Lab1A: Cyber Reconnaissance OPs

Lab Description:

In this lab, you will learn how to use penetration tools such as `nmap` and `OpenVAS` to scan a vulnerable machine, identify vulnerabilities and analyze their impact. The goal is to teach you the basics of reconnaissance phase of the ethical hacking process. We will use two virtual machines: One is a Kali Linux with `nmap` and `OpenVAS` installed and the other one is an intentionally vulnerable Metasploitable 2. We will use `nmap` and `OpenVAS` on Kali Linux to scan the vulnerable machine Metasploitable 2.

Role:

Consider yourself to be a cybersecurity professional conducting practical ethical hacking studies on a client company system to detect the vulnerabilities in the systems so as to offer insights to develop a defense strategy for your client.

Audience:

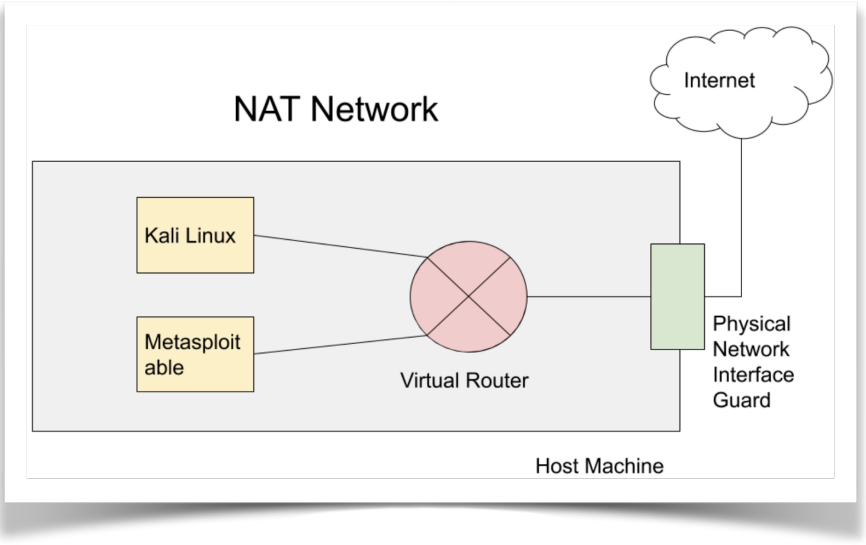
The lab report should be written towards the client company Information Technology department with vulnerability analysis. Assume that the reader understands computer systems and networks and information technology.

Experimental Environment:

You will work on a virtual environment with VirtualBox where the virtual machines, i.e., Kali Linux VM and Metasploitable 2 VM are imported.

- Kali Linux VM: The machine that contains the penetration testing and hacking tools.
- Metasploitable VM: The machine that you will hack.

A virtual networking environment will be setup as shown below which creates an isolated environment for hacking while the outsider attacks cannot reach Metasploitable 2.



You will first go through a tutorial with step-by-step instructions to learn how to use the popular penetration testing tool, including `nmap` for port scanning and `OpenVAS` for vulnerability assessment.

`nmap` (Network Mapper) is an open source tool for network exploration and security auditing. Though it was designed to rapidly scan large networks, we use it to scan the target host in this lab. `nmap` options are summarized in the manual page.

`OpenVAS` (Vulnerability Assessment System) is an open-source framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.

Lab Tasks:

1. Follow the lab tutorial and finish the two tasks given in the tutorial (Task 1 is required but for self-grading).
2. Use `nmap` to scan *all* TCP ports on the target remote host with *SYN* packets from the attack system and find out which ports are open, which are closed, and which are filtered.
3. Use `nmap` to scan the target and find the software *version* of the *OS* and the running *services* (list at least 3 of them).
4. Use `OpenVAS` to configure scanning tasks and find vulnerabilities of the remote target, and interpret the scan results of a vulnerability at severity level of 10 (excluding UnrealIRCd vulnerability). Assess this vulnerability and find the corresponding exploit.

