Analyzing Network Structure and Security

Analyzing Network Structure and Security

Analyzing network structure and security is a foundational activity in cybersecurity. This process involves evaluating the components of a network, identifying potential vulnerabilities, and implementing controls to protect against threats.

Network Structure Analysis:

- Inventory of all connected devices, such as routers, switches, servers, and endpoints.
- Mapping of data flow and interconnections across the network.
- Identification of critical network segments that support essential business operations.

Security Analysis:

- Assessment of current firewall configurations and access control lists (ACLs).
- Evaluation of authentication and authorization mechanisms.
- Review of encryption protocols used for data in transit and at rest.
- Identification of unpatched systems or outdated firmware.

Best Practices:

- Segmentation of networks to isolate sensitive systems.
- Implementation of intrusion detection and prevention systems (IDS/IPS).
- Regular vulnerability scanning and penetration testing.
- Use of multi-factor authentication (MFA) for accessing critical systems.

Outcome:

Analyzing network structure and security helps ensure that systems are adequately protected,

aligned with best practices, and capable of resisting modern cyber threats. This step is crucial in both proactive defense and regulatory compliance.