Week 2 – Security Planning and Threat Model

Introduction

Week 2 focuses on planning a security baseline and defining a performance testing methodology for the Ubuntu server. This includes SSH hardening, firewall rules, access control, and identifying potential security threats.

Security Baseline Checklist

Security Control	Action Taken
SSH Hardening	Key-based authentication enabled; password authentication disabled
Firewall	Configured UFW to allow only SSH from workstation (`192.168.56.102`)
User Privileges	Created non-root admin user; restricted root login
Automatic Updates	Enabled unattended-upgrades for security patches
Access Control	SELinux/AppArmor to be configured in Week 5

Threat Model

Three potential security threats and mitigation strategies:

Threat	Description	Mitigation
Unauthorized SSH Access	Brute-force login attempts	Key-based authentication, UFW restricted IP
Service Exploitation	Vulnerable running services	Disable unnecessary services, monitor logs

Privilege Escalation	Users gaining root privileges	Enforce sudo rules, non-root admin accounts

Performance Testing Plan

- All monitoring and testing performed via SSH from Fedora workstation
- Metrics to track: CPU, memory, disk I/O, network latency, and service response times
- Applications chosen in Week 3 will simulate different workloads (CPU, RAM, I/O, network)
  I will send screenshot of this in week 3

Reflection

Planning a security baseline ensures the server is hardened before applications are installed. Defining potential threats and mitigations early reduces risk and ensures systematic evaluation. This week reinforced the importance of security-first planning in system administration.