HOW TO PERFORM A VULNERABILITY ASSESSMENT: STEP BY STEP

BY IZZMIER IZZUDDIN

Example 1: Vulnerability Assessment of a Web Application

1. Scope Definition

- **System:** E-commerce web application
- **Components:** Web server, application server, database server
- **Assessment Tools:** Nmap, OpenVAS, OWASP ZAP, Nessus

2. Data Collection

- **Network Scan:** Using Nmap to identify open ports and services.
- **Vulnerability Scan:** Using OpenVAS and Nessus to find known vulnerabilities.
- **Web Application Scan:** Using OWASP ZAP to test for web application vulnerabilities.

3. Performing the Assessment

Network Scan with Nmap

nmap -sS -p 1-65535 -v -O -sV izzmier.com

Results:

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.4 (protocol 2.0)
80/tcp open http Apache httpd 2.4.29
443/tcp open https Apache httpd 2.4.29
3306/tcp open mysql MySQL 5.7.21

Vulnerability Scan with OpenVAS

Results:

- **CVE-2018-11776:** Apache Struts Remote Code Execution Vulnerability
- **CVE-2017-5638:** Apache Struts Remote Code Execution Vulnerability
- **CVE-2019-5489:** Linux Kernel TCP SACK Panic

Web Application Scan with OWASP ZAP

Results:

- **SQL Injection:** Found in the login form, parameter username
- **Cross-Site Scripting (XSS):** Found in the search functionality
- **Cross-Site Request Forgery (CSRF):** Missing CSRF tokens on critical actions

4. Data Analysis

- **Apache Struts Vulnerabilities (CVE-2018-11776 and CVE-2017-5638):**
    - **Impact:** Remote code execution, potential full system compromise

    - **Fix:** Update Apache Struts to the latest version
- **Linux Kernel TCP SACK Panic (CVE-2019-5489):**
    - **Impact:** Denial of Service
    - **Fix:** Apply patches provided by the Linux distribution
- **SQL Injection:**
    - **Impact:** Unauthorized data access, data modification, potential full system compromise
    - **Fix:** Use prepared statements and parameterized queries
- **Cross-Site Scripting (XSS):**
    - **Impact:** User session hijacking, defacement, and phishing
    - **Fix:** Implement input validation and output encoding
- **Cross-Site Request Forgery (CSRF):**
    - **Impact:** Unauthorized actions performed on behalf of authenticated users
    - **Fix:** Implement CSRF tokens in forms and critical actions

5. Reporting

Executive Summary: The e-commerce web application is exposed to several high-risk vulnerabilities, including remote code execution, SQL injection, and XSS. Immediate actions should be taken to patch the systems and secure the application to prevent potential exploits.

Detailed Report:

- **Vulnerabilities Found:**
    - Apache Struts Remote Code Execution (CVE-2018-11776, CVE-2017-5638)
    - Linux Kernel TCP SACK Panic (CVE-2019-5489)
    - SQL Injection in login form
    - Cross-Site Scripting in search functionality
    - Cross-Site Request Forgery in critical actions
- **Recommendations:**
    - Update and patch Apache Struts
    - Patch the Linux kernel
    - Implement prepared statements for database interactions
    - Validate and sanitize user inputs
    - Implement CSRF protection mechanisms

6. Remediation

- **Patching and Updating:**
    - Update Apache Struts and Linux kernel to the latest versions
- **Code Fixes:**
    - Implement secure coding practices for SQL queries and input handling
- **Configuration Changes:**
    - Harden server configurations to reduce attack surface
- **Monitoring:**
    - Set up continuous monitoring and regular vulnerability scans to detect and address new vulnerabilities promptly

Example 2: Vulnerability Assessment of a Corporate Network

1. Scope Definition

- **System:** Corporate internal network
- **Components:** User workstations, servers, network devices (routers, switches), printers
- **Assessment Tools:** Nmap, Nessus, Wireshark, Metasploit

2. Data Collection

- **Network Mapping:** Using Nmap to identify devices and open ports.
- **Vulnerability Scan:** Using Nessus to find known vulnerabilities.
- **Packet Analysis:** Using Wireshark to analyse network traffic.
- **Penetration Testing:** Using Metasploit for targeted exploits.

