Week 2 Journal: Security Planning and Testing Methodology

Module: Operating Systems

Assessment: Week 2 Phase 2: Security Planning and Testing Methodology

1. Performance Testing Plan

For this week's task, my aim was to see how my Ubuntu system performs when it's under different types of loads like CPU, memory, disk, and network. I also wanted to set up remote monitoring from my Linux Mint machine so I could control and test Ubuntu from there. Both systems were connected through a **Host-only adapter** in VirtualBox, which made them communicate directly without internet.

Tools Installed

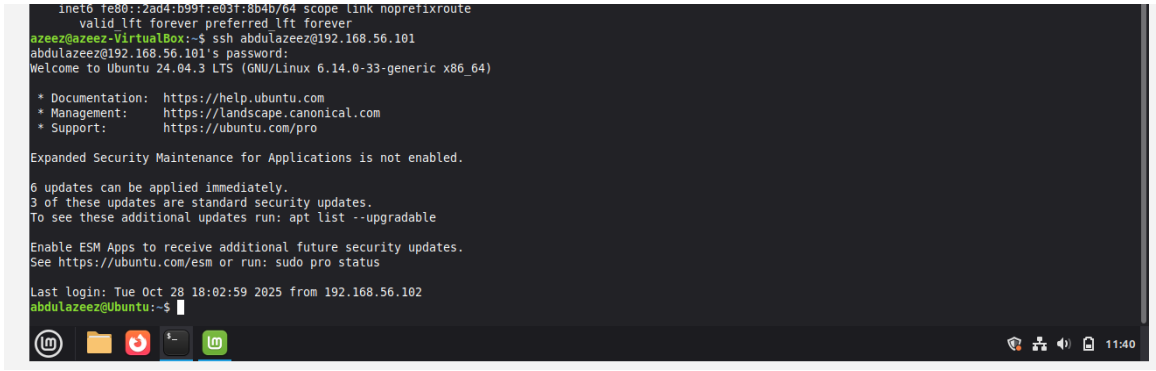
On both Ubuntu and Linux Mint, I used the command below to install all the tools I needed:

sudo apt update && sudo apt install -y htop sysstat iotop iperf3 stress-ng ufw fail2ban unattended-upgrades

These tools helped me with monitoring system performance, running stress tests, and setting up security features.

