PERFORM A VULNERABILITY ASSESSMENT OF A SAMPLE WEB APPLICATION

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):

o Impact: Remote code execution, potential full system compromise

o Fix: Update Apache Struts to the latest version

• Linux Kernel TCP SACK Panic (CVE-2019-5489):

o Impact: Denial of Service

o Fix: Apply patches provided by the Linux distribution

• SQL Injection : -

o Impact: Unauthorized data access, data modification, potential full system compromise

o Fix: Use prepared statements and parameterized queries

• Cross-Site Scripting (XSS) :-

o Impact: User session hijacking, defacement, and phishing

o Fix: Implement input validation and output encoding

• Cross-Site Request Forgery (CSRF) :-

o Impact: Unauthorized actions performed on behalf of authenticated users

o 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 :-

o Apache Struts Remote Code Execution (CVE-2018-11776, CVE-2017-5638)

o Linux Kernel TCP SACK Panic (CVE-2019-5489)

o SQL Injection in login form

o Cross-Site Scripting in search functionality

o Cross-Site Request Forgery in critical actions

• Recommendations :-

o Update and patch Apache Struts

o Patch the Linux kernel

o Implement prepared statements for database interactions

o Validate and sanitize user inputs

o Implement CSRF protection mechanisms

6. Remediation :-

• Patching and Updating:

o Update Apache Struts and Linux kernel to the latest versions

• Code Fixes:

o Implement secure coding practices for SQL queries and input handling

• Configuration Changes:

o Harden server configurations to reduce attack surface

• Monitoring:

o Set up continuous monitoring and regular vulnerability scans to detect and address new vulnerabilities promptly

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):

o Impact: Arbitrary file read, potential information disclosure

o Fix: Apply patches from Pulse Secure

• Citrix ADC Vulnerability (CVE-2019-19781):

o Impact: Directory traversal, remote code execution

o Fix: Apply patches from Citrix

• Windows CryptoAPI Spoofing Vulnerability (CVE-2020-0601):

o Impact: Spoofing of cryptographic operations

o Fix: Apply patches from Microsoft

• SMBGhost Vulnerability (CVE-2020-0796):

o Impact: Remote code execution

o Fix: Apply patches from Microsoft

• SQL Injection:

o Impact: Unauthorized data access, data modification, potential full system compromise

o 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)

o SMBGhost (CVE-2020-0796)

o SQL Injection in transaction history search form

o Cross-Site Scripting in feedback form

o Cross-Site Request Forgery in fund transfer functionality

o Insecure Direct Object References in account management functions

• Recommendations:

o Apply patches for Pulse Secure VPN, Citrix ADC, and Windows CryptoAPI vulnerabilities

o Implement secure coding practices for SQL queries and input handling

o Implement input validation and output encoding to prevent XSS

o Ensure proper authorization checks to prevent IDOR

o Implement encryption for sensitive data transmission

o Replace unencrypted protocols with secure alternatives (e.g., SFTP)

6. Remediation

• **Patching:**

o Apply all relevant patches and updates for identified vulnerabilities

• Encryption:

o Implement TLS/SSL for all sensitive data transmissions

o Replace FTP with SFTP

• Code Fixes:

o Use prepared statements for database interactions

o Validate and sanitize user inputs

• Configuration Changes:

o Harden server configurations to reduce attack surface

• Monitoring and Continuous Improvement:

o Regularly update systems and apply patches

o Conduct periodic vulnerability assessments and penetration tests

o Implement continuous network monitoring to detect and respond to threats promptly