Part 3: Network Hardening Plan

CYB540G: NETWORK AND INTERNET SECURITY

Jorge, Nsundidi
CANISIUS UNIVERSITY | 2001 MAIN ST, BUFFALO, NY 14208

Table of Contents

Network Hardening Plan

Immediate Actions

Router Configuration

- To start with, immediate actions will focus on device configuration. **Router Configuration** includes updating firmware to the latest version to patch CVE-2021-20090 and other vulnerabilities, changing the default admin password, and disabling remote management access.

- Additionally, HTTPS will be enabled for the administrative web interface, and an SSL certificate will be obtained. Telnet will be disabled in favor of SSH with secure configuration (SSH v2), and SNMP access will be restricted with the default community string changed.

Firewall Configuration

- For **Firewall Configuration**, it is critical to update OpenSSL to the latest version and restrict management access to internal IPs only, while disabling HTTP access. Access control lists (ACLs) will be configured to allow only trusted IP addresses for VPN connections, and ICMP responses will be blocked on the external-facing interface.

- In terms of **Web Server Configuration**, the plan is to update Apache to the latest version (2.4.53 or later) to patch CVE-2022-23943, obtain a new SSL certificate, and install it on the server. Weak ciphers and outdated SSL/TLS versions (such as SSLv3) will be disabled, and strong SSL/TLS protocols (1.2 or 1.3) will be configured. Additionally, directory listing will be disabled, and Apache version information will be hidden.

- The **Database Configuration** involves changing the default MySQL credentials and updating the database to the latest version, along with enabling SSL/TLS for database connections.

- For **Laptop and Desktop Configuration**, all pending critical and security updates will be installed, and strong password policies will be enabled to ensure all devices are up to date.

Firewall Rules

- Regarding firewall rules, **External Firewall Rules** will block all incoming traffic on ports 22 (SSH), 23 (Telnet), and 80 (HTTP) from external IPs while allowing incoming traffic on port 443 (HTTPS) for the web server. It is also essential to allow incoming traffic on port 22 (SSH) from trusted internal IPs for administrative access.

- On the other hand, **Internal Firewall Rules** will block all incoming traffic on ports 22 (SSH), 23 (Telnet), and 80 (HTTP) from internal IPs while allowing incoming traffic on port 443 (HTTPS) for the web server.

Encryption

- In terms of encryption, **SSL/TLS** protocols will be enforced (1.2 or 1.3) for all public-facing web servers, with weak ciphers and outdated SSL/TLS versions (like SSLv3) disabled.

- Additionally, **SSH** will utilize SSH v2 for secure remote access, and strong encryption algorithms (e.g., AES-256) will be configured.

Network Segmentation

- Network segmentation will be achieved through the implementation of **VLANs** to segment the network into different zones based on functionality and sensitivity, along with configuring ACLs to restrict traffic between VLANs.

- Furthermore, **subnets** will be implemented to further segment the network and restrict traffic.

Monitoring and Maintenance

Regular Updates

- Lastly, ongoing monitoring and maintenance are crucial. **Regular Updates** will be scheduled for all devices and software to ensure the latest security patches are applied. Monitoring tools will be set up to detect and alert on potential security issues, and logs will be reviewed regularly to identify and address potential security threats.

Security Audits

- Additionally, **Security Audits** will be conducted regularly to identify vulnerabilities and weaknesses, ensuring that any identified issues are addressed promptly.

Training and Awareness

- To support these efforts, **Training and Awareness** programs will be provided to all users to ensure they understand the importance of security and their role in maintaining it.

By implementing these measures, we can significantly enhance the security of the network and mitigate the risk of security breaches. Regular monitoring and maintenance will ensure ongoing security over time.