# Cyber 262 Lab: GROUP Lab - OpenVAS Scan-Patch-Verify

# Tasks

1. **Perform a vulnerability scan of the Metasploitable Machine**
2. **Exploit and Patch Vulnerability**
3. **Challenge and Analysis**

# Group Work and What to Submit

**This is a group lab** and while each team member should run through the lab on their own we only need one official report submitted. There are some questions that require a response from each team member and they are indicated in this report. All other questions, mainly screen shots only require one screen shot from the team. This is a detailed lab with several deliverables so to keep students on track the instructor may request that "drafts" are submitted prior to the final deadline.

# Introduction

In this lab we will be conducting a vulnerability scan of the Metasploitable VM in Practice Labs. Metasploitable is an intentionally vulnerable server image produced to practice penetration testing and security research. Due to the severe vulnerabilities of this machine, it is crucial to keep it hidden from the public internet. This means that vulnerabilities must be fixed on the machine without updating services.

To scan the Metasploitable machine, we will use the OpenVAS Scanner tool. The **Open V**ulnerability **A**ssessment **S**canner is an ‘all-in-one’ vulnerability scanning tool used by many organizations and community members. OpenVAS is distributed by ‘Greenbone Networks’ who also design the Web UI used to start scans and create dashboards to visualize present threats on a network. The free to use ‘Greenbone Community Edition’ (GCE) comes pre-installed on most Kali Linux distributions under the Vulnerability Analysis application folder.

OpenVAS stays up to date with current vulnerabilities with near daily updates called NVT Feeds (Network Vulnerability Tests). NVT’s use large databases of know vulnerabilities, such as CVEs, which help to detect vulnerabilities on single machines or whole enterprise networks.

For more information and reference to some OpenVAS commands:

<https://tools.kali.org/vulnerability-analysis/openvas>

# Deliverables for Lab Reports

Refer to the assignment directions in Canvas for reporting requirements. The directions below will indicate when a Screen Shot or Question Response/Analysis is to be provided by the student for the report.

Do not use this document as your Lab report, create a new document based on the Canvas assignment directions.

# Learning Objectives

The Learning Objectives for this Lab align with the course objectives for this lesson in Canvas.

# Lab Topology

For this lab we will utilize the following PLAB Server;

**Metasploitable** (Victim) 192.168.0.6

**PLABKALI** (Attacker) 192.168.0.4

To access the required systems please open one of the practice lab assignments on the left side which will give you access to the servers.

# Task 1 – Perform OpenVAS Vulnerability Scan

In this task we will conduct a Vulnerability scan of the Metasploitable machine using OpenVAS. We will use the Kali machine to perform this scan, as well as to exploit some vulnerabilities. The OpenVAS scan will take some time, not everyone will have their scan finish.

1. Power on the servers (**metasploitable and plabkali**).

* Wait for both machines to fully power on

1. Login to the Metasploitable machine via its Command Line Interface

* **Username: msfadmin**
* **Password: msfadmin**

1. Login to the Kali machine and create a new OpenVAS user.

* Username: **root**
* Password: **Passw0rd**
* Open a terminal window by ‘**double-clicking’** LXTerminal on the Kali Desktop. Enter the following command to create a new OpenVAS user**. Use your PSU-ID** **as your username.**

**openvasmd --create-user psu123**

* When you create a new user for OpenVAS, it automatically generates a unique password for the account. Highlight the password and copy it to login to the OpenVAS service.



*Figure 1.1 – Create User command with Password*

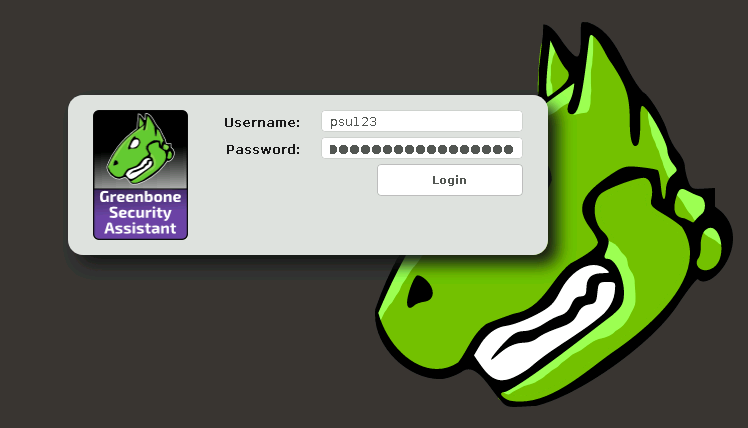
**1.1** (Screen shot) - Take a screen shot showing your ‘create user’ command along with the generated password.

1. Launch OpenVAS

The OpenVAS start service launches and performs a setup on the command line. Once it finishes the setup, a Firefox page automatically opens taking you to ‘**Greenbone Security Assistant**.’ GSA is a dashboard and GUI client for OpenVAS, allowing for easier scan setup, reports, and visualization using custom dashboards.

