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).

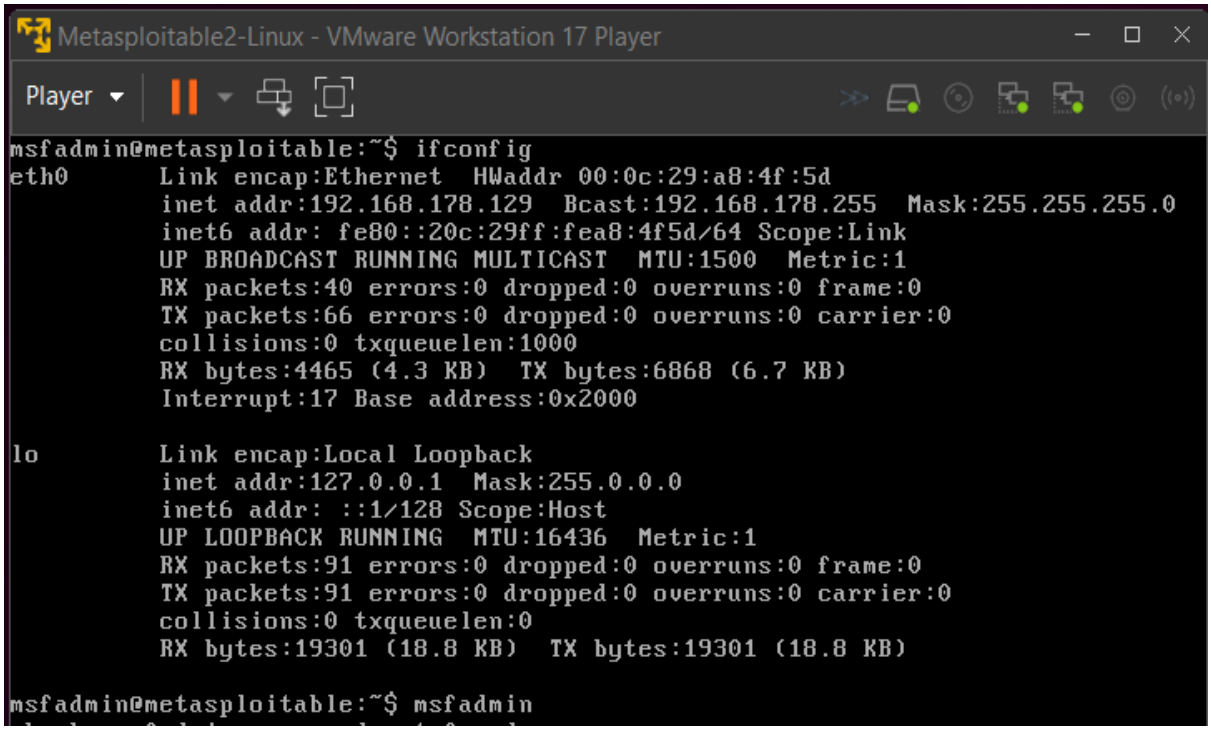
Procedure

- ✓ **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.



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.

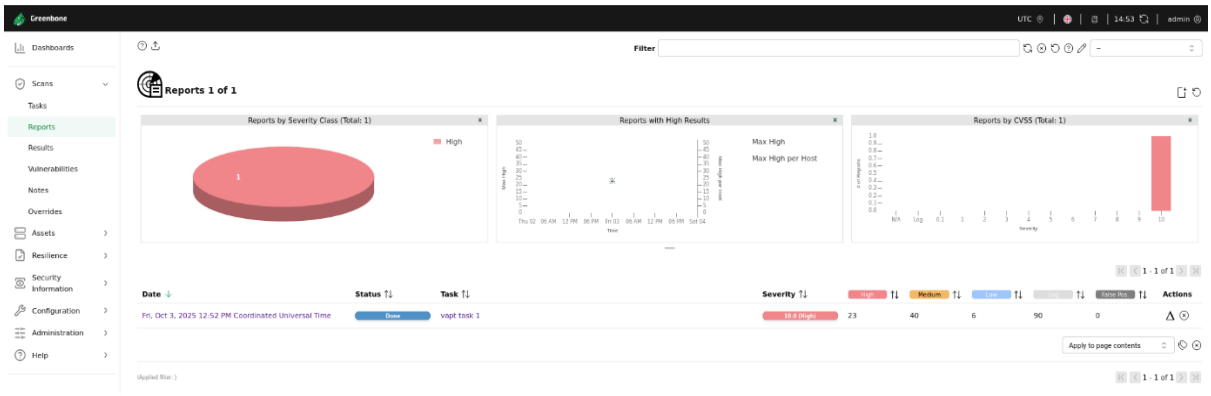
Procedure

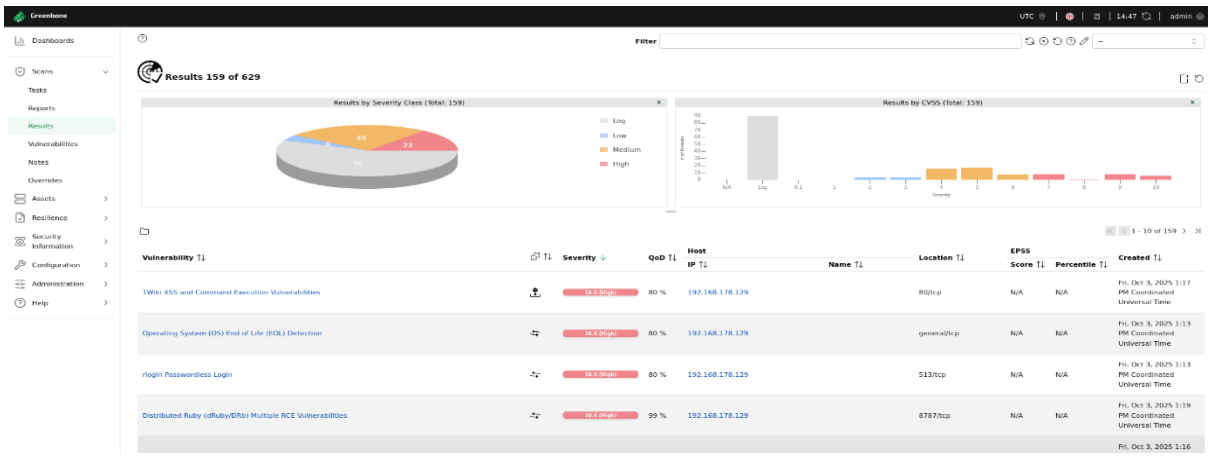
- ✓ **OpenVAS Scan**:
  - Started the OpenVAS service: sudo gvm-start
  - Accessed the Greenbone web interface at https://127.0.0.1:9392
  - Configured and launched a full and fast scan against the Metasploitable 3 IP address.
- ✓ **Nikto Scan**:
  - Executed a basic web vulnerability scan: nikto -h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

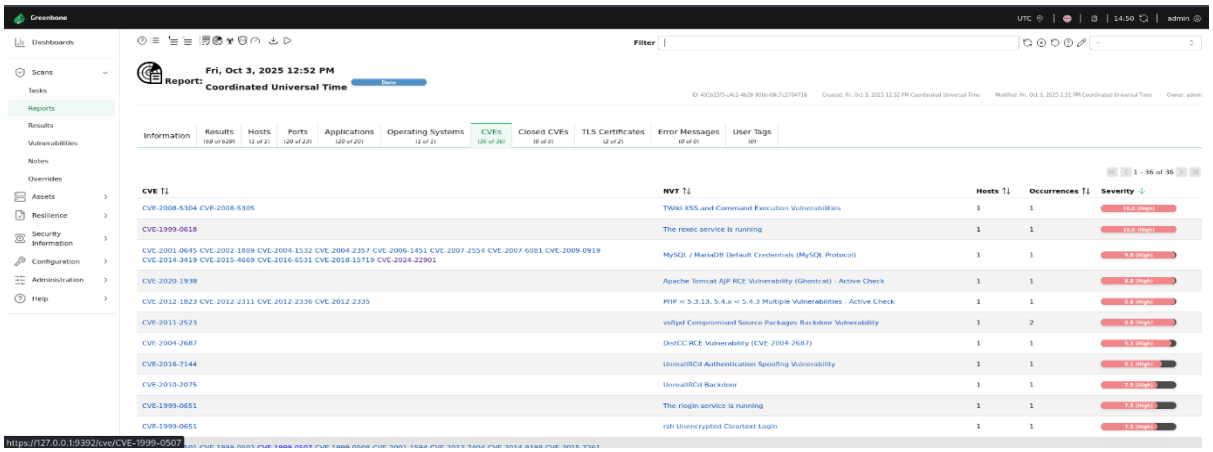
Results

✓ **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)







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

- Outdated server versions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

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

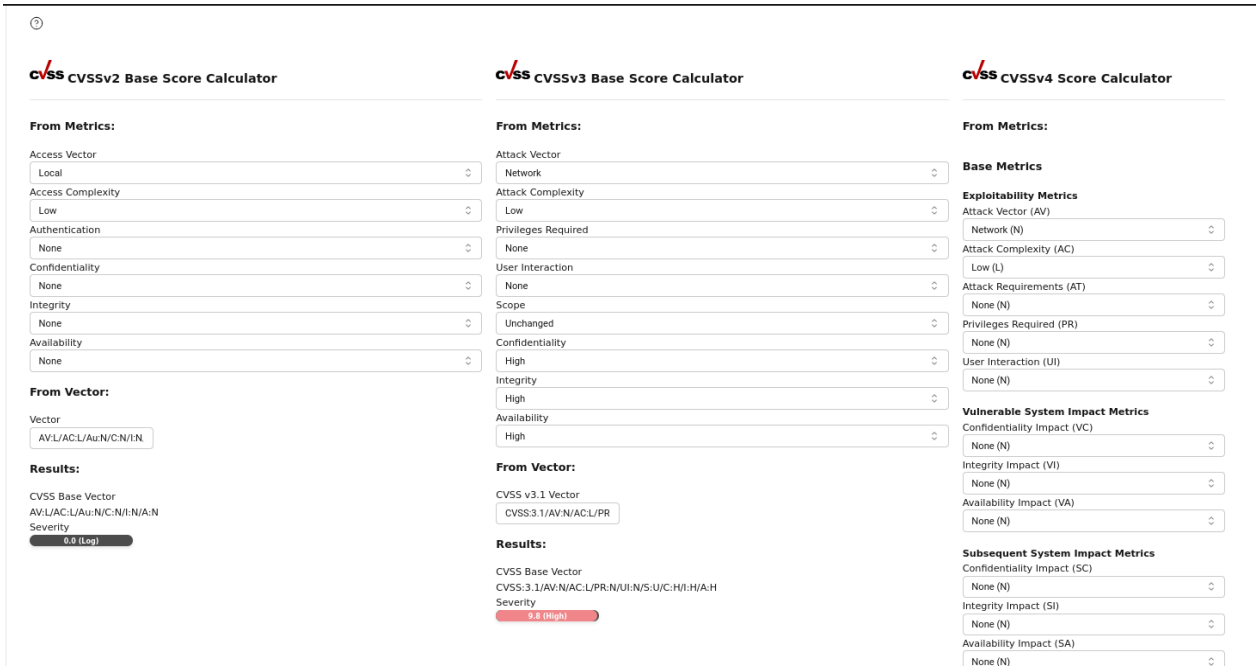
A basic risk assessment was conducted to prioritize the identified vulnerabilities based on their severity and potential impact.

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).



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