Experiment 2: Vulnerability Scanning & Assessment

Scenario:

After mapping the network, you've discovered a web server and a file-sharing server.

Management wants a vulnerability assessment of these targets to identify known weaknesses

before attackers can exploit them.

Tasks:

- Use OpenVAS to perform a comprehensive vulnerability scan on a Linux-based server (Metasploitable 2).
- Run Nikto against the web application (e.g., DVWA) to find outdated server software, dangerous file uploads, or default credentials.
- Assess the severity and relevance of each discovered vulnerability.

Deliverable:

A vulnerability assessment report with CVE references and risk ratings.

TASK 1

INTRODUCTION TO NIKTO

Nikto is a free, open-source web server vulnerability scanner widely used in penetration testing and vulnerability assessments. It helps identify misconfigurations and security issues in web applications by scanning for outdated server software, dangerous files or scripts, default credentials, misused HTTP methods, and missing security headers. Nikto also detects known vulnerabilities, some of which are mapped to public CVEs (Common Vulnerabilities and Exposures), making it a powerful tool for quick reconnaissance and reporting. It is especially useful for testing vulnerable environments like DVWA (Damn Vulnerable Web Application).

Steps to Use Nikto:

Step 1: Run the Nikto Scan

Command:

nikto -h http://< metasploitable_IP >/dvwa/

Where:

- nikto → Starts the Nikto vulnerability scanner
- -h → Sets the target host (IP address or URL)

Step 2: Wait for the Scan to Complete

Step 3: Review the Output

- Check for warnings in the results (e.g., outdated software, exposed files).
- Look for CVE numbers to identify specific vulnerabilities.
- Focus on high-risk issues, like outdated software or dangerous settings.
- Find suggested fixes (e.g., update software, disable unsafe methods).

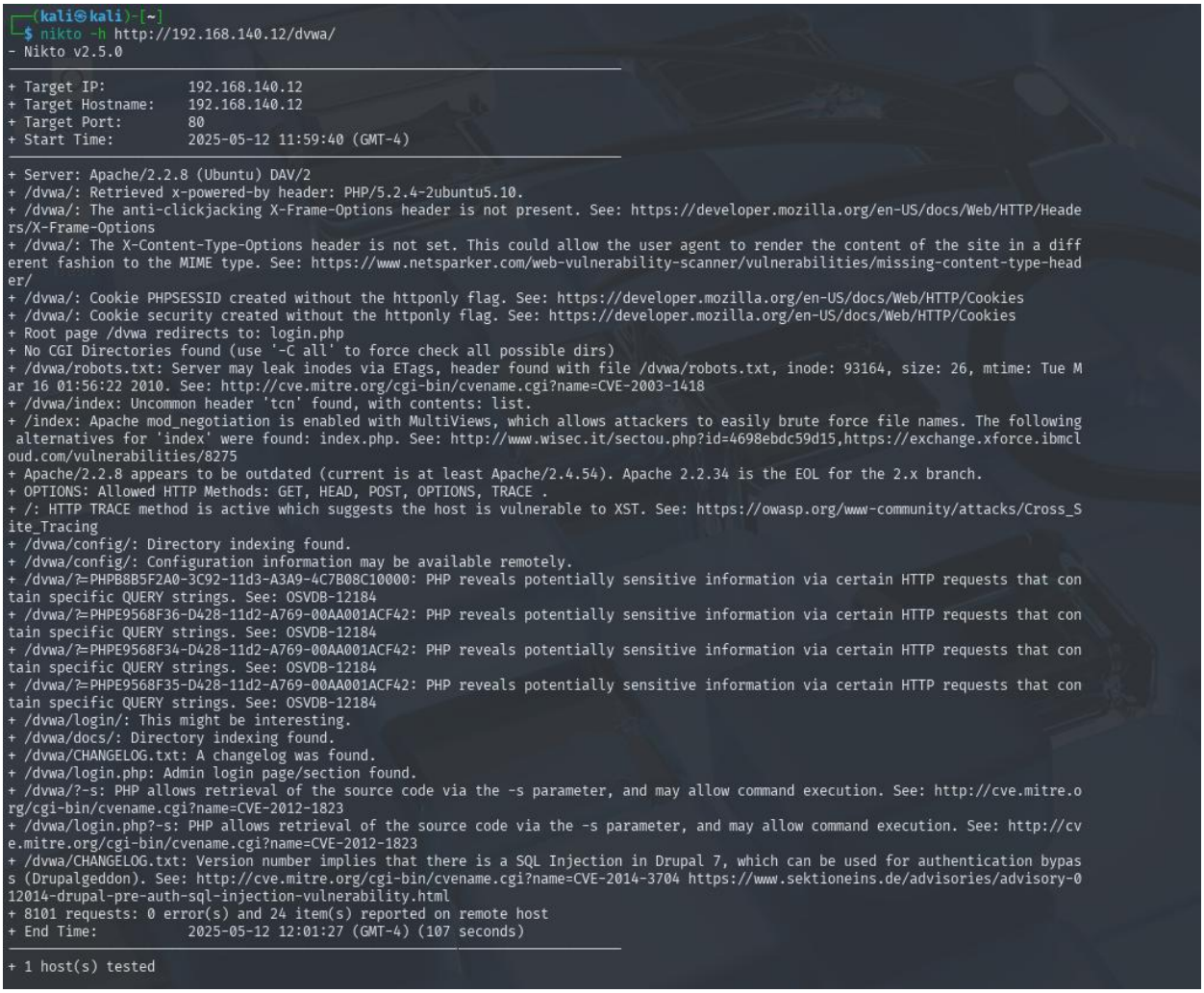
Step 4: Analyze CVEs for More Details

1. Find CVE IDs in the Nikto output (e.g., CVE-2003-1418).
2. Go to these websites:
    - CVE.org – Basic info
    - NVD.nist.gov – More details
3. Search the CVE number on both sites.
4. Read the info:
    - What is the problem?
    - Which software is affected?
    - How risky it is?
5. Check if a fix is available (like update or patch).
6. Decide how to fix it (e.g., update, change settings, or disable unsafe options).

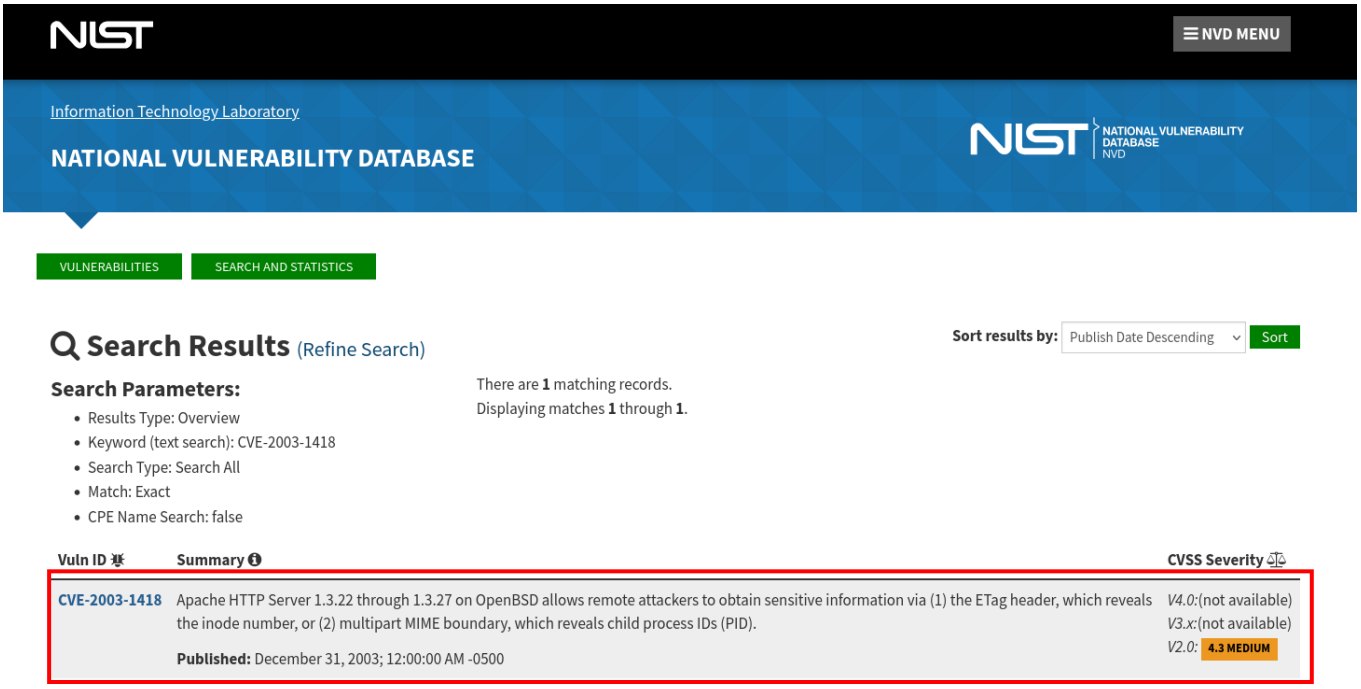
– Created with passion

Output:

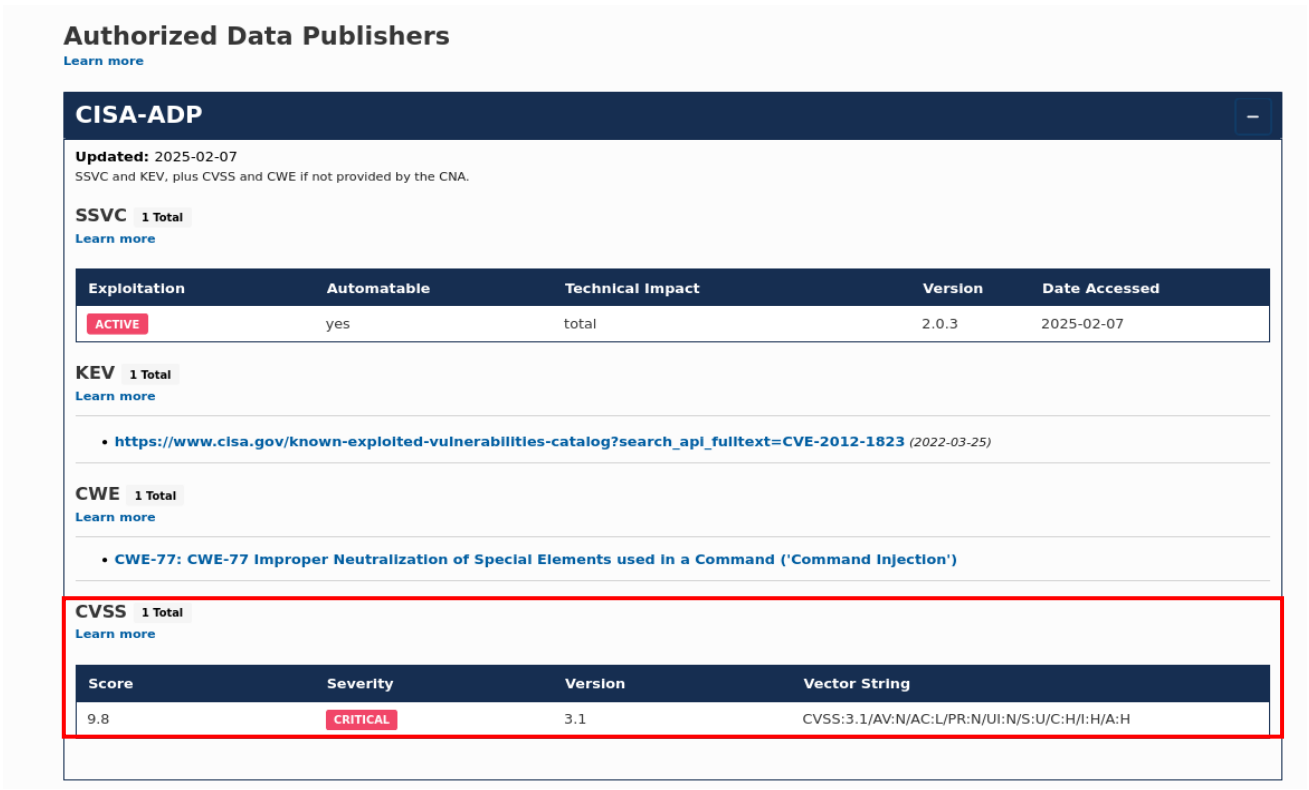
Nikto Scan Output



CVE Details for CVE-2003-1418



CVE Details for CVE-2012-1823



– Created with passion

TASK 2

INTRODUCTION TO OPENVAS

OpenVAS (Open Vulnerability Assessment Scanner) is a free and open-source tool used to scan systems and networks for security vulnerabilities. It is part of the Greenbone Vulnerability Management (GVM) framework. OpenVAS works by checking a target system against a large database of known security issues, called Network Vulnerability Tests (NVTs). It helps security professionals and students find weaknesses such as outdated software, misconfigurations, and potential exploits. OpenVAS is commonly used to scan machines like Metasploitable 2 in lab environments to practice identifying and fixing vulnerabilities in a safe way.

Step 1: Install OpenVAS (GVM)

