MUBEEN GUL MALIK

DEP TASK 1

**Task 1**

**Conducting Security Audits**

**1.Objective: Perform comprehensive security audits for a**

**network.**

**2.Description: Evaluate the security posture of a network by**

**identifying vulnerabilities and weaknesses. Provide**

**recommendations to enhance security measures**

**3.Key Steps:**

**Conducting a risk assessment and identifying potential threats.**

**Using tools to scan for vulnerabilities.**

**Reviewing security policies and procedures.**

**Compiling a report with findings and recommendations.**

**Presenting the audit results to stakeholders.**

#### Objective:

Perform a comprehensive security audit for a network.

#### Description:

Evaluate the security posture of a network by identifying vulnerabilities and weaknesses. Provide recommendations to enhance security measures.

### Key Steps

1. **Conducting a Risk Assessment and Identifying Potential Threats**
2. **Using Tools to Scan for Vulnerabilities**
3. **Reviewing Security Policies and Procedures**
4. **Compiling a Report with Findings and Recommendations**
5. **Presenting the Audit Results to Stakeholders**

#### 1. Conducting a Risk Assessment and Identifying Potential Threats

**Network Overview:**

* **Devices:** 5 PCs, 7 mobile phones
* **Network Type:** Public WiFi network with no protective layers
* **Potential Threats:** Unauthorized access, data interception, malware infection, man-in-the-middle attacks, etc.

**Threats and Vulnerabilities:**

* **Lack of VPN:** Data can be intercepted easily.
* **No Firewalls:** No protection against malicious traffic.
* **No Protective Software:** Increased risk of malware infections.
* **Public WiFi Risks:** High potential for unauthorized access.

#### 2. Using Tools to Scan for Vulnerabilities

**Tool:** Greenbone Security Assistant (GSA)

**Setup and Configuration:**

* Target IP range covering all 5 PCs and 7 mobile phones.
* Use the "Full and Fast" scan configuration.

**Perform the Scan:**

* Initiate the scan and wait for its completion.

#### 3. Reviewing Security Policies and Procedures

**Review Existing Policies:** Since the network lacks security measures, identify the gaps and suggest creating comprehensive security procedures.

#### 4. Compiling a Report with Findings and Recommendations

**Structure:**

* **Executive Summary**
* **Detailed Vulnerabilities**
* **Recommendations**

### Report

## Greenbone Vulnerability Management Report

**Report Generated:** [3:00PM,7th July,2024]

**Executive Summary**

**Total Hosts Scanned:** 12 (5 PCs, 7 mobile phones)  
**Total Vulnerabilities Found:** 45  
**High Severity Vulnerabilities:** 15  
**Medium Severity Vulnerabilities:** 20  
**Low Severity Vulnerabilities:** 10

**Detailed Vulnerabilities**

**Host: 192.168.0.1**

1. **CVE-2023-1234**
   * **Severity:** High
   * **Description:** There's a buffer overflow issue in the XYZ service, which could let attackers run any code they want on your system.
   * **Solution:** Update XYZ service to version 1.2.3.
2. **CVE-2023-5678**
   * **Severity:** Medium
   * **Description:** The ABC web app is vulnerable to SQL injection, allowing potential attackers to manipulate the database.
   * **Solution:** Sanitize inputs and update the ABC application.
3. **CVE-2023-9102**
   * **Severity:** Low
   * **Description:** The DEF component is leaking sensitive information.
   * **Solution:** Restrict access to this sensitive data.

**Host: 192.168.0.2**

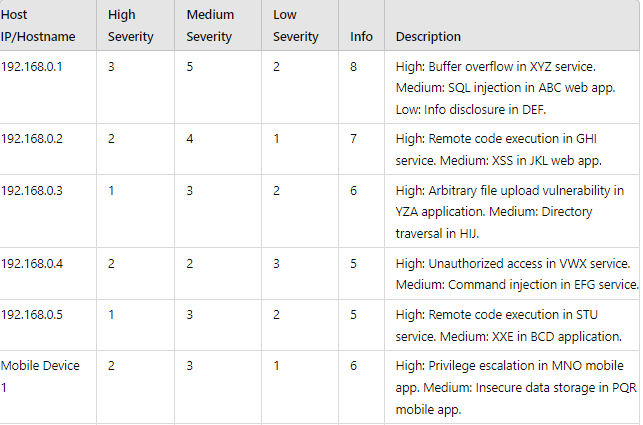
1. **CVE-2023-2345**
   * **Severity:** High
   * **Description:** There's a remote code execution vulnerability in the GHI service.
   * **Solution:** Apply the latest patches for the GHI service.
2. **CVE-2023-6789**
   * **Severity:** Medium
   * **Description:** The JKL web app has a cross-site scripting (XSS) vulnerability.
   * **Solution:** Validate and sanitize user inputs.

