PART 2: Vulnerability Analysis and Recommendations

CYB540G: NETWORK AND INTERNET SECURITY

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

PART 2: Vulnerability Analysis and Recommendations

Date: October 9th, 2024

Assessed by: Nsundidi Jorge

This report summarizes the results of a vulnerability assessment conducted on the internal network using Nessus. Both internal and external scans were performed on a range of systems to identify security weaknesses that could be exploited by attackers. The purpose of this assessment is to provide insight into the current security posture and offer recommendations to mitigate identified vulnerabilities.

Table of Contents

INTERNAL SCAN REPORT
ANALYSIS AND RECOMMENDATIONS

1. Critical Vulnerabilities and Devices at Highest Risk:

Router (192.168.1.1):

- CVE-2021-20090 (Path Traversal): High-risk as it allows attackers to access unauthorized directories. This vulnerability could expose sensitive internal data.
- Weak SNMP Community String: Using the default "public" string makes the router vulnerable to unauthorized monitoring and network configuration.
- Open Telnet Port (Port 23): Telnet is unencrypted, enabling attackers to intercept and manipulate communications.
- Outdated SSH Protocol (SSH v1): Insecure encryption used in SSH could lead to exposure of credentials.
- HTTP Web Interface: Lacks encryption, increasing susceptibility to MITM attacks during administrative tasks.

Switch (192.168.1.2):

- VLAN Hopping Attack: Misconfigured VLANs could allow an attacker to move between VLANs, bypassing network segmentation.

Firewall (192.168.1.3):

- Weak Firewall Rules: Open management ports accessible externally pose a significant risk, allowing unauthorized users to access administrative interfaces.
- Outdated OpenSSL: Vulnerable OpenSSL can be exploited for various cryptographic attacks.

Web Server (192.168.1.10):

- CVE-2022-23943 (Apache HTTP Server mod_lua RCE): Allows remote attackers to execute arbitrary code, which is a critical risk to web server integrity.
- Weak SSL/TLS Configurations: Using weak ciphers and SSLv3 increases the risk of encrypted data being decrypted by attackers.

Database (192.168.1.11):

- Default MySQL Credentials: Having default credentials enables attackers to gain administrative control over the database.
- CVE-2021-27928 (Privilege Escalation): This allows malicious users to escalate privileges, potentially leading to unauthorized data manipulation.

Laptop 1 (192.168.1.20):

- Unpatched Windows Vulnerabilities: Missing critical patches (like PrintNightmare) makes the laptop vulnerable to known exploits.

Desktop 1 (192.168.1.21):

- Outdated RDP Protocol: BlueKeep vulnerability could allow attackers to execute arbitrary code remotely, potentially compromising the desktop.

2. Recommendations for Remediation Vulnerabilities

Router (192.168.1.1)

1. **CVE-2021-20090 (Path Traversal Vulnerability)**:
   - **Step 1**: Identify the router's current firmware version through its web interface or CLI.
   - **Step 2**: Visit the router vendor's website and download the latest firmware.
   - **Step 3**: Follow the vendor's instructions to upload and install the firmware update. Ensure the router reboots to apply changes.
   - **Step 4**: After the update, verify that the version is correct and the vulnerability is patched.

2. **Weak SNMP Community String**:
   - **Step 1**: Log into the router's web interface or CLI.
   - **Step 2**: Navigate to the SNMP settings.
   - **Step 3**: Change the default "public" string to a unique, complex string (e.g., "Qxw8K!#4").
   - **Step 4**: Disable SNMP if it's not required for network monitoring.
   - **Step 5**: Test SNMP settings by attempting an SNMP query using the new string.

3. **Open Telnet Port (Port 23)**:
   - **Step 1**: Access the router’s settings through its web interface or CLI.
   - **Step 2**: Navigate to the **Services** or **Remote Management** settings.
   - **Step 3**: Disable Telnet by toggling the option off.
   - **Step 4**: Enable SSH and configure SSH version 2.
   - **Step 5**: Test SSH connectivity to ensure it's working and Telnet is disabled.

