Cybersecurity Lab Portfolio - Alen Guner

Lab: Network Segmentation & Defense-in-Depth Design

Objective:

Design and simulate a segmented network architecture to prevent lateral movement and reduce attack surface. Demonstrate layered security and VLAN separation using pfSense or Cisco Packet Tracer.

Tools Used:

- pfSense Firewall (or Cisco Packet Tracer)
- VirtualBox or GNS3
- Linux VMs for endpoints
- Wireshark for traffic inspection
- Optional: Nmap for internal scanning tests

Steps Taken:

1. Network Design:
- Created a 3-zone network: Public (DMZ), Internal (LAN), and Management VLANs.
- Assigned unique subnets to each zone and configured interface routing.

2. Firewall Configuration:
- Set up pfSense to restrict inter-VLAN traffic.
- Allowed only essential communication (e.g., Web server access from Public to DMZ).

3. Access Control:
- Implemented rule sets to block lateral movement (e.g., no LAN <-> LAN unless authorized).
- Added logging for all deny rules to monitor intrusion attempts.

4. Simulation & Testing:
- Deployed VMs in each zone to simulate users and services.
- Used Nmap to simulate attacker trying to pivot across network zones.

5. Logging & Monitoring:
- Verified segmentation with Wireshark packet capture.
- Created rule to alert on blocked access attempts between segments.

Outcome / What I Learned:

- Designed and tested a basic segmented network with three isolated zones.
- Gained experience configuring firewall rules and interface routing.
- Understood how segmentation reduces risk of lateral movement.
- Learned how to validate network isolation using real tools.

Keywords:

Cybersecurity Lab Portfolio - Alen Guner

Network Segmentation, pfSense, VLAN, Lateral Movement, Firewall, DMZ, Defense in Depth, VirtualBox, Packet Tracer