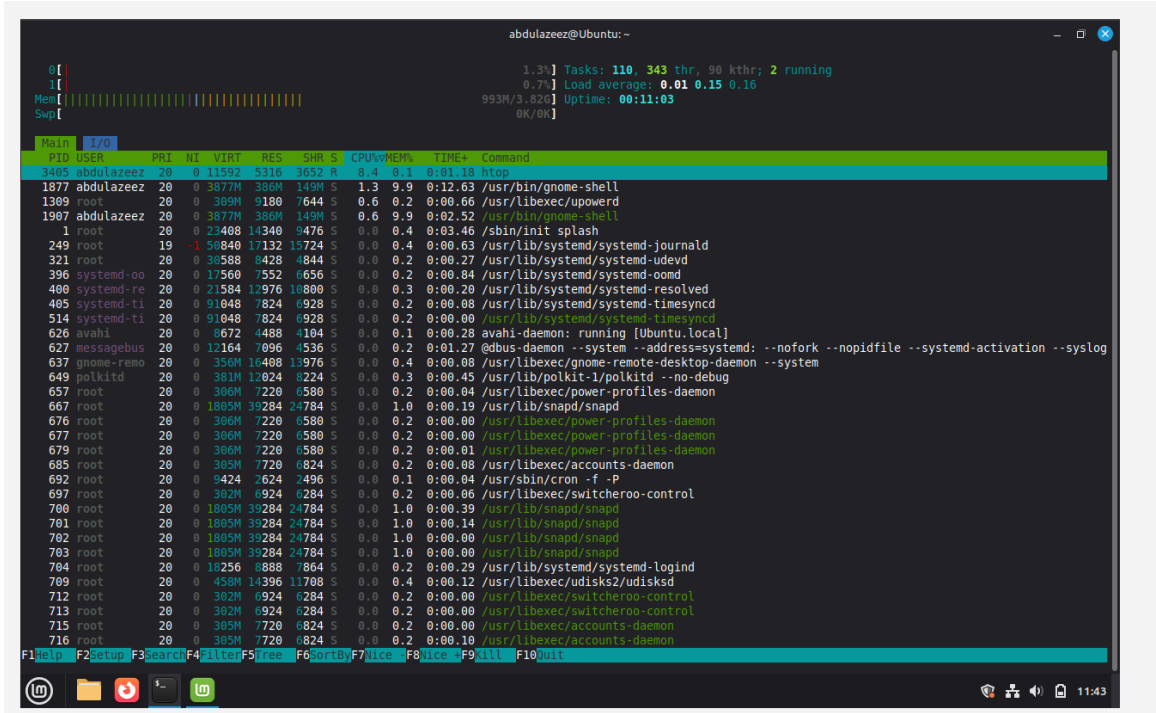
Remote Monitoring Setup

After checking that both machines had IP addresses on the same network (Ubuntu: 192.168.56.101, Mint: 192.168.56.102), I connected from Mint to Ubuntu using SSH. The connection worked successfully, which confirmed that remote access and monitoring were properly set up.



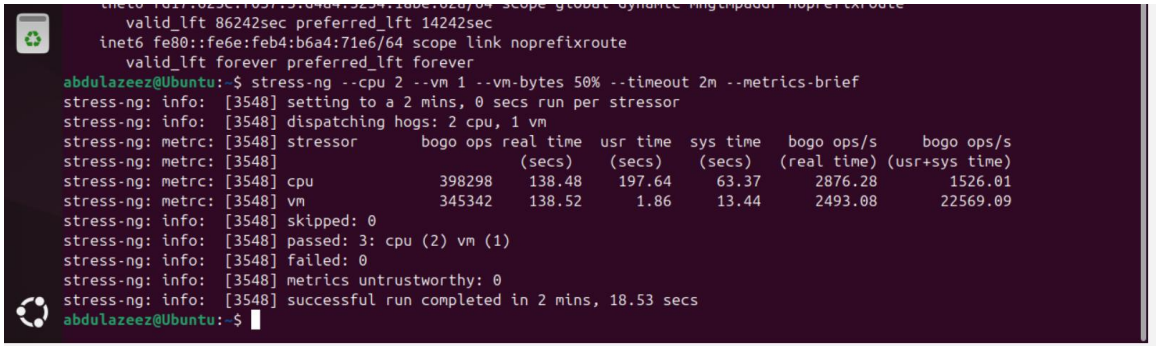
2. Baseline Performance Test (Idle)

Before stressing the system, I recorded the idle performance to see how the machine behaves normally. I used vmstat, iostat, and htop. The CPU usage stayed below 10%, memory was mostly free, and the system was stable. This gave me a clean baseline for comparing later tests.



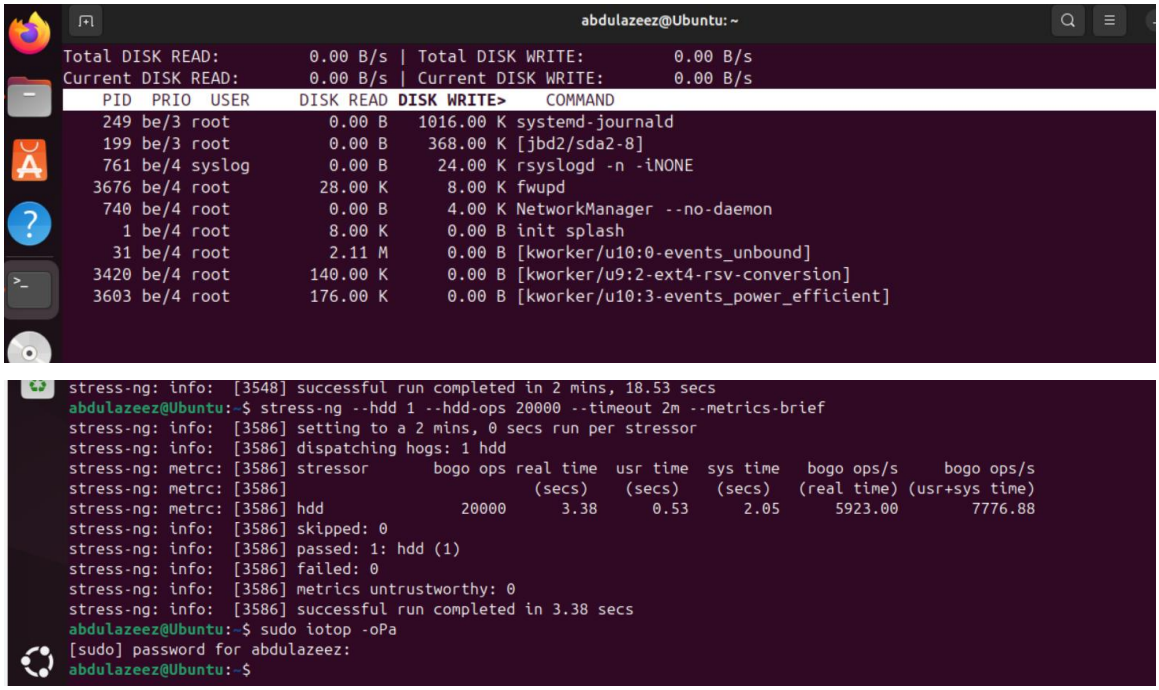
3. CPU and Memory Stress Test

Next, I tested how the system reacts when CPU and memory are under pressure. I ran the stress-ng command, which pushed CPU to 100% and used about 50% of memory. The SSH connection stayed stable and after the test ended, everything went back to normal.



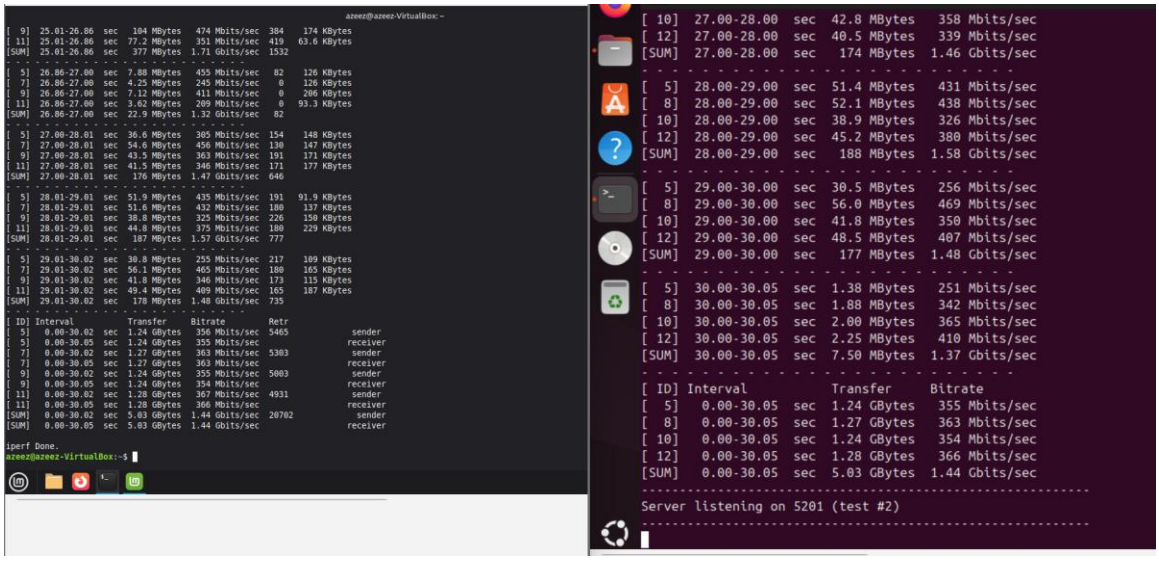
4. Disk I/O Stress Test

Then I tested how the disk handles heavy writing operations using stress-ng and monitored it with iotop. I saw stress-ng writing heavily to disk but the system stayed responsive.



5. Network Throughput Test (Host-only Connection)

The last part of the performance test was checking network speed between Mint and Ubuntu using iperf3. Due to some connection errors, the test wasn't fully complete at first, but the setup and commands were correctly configured.