Lab Reporting Requirements:

- Write a security professional report. Use snapshots to indicate the commands you use and the scan reports that you receive. Provide detailed analysis and offer insights based on the scan and assessment reports that you receive. The BEST report will be recognized with **bonus** points.
- Work on the report by following the template of Penetration Testing Lab Report as attached on the last page.
  - ***Problem scope***: Thoroughly investigate the background and motivation information.
  - ***Methods and approaches***: Elaborate methods and techniques developed and used to achieve the tasks. Discuss the design tradeoffs and performance evaluations.
  - **Data delivery**: Experiment data is complete and relevant, illustrating in appropriate ways such as tables and graphs. Questions if any are answered completely and correctly.
  - ***Lab summary***: The report is well concluded by summarizing experiment, citing data, providing insights and findings, and offering comments and suggestions to the company's IT department.
  - ***Report quality***: Report is well organized and cohesive and contains no technical errors. Report presentation seems well polished.

Submission Deadline:

Submit the lab report via Blackboard on or before **Wednesday, Feb. 3, 2021**.

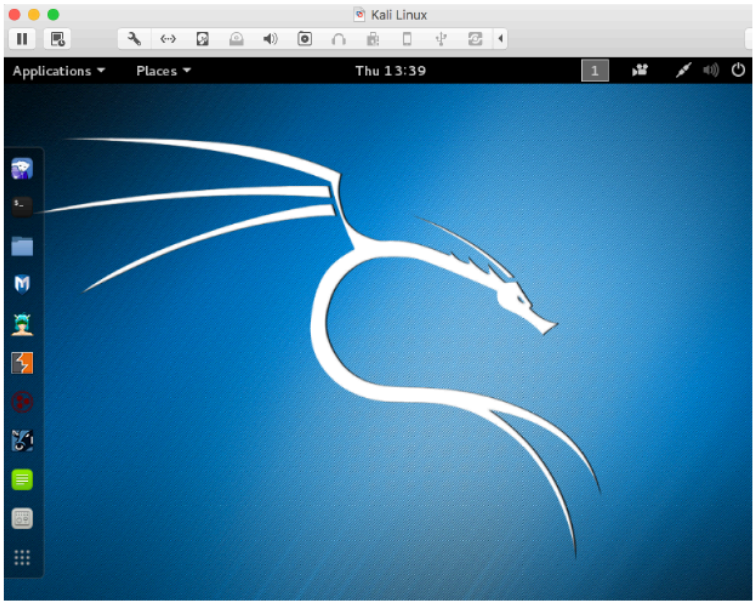
Grading Policy:

The total mark is 100 points breaking down into:
- Design and develop scan and vulnerabilities assessment process, 25%
- Fulfill penetration test tasks, 35%
- Analysis and Reporting, 40%
- Bonus: performance optimization, 10%

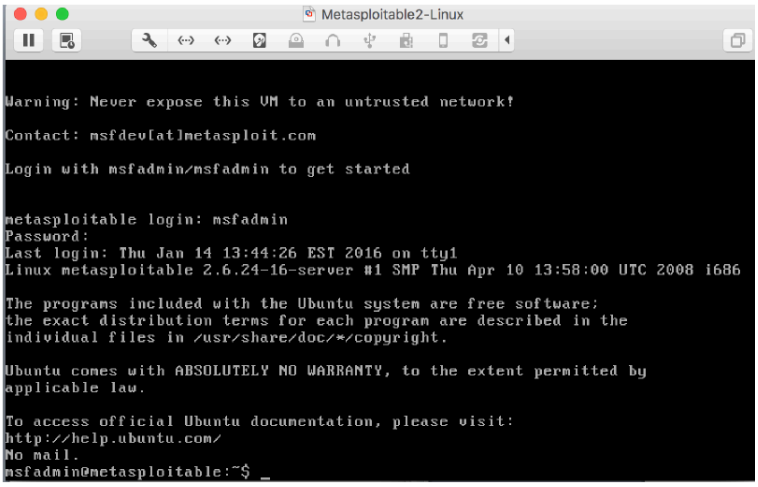
Lab Tutorial

Starting the virtual machines

- Open VirtualBox. We will use two VMs: the Kali Linux and the Metasploitable 2.
- Open the Kali Linux VM in the VirtualBox Manager. When the Kali Linux login screen appears, Login the Kali Linux with username “root”, and password “toor”. The screen snapshot after login is shown on the right.



- Now that your Kali Linux machine is up and running, you will also need to launch your Metasploitable 2 VM so that you can attack against. Select Metasploitable 2 VM from the list in VirtualBox Manager. Wait for the terminal to finish loading. Your