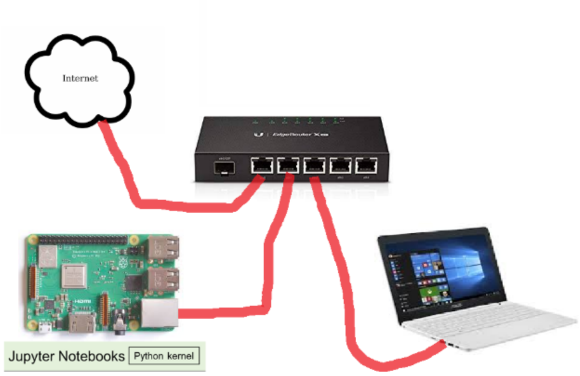
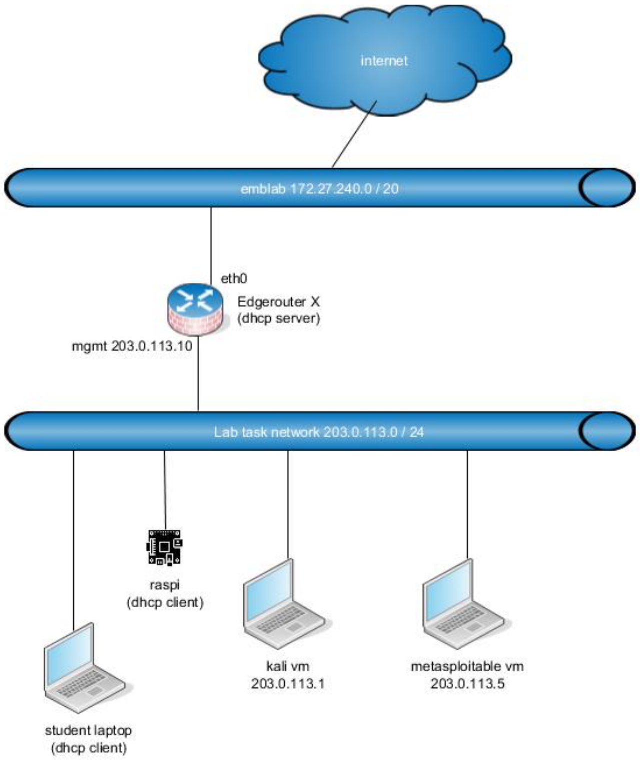
ms





# Lab – Use OpenVAS for Vulnerability Assessment

## Addressing Table

| Device | IP Address | Subnet Mask |
|---|---|---|
| Kali | 203.0.113.xx | 255.255.255.0 |
| Metasploitable | 203.0.113.xx | 255.255.255.0 |

## Objectives

**Part 1: Exploring OpenVAS**

**Part 2: Configuring a Vulnerability Scan**

**Part 3: Reviewing the Results**

## Background / Scenario

Open Vulnerability Assessment System (OpenVAS) is a framework that provides services and tools for vulnerability scanning and management. Network Vulnerability Tests (NVT) are used by OpenVAS to checking existing security issues. NVTs are developed based on Common Vulnerabilities and Exposures (CVE).

CVE is a category of known security threats. The threats are divided into two categories: vulnerabilities and exposures. The entries provide an identification number, a description, and public references regarding the cybersecurity vulnerabilities. The goal of the CVE is to allow the sharing of data easier across different vulnerability tools, repositories, and services. A CVE is associated with a Common Vulnerability Scoring System (CVSS).

The CVSS provides an open and standardized way for scoring. The scoring system allows an organization to prioritize which vulnerabilities to fix and access the impact of the vulnerabilities on their systems.

In this lab, you will use OpenVAS to perform a vulnerability scan on the Metasploitable VM and review the vulnerability assessment report from the scan.

## Required Resources

□ Host computer with at least 4 GB of RAM and 15 GB of free disk space

□ Oracle VirtualBox

□ IoT Security Kali and Metasploitable VMs

# Part 1: Installing OpenVAS

a. Install openvas

```
└─$ sudo apt install openvas
```

b. Current openvas setup requires that Postgresql-16 is served on local port 5432. On kali linux, version 15 is served on that port and version 16 on port 5433. You need to exchange these two ports in configs (scroll down in each file until you find port, edit, save changed file with ctrl-s and exit with ctrl-x)

```
└─$ sudo nano /etc/postgresql/15/main/postgresql.conf
```

and

```
└─$ sudo nano /etc/postgresql/16/main/postgresql.conf
```

and then restart postgresql

```
└─$ sudo service postgresql restart
```

c. Install vulnerability databases (this will take quite long time... an hour or so)

```
└─$ sudo gvm-setup
```

d. Check the setup

```
└─$ sudo gvm-check-setup
```

# Part 2: Exploring OpenVAS

a. Start Metasploitable and Kali VMs.

b. Log into Metasploitable VM.

username: **msfadmin**

password: **msfadmin**

c. Enter the command **ifconfig** at the prompt to determine the IP address of Metasploitable VM.

What is the IP address? 203.0.113.47

d. Log into IoTSec Kali VM.

e. Open a terminal in IoTSec Kali VM and ping Metasploitable VM to verify connectivity. If it is not successful, verify that both the Metasploitable and Kali VMs are using the same VM network.

f. In a terminal, enter the command **openvas-start** to start OpenVAS service.

```
└─$ openvas-start
[*] Please wait for the OpenVAS services to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392
<some output omitted.>
```

g. In a terminal, enter the command **more lab_support_files/openvas_info** to view the content in the file **openvas-info** for the username and password info to access OpenVAS in the web browser.

```
└─$ more lab_support_files/openvas_info
User: admin
Pass: b0b22778-f1d5-459f-8320-4c47bad49942

Greenbone Web Interface:
https://127.0.0.1:9392
or
https://localhost:9392
```

h. After you have logged into OpenVAS, notice that the Dashboard provides with Information regarding the tasks, CVEs, hosts topology and NVTs at a glance.

How many total CVEs are loaded into OpenVAS? 230045

How many total NVT are loaded into OpenVAS? 133243

You can also click the different parts of the graphs to review the CVE or NVT details.

Now you are ready to start a vulnerability scan.

## Part 3: Configuring a Vulnerability Scan

### Step 1: Create the target.

In this step, you will configure Metasploitable VM as the target of your vulnerability scan.

a. Click **Configuration** -> **Targets**.

b. Click the white star in the blue box icon in the upper left-hand corner below the Dashboard menu.

c. When the New Target dialog box appears, enter the following information:

Name: **Metasploitable VM**

Manual: **203.0.113.5**

Alive Test: **Consider Alive**.

d. Click **Create**.

### Step 2: Create a task.

In this step, you will configure a task to perform a vulnerability scan on Metasploitable VM.

a. Click **Scans** -> **Tasks**.

b. You will see a welcome page if this is the first visit to the Tasks page.

c. Click the white star in the blue box icon in the upper left-hand corner below the Dashboard menu. Select **New Task**.

d. Name it **Metasploitable**. Verify **Metasploitable VM** is selected in the Scan Targets field. Click **Create** to a new task. Leave the other settings as is.

e. The new **Metasploitable** is listed in the Tasks list. Click the **Start** button under the Actions menu associated with Task1.

f. The status for Metasploitable has been changed to Requested.

g. Verify that the web page will be refreshed automatically in the dropdown menu in the green banner at the top of the page. Choose the desired refresh rate in the dropdown menu.

## Part 4: Reviewing the Results

While the scanning toward Metasploitable VM continues, you can review reports that have been previously generated. The entire scan toward Metasploitable VM will take about 40 minutes to finish.

a. Click **Scans** > **Results** to review previously generated reports.

b. Review the list of vulnerability. Report the findings in the results for the different level of severity.

c.

**Severity: Low**

What is the IP address and port number on the host? 203.0.113.47 on port 25.

What is the vulnerability and its impact?

R: This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack. Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

What is the provided solution?

R: - Remove support for 'DHE_EXPORT' cipher suites from the service

- If running OpenSSL update to version 1.0.2b or 1.0.1n or later.

**Severity: Low**

What is the IP address and port number on the host? 203.0.113.47 (general/icmp).

What is the vulnerability and its impact?

R: The remote host responded to an ICMP timestamp request. This information could theoretically be used to exploit weak time-based random number generators in other services.

What is the provided solution?

R: Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely

- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Severity: Medium**

What is the IP address and port number on the host? 203.0.113.47 on port 80.

What is the vulnerability and its impact?

R: TWiki is prone to CSRF vulnerability. Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.

What is the provided solution?

R: Upgrade to TWiki version 4.3.2 or later.

**Severity: High**

What is the IP address and port number on the host? 203.0.113.47 on port 2121.

What is the vulnerability and its impact?

R: It was possible to login into the remote FTP server using weak/known credentials. This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

What is the provided solution?

R: Changing the passwords as soon as possible.