3. Performing the Assessment

Network Mapping with Nmap

nmap -sP 192.168.1.0/24

Results:

Nmap scan report for 192.168.1.1
Host is up (0.00023s latency).
MAC Address: 00:0C:29:9D:5C:91 (VMware)

Nmap scan report for 192.168.1.2
Host is up (0.00025s latency).
MAC Address: 00:0C:29:58:12:34 (VMware)

nmap -sS -p 1-65535 192.168.1.1

Results:

PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp open https
3389/tcp open ms-wbt-server

Vulnerability Scan with Nessus

Results:

- **CVE-2019-0708:** Remote Desktop Services Remote Code Execution Vulnerability (BlueKeep)

- **CVE-2017-0144:** SMB Remote Code Execution Vulnerability (EternalBlue)
- **CVE-2020-0796:** SMBv3 Remote Code Execution Vulnerability (SMBGhost)

Packet Analysis with Wireshark

Results:

- Detected plain text transmission of sensitive data (e.g., passwords)
- Excessive broadcast traffic indicating potential network misconfigurations

Penetration Testing with Metasploit

Steps:

```
use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
set RHOST 192.168.1.1
exploit
```

Results:

- Successful exploitation of BlueKeep vulnerability leading to remote code execution on the target machine.

4. Data Analysis

- **BlueKeep Vulnerability (CVE-2019-0708):**
  - **Impact:** Remote code execution, potential full system compromise
  - **Fix:** Apply patches from Microsoft
- **EternalBlue Vulnerability (CVE-2017-0144):**
  - **Impact:** Remote code execution, potential for ransomware attacks
  - **Fix:** Apply patches from Microsoft
- **SMBGhost Vulnerability (CVE-2020-0796):**
  - **Impact:** Remote code execution
  - **Fix:** Apply patches from Microsoft
- **Plain Text Data Transmission:**
  - **Impact:** Data leakage, potential for credential theft
  - **Fix:** Implement encryption protocols (e.g., TLS/SSL) for sensitive data transmission
- **Excessive Broadcast Traffic:**
  - **Impact:** Network congestion, potential for Denial of Service
  - **Fix:** Investigate and reconfigure network devices to minimize unnecessary broadcast traffic

5. Reporting

Executive Summary: The corporate network is exposed to several critical vulnerabilities, including BlueKeep and EternalBlue, which could allow attackers to gain unauthorized access

and control over systems. Immediate action is required to patch these vulnerabilities and secure the network against potential exploits.

Detailed Report:

- **Vulnerabilities Found:**
  - BlueKeep (CVE-2019-0708)
  - EternalBlue (CVE-2017-0144)
  - SMBGhost (CVE-2020-0796)
  - Plain text transmission of sensitive data
  - Excessive broadcast traffic
- **Recommendations:**
  - Apply patches for BlueKeep, EternalBlue, and SMBGhost vulnerabilities
  - Implement encryption for sensitive data transmission
  - Reconfigure network devices to reduce unnecessary broadcast traffic

6. Remediation

- **Patching:**
  - Apply all relevant patches and updates for identified vulnerabilities
- **Encryption:**
  - Implement TLS/SSL for all sensitive data transmissions
- **Network Configuration:**
  - Optimize network configurations to minimize broadcast traffic
- **Monitoring and Continuous Improvement:**
  - Regularly update systems and apply patches
  - Conduct periodic vulnerability assessments and penetration tests
  - Implement continuous network monitoring to detect and respond to threats promptly

Example 3: Vulnerability Assessment of a Healthcare System

1. Scope Definition

- **System:** Hospital's healthcare information system (HIS)
- **Components:** Electronic Health Record (EHR) system, medical devices, patient portals, internal network
- **Assessment Tools:** Nmap, Nessus, OpenVAS, OWASP ZAP, Wireshark

2. Data Collection

- **Network Mapping:** Using Nmap to identify devices and open ports.
- **Vulnerability Scan:** Using Nessus and OpenVAS to find known vulnerabilities.
- **Web Application Scan:** Using OWASP ZAP to test for web application vulnerabilities.
- **Packet Analysis:** Using Wireshark to analyse network traffic.

3. Performing the Assessment

Network Mapping with Nmap

nmap -sP 10.0.0.0/24

Results:

Nmap scan report for 10.0.0.1
Host is up (0.00023s latency).
MAC Address: 00:1A:2B:3C:4D:5E (Cisco Systems)

Nmap scan report for 10.0.0.2
Host is up (0.00025s latency).
MAC Address: 00:1A:2B:3C:4D:5F (Dell)

nmap -sS -p 1-65535 10.0.0.1

Results:

PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
443/tcp open https
3306/tcp open mysql
3389/tcp open ms-wbt-server

Vulnerability Scan with Nessus and OpenVAS

Results:

- **CVE-2019-0708:** Remote Desktop Services Remote Code Execution Vulnerability (BlueKeep)
- **CVE-2020-3452:** Cisco ASA Path Traversal Vulnerability
- **CVE-2020-5902:** F5 BIG-IP Remote Code Execution Vulnerability
- **CVE-2021-26855:** Microsoft Exchange Server Remote Code Execution Vulnerability

Web Application Scan with OWASP ZAP

Results:

- **SQL Injection:** Found in the patient registration form, parameter patientID
- **Cross-Site Scripting (XSS):** Found in the patient portal comments section
- **Insecure Direct Object References (IDOR):** Found in the medical record access functionality

Packet Analysis with Wireshark

Results:

- Detected plain text transmission of patient data
- Detected unencrypted FTP traffic

4. Data Analysis

- **BlueKeep Vulnerability (CVE-2019-0708):**
  - **Impact:** Remote code execution, potential full system compromise
  - **Fix:** Apply patches from Microsoft
- **Cisco ASA Path Traversal Vulnerability (CVE-2020-3452):**
  - **Impact:** Unauthorized access to sensitive files and directories
  - **Fix:** Apply patches from Cisco
- **F5 BIG-IP Vulnerability (CVE-2020-5902):**
  - **Impact:** Remote code execution, full system compromise
  - **Fix:** Apply patches from F5 Networks
- **Microsoft Exchange Server Vulnerability (CVE-2021-26855):**
  - **Impact:** Remote code execution, potential data breach
  - **Fix:** Apply patches from Microsoft
- **SQL Injection:**
  - **Impact:** Unauthorized data access, data modification
  - **Fix:** Use prepared statements and parameterized queries
- **Cross-Site Scripting (XSS):**
  - **Impact:** User session hijacking, defacement, and phishing
  - **Fix:** Implement input validation and output encoding
- **Insecure Direct Object References (IDOR):**
  - **Impact:** Unauthorized access to other users' data
  - **Fix:** Implement proper authorization checks
- **Plain Text Data Transmission:**
  - **Impact:** Data leakage, potential for credential theft

    - **Fix:** Implement encryption protocols (e.g., TLS/SSL) for sensitive data transmission
- **Unencrypted FTP Traffic:**
    - **Impact:** Potential data interception and manipulation
    - **Fix:** Replace FTP with secure alternatives (e.g., SFTP)

5. Reporting

Executive Summary: The hospital's healthcare information system has several critical vulnerabilities, including BlueKeep, Cisco ASA, and F5 BIG-IP remote code execution vulnerabilities, as well as SQL injection and XSS in the web application. These issues pose significant risks to patient data confidentiality and system integrity. Immediate remediation is necessary to protect sensitive health information and ensure system security.

Detailed Report:

- **Vulnerabilities Found:**
    - BlueKeep (CVE-2019-0708)
    - Cisco ASA Path Traversal (CVE-2020-3452)
    - F5 BIG-IP (CVE-2020-5902)
    - Microsoft Exchange Server (CVE-2021-26855)
    - SQL Injection in patient registration form
    - Cross-Site Scripting in patient portal comments section
    - Insecure Direct Object References in medical record access
    - Plain text transmission of patient data
    - Unencrypted FTP traffic
- **Recommendations:**
    - Apply patches for BlueKeep, Cisco ASA, F5 BIG-IP, and Microsoft Exchange vulnerabilities
    - Implement secure coding practices for SQL queries and input handling
    - Implement input validation and output encoding to prevent XSS
    - Ensure proper authorization checks to prevent IDOR
    - Implement encryption for sensitive data transmission
    - Replace FTP with secure alternatives (e.g., SFTP)

6. Remediation

- **Patching:**
    - Apply all relevant patches and updates for identified vulnerabilities
- **Encryption:**
    - Implement TLS/SSL for all sensitive data transmissions
    - Replace FTP with SFTP
- **Code Fixes:**
    - Use prepared statements for database interactions
    - Validate and sanitize user inputs
- **Configuration Changes:**
    - Harden server configurations to reduce attack surface

- **Monitoring and Continuous Improvement:**
  - Regularly update systems and apply patches
  - Conduct periodic vulnerability assessments and penetration tests
  - Implement continuous network monitoring to detect and respond to threats promptly

Example 4: Vulnerability Assessment of a Financial Institution's Online Banking System

1. Scope Definition

- **System:** Online banking system of a financial institution
- **Components:** Web application, database servers, internal network, third-party integrations (APIs)
- **Assessment Tools:** Nmap, Nessus, OWASP ZAP, Burp Suite, Metasploit

2. Data Collection

- **Network Mapping:** Using Nmap to identify devices and open ports.
- **Vulnerability Scan:** Using Nessus to find known vulnerabilities.
- **Web Application Scan:** Using OWASP ZAP and Burp Suite to test for web application vulnerabilities.
- **Penetration Testing:** Using Metasploit for targeted exploits.

