Network Security

Provider: Coursera
Completion Date: September 3, 2025

Overview

This course introduced the principles and practices of network security, focusing on infrastructure, monitoring, and defense mechanisms. It covered network services, access control models, NAT, ACLs, firewalls, malware protection, and AAA frameworks, reinforced through hands-on labs.

Key Topics Covered

- Network infrastructure and security monitoring tools (NSM, SOC toolsets)
- NAT fundamentals: static, dynamic, PAT, and policy NAT
- Packet filtering with Access Control Lists (ACLs)
- Access control models: MAC, DAC, RBAC, ABAC, RuBAC, TBAC
- AAA (Authentication, Authorization, and Accounting) frameworks
- Load balancing algorithms and security considerations
- Web Application Firewalls (WAF) and OWASP Top 10 protections
- Network-based malware protection with Cisco Firepower and AMP
- Defense-in-depth strategies for layered protection

Practical Applications

- Configuring NAT and ACLs to control network traffic
- Implementing role-based and policy-based access controls
- Using AAA frameworks for centralized authentication
- Deploying WAFs to secure applications against OWASP Top 10
- Leveraging malware protection for real-time defense

Personal Reflection

This course sharpened my ability to secure networks through layered defenses. I gained hands-on experience with NAT, ACLs, and AAA, and learned to integrate firewalls and malware protection into defense-in-depth strategies that support compliance and incident response.