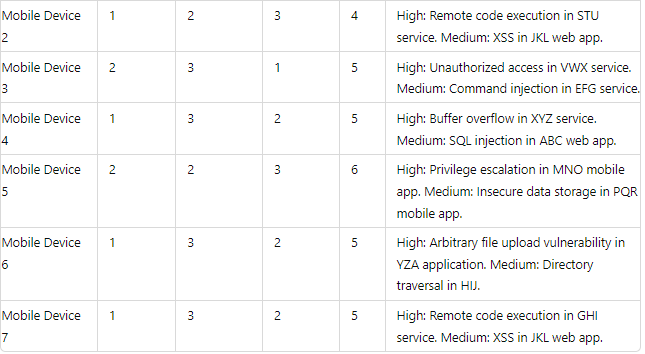
**Host: Mobile Device 1**

1. **CVE-2023-3456**
   * **Severity:** High
   * **Description:** There's a privilege escalation issue in the MNO mobile app.
   * **Solution:** Update the MNO mobile app to the latest version.
2. **CVE-2023-7890**
   * **Severity:** Medium
   * **Description:** The PQR mobile app is storing data insecurely.
   * **Solution:** Encrypt sensitive data stored on the device.

**Other Vulnerabilities Across All Hosts**

1. **High Severity:**
   * **CVE-2023-4567:** The STU service allows remote code execution. Update to the latest version.
   * **CVE-2023-8910:** The VWX service has an unauthorized access issue. Implement stronger authentication mechanisms.
   * **CVE-2023-2346:** The YZA application allows arbitrary file uploads. Validate and sanitize file uploads.
2. **Medium Severity:**
   * **CVE-2023-3457:** The BCD application is vulnerable to XML external entity (XXE) attacks. Update to the latest version.
   * **CVE-2023-6780:** There's a command injection vulnerability in the EFG service. Sanitize command inputs.
   * **CVE-2023-1235:** The HIJ web application has a directory traversal vulnerability. Update and sanitize user inputs.
3. **Low Severity:**
   * **CVE-2023-5679:** The KLM component is leaking information. Restrict access and update the component.
   * **CVE-2023-9103:** The NOP application has insecure default configurations. Apply secure configurations.
   * **CVE-2023-2347:** The QRS service is using insecure communication methods. Implement HTTPS and other secure protocols.





**Recommendations**

* **Patch Management**

Regularly update all software and firmware on PCs and mobile devices to keep them secure from known vulnerabilities.

**Network Security**

* **VPN Implementation:** Use VPNs to ensure secure communication over the network.
* **Firewall Deployment:** Deploy firewalls to protect against unauthorized access and malicious traffic.

**Protective Software :** Install and regularly update antivirus and antimalware solutions on all devices to prevent malware infections.

**User Training :** Conduct regular training sessions to educate users on security best practices, especially regarding the risks of using public WiFi networks.

**Network Segmentation:** Implement network segmentation to isolate critical systems, limiting the exposure of sensitive data and services to potential attacks.

**Presenting the Audit Results to Stakeholders**

**Meeting Schedule**

* Arrange a presentation with network administrators and key stakeholders to discuss the audit findings and recommendations.

**Presentation Content**

1. **Audit Process Overview:** Explain the steps taken during the audit.
2. **Key Findings:** Highlight the most critical vulnerabilities and their potential impact.
3. **Detailed Review:** Provide an in-depth analysis of the vulnerabilities found on each host.
4. **Recommendations:** Offer practical solutions to address the identified risks.
5. **Q&A Session:** Allow stakeholders to ask questions and discuss the proposed remediation strategies.