****

**Course: CYB302**

 **Ethical Hacking
(Canadian Context)**

 **Lab 5: Interpreting Vulnerability Scans and
Penetration Testing Plan Development**

**Coordinator and Instructor:**

 **Muhamma Saleem**

**Student Name: Olushola Enoch Bayode**

**Student ID: 23077087**

**Section: 3rd Semester**

**Activity 1: Analyzing a CVSS Vector**

The Common Vulnerability Scoring System (CVSS) vector comprises of various components that explains the seriousness and how exploitable a vulnerability is. Here is the breakdown of the CVSS vectors for both vulnerabilities.

**SSL Certificate Cannot Be Trusted**

* **CVSS v3.0 Vector:** CVSS:3.0/AV: N/AC: L/PR:N/UI:N/S:U/C:L/I:L/A:N
	+ **AV (Attack Vector: Network - N):** Over the network attack.
	+ **AC (Attack Complexity: Low - L):** The attack does not require special conditions.
	+ **PR (Privileges Required: None - N):** No authentication or privileges exploitation needed.
	+ **UI (User Interaction: None - N):** No need for user interaction for the attack to be carried out.
	+ **S (Scope: Unchanged - U):** The impact remains within the same security scope.
	+ **C (Confidentiality Impact: Low - L):** Some information could be disclosed.
	+ **I (Integrity Impact: Low - L):** There is a minor impact on data integrity.
	+ **A (Availability Impact: None - N):** No impact on availability.
* **CVSS v3.0 Base Score:** **6.5** (Medium)

**Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key**

* **CVSS v3.0 Vector:** CVSS:3.0/AV: N/AC: L/PR:N/UI:N/S:U/C:L/I:N/A:N
	+ **AV (Attack Vector: Network - N):** The attack can be remotely carried out.
	+ **AC (Attack Complexity: Low - L):** No special conditions are required to exploit this.
	+ **PR (Privileges Required: None - N):** Authentication is not required.
	+ **UI (User Interaction: None - N):** User interaction not needed.
	+ **S (Scope: Unchanged - U):** The impact is within confined the vulnerable component.
	+ **C (Confidentiality Impact: Low - L):** Some information such like PSK may be exposed.
	+ **I (Integrity Impact: None - N):** No impact on data integrity.
	+ **A (Availability Impact: None - N):** It has no effect on system availability.
* **CVSS v3.0 Base Score:** **5.3** (Severity is Medium)

In conclusion the IKE Aggressive Mode issue is of concern, as it could allow an attacker to brute-force VPN pre-shared keys, possibly leading to unpermitted network access.

**Activity 2: Developing a Penetration Testing Plan**

Penetration Testing Plan for MCDS, LLC

1. Introduction

It is a plan for the web server of MCDS, LLC to be penetrated and tested for vulnerabilities in penetration testing. The test will be carried out on ethical grounds and would only be carried out with special permission from the organization.

2. Vulnerabilities Found

Vulnerability 1: [Identify vulnerability, e.g., SQL Injection]

•Describe: The web application does not properly validate user input and is therefore exposed to SQL injection attacks.

•Effect: Attacker can obtain sensitive information, manipulate the database, or gain administrative priviledge.

•Exploitation Plan:

\*Scan SQL injection vectors using automated tools like sqlmap. \*\*

\*Manually carry out SQL injections by specially designed payloads e.g. "0 or "1"".

\*Steal the user credentials and the privilege escalation if possible.

Vulnerability 2: [Identify vulnerability, e.g., Cross-Site Scripting (XSS)]

• Description: The web server does not validate user input within form fields, and it causes stored and reflected XSS attacks.

• Effect: Session cookies of the users are stolen by the attackers, and they are able to deface web sites or deliver bad payloads.

• Exploitation Plan:

embed malicious JavaScript into input fields.

Analyze payload execution using Burp Suite.

Steal session tokens and obtain privilege escalation.

3. Information Gathering

To define the scope of penetration testing, following steps of reconnaissance will be followed:

3.1. Domain and Network Foot printing

• Identify MCDS-held domain names through performing WHOIS lookup.

• Identify public service IP ranges by using network scanning with tools like Nmap and Shodan or kismet.

3.2. Harvesting Email
• Utilize theHarvester (or e-mail addresses found at social medias and company website) to fetch public email addresses and other information when necessary.
• Overtake employees' name from the MCDS's’ website along with the social networking links of the employees.

3.3. Physical and Organizational Reconnaissance
• Track the real office directions of MCDS on Google Maps and company directories.
•After analyzing the organizational structure and roster page at LinkedIn, a job search engine, and other career sites, you can research the organizational chart and the employee list of the company.

