Topic 6 Discussion 1

You head up a small team of IT and cyber professionals tasked with ensuring network security. A recent malware has come to light that involves exploiting several ports and protocols, specifically port 22, port 25, port 53 TCP, port 80, and port 8080. Identify each of the ports and protocols associated. What compensating controls could be utilized to ensure security?

Hello Class,

Ports and Protocols

Port 22 (TCP)

Protocol: SSH (Secure Shell)

Usage: Used for secure remote administration and file transfers.

Port 25 (TCP)

Protocol: SMTP (Simple Mail Transfer Protocol)

Usage: Primarily used for sending emails between servers.

Port 53 (TCP/UDP)

Protocol: DNS (Domain Name System)

Usage: Resolves domain names to IP addresses; can be exploited for DNS amplification attacks.

Port 80 (TCP)

Protocol: HTTP (Hypertext Transfer Protocol)

Usage: Used for web traffic; unsecured web communications.

Port 8080 (TCP)

Protocol: HTTP (alternative port)

Usage: Often used for web servers and proxy services; can be a target for web-based attacks.

Compensating Controls

Compensating controls are measures taken to address any weaknesses of existing controls or to compensate for the inability to meet specific security requirements due to various different constraints(Team82, 2023).

Firewalls:

Configure firewalls to restrict access to these ports based on the principle of least privilege. Only allow necessary traffic.

Intrusion Detection and Prevention Systems (IDPS):

Deploy IDPS to monitor network traffic for suspicious activities and potential threats.

Network Segmentation:

Segment the network to isolate critical systems and limit the spread of malware.

Regular Updates and Patch Management:

Ensure that all systems and applications are regularly updated to protect against known vulnerabilities.

Strong Authentication Mechanisms:

Implement multi-factor authentication (MFA) for services using these ports, especially for SSH (port 22).

Email Filtering:

Use advanced email filtering solutions to detect and block malicious emails that may exploit SMTP (port 25).

DNS Security Measures:

Implement DNSSEC (Domain Name System Security Extensions) to protect against DNS spoofing and amplification attacks.

Web Application Firewalls (WAF):

Use WAFs to protect web applications from common threats targeting HTTP traffic on ports 80 and 8080.

References:

Schrader, D. (2024, September 3). *Identifying Common Open Port Vulnerabilities in Your Network*. Netwrix.com. https://blog.netwrix.com/open-ports-vulnerability-list

Team82. (2023, April 6). *The Importance of Compensating Controls in Cybersecurity*. Claroty. https://claroty.com/blog/ot-icefall-vulnerabilities-underscore-the-importance-of-compensating-controls