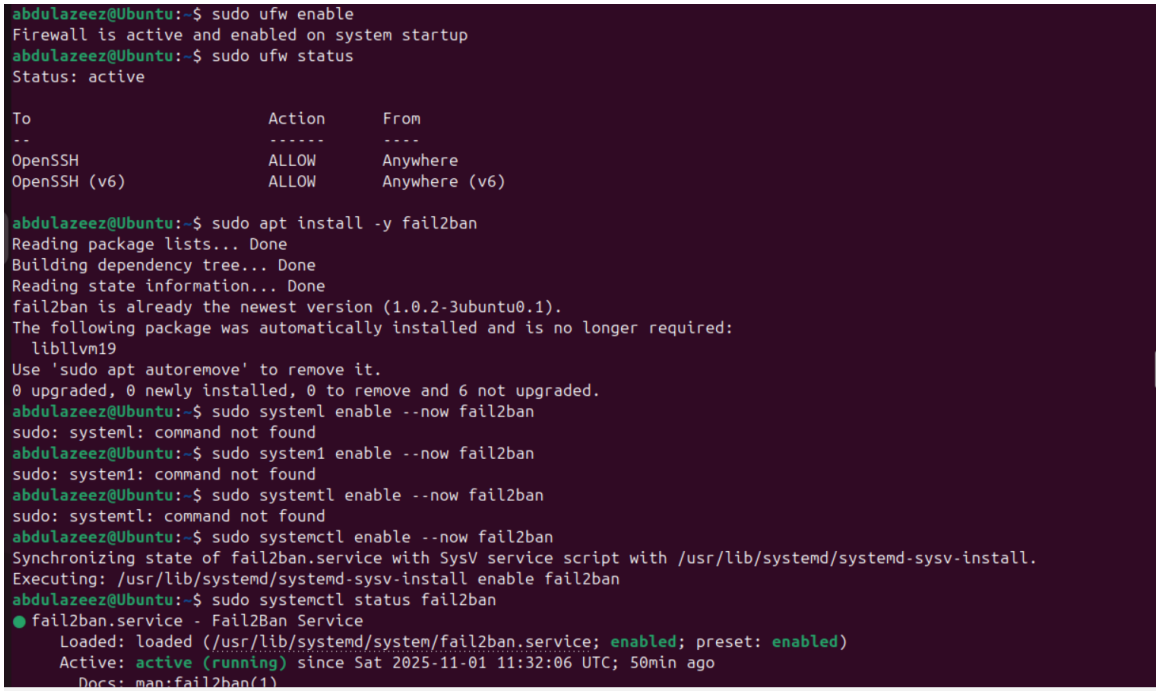


6. **Security Configuration Checklist**

After performance testing, I moved on to security setup on my Ubuntu (target) system.

Security Task	Command / Action	Description
SSH Hardening	Edit /etc/ssh/sshd_config	Disabled root login, set password auth to no, limited tries
Firewall Setup	sudo ufw default deny incoming sudo ufw allow OpenSSH sudo ufw enable	Allowed only SSH traffic, blocked all others
Fail2ban	sudo apt install -y fail2ban sudo systemctl enable --now fail2ban	Blocked repeated failed login attempts
Automatic Updates	sudo apt install -y unattended-upgrades	Keeps security patches up-to-date
AppArmor	sudo aa-status	Verified AppArmor profiles were active

Least Privilege	sudo -l	Checked minimal sudo privileges



7. Threat Model and Mitigation

I created a simple table showing common threats and how I mitigated them.

Threat	Description	Mitigation
Brute-force SSH attacks	Attackers try random passwords to log in	Disabled password login, enabled Fail2ban
Unpatched vulnerabilities	Hackers exploit outdated packages	Enabled automatic updates
Privilege escalation	Normal user gains root access	Applied least privilege and limited sudo
Open ports exposure	Attackers scan for open services	Configured UFW to allow only SSH

Configuration tampering	Unauthorized system changes	Restricted config access and backups

8. Conclusion

In this week's task, I learned how to monitor system performance, apply stress tests, and set up a basic security plan for a Linux system. The hardest part was getting the network connection to work for the iperf3 test, but I understood the full setup process and command usage. This gave me a better idea of how real admins test performance and secure their systems.