

Vulnerability Security Assessment Report

Introduction

This report documents the practical tasks performed to understand and apply foundational security assessment principles. The objective was to gain hands-on experience in Vulnerability Assessment and Penetration Testing (VAPT) methodology, risk assessment, and compliance alignment using open-source tools. The activities included setting up a test lab with Kali Linux and Metasploitable 2, conducting vulnerability scans with OpenVAS and Nikto, performing a basic risk assessment using the CVSS framework, and documenting findings in a structured report.

Main Content

Setting Up the Testing Environment

Overview

A controlled lab environment was established to safely conduct security assessments without affecting production systems. This involved installing an attacker machine (Kali Linux) and a target machine (Metasploitable 2).

Procedure

- ✓ **Kali Linux:** Installed as the primary penetration testing platform.
- ✓ **Metasploitable 2:** Downloaded and built from GitHub to serve as an intentionally vulnerable virtual machine.



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)



- ✓ **VirtualBox:** Configured to host both VMs, ensuring they were on the same NAT network for communication.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:a8:4f:5d
          inet addr:192.168.178.129 Bcast:192.168.178.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea8:4f5d/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:40 errors:0 dropped:0 overruns:0 frame:0
             TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:4465 (4.3 KB) TX bytes:6868 (6.7 KB)
             Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
             UP LOOPBACK RUNNING MTU:16436 Metric:1
             RX packets:91 errors:0 dropped:0 overruns:0 frame:0
             TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ msfadmin
```

Vulnerability Scanning with OpenVAS and Nikto

Overview

Vulnerability scanning was performed to identify known security weaknesses in the target system (Metasploitable 3). OpenVAS was used for a comprehensive network scan, while Nikto focused on web application vulnerabilities.