3.4. Document Metadata Analysis
• Use ExifTool to scrape public document metadata (e.g., PDFs, DOCX), and thus make metadata available that are publicly accessible in RTF, DOC, PDF, DOCX, ODT, and similar file formats.
• Gather personal data related to users like used usernames, software versions, and the content that is hidden (steganography, etc.), XF data, etc.

3.5. Tech Stack Identification
• Get technology details by using Wappalyzer and WhatWeb servers scripts on web pages.
• Check previously identified vulnerability by looking for software in-betweens and common vulnerabilities.

3.6. Remote Access and Social Engineering Analysis
• Check if MCDS has VPN or remote access for its employees.
• Identify social engineering to the point of demonstrating that it can foster a security issue, like a phishing attack and then disclose the event and resources and/or services found.

4. Testing Methodology

1. Reconnaissance: Acquire information about MCDS infrastructure through different methods.
2. Scanning: The process decreases the risk of security breaches through ports and services accordingly.
3. Exploitation: The company must consider ethical ways before trying to exploit a weakness.
4. Post-Exploitation: Facilitate opportunities for privilege

**Part2**

**Penetration Testing Plan for MCDS, LLC Web Server Vulnerabilities**

* This plan analyzes the three vulnerabilities that have been acknowledged in MCDS web server, determines their relative importance, and provides some exploitation strategies.
1. Web Server HTTP Header Internal IP Disclosure
Severity: Low
CVSS Base Score: 2.6
Assessment & Significance:
• Showing internal IP address is an opportunity for attackers to gather relevant identification data.
• This on its own is not a common threat but it can be used in concert with other vulnerabilities.
• An attacker may employ the internal IP to avoid security controls such as firewall rules that prevent access to the outside world.
Exploitation Approach:
• Through HTTP requests, an attacker may ask for a server to tell if it has leaked internal IP with the information.
• Extracting of the internal addresses through HTTP headers (e.g., Location, Via, Received).
• Use the internal IP to detect the lateral movement, recognize internal resources, or bypass some security measures.
Potential Outcomes:
• Making a tree showing the internal network structure.
• Finding misconfigured services will not be a problem.
• Additional attacks such as server-side request forgery (SSRF) or privilege escalation.

2. CGI Generic SQL Injection (Blind, Time-Based)
Severity: High
CVSS Base Score: 7.5
Assessment & Significance:
• It is a very threatening vulnerability because the attacker can play with the backend database directly.
• Through the method of successful SQL injection, an attacker may steal data, go around authentication, and remotely control the system.
• Cluttered SQL Injections are the one kinds of bugs in a web application, that are hard to distinguish but still grant the possibility to get a grip over the whole database. Exploitation Approach:• Use of SQL code for generating wait time by SLEEP() function or WAITFOR DELAY.

* Example payload: ' OR IF(1=1, SLEEP(5), 0) --
* Automate exploitation using tools like **sqlmap**:
* sqlmap -u "http://target-site.com/page.php?id=1" --dbs --time-sec=5
* Extract **database names, tables, usernames, and passwords**.
* If successful, attempt **privilege escalation** or **command execution**.

**Potential Outcomes:**

* Access to **delicate user data** (usernames, passwords, financial data).
* Ability to **alter or erase database records**.
* Potential access to **admin accounts** and **more system compromise**.

**3. SSLv3 POODLE Vulnerability**

**Severity:** Medium
**CVSS Base Score:** 4.3

**Assessment & Significance:**

* POODLE (Padding Oracle on Downgraded Legacy Encryption) exploits SSLv3 flaws to perform **man-in-the-middle (MITM) attacks**.
* Attackers can decipher SSL-encrypted traffic by exploiting **Cipher Block Chaining mode vulnerabilities**.
* The impact is **significant for outdated systems** that still support SSLv3.

**Exploitation Approach:**

* **Force a downgrade attack** to SSLv3 using MITM techniques.
* Capture encrypted traffic and attempt **byte-by-byte decryption** using a padding oracle attack.
* Use tools like **SSLScan** or **Nmap** to check SSLv3 support:
* Nmap --script ssl-poodle -p 443 target-site.com
* When successful, pull-out **unencrypted session cookies or credentials**.

**Potential Outcomes:**

* Session hijacking (stealing login tokens or cookies).
* Deciphering of sensitive HTTPS communications.
* Further MITM exploitation leading to data manipulation or injection attacks.

**Conclusion & Prioritization of Exploits:**

1. SQL Injection (High Priority) – Provides direct access to the database.
2. POODLE (Medium Priority) – If SSLv3 is enabled, attempt MITM attack to decode traffic.
3. Internal IP Disclosure (Low Priority) – Uses reconnaissance data to support other attacks.