4. **Outdated SSH Protocol (SSH v1)**:
   - **Step 1**: Access the router’s configuration interface.
   - **Step 2**: Find the SSH settings (usually under **Remote Access** or **Security**).
   - **Step 3**: Change the protocol from SSH v1 to SSH v2.
   - **Step 4**: Restart the SSH service and test it to verify the change.

5. **HTTP Web Interface (Uses HTTP instead of HTTPS)**:
   - **Step 1**: Navigate to the router’s Management or Remote Access section.
   - **Step 2**: Enable HTTPS for the administrative web interface.
   - **Step 3**: Obtain an SSL certificate (self-signed or from a CA).
   - **Step 4**: Install the SSL certificate on the router.
   - **Step 5**: Test the web interface to ensure it's accessible over HTTPS.

Switch (192.168.1.2)

1. **VLAN Hopping Attack Possible**:
   - **Step 1**: Access the switch via web interface or CLI.
   - **Step 2**: Ensure VLAN tagging is properly configured on trunk ports (use only tagged VLANs).
   - **Step 3**: Disable DTP (Dynamic Trunking Protocol) on trunk ports to prevent VLAN hopping.
   - **Step 4**: Assign all access ports to specific VLANs and mark them as access ports only.
   - **Step 5**: Test VLAN segmentation by simulating traffic between VLANs and ensuring they are isolated.

2. **No Security Logging Configured**:
   - **Step 1**: Access the switch's settings.
   - **Step 2**: Enable logging of all critical events (e.g., access violations, configuration changes).
   - **Step 3**: Set up a logging server (Syslog) to collect logs or save them locally on the switch.
   - **Step 4**: Test by generating a few events (like admin logins) and verifying logs are captured.

3. **Outdated Firmware**:
   - **Step 1**: Identify the current firmware version.
   - **Step 2**: Download the latest firmware from the switch manufacturer's website.
   - **Step 3**: Follow the vendor's instructions to update the firmware.
   - **Step 4**: Reboot the switch after the update and verify that the new firmware is installed.

Firewall (192.168.1.3)

1. **Weak Firewall Rules**:
   - **Step 1**: Access the firewall's management interface.
   - **Step 2**: Locate open management ports (e.g., HTTP, SSH) in the firewall rules.
   - **Step 3**: Restrict management access to internal IPs only by setting up **allow** rules for internal IP ranges.
   - **Step 4**: Switch the HTTP management interface to HTTPS by obtaining an SSL certificate and applying it.
   - **Step 5**: Test firewall access from internal and external networks to verify restrictions.

2. **Outdated OpenSSL Version**:
    - **Step 1**: Check the firewall's current OpenSSL version.
    - **Step 2**: Download the latest OpenSSL version from the firewall vendor or install it through a software package manager.
    - **Step 3**: Update the OpenSSL library on the firewall.
    - **Step 4**: Reboot the firewall (if necessary) and test the encryption functionality to ensure it's using the updated OpenSSL version.

Printer (192.168.1.5)

1. **Open Printer Ports (9100, 515)**:
    - **Step 1**: Access the printer's web interface or admin panel.
    - **Step 2**: Disable unused protocols (like **JetDirect (Port 9100)** and **LPD (Port 515)**) unless necessary.
    - **Step 3**: If printing is required, ensure it is done over a secure protocol such as IPP over HTTPS.
    - **Step 4**: Test printer functionality to verify that the unused protocols are disabled.

Web Server (192.168.1.10)

1. **CVE-2022-23943 (Apache HTTP Server mod_lua RCE)**:
    - **Step 1**: Check the current Apache version by running apachectl -v.
    - **Step 2**: Download and install the latest version of Apache (2.4.53 or later) from the official website.
    - **Step 3**: Restart the Apache service: sudo systemctl restart apache2.
    - **Step 4**: Verify the installation by checking the version again.

2. **Weak SSL/TLS Configuration**:
    - **Step 1**: Access the Apache SSL configuration file (e.g., /etc/apache2/sites-available/default-ssl.conf).
    - **Step 2**: Disable weak ciphers (SSLv3) and configure the server to use strong ciphers (e.g., TLS 1.2 or TLS 1.3).
    - **Step 3**: Save the configuration and restart Apache to apply changes.
    - **Step 4**: Test using an SSL checker to ensure strong encryption.

3. **Directory Listing Enabled**:
    - **Step 1**: Open the Apache configuration file and find the Options directive for the affected directory.
    - **Step 2**: Modify the line to include Options -Indexes.
    - **Step 3**: Save the file and restart Apache to apply changes.
    - **Step 4**: Test by accessing the directory in a browser to ensure listing is disabled.

4. **Exposed Server Info**:
    - **Step 1**: In the Apache config file, locate the ServerTokens and ServerSignature directives.
    - **Step 2**: Set ServerTokens to Prod and ServerSignature to Off.
    - **Step 3**: Restart Apache to apply changes.
    - **Step 4**: Test by checking the HTTP response headers to ensure version info is hidden.

Database (192.168.1.11)

1. **Default MySQL Credentials**:
    - **Step 1**: Log in to MySQL using the default credentials.
    - **Step 2**: Change the root password
    - **Step 3**: Log out and back in to verify the new credentials.

2. **CVE-2021-27928 (Privilege Escalation)**:
    - **Step 1**: Check the current MySQL version by running mysql --version.
    - **Step 2**: Download and install the latest security patches or upgrade MySQL to the latest version.
    - **Step 3**: Restart the MySQL service to apply updates.
    - **Step 4**: Verify by running mysql --version again.

3. **No SSL/TLS for Database Connections**:
    - **Step 1**: Generate an SSL certificate (self-signed or from a CA) for MySQL.
    - **Step 2**: Enable SSL in the MySQL configuration file (my.cnf) by adding:
      require_secure_transport = ON
    - **Step 3**: Restart MySQL and verify SSL is working by checking the connection encryption.

Laptop 1 (192.168.1.20)

1. **Unpatched Windows Vulnerabilities**:
    - **Step 1**: Open Windows Update and check for available updates.
    - **Step 2**: Install all pending critical and security updates.
    - **Step 3**: Restart the laptop to apply updates.

2. **Weak Password Policy**:
    - **Step 1**: Open **Local Group Policy Editor** (gpedit.msc).
    - **Step 2**: Navigate to **Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy**.
    - **Step 3**: Enable policies requiring strong passwords, e.g., minimum password length, complexity, and expiration.
    - **Step 4**: Apply and enforce the policy.

Desktop 1 (192.168.1.21)

1. **Outdated RDP Protocol**:
   - **Step 1**: Open **Control Panel > System > Remote Settings**.
   - **Step 2**: Enable **Network Level Authentication (NLA)** for remote connections.
   - **Step 3**: Ensure Windows is up to date and install any available RDP security updates.
   - **Step 4**: Test the RDP connection and ensure it's using the latest version and NLA.

3. Highlight External-Facing Risks**:**

1. Router (192.168.1.1):

- **CVE-2021-20090 and Open Management Ports**: External exposure of router management interfaces could lead to unauthorized access and configuration changes. Mitigation involves updating the firmware, changing default credentials, and restricting management access via internal IPs.

2. Firewall (192.168.1.3):

- **Weak Firewall Rules**: Having open management ports (HTTP) exposed to the external network is a severe risk. Mitigation steps include restricting management access to internal IPs and switching to HTTPS.

3. Web Server (192.168.1.10):

- **CVE-2022-23943 and Weak SSL/TLS**: The web server’s mod_lua vulnerability and weak SSL/TLS configurations expose it to remote code execution and data breaches. Mitigation involves upgrading Apache, configuring strong SSL/TLS, and disabling vulnerable cipher suites.

EXTERNAL SCAN REPORT
ANALYSIS AND RECOMMENDATIONS

1. Critical Vulnerabilities and Devices at Highest Risk

High-Risk Devices:

- **Router (203.0.113.1)**: This device has multiple critical vulnerabilities, including a path traversal flaw (CVE-2021-20090), weak administrative credentials, and exposed services like HTTP and SSH. These issues make the router highly susceptible to unauthorized access and exploitation.

- **Web Server (203.0.113.10)**: This web server is at high risk due to CVE-2022-23943, an Apache mod_lua remote code execution vulnerability, and an expired SSL certificate. The combination of these vulnerabilities exposes the server to potential code execution attacks and compromised HTTPS security.

- **Firewall (203.0.113.3)**: The exposed management interface on the public internet (HTTP and HTTPS) presents a high-risk vector, making this firewall device vulnerable to unauthorized access. The outdated OpenSSL version compounds the risk, as it may have unpatched vulnerabilities.

Services and Protocols Representing the Greatest Security Threats:

- **HTTP/HTTPS (Router & Firewall)**: HTTP is unencrypted, and exposing both HTTP and HTTPS management interfaces publicly poses a severe risk of unauthorized access.

- **SSH (Router & Web Server)**: The open SSH port without proper IP restrictions is vulnerable to brute force attacks.

- **VPN IKE (Firewall)**: Open VPN ports without access controls could lead to denial of service (DoS) or credential stuffing attacks.

2. Recommendations for Remediating Vulnerabilities

Router (203.0.113.1)
Path Traversal (CVE-2021-20090):

1. **Access Router Admin Interface**:
    - Open a web browser.
    - Enter the router's IP address (e.g., 203.0.113.1).
    - Log in using the current credentials (ensure these are secure and not default).
2. **Update Firmware**:
    - Navigate to the **Firmware Update** section (often found under **Administration** or **System**).
    - Check for available updates and download the latest firmware from the router manufacturer's website.
    - Upload the firmware file to the router and initiate the update.
    - **Reboot** the router to apply the new firmware.
3. **Disable External Management**:
    - Locate the **Remote Management** or **External Management** option.
    - Disable it or restrict management to specific internal IP addresses.

Weak Administrative Credentials:

1. **Change Default Admin Password**:
    - Log into the router's web interface.
    - Go to the **Admin Settings** or **Security Settings** section.
    - Change the password to a strong, unique one (use a password manager if necessary).
    - **Password Guidelines**: 12-16 characters, a mix of upper/lowercase letters, numbers, and special characters.

2. **Disable Remote Management**:
    - In the router settings, find the **Remote Management** option.
    - Turn off **Remote Management** if not required or allow access only from specific trusted IPs.

Open HTTP Web Interface:

1. **Switch from HTTP to HTTPS**:
    - In the router settings, go to **Web Interface Settings** or **Remote Access Settings**.
    - Enable **HTTPS** access for the administrative interface.
    - Disable **HTTP** access entirely for remote management to prevent unencrypted access.

2. **Disable Remote Management if Unnecessary**:
    - If remote management is not essential, disable it to prevent exposure to external threats.

Open SSH Port (22):

1. **Restrict SSH Access**:
    - Navigate to the **SSH Settings** under **Remote Access**.
    - Create an **Access Control List (ACL)** to allow only specific IP addresses (e.g., from a trusted admin network).
2. **Disable SSH**:
    - If SSH is not needed, disable it in the router's settings entirely to prevent unauthorized access attempts.

Disable ICMP (Ping Requests Allowed):

1. **Block ICMP Responses**:
    - Go to **Firewall Settings** or **Security Settings** in the router.
    - Disable **ICMP Echo Requests** or **Ping Responses** for external IPs.

Web Server (203.0.113.10)
CVE-2022-23943 (Apache mod_lua Remote Code Execution):

1. **Update Apache HTTP Server**:
    - SSH into the server using a terminal.
    - Run the following commands to update Apache:
      sudo apt-get update
      sudo apt-get install apache2
    - Check that the Apache version is 2.4.53 or later:
      apache2 -v
    - Restart Apache to apply the updates:
      sudo systemctl restart apache2

Expired SSL Certificate:

1. **Obtain a New SSL Certificate**:
    - Go to a Certificate Authority (e.g., Let's Encrypt, DigiCert, or Comodo).
    - Purchase or generate a new SSL certificate.

2. **Install the New SSL Certificate**:
    - Upload the new certificate to the server:
      sudo cp new_certificate.crt /etc/ssl/certs/
      sudo cp new_private.key /etc/ssl/private/

    - Update Apache's configuration file (/etc/apache2/sites-available/your-site.conf) with the new certificate paths:
      SSLCertificateFile /etc/ssl/certs/new_certificate.crt
      SSLCertificateKeyFile /etc/ssl/private/new_private.key

    - Reload Apache to apply the new certificate:
      sudo systemctl reload apache2

Weak SSL/TLS Configuration:

1. **Disable SSLv3 and Weak Ciphers**:
    - Edit the Apache configuration file (/etc/apache2/mods-available/ssl.conf):
      SSLProtocol All -SSLv2 -SSLv3
      SSLCipherSuite HIGH:!aNULL:!MD5
    - Reload Apache to apply the changes:
      sudo systemctl reload apache2

Disable Directory Listing:

1. **Modify Apache Configuration**:
    - Open the main Apache configuration file (/etc/apache2/apache2.conf) or specific virtual host config (/etc/apache2/sites-available/your-site.conf).
    - Set Options -Indexes in the relevant directory section:

      <Directory /var/www/html>
      Options -Indexes
      </Directory>
    - Restart Apache to apply:
      sudo systemctl restart apache2

Hide Apache Version Information:

1. **Modify ServerTokens and ServerSignature**:
    - In the Apache config file (/etc/apache2/conf-available/security.conf), change:
      ServerTokens Prod
      ServerSignature Off
    - Reload Apache:
      sudo systemctl reload apache2

Add HSTS Header:

1. **Add Strict Transport Security Headers**:
    - Edit the Apache virtual host configuration file:
      Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains; preload
    - Ensure mod_headers is enabled:
      sudo a2enmod headers
    - Reload Apache:
      sudo systemctl reload apache2

Firewall (203.0.113.3)
Exposed Management Interface:

1. **Restrict Access to the Management Interface**:
    - Log into the firewall's management interface.
    - Find the **Access Control Settings** or **Interface Settings**.
    - Configure access restrictions to allow only trusted internal IP addresses (e.g., 192.168.1.0/24).

2. **Disable HTTP Access**:
    - Disable HTTP access entirely for management and force the use of HTTPS only.

Outdated OpenSSL Version:

1. **Update OpenSSL**:
    - SSH into the firewall if necessary.
    - Update OpenSSL:
      sudo apt-get update
      sudo apt-get install openssl
    - Check the OpenSSL version to confirm it's updated:
      openssl version

Open VPN IKE Port (500):

1. **Apply Access Control Lists (ACLs)**:
    - Navigate to **VPN Settings** on the firewall.
    - Create an ACL to allow VPN connections only from trusted IP addresses.
    - Configure the firewall to deny connections from all other IPs.

Disable ICMP Responses:

1. **Block ICMP on External Interface**:
    - Go to **Firewall Rules** or **Security Settings**.
    - Disable ICMP Echo Requests on the external-facing interface.

2. Highlight External-Facing Risks

Critical External-Facing Vulnerabilities:

- **Exposed Management Interfaces (Router and Firewall)**: Both the router and firewall expose management interfaces over HTTP and HTTPS to the public internet, posing a critical risk of unauthorized access or credential brute force attacks.

- **Path Traversal Vulnerability in Router**: This flaw (CVE-2021-20090) in the router's web interface could allow attackers to gain access to sensitive directories and files, leading to further exploitation.

- **Expired SSL Certificate (Web Server)**: An expired SSL certificate on the web server could allow attackers to intercept HTTPS traffic and perform man-in-the-middle (MITM) attacks, compromising data confidentiality.

Mitigation Strategies:

- **Restrict Management Access**: Ensure that management interfaces for both the router and firewall are only accessible from trusted internal IPs. Disable remote management completely where feasible.

- **Patch and Update**: Apply all firmware and software patches promptly, especially for critical vulnerabilities like CVE-2021-20090 and CVE-2022-23943.

- **Enhance SSL/TLS Security**: Ensure all public-facing web servers have valid SSL certificates and disable weak ciphers and outdated SSL/TLS versions (like SSLv3). Enforce modern TLS protocols (1.2 or 1.3).

- **Harden VPN Access**: Apply strict access control lists (ACLs) for VPN connections, allowing only trusted IP addresses to connect.

- **Disable Unnecessary Services**: Disable ICMP responses, close unnecessary ports, and restrict or disable services like SSH unless explicitly needed, ensuring they are configured securely.

PART 3: 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.

Prepared by: Nsundidi Jorge
Role: Cybersecurity Analyst