Network Segmentation

Task:

Implement network segmentation to isolate critical systems and limit lateral movement of attackers.

What is Network Segmentation?

Network segmentation is a security strategy that divides a network into smaller, isolated segments to enhance security. By restricting access between segments, it limits an attacker's ability to move laterally within a compromised network, reducing the potential damage of a breach.

Steps to Implement Network Segmentation

1. Identify Critical Assets

Determine which systems, applications, and data require protection.

2. Define Security Zones

Segment the network into zones based on sensitivity and access needs (e.g., internal, external, restricted).

3. Implement Access Controls

Use firewalls, VLANs, and access control lists (ACLs) to regulate communication between segments.

4. Monitor and Enforce Policies

Continuously monitor network traffic and enforce segmentation policies to prevent unauthorized access.

5. Test and Optimize Segmentation

Regularly assess segmentation effectiveness through penetration testing and security audits.

Network Segmentation Best Practices:

- Cisco Network Segmentation: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-segmentation.html
- NIST Guidelines on Network Segmentation: https://csrc.nist.gov/publications/detail/sp/800-125a/final
- Palo Alto Networks Segmentation Guide:

https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation