Cyber Security Internship Report

Task 15: Vulnerability Assessment & Risk Prioritization

Name: Mohammed Nihal
Environment: Kali Linux (VirtualBox) on Windows 11 Host
Tool Attempted: OpenVAS (Greenbone Vulnerability Manager)

Objective

The objective of this task was to perform a vulnerability assessment on a target system using OpenVAS, analyze identified vulnerabilities, map them to CVE and CVSS scores, classify risks, and prioritize remediation steps.

Tool Overview: OpenVAS (GVM)

OpenVAS (Greenbone Vulnerability Manager) is an open-source vulnerability scanning solution used to detect security weaknesses in systems and networks. It utilizes vulnerability feeds that include NVTs (Network Vulnerability Tests), SCAP data, and CERT advisories.

OpenVAS Installation & Setup Attempt

- Installed GVM using: sudo apt install gvm -y
- Executed initial setup using: sudo gvm-setup
- Attempted feed synchronization using: sudo greenbone-feed-sync
- Started services using: sudo gvm-start
- Attempted to create scan target (127.0.0.1)

Issue Encountered: Feed Synchronization Failure

During setup, the vulnerability feed synchronization failed due to a DNS resolution error inside the Kali Linux virtual machine. The error message indicated 'Temporary failure in name resolution' when attempting to connect to feed.community.greenbone.net.

Observed Error:
rsync: getaddrinfo: feed.community.greenbone.net:873: Temporary failure in name resolution

Root Cause Analysis

Network testing revealed that the Kali Linux VM was unable to reach external hosts. Ping tests resulted in 'Destination Host Unreachable' with 100% packet loss. This indicates a VirtualBox network configuration issue preventing internet connectivity. Because OpenVAS relies on external vulnerability feeds, the setup could not complete successfully.

Impact of the Issue

- SCAP data was not downloaded.
- CERT vulnerability data was not synchronized.
- Default port lists were not created.
- Unable to create scan targets.
- Vulnerability scan could not be executed.

Vulnerability Risk Prioritization Methodology

Although the scan could not be completed, vulnerability risk prioritization methodology was studied and documented.

CVSS Score	Severity Level	Priority
9.0 – 10.0	Critical	Priority 1 (Immediate Fix)
7.0 – 8.9	High	Priority 2
4.0 – 6.9	Medium	Priority 3
0.1 – 3.9	Low	Priority 4

Key Concepts Reviewed

- Vulnerability Assessment: Process of identifying and evaluating security weaknesses.
- CVE: Unique identifier for publicly disclosed vulnerabilities.
- CVSS: Standard scoring system (0–10) measuring vulnerability severity.
- VA vs Penetration Testing: VA identifies weaknesses; penetration testing exploits them.

Conclusion

The OpenVAS vulnerability assessment setup was initiated but could not be completed due to a VirtualBox network configuration issue that prevented feed synchronization. Despite the technical limitation, the vulnerability assessment workflow, risk classification methodology, and CVE/CVSS prioritization framework were thoroughly studied and documented. This task provided practical understanding of vulnerability management processes and real-world troubleshooting in security tool deployment.