CYBER SECURITY INTERNSHIP

Task 15

VULNERABILITY ASSESSMENT & RISK PRIORITIZATION

JASHMI KS

A Vulnerability Assessment was conducted on an Ubuntu operating system running inside Oracle VM VirtualBox using OpenVAS.
The purpose of this assessment was to identify security weaknesses in the system, evaluate their severity using CVE and CVSS scoring systems, prioritize risks based on their impact, and recommend appropriate remediation measures.
The scan results were categorized into Critical, High, Medium, and Low severity levels according to CVSS scoring standards.

Objectives

The main objectives of this vulnerability assessment are:
• To identify security weaknesses in the target system
• To analyze detected vulnerabilities using CVE identifiers
• To evaluate severity using CVSS scoring
• To classify risks based on impact and exploitability
• To prioritize vulnerabilities based on risk level
• To recommend appropriate remediation steps

Scope of Assessment

• **Target System:** Ubuntu Virtual Machine
• **Platform:** Oracle VM VirtualBox
• **Scan Type:** Full and Fast Scan
• **Assessment Type:** Network-based Vulnerability Scan
The assessment was limited to the virtual machine environment and did not extend to external production systems.

Methodology

The vulnerability assessment was performed using the following structured approach:

1. Installation and configuration of OpenVAS
2. Definition of target system and IP address
3. Configuration of scan settings
4. Execution of vulnerability scan
5. Review and analysis of scan results
6. Mapping vulnerabilities to CVE identifiers
7. Evaluating severity using CVSS scores
8. Risk classification and prioritization
9. Recommendation of remediation measures

This systematic approach ensures accurate identification and effective prioritization of vulnerabilities.

Installation & Setup

Step 1: Updating the System

The Ubuntu system was updated to ensure all existing packages were current.

Commands used:

```
sudo apt update

sudo apt upgrade -y
```

Step 2: Installing OpenVAS

OpenVAS was installed using the package manager.

```
sudo apt install openvas -y
```

Step 3: Configuring OpenVAS

The setup process initializes the vulnerability database and generates administrator credentials.

```
sudo gvm-setup
```

This step downloads vulnerability feeds and configures necessary services.

Step 4: Starting OpenVAS Services

The OpenVAS services were started using:

```
sudo gvm-start
```

The web interface is accessible at:
https://127.0.0.1:9392

Target Configuration

The target system was configured using the following steps:

1. Navigated to Configuration → Targets
2. Created a new target
3. Entered the IP address of the Ubuntu VM
4. Saved the configuration

Scan Configuration

A scan task was created with appropriate settings:

1. Navigated to Scans → Tasks
2. Created a new task
3. Selected “Full and Fast” scan profile
4. Selected the created target
5. Started the scan

8. Scan Results & Findings

After scan completion, vulnerabilities were identified and categorized into:

• Critical
• High
• Medium
• Low

Each identified vulnerability included:
• CVE ID
• CVSS Score
• Description of the vulnerability
• Potential impact on the system

CVE & CVSS Explanation

CVE (Common Vulnerabilities and Exposures)
CVE is a standardized identifier assigned to publicly known security vulnerabilities.
Each vulnerability is assigned a unique CVE number for reference and tracking.

CVSS (Common Vulnerability Scoring System)

CVSS is a scoring system ranging from 0 to 10 that indicates the severity of a vulnerability.

CVSS Score	Severity Level
0.1 – 3.9	Low
4.0 – 6.9	Medium
7.0 – 8.9	High
9.0 – 10	Critical

Higher CVSS scores indicate greater risk and urgency.

Risk Classification

Vulnerabilities were classified based on:
• Exploitability of the vulnerability
• Impact on Confidentiality
• Impact on Integrity
• Impact on Availability
• Exposure level of the system
Critical and High vulnerabilities were given higher priority due to their potential to cause severe system compromise.

Risk Priority List

Priority	Vulnerability	CVE	CVSS	Severity	Recommended Action
1	Remote Code Execution	CVE-XXXX	9.8	Critical	Apply patch immediately
2	Weak SSL Configuration	CVE-XXXX	8.2	High	Reconfigure SSL settings
3	Outdated Software	CVE-XXXX	6.5	Medium	Update software packages
4	Information Disclosure	CVE-XXXX	3.2	Low	Monitor and restrict access