3. Performing the Assessment

Network Mapping with Nmap

nmap -sP 192.168.100.0/24

Results:

Nmap scan report for 192.168.100.1
Host is up (0.0012s latency).
MAC Address: 00:1D:7E:BB:3E:A5 (Cisco Systems)

Nmap scan report for 192.168.100.2
Host is up (0.0013s latency).
MAC Address: 00:1A:4D:2E:5A:9F (Dell)

nmap -sS -p 1-65535 192.168.100.1

Results:

PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp open https
3306/tcp open mysql
8080/tcp open http-proxy

Vulnerability Scan with Nessus

Results:

- **CVE-2019-11510:** Pulse Secure VPN Arbitrary File Read Vulnerability
- **CVE-2019-19781:** Citrix ADC Directory Traversal Vulnerability
- **CVE-2020-0601:** Windows CryptoAPI Spoofing Vulnerability
- **CVE-2020-0796:** SMBv3 Remote Code Execution Vulnerability (SMBGhost)

Web Application Scan with OWASP ZAP and Burp Suite

Results:

- **SQL Injection:** Found in the transaction history search form, parameter transactionID
- **Cross-Site Scripting (XSS):** Found in the feedback form
- **Cross-Site Request Forgery (CSRF):** Found in the fund transfer functionality
- **Insecure Direct Object References (IDOR):** Found in account management functions

Penetration Testing with Metasploit

Steps:

use exploit/windows/smb/ms17_010_eternalblue
set RHOST 192.168.100.2
exploit

Results:

- Successful exploitation of EternalBlue vulnerability leading to remote code execution on the target machine.

4. Data Analysis

- **Pulse Secure VPN Vulnerability (CVE-2019-11510):**
  - **Impact:** Arbitrary file read, potential information disclosure
  - **Fix:** Apply patches from Pulse Secure
- **Citrix ADC Vulnerability (CVE-2019-19781):**
  - **Impact:** Directory traversal, remote code execution
  - **Fix:** Apply patches from Citrix
- **Windows CryptoAPI Spoofing Vulnerability (CVE-2020-0601):**
  - **Impact:** Spoofing of cryptographic operations
  - **Fix:** Apply patches from Microsoft
- **SMBGhost Vulnerability (CVE-2020-0796):**
  - **Impact:** Remote code execution
  - **Fix:** Apply patches from Microsoft
- **SQL Injection:**
  - **Impact:** Unauthorized data access, data modification, potential full system compromise
  - **Fix:** Use prepared statements and parameterized queries
- **Cross-Site Scripting (XSS):**
  - **Impact:** User session hijacking, defacement, phishing

    - **Fix:** Implement input validation and output encoding
- **Cross-Site Request Forgery (CSRF):**
    - **Impact:** Unauthorized actions performed on behalf of authenticated users
    - **Fix:** Implement CSRF tokens in forms and critical actions
- **Insecure Direct Object References (IDOR):**
    - **Impact:** Unauthorized access to other users' data
    - **Fix:** Implement proper authorization checks

5. Reporting

Executive Summary: The online banking system has several critical vulnerabilities, including Pulse Secure VPN, Citrix ADC, SMBGhost, and EternalBlue. Additionally, SQL injection, XSS, and CSRF vulnerabilities were identified in the web application. These issues pose significant risks to the security and integrity of the financial institution's systems and data. Immediate remediation is necessary to protect sensitive customer information and ensure system security.

Detailed Report:

- **Vulnerabilities Found:**
    - Pulse Secure VPN Arbitrary File Read (CVE-2019-11510)
    - Citrix ADC Directory Traversal (CVE-2019-19781)
    - Windows CryptoAPI Spoofing (CVE-2020-0601)
    - SMBGhost (CVE-2020-0796)
    - SQL Injection in transaction history search form
    - Cross-Site Scripting in feedback form
    - Cross-Site Request Forgery in fund transfer functionality
    - Insecure Direct Object References in account management functions
- **Recommendations:**
    - Apply patches for Pulse Secure VPN, Citrix ADC, and Windows CryptoAPI vulnerabilities
    - Implement secure coding practices for SQL queries and input handling
    - Implement input validation and output encoding to prevent XSS
    - Ensure proper authorization checks to prevent IDOR
    - Implement encryption for sensitive data transmission
    - Replace unencrypted protocols with secure alternatives (e.g., SFTP)

6. Remediation

- **Patching:**
    - Apply all relevant patches and updates for identified vulnerabilities
- **Encryption:**
    - Implement TLS/SSL for all sensitive data transmissions
    - Replace FTP with SFTP
- **Code Fixes:**
    - Use prepared statements for database interactions
    - Validate and sanitize user inputs

- **Configuration Changes:**
  - Harden server configurations to reduce attack surface
- **Monitoring and Continuous Improvement:**
  - Regularly update systems and apply patches
  - Conduct periodic vulnerability assessments and penetration tests
  - Implement continuous network monitoring to detect and respond to threats promptly