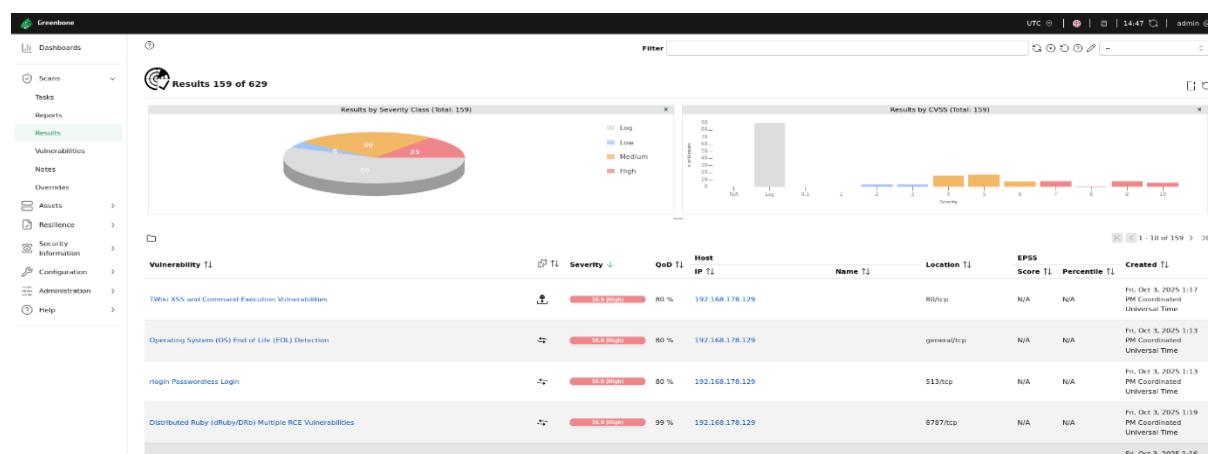
Procedure

- ✓ **OpenVAS Scan:**
 - Started the OpenVAS service: sudo gvm-start
 - Accessed the Greenbone web interface at https://127.0.0.1:9392
 - Configured and launched a full and fast scan against the Metasploitable 3 IP address.
- ✓ **Nikto Scan:**
 - Executed a basic web vulnerability scan: nikto -h http://<target_ip>



Results

- ✓ **OpenVAS:** Identified multiple vulnerabilities, including:
 - Outdated software (e.g., Apache Tomcat, OpenSSH)
 - Weak configurations and default credentials
 - CVSS scores ranged from 5.0 (Medium) to 10.0 (Critical)



Report: Fri, Oct 3, 2025 12:52 PM Coordinated Universal Time										
Information	Results (159 of 629)	Hosts (21 of 21)	Ports (209 of 221)	Applications (209 of 201)	Operating Systems (12 of 21)	CVEs (159 of 240)	Closed CVEs (0 of 0)	TLS Certificates (12 of 21)	Error Messages (0 of 0)	User Tags (0)
CVE TI	NVT TI									
CVE-2008-5304 CVE-2008-5305	TWSI XSS and Command Execution Vulnerabilities									
CVE-1999-0618	The reexec service is running									
CVE-2001-0045 CVE-2002-1809 CVE-2004-1532 CVE-2004-2357 CVE-2006-1451 CVE-2007-2554 CVE-2007-6001 CVE-2009-0919	MySQL / MariaDB Default Credentials (MySQL Protocol)									
CVE-2014-3419 CVE-2015-4669 CVE-2016-6511 CVE-2018-15719 CVE-2024-22801	Apache Tomcat AJP RCE Vulnerability (Ghostcat) - Active Check									
CVE-2020-1938	PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check									
CVE-2012-1823 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335	vfdtpd Compromised Source Packages: Baseline Vulnerability									
CVE-2011-2523	(DotCC) RCE Vulnerability (CVE-2104-2697)									
CVE-2004-2687	Unauthenticated Authentication Spoofing Vulnerability									
CVE-2016-7144	Unauthenticated Backend									
CVE-2010-2075	The rlogin service is running									
CVE-1999-0651	rsh Unencrypted Cleartext Login									
CVE-1999-0651										



- ✓ **Nikto:** Highlighted web-specific issues such as:

- Outdated server versions
- Potentially risky HTTP methods (e.g., PUT, DELETE)

```
[kali㉿kali:~]
└─$ nikto -h 192.168.178.129 -o output.txt
- Nikto v2.5.0

+ Target IP:          192.168.178.129
+ Target Hostname:    192.168.178.129
+ Target Port:        80
+ Start Time:         2025-10-03 12:29:53 (GMT-4)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved X-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ //: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ //: 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/
+ Apache/2.2.8 appears to be outdated (current version at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ Indexing: Enabled. For more information see: http://www.wisec.it/indexing.html
+ //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.ibmcloud.com/vulnerabilities/8275
+ //: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ //: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /index: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPE8B85F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/Changelog: phpMyAdmin leak inodes via ETags, header found with file /phpMyAdmin/Changelog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2003, url: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/Changelog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-icongreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/Documentation: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ #wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2025-10-03 12:30:32 (GMT-4) (39 seconds)

+ 1 host(s) tested
```

Documenting Findings

Overview

- ✓ Findings from the vulnerability scans were systematically recorded for analysis and reporting. This process transforms raw scan data into an actionable, prioritized list of security issues.

Procedure

- ✓ **Tool Used:** A structured table was created to log all findings. For this example, the data is presented below in a tabular format, replicating what would be created in **Google Sheets** or **Microsoft Excel**.
- ✓ **Data Points Recorded:**
- IP Address and Hostname
 - Open Ports and Services (from Nmap scans)
 - Vulnerability Description
 - CVE ID (if available)
 - CVSS Score
 - Risk Level (High/Medium/Low)

- ✓ **Evidence:** Screenshots of critical tool outputs, such as the Nmap scan results, were taken to serve as evidence.

Results

A structured vulnerability log was created, enabling clear tracking and prioritization of issues. The log highlights the most severe vulnerabilities discovered on the target system 192.168.178.129

Vulnerability Log (Critical & High Severity Findings)

IP Address	Hostname	Port/Service	Vulnerability Description	CVE ID	CVSS Score	Risk Level
192.168.178.129	-	80/tcp (Apache)	TWiki is prone to Cross-Site Scripting (XSS) and Command Execution vulnerabilities due to improper input sanitization.	CVE-2008-5304, CVE-2008-5305	10.0	Critical
192.168.178.129	-	6200/tcp	Backdoor shell port activated by the compromised vsftpd service.	CVE-2011-2523	9.8	Critical
192.168.178.129	-	3306/tcp (MySQL)	MySQL allows login as user 'root' with an empty password using default credentials.	Multiple	9.8	Critical
192.168.178.129	-	5900/tcp (VNC)	VNC server authentication bypassed with the weak password 'password'.	-	9.0	High



Risk Assessment Using CVSS and Risk Matrix

Overview

A basic risk assessment was conducted to prioritize the identified vulnerabilities based on their severity and potential impact.

Procedure

- ✓ **CVSS Scoring:** Used the NVD CVSS Calculator to calculate or verify scores for key vulnerabilities.
- ✓ **Risk Matrix:** Created a 3x3 matrix (Likelihood vs. Impact) in a spreadsheet to categorize risks as High, Medium, or Low.

Results

- ✓ **High Risk:** Vulnerabilities with CVSS scores ≥ 7.0 (e.g., remote code execution flaws).
- ✓ **Medium Risk:** Scores between 4.0 - 6.9 (e.g., information disclosure).
- ✓ **Low Risk:** Scores < 4.0 (e.g., low-impact configuration issues).

①

CVSSv2 Base Score Calculator

From Metrics:

Access Vector	Local
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity	None
Availability	None

From Vector:

Vector	AV:L/AC:L/Au:N/C:N/I:N
--------	------------------------

Results:

CVSS Base Vector	AV:L/AC:L/Au:N/C:N/I:N/A:N
Severity	6.0 (Log)

CVSSv3 Base Score Calculator

From Metrics:

Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

From Vector:

CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
------------------	--

Results:

CVSS Base Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Severity	9.8 (High)

CVSSv4 Score Calculator

From Metrics:

Base Metrics

Exploitability Metrics

Attack Vector (AV)	Network (N)
Attack Complexity (AC)	Low (L)
Attack Requirements (AT)	None (N)
Privileges Required (PR)	None (N)
User Interaction (UI)	None (N)

Vulnerable System Impact Metrics

Confidentiality Impact (VI)	None (N)
Integrity Impact (VI)	None (N)
Availability Impact (VA)	None (N)

Subsequent System Impact Metrics

Confidentiality Impact (SC)	None (N)
Integrity Impact (SI)	None (N)
Availability Impact (SA)	None (N)

Conclusion

This exercise provided practical exposure to the core components of a security assessment:

- ✓ **Vulnerability Scanning** with OpenVAS and Nikto highlighted the importance of identifying and cataloging security weaknesses.
- ✓ **Risk Assessment** using CVSS and a risk matrix demonstrated how to prioritize remediation efforts effectively.
- ✓ **Documentation and Reporting** reinforced the need for clear, structured communication of technical findings to support decision-making.

These activities collectively build essential skills for performing security assessments and contributing to organizational security posture. Future work could include deeper penetration testing with Metasploit, automated reporting scripts, and compliance checks against specific standards like CIS Benchmarks.

References

- ✓ OpenVAS (Greenbone) Documentation: <https://www.greenbone.net>
- ✓ Nmap Reference Guide: <https://nmap.org/book/man.html>
- ✓ OWASP Top 10: <https://owasp.org/www-project-top-ten/>
- ✓ NVD CVSS Calculator: <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>
- ✓ Metasploitable 2 GitHub: <https://github.com/rapid7/metasploitable3>
- ✓ OWASP ZAP: <https://www.zaproxy.org>
- ✓ Dradis CE: <https://dradisframework.com/ce/>
- ✓ Pentest-Tools Report Templates: <https://pentest-tools.com>