

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- Run Nikto against the web application (e.g., DVWA) to find outdated server software, dangerous file uploads, or default credentials.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 It helps identify misconfigurations and security issues in web applications by scanning for outdated server software, dangerous files or scripts, default credentials, misused HTTP methods, and missing security headers.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- Check for warnings in the results (e.g., outdated software, exposed files).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- Focus on high-risk issues, like outdated software or dangerous settings.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).

Output:

Nikto Scan Output

```
(kali㉿kali)-[~]
$ nikto -h http://192.168.140.12/dvwa/
- Nikto v2.5.0

+ Target IP:          192.168.140.12
+ Target Hostname:    192.168.140.12
+ Target Port:        80
+ Start Time:         2025-05-12 11:59:40 (GMT-4)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /dvwa/: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /dvwa/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /dvwa/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /dvwa/: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /dvwa/: Cookie security created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Root page /dwa redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /dvwa/robots.txt: Server may leak inodes via ETags, header found with file /dvwa/robots.txt, inode: 93164, size: 26, mtime: Tue Mar 16 01:56:22 2010. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /dvwa/index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /dvwa/config/: Directory indexing found.
+ /dvwa/config/: Configuration information may be available remotely.
+ /dvwa/?=PHPB8B5F2A0-3C92-1103-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /dvwa/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /dvwa/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /dvwa/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /dwa/login/: This might be interesting.
+ /dwa/docs/: Directory indexing found.
+ /dwa/CHANGELOG.txt: A changelog was found.
+ /dwa/login.php: Admin login page/section found.
+ /dwa/?-s: PHP allows retrieval of the source code via the -s parameter, and may allow command execution. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1823
+ /dwa/login.php?-s: PHP allows retrieval of the source code via the -s parameter, and may allow command execution. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1823
+ /dwa/CHANGELOG.txt: Version number implies that there is a SQL Injection in Drupal 7, which can be used for authentication bypass (Drupalgeddon). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3704 https://www.sektion eins.de/advisories/advisory-012014-drupal-pre-auth-sql-injection-vulnerability.html
+ 8101 requests: 0 error(s) and 24 item(s) reported on remote host
+ End Time:           2025-05-12 12:01:27 (GMT-4) (107 seconds)

+ 1 host(s) tested
```

CVE Details for CVE-2003-1418

NIST
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES SEARCH AND STATISTICS

Q Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): CVE-2003-1418
- Search Type: Search All
- Match: Exact
- CPE Name Search: false

There are 1 matching records.
Displaying matches 1 through 1.

Vuln ID	Summary	CVSS Severity
CVE-2003-1418	Apache HTTP Server 1.3.22 through 1.3.27 on OpenBSD allows remote attackers to obtain sensitive information via (1) the ETag header, which reveals the inode number, or (2) multipart MIME boundary, which reveals child process IDs (PID).	V4.0:(not available) V3.x:(not available) V2.0: 4.3 MEDIUM

Published: December 31, 2003; 12:00:00 AM -0500

CVE Details for CVE-2012-1823

Authorized Data Publishers
[Learn more](#)

CISA-ADP

Updated: 2025-02-07
SSVC and KEV, plus CVSS and CWE if not provided by the CNA.

SSVC 1 Total
[Learn more](#)

Exploitation	Automatable	Technical Impact	Version	Date Accessed
ACTIVE	yes	total	2.0.3	2025-02-07

KEV 1 Total
[Learn more](#)

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2012-1823 (2022-03-25)

CWE 1 Total
[Learn more](#)

- [CWE-77: CWE-77 Improper Neutralization of Special Elements used in a Command \('Command Injection'\)](#)

CVSS 1 Total
[Learn more](#)

Score	Severity	Version	Vector String
9.8	CRITICAL	3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

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>

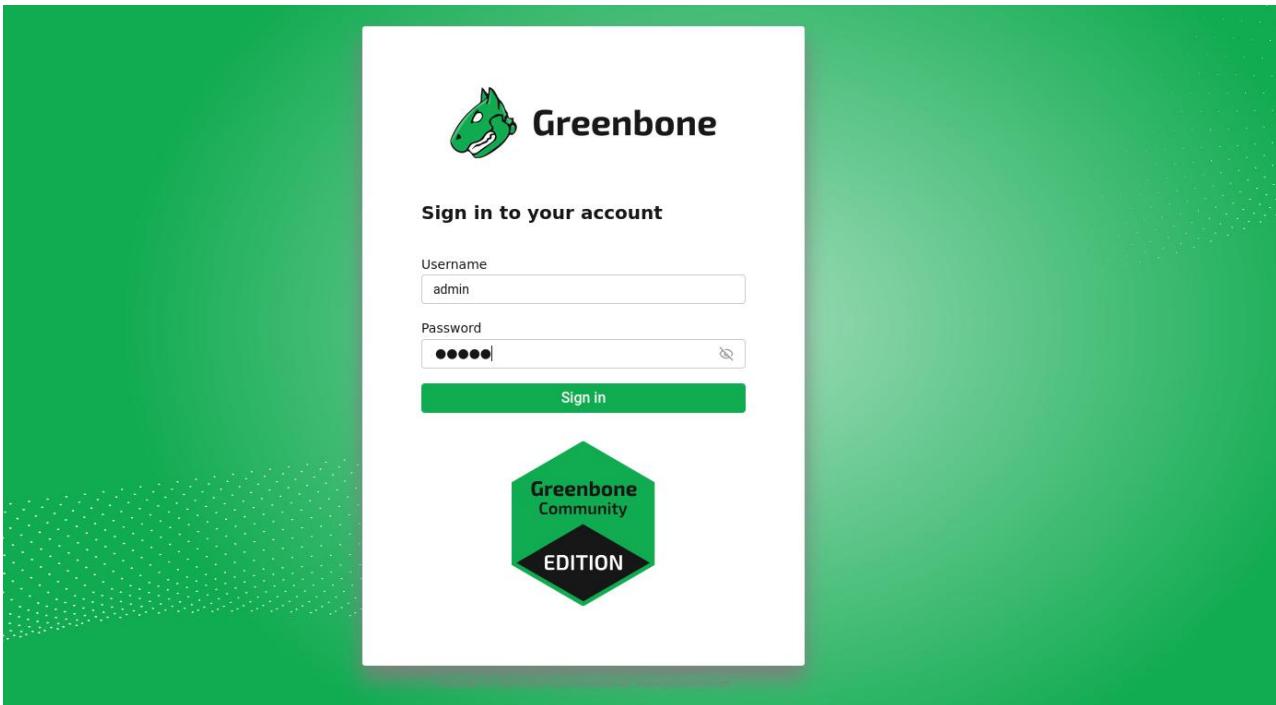
Username: admin

Password: shown during gvm-setup

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

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.