sudo apt install gvm

Step 2: Set up OpenVAS

sudo gvm-setup

Step 3: Check Installation

sudo gvm-check-setup

Step 4: Start OpenVAS Services

sudo gvm-start

Step 5: Login to the Web Interface

https://localhost:9392

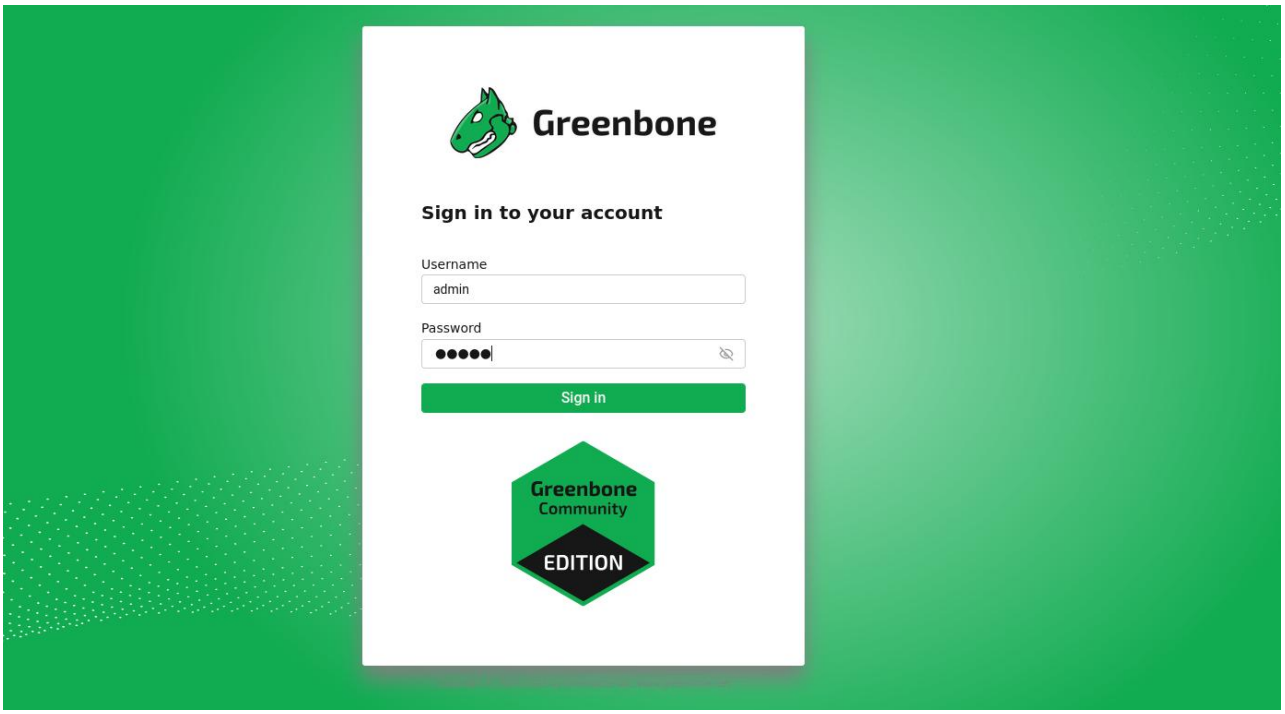
Username: admin
Password: shown during gvm-setup

– Created with passion

Optional: Reset Password (if forgotten)

sudo gvmd --user=admin --new-password=YourNewPassword

Output



Vulnerability Assessment Report

1. Outdated Server Software – It detects Apache 2.2.8, which is obsolete and has known vulnerabilities.
2. Missing Security Headers – e.g., X-Frame-Options, X-Content-Type-Options.
3. Information Disclosure – /phpinfo.php reveals sensitive server configuration.
4. HTTP Methods – Finds that TRACE is enabled, which can be used for XST attacks.
5. Directory Browsing Enabled – /doc/ directory is accessible and potentially exposes files.
6. Apache Features Like mod_negotiation – Can be used for brute-forcing file names.
7. Identifies Potential CVEs – e.g., CVE-1999-0678 related to HTTP response issues.

In short: Nikto is identifying misconfigurations, outdated software, and insecure settings that an attacker could exploit.

CVE ID	Description	Risk Rating
CVE-2003-1418	A flaw in old PHP versions that can cause the server to behave unexpectedly.	4.3 (Medium, CVSS 2.0)
CVE-2012-1823	A serious bug in PHP-CGI that lets attackers run code on the server remotely.	9.8 (Critical, CVSS 3.x) 7.5 (High, CVSS 2.0)
Outdated Apache Server	Apache/2.2.8 is end-of-life and has multiple known exploits.	High
Outdated PHP Version	PHP 5.2.4 is no longer supported; contains numerous vulnerabilities.	High
Missing X-Frame-Options Header	Allows clickjacking attacks	Medium
Missing X-Content-Type-Options Header	May lead to MIME sniffing attacks.	Medium
HTTP TRACE Method Enabled	Could be exploited for Cross-Site Tracing (XST).	High

– Created with passion

Conclusion

In this experiment, we used Nikto, a web vulnerability scanner, to assess the security of the DVWA web application. Nikto helped us find issues like outdated software, exposed files, and other common web vulnerabilities. Each finding was linked to known security problems (CVEs), and we reviewed their risk levels to understand how serious they were. In addition, we used OpenVAS, a powerful system vulnerability scanner, to perform a deeper analysis of the Metasploitable 2 virtual machine. OpenVAS identified system-level vulnerabilities that go beyond web issues, such as outdated services and insecure configurations. Based on both Nikto and OpenVAS results, we recommended important fixes like updating software, securing configurations, and disabling risky features to enhance the overall security of the system.

****

– Created with passion