**Perform these steps to start OpenVAS and access Greenbone Security Assistant:**

* On the Kali machine, click on the icon in the ‘top-left’ task bar
* Navigate to **02 Vulnerability Analysis -> OpenVAS Scanner -> openvas start**
* Click on ‘**openvas start**’ a terminal window will pop up as OpenVAS boots up. A Firefox window will appear once it is fully running.
* When prompted about the Security Risk, click ‘**Advanced**’ and ‘**Accept the Risk and Continue.’**
* Login to the Greenbone Security Assistant using your **PSU-ID and copied password** from earlier. Click Login to continue.



*Figure 1.2 Greenbone Login screen*

1. Scan the Metasploitable machine

GSA offers multiple scanning methods depending on the application of your machines. More intensive scans take much longer to complete. Even the default scan option may take upwards of an hour. Follow the steps below to access the Task Wizard and start a default scan of the Metasploitable machine.

* From the main GSA dashboard screen, hover over ‘**Scans**’ along the top toolbar and click on ‘**Tasks**.’
* A message will pop up about the Task Wizard and various options. Click the ‘**X**’ to close this message. Because we are scanning one machine and not an entire network or subnet, we will use the Task Wizard for our scan.
* Click on the purple ‘**wand**’ icon in the top left of your screen, and then click ‘**Task Wizard**.’



*Figure 1.3 Task Wizard Icon*

* In the Task Wizard pop-up box, all you need to enter is the IP address of the machine you would like to scan. Enter the IP of the Metasploitable machine, and then click ‘**Start Scan.’**

**192.168.0.6**

1.2 **(Screenshot)** – Take a screenshot showing that you have started the scan. Make sure your screenshot shows your PSU-ID login in the top-right, as well as the status of your scan. ‘Requested’ or ‘1%’ status is fine.

* Full vulnerability scans take a while to complete; you are not expected to show proof of a completed scan. **Minimize the Firefox window and return to the Metasploitable machine**.
* Automated vulnerability scanners, such as OpenVAS, probe the target host for common or known vulnerabilities. This means they constantly send packets and try to connect to the target host. Whether the packets are malicious or not, the host is likely logging the probes and connection attempts.

1.3 **(Screenshot)** – Perform some research and find where log files are stored on the machine. Play the part of a Security Admin and use the **tail -f** command to show evidence from at least one system log file to show you are being actively scanned by an adversary (192.168.0.3). Show at least 3 concerning connection attempts in your screenshot.

(**BONUS**) – Extra credit if you can capture the **“*Magic Fairy Dust.”***

1.4 **(Individual Questions and Research)** – On the Canvas page for this lab, you will find a complete OpenVAS scan report of the Metasploitable machine. Take a look at the vulnerabilities present on the machine. **Each Team Member** **should** **choose 2 vulnerabilities from the report and explain how these could severely impact an organization. Relate your answer to the CIA Triad. Answers should explain the issue and the potential fallout in a short paragraph or two. List the name of the team member and their two contributions below.**

# Task 2: Exploit and Patch Vulnerability

In this task we will take a look at a vulnerability and then try to patch it. The vulnerability we are focusing on is a ‘**vsftpd-backdoor.**’ Exploiting this vulnerability gives instant root access to remote users. Let’s change that.

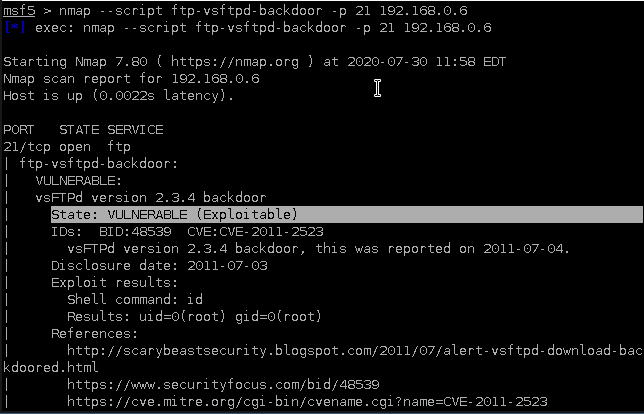
1. First, we need to verify that this vulnerability exists

* On the KALI machine, open a LXTerminal window and start Metasploit using the following command:

**msfconfole**

* Once Metasploit console has started ( **msf5 >** ), use the following nmap command to check if the Metasploitable machine is vulnerable to this exploit:

**nmap --script ftp-vsftpd-backdoor -p 21 192.168.0.6**

****

*Figure 2.1 – Nmap Script Scan*

2.1 (Screenshot) – Take a screenshot showing your output of the Nmap command.

1. Exploit the vulnerability

Now that we know the machine is vulnerable, lets use Metasploit to exploit the backdoor.

* In the msfconsole shell ( **msf5 >** ), search for the service we will be exploiting

**search vsftpd**

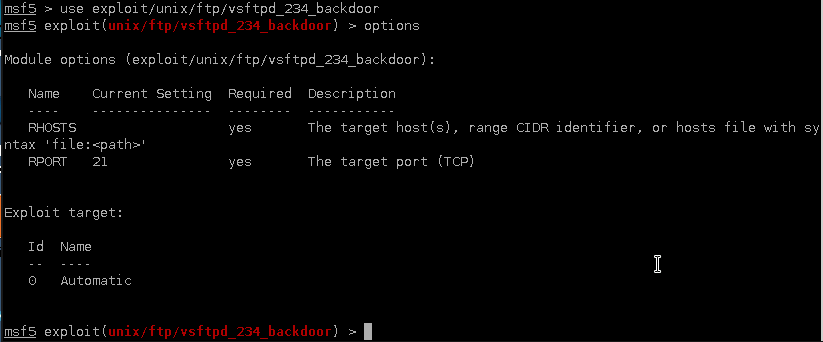
****

*Figure 2.2 – vsftpd Search Results*

* The file path for this exploit is written under **‘Name’** in the search results. With the ‘**use’** command, tell Metasploit to load this exploit. Once loaded, type **‘options’** to view the required input.

**use exploit/unix/ftp/vsftpd\_234\_backdoor**

**options**

****

*Figure 2.3 – vsftpd exploit options*

* As you can see there are only 2 options needed. The port number is already set to 21, so we do not need to change that. Set RHOSTS to the Metasploitable IP address.

**set RHOSTS 192.168.0.6**

* With the host set, we are ready to run the exploit. The first time it runs, you may receive the message, **‘Exploit Completed, but no session was created,’** in this case simply run the exploit again.

**run**

**run**

* Once your shell has opened, take a look at the destination port we’ve connected to.

2.2 (Screenshot) – Once you have opened a session, type ‘whoami’ to prove you are root, then type ‘hostname’ to prove you are connected to Metasploitable.

* Type ‘exit’ and hit enter to return to msfconsole.

1. Patch the vulnerability

We really do not want random users having Root access on our machines, so let’s patch this backdoor. There are many ways we can do this. If you noticed, the exploit opens a shell connection on port 6200. The easiest way for us to patch is by simply dropping packets coming into port 6200 on Metasploitable.

* Return to the Metasploitable shell to add the firewall rules. Make sure to use sudo as only root users can add firewall rules.
* Enter the following commands to block traffic on port 6200.

**sudo iptables -A INPUT -p tcp --dport 6200 -j DROP**

**sudo iptables -A INPUT -p udp --dport 6200 -j DROP**

* Jump back to the Kali machine to test your patch.

* + If your exploit is still loaded, go ahead and run it. If not, refer to part B of this task to load the exploit in msfconsole.

* + Run the exploit a few times to ensure that your patch is working.

2.3 (Screenshot) – Prove that your patch worked. Take a screenshot of at least 2 failed exploit attempts.

# Task 3: Research and Patch

In this task we will take a look at another vulnerability, only this time you will need to do some research and figure out how to patch it. The vulnerability we are focusing on is a ‘**ingreslock backdoor.**’ Similar to the vsftpd backdoor, exploiting this vulnerability gives instant root access to remote users. Let’s change that, too.

1. First, we need to verify that this vulnerability exists on the machine

* The ingreslock backdoor is accessible with a netcat connection on port 1524. Enter the following command to check for the vulnerability.

**nc 192.168.0.6 1524**

3.1 (Screenshot) – Take a screenshot showing the result of your netcat command.

1. Research a patch

* Do some research and figure out how to patch this vulnerability.
* NOTE:
  + You will need to make changes directly on Metasploitable machine.
  + You will need to make changes to another ‘ **.conf** ‘ file.
  + You will need to **‘Reboot’** the machine to verify your patch.
    - PracticeLabs allows you to do this where you can Power On/Off.
    - If you click Reset on accident, you may have to restart your patch.
  + Metasploitable is not connected to public internet, updating is not an option.
  + **Google is your friend.**

3.2 (Screenshot) – Prove that your patch works. Redo the netcat command above and take a screenshot of the results.

3.3 (Question) – How did you patch this vulnerability? Document and provide the changes you made to the Metasploitable machine. Be as thorough as possible in your documentation.

# Task 4: Challenge and Analysis

In this task, **each team membe**r will pick a vulnerability from the OpenVAS scan report in Canvas, research and try to implement a patch.

1. Choose a Vulnerability

* Open the OpenVAS scan report in canvas and look through the vulnerabilities present on the Metasploitable machine. Read all available information.
* Do some preliminary research to make sure a fix is feasible. Remember we cannot simply update the services.
* Some vulnerabilities (OS End of Life) cannot be patched.

1. Research and Implement a Patch

* Do what you can to resolve your chosen vulnerability. Use the resources available to you.
* Document **everything**.
* Remember there should be different response for these questions from each team member.

4.1 **(Individual Questions and Research)** – Which vulnerability did each team member choose? Be specific in what information you gained from the OpenVAS Scan Report?

4.2 **Individual Questions and Research)** – How/Where did you research this vulnerability? What information did you gather? Were you able to exploit the vulnerability?

4.3 **(Individual Questions and Research)** – Were you able to patch the vulnerability? In a short paragraph, explain the steps you took to remediate the vulnerability, and whether your patch was effective or not.

4.4 **(Individual Questions and Research)** – Pretend you found this vulnerability on an Organization’s machine. How would you explain to them the present risk, and why they should patch the vulnerability?