

Lab 7 – Vulnerability Scanning

Lab Objectives

Upon completion of this lab, you will be able to perform the following:

- Become familiar with *OpenVAS and other vulnerability scanners*
- Become familiar with vulnerability scanning reports and how to interpret them

Lab Materials

- Tools and utilities:
 - Product: OpenVAS
 - Installed on Kali: yes, but needs setup
 - Manufacturer: Greenbone
 - Product: Nikto
 - Installed on Kali: yes
 - Creator: Chris Sullo
 - Web site: <https://cirt.net/Nikto2>
 - Kali Linux VM

Lab Instructions

- Complete this lab;
- Enter your name and student ID above (Example: Ignatius Michael - Imichael);
- Answer questions and add screenshots into the corresponding textboxes;
- Save the file on your computer for future reference;
- Save the file again as a “.pdf” file;
- Submit the PDF file for grading.

Introduction

OpenVAS is an opensource vulnerability scanning software. This software is capable of scanning large networks and identifying vulnerable services and configuration.

The reports generated by this vulnerability scanner are thorough and can be very helpful in ethical hacking, as well as defensive security.

Part 1: Setting up OpenVAS (to be done at home before the lab)

This step is time consuming. Therefore, you're expected to complete it at home before the lab session.

1. Start your Kali machine, and perform "sudo apt update", and "sudo apt upgrade" at the command prompt.
2. Install openvas on your kali machine using:

sudo apt install openvas

3. Before we start setting it up, you will need to make the following configuration changes.

sudo nano /etc/postgresql/16/main/postgresql.conf

Look for the port number of postgresql server, and change it to 5432

```
port = 5432                                # (change required if you're moving listening port)
max_connections = 100                      # (change required when you increase max_connections)
#reserved_connections = 0                  # (change required when you increase max_connections)
#superuser_reserved_connections = 3        # (change required when you increase max_connections)
```

Press Ctrl+O to save the file, and press Enter. Then press Ctrl-X to exit.

sudo nano /etc/postgresql/15/main/postgresql.conf

Look for the port number of postgresql server, and change it to 5433

Press Ctrl+O to save the file, and press Enter. Then press Ctrl-X to exit.

Restart the postgresql service:

sudo systemctl restart postgresql

4. Start the initial setup of openvas using the command:

sudo gvm-setup

5. The setup process might take a few hours. In this process, the software is downloading all vulnerability signatures database. Let it finish!
6. At the end of the setup process, openvas will give you a randomly generated password for the 'admin' user. Create a blank text file on your desktop, and paste the password in it. DO NOT lose the password. You won't be able to reset it easily.
7. Now, you can check that the installation went well by running:

sudo gvm-setup-check

At the end of the check, you should get a message that says:

"It seems like your GVM-22.5.0 installation is OK."

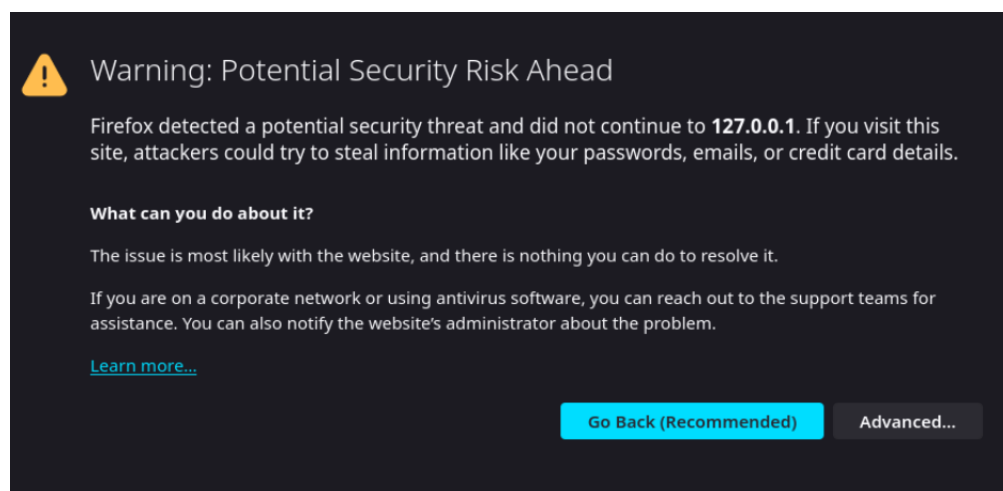
8. Once finished, you can start the openvas service using the command:

sudo gvm-start

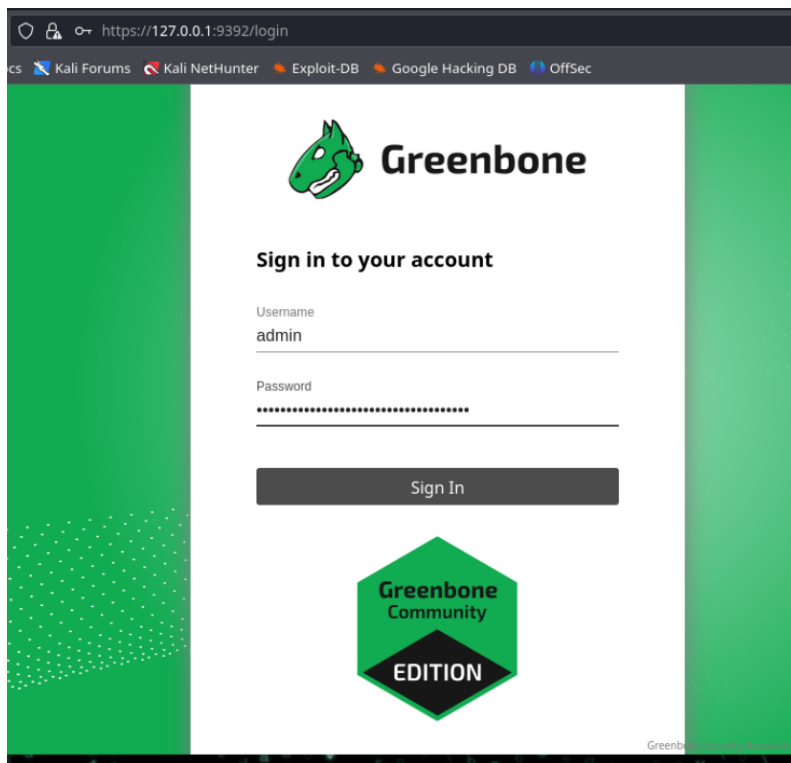
Keep in mind that OpenVAS is a web-based service. Once you start the service, keep the terminal window open, and go to your web browser. Navigate to:

<https://127.0.0.1:9392>

You will get a certificate error. Click on "advanced", and "Accept Risk and Continue".



If everything looks good, and you have the login webpage, Part 1 is done!



It is recommended that you leave the VM on at this stage for about an hour to make sure that all the necessary configuration steps are performed in the background by OpenVAS.

If you face issues in running openvas, try doing the following:

```
sudo gvm-stop
```

```
sudo runuser -u _gvm -- greenbone-nvt-sync
```

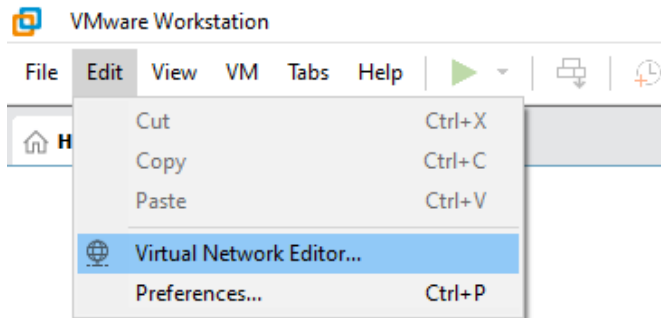
```
sudo gvm-start
```

Part 2: Connecting your Kali machine to the security lab network:

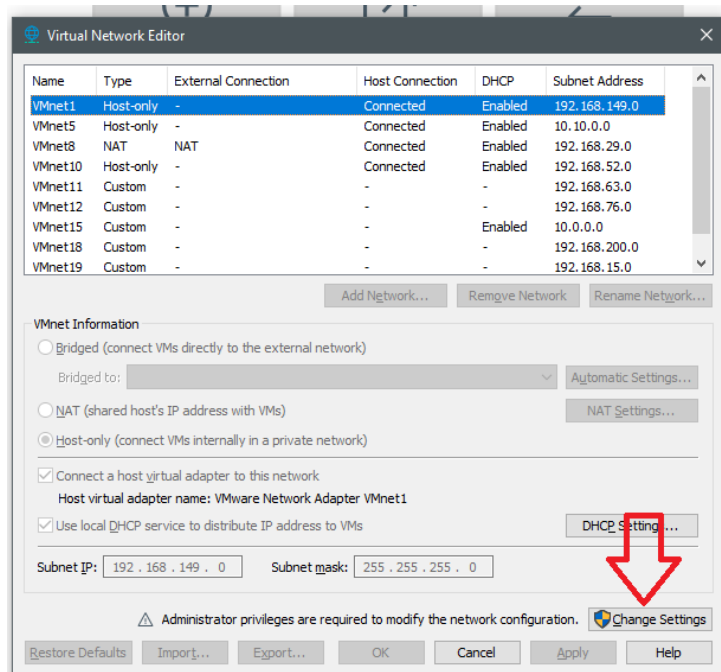
1. The physical machines in the lab are connected to more than one network through more than one NIC card. ? First, you'll need to find which card is "REALTEK" with an IP address in the range 172.16.x.x/28. On your physical machine, goto "start" and search "cmd" and hit Enter.
2. Run the following command:

```
ipconfig /all
```

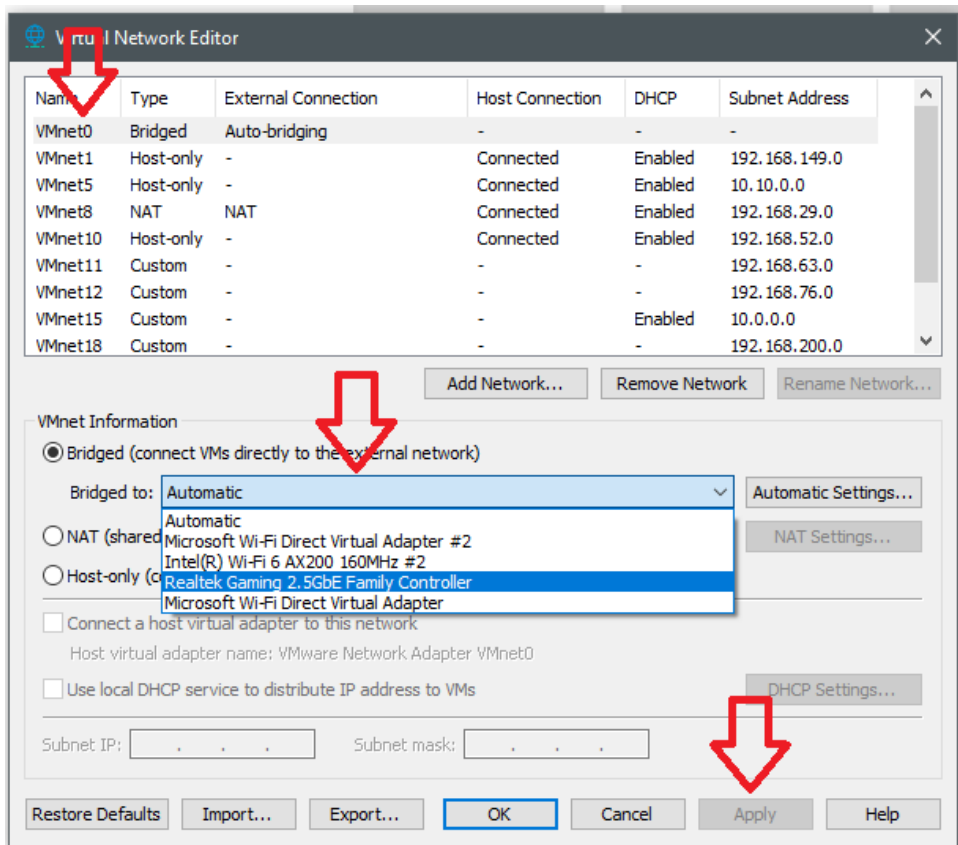
- Identify which NIC card has the 172.16.x.x IP address.
- Go to VMWare Workstation. On the top menu, choose “Edit”>>”Virtual Network Editor”



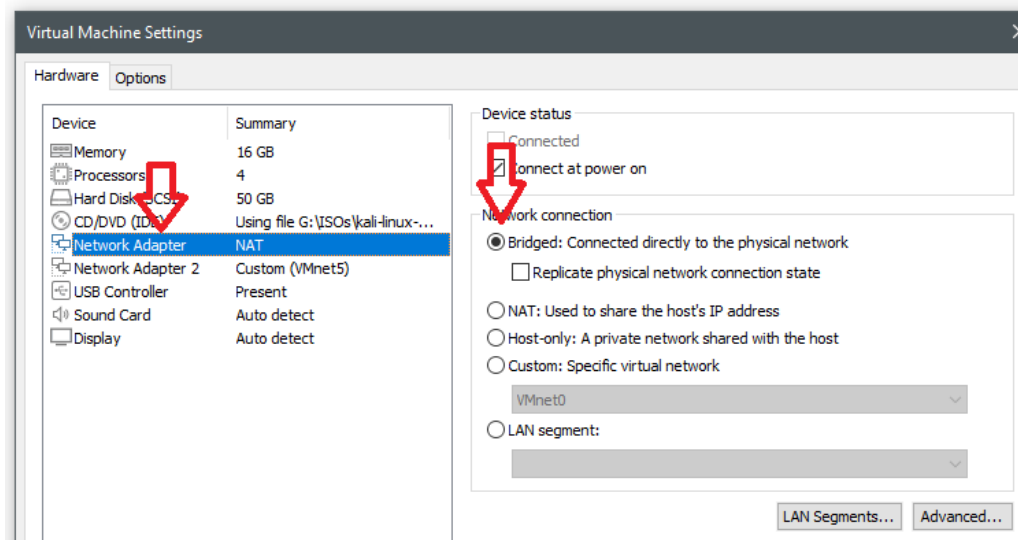
- Click on “Change settings..”



- Click on the settings of “Vmnet0” which is the bridging network setup, and click on the dropdown menu to choose the NIC card that you have identified in step 3. Then click apply..



7. Before starting your Kali VM, change the network connection to “Bridged”.



Check the “Replicate physical network connection state” checkbox.

8. Start your Kali VM.
9. After booting, run “ifconfig” command.

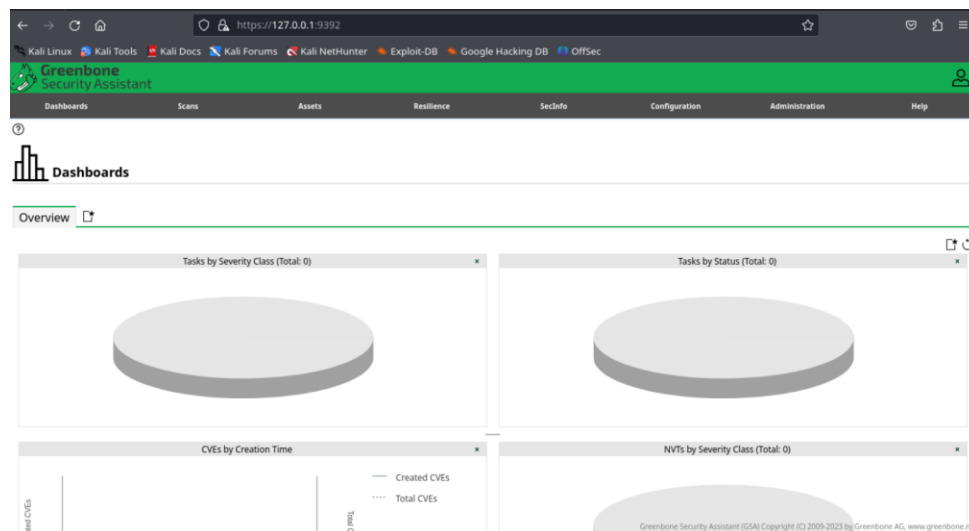
10. The Kali VM IP address should be in the 172.16.x.x range.

Part 3: Performing vulnerability scan using OpenVAS

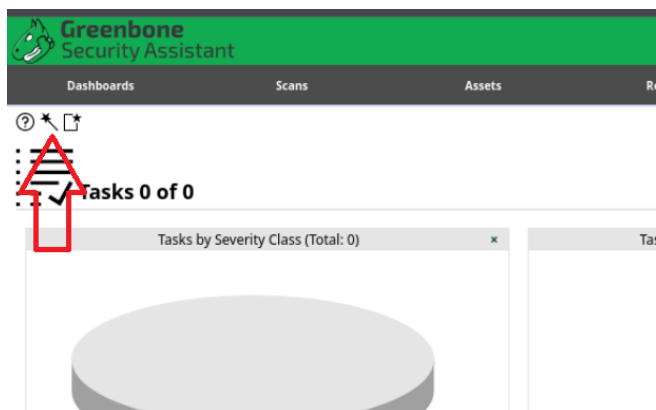
1. First, ping to the scanning target 172.16.11.5 to ensure that it is reachable.
2. Start OpenVAS service:

sudo gvm-start

3. Navigate to <https://127.0.0.1:9392> and login with username 'admin' and the password that was shared with you in part 1.
4. Once you're logged in, you will see a screen similar to this one.




5. Click on “Scans”, and then “Tasks”. We will create our first scanning task by clicking on the task wizard:



Then choose “Task Wizard”

6. Type the IP address of the target: 172.16.11.5

Task Wizard




Quick start: Immediately scan an IP address
IP address or hostname:
The default address is either your computer or your network gateway.
As a short-cut the following steps will be done for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away

As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.

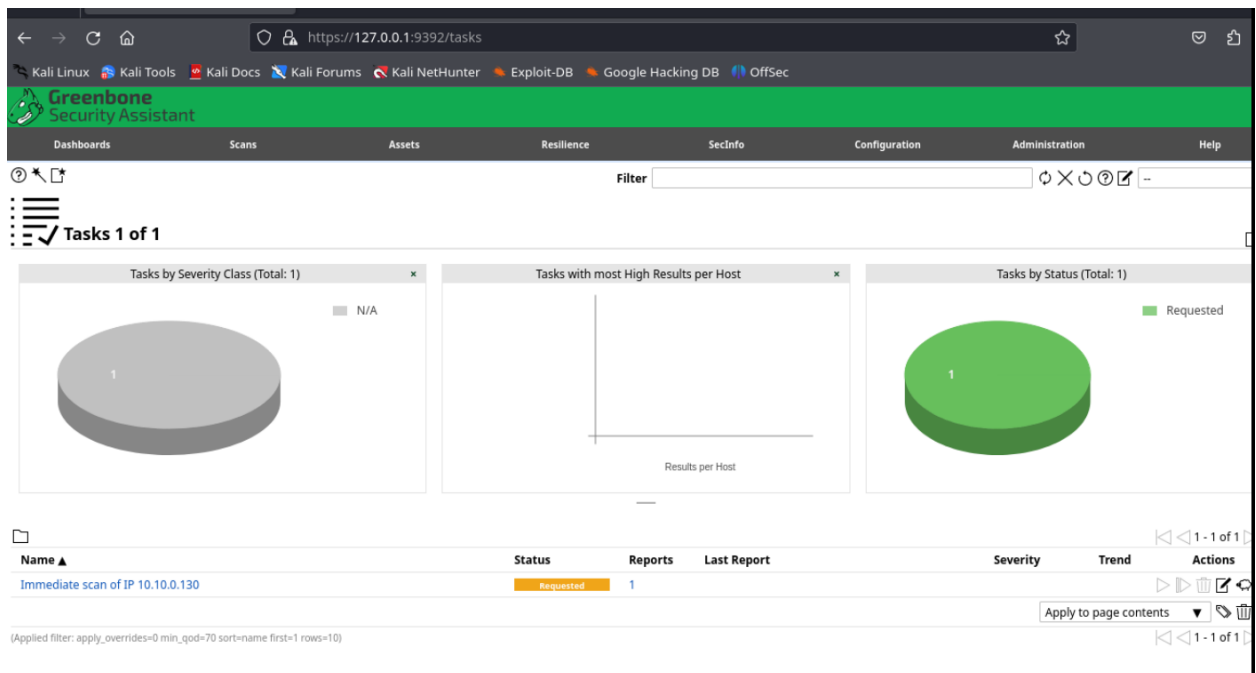
The Target and Task will be created using the defaults as configured in "My Settings".

By clicking the New Task icon  you can create a new Task yourself.

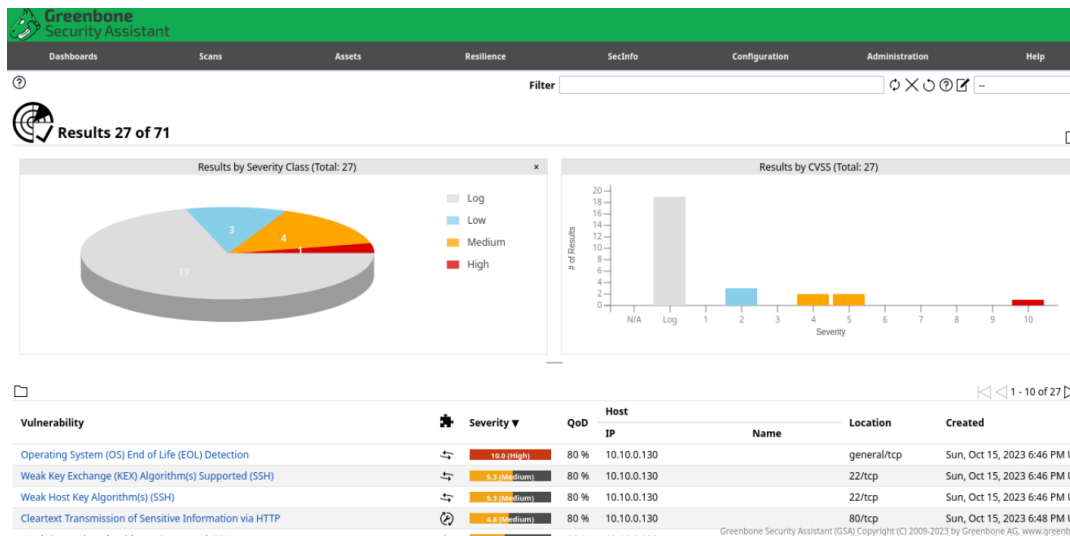
Cancel

Start Scan

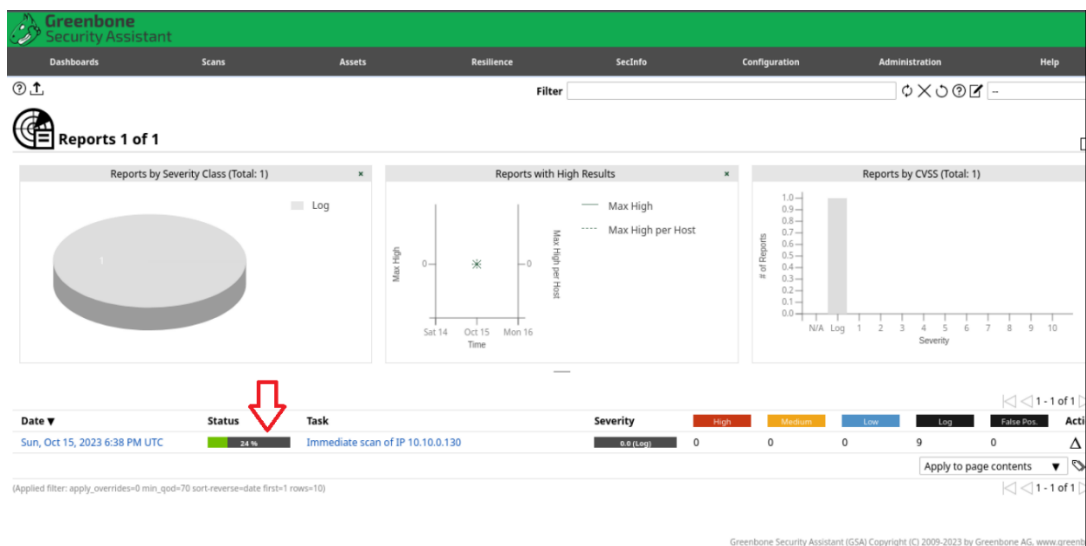
7. The scan can take a long time. Sometimes more than 30 minutes. You can track the scan status on the tasks interface:



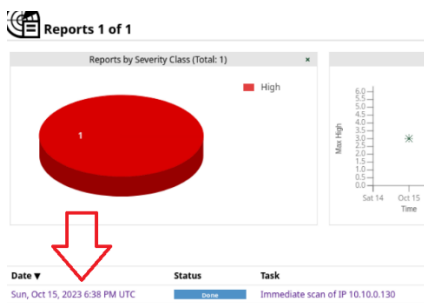
You can also see the current status of the results by clicking on "Scans", and then "Results". Remember that these might not be the final results.



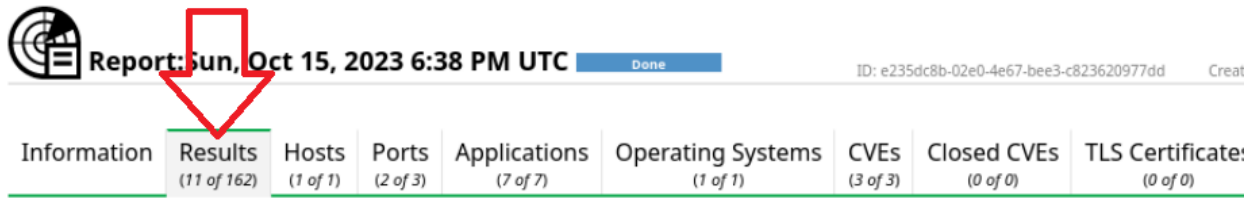
- The final report will get generated at the end of the scan, and can be accessed through “Scans” > “Reports”. The percentage of completion is shown in this interface as well.



- Once the scan is complete, click on the report:



10. Go through several tabs within the report. Take a look at the information provided. Click “Results” to see the detected vulnerabilities sorted according to their CVSS score.



| | | | | | | | | |
|-------------|-------------------------------|-------------------|-------------------|--------------------------|-------------------------------|------------------|-------------------------|------------------------------|
| Information | Results (11 of 162) | Hosts (1 of 1) | Ports (2 of 3) | Applications (7 of 7) | Operating Systems (1 of 1) | CVEs (3 of 3) | Closed CVEs (0 of 0) | TLS Certificate: (0 of 0) |
|-------------|-------------------------------|-------------------|-------------------|--------------------------|-------------------------------|------------------|-------------------------|------------------------------|

| Vulnerability | Severity ▼ | QoD | Host IP |
|--|--------------|------|-------------|
| Operating System (OS) End of Life (EOL) Detection | 10.0 (High) | 80 % | 10.10.0.130 |
| Drupal Core Critical RCE Vulnerability (SA-CORE-2018-002) - Active Check | 9.8 (High) | 98 % | 10.10.0.130 |
| Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check | 7.5 (High) | 98 % | 10.10.0.130 |
| Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) | 5.3 (Medium) | 80 % | 10.10.0.130 |
| Weak Host Key Algorithm(s) (SSH) | 5.3 (Medium) | 80 % | 10.10.0.130 |
| Sensitive File Disclosure (HTTP) | 5.0 (Medium) | 70 % | 10.10.0.130 |
| Cleartext Transmission of Sensitive Information via HTTP | 4.8 (Medium) | 80 % | 10.10.0.130 |
| Weak Encryption Algorithm(s) Supported (SSH) | 4.3 (Medium) | 80 % | 10.10.0.130 |

Click on a vulnerability to show details about it.

Part 4: Performing vulnerability scan using nikto

1. Open a new terminal window, and run the command:

```
nikto -h http://172.16.11.5 > nikto-scan-172.16.11.5.txt
```

this command will store the output of nikto scan in a text file.

2. Take a look at the contents of the scan file using ‘cat’:

```
cat nikto-scan-172.16.11.5.txt
```

3. Look for vulnerabilities that were found by nikto but not found by OpenVAS.

Note: You can reset OpenVAS password using this command:
sudo gvmc --user=admin --new-password=passwd;

Submit your lab using the submission form



- Doublecheck all your answers.
- Save the file on your computer for future reference.
- Save the file again as a “.pdf” file.
- Submit the PDF file for grading.

