after editing the SSH configuration file and restarting the SSH service. The connection was successful, displaying the “Welcome to Ubuntu 22.04.5 LTS” message, which validated remote access to the server.

Additionally, I recorded live performance data on the server by running the top, free -h, and df -h commands, which allowed me to monitor CPU utilisation, memory availability, and disk space usage during the SSH session. Finally, I ran several ping tests to document ongoing connection stability and ensure consistent communication performance between the two virtual machines.

Testing Result

- Network connection between both systems was stable and consistent.

- SSH access was secure and responsive.
- Average ping latency: 0.9 ms.
- System resources remained under 10% usage during SSH sessions

Security Configuration Checklist

Security Feature	Action Taken	Purpose / Justification
SSH Configuration	Enabled SSH server on Ubuntu, edited /etc/ssh/sshd_config	Allows remote login and control from Mint
Root Login Disabled	PermitRootLogin no	Protects against direct root attacks
Password Authentication Enabled	PasswordAuthentication yes	Allows controlled testing before switching to key-based login
Firewall Configuration (UFW)	Installed and allowed only port 22	Restricts open ports for security
Automatic Updates	Enabled using sudo apt update && sudo apt upgrade -y	Keeps the server patched with latest fixes
User Privilege Management	Operated using admin account instead of root	Prevents system-level mistakes
Network Isolation	Used Host-Only Adapter network	

Threat Model

Threat	Description	Mitigation Strategy
Unauthorized Root Access	Attackers could log in as root and gain full control.	Disabled root login (PermitRootLogin no)
Brute Force Login Attempts	Repeated password guesses over SSH.	Restricted login to a single admin user;

		could add fail2ban if needed.
Unpatched Vulnerabilities	Outdated system packages expose exploits.	Enabled automatic updates and used apt upgrade -y.
Network Exposure	External systems connecting to VMs.	Used isolated Host-Only network to keep VMs local only.

Challenges and Troubleshooting Process

This whole process has been the most technically challenging so far. The main goal (establishing a secure SSH connection between Linux Mint and Ubuntu Server) involved several issues that required step-by-step debugging:

Issue	**What Happened**	**Solution Implemented**
SSH login kept failing (Permission denied)	Initially, the SSH service wasn't properly configured, and root login was blocked.	Edited /etc/ssh/sshd_config, enabled PasswordAuthentication yes, restarted SSH.
SSH service refused to start	Errors in sshd_config syntax caused restart failures.	Reviewed configuration carefully, fixed indentation and removed bad lines.
"Network unreachable" when trying to connect	VirtualBox network adapters were misconfigured.	Switched both VMs to Host-Only Adapter, assigned them to the same network.
"Activation of network connection failed"	Linux Mint couldn't detect adapter.	Created a new "HostNetwork" under VirtualBox Network Manager and reattached it to both VMs.
Incorrect IP addresses	Ubuntu and Mint used different subnets.	Ensured both were in the 192.168.56.x range.
Connection finally succeeded after many attempts	SSH and ping verified communication.	

After many restarts, configuration changes, and verification commands, both systems finally connected successfully, with the Linux Mint terminal displaying **“**Welcome to Ubuntu 22.04.5 LTS.”

Final Network Setup Summary

Component	Details
Workstation (Linux Mint)	IP: 192.168.56.3
Server (Ubuntu Server)	IP: 192.168.56.2
Connection Type	Host-Only Adapter
Ping Status	0% packet loss
SSH Access	Successful (admin@192.168.56.2)
Firewall	UFW enabled on port 22 only

Reflection

At the start of this project, connecting two VMs seemed simple, but it evolved into an in-depth learning experience in Linux networking and security. I encountered multiple errors with SSH, adapter configuration, and permission settings, but with each fix, I gained a clearer understanding of how Linux servers communicate securely.

The final successful connection confirmed that my Ubuntu Server could now be managed remotely from my Linux Mint workstation in a safe, isolated environment. Configuring SSH and a firewall provided me with first-hand experience of how servers are secured in real organisations. This exercise boosted my confidence in troubleshooting, navigating the command line, and understanding the fundamentals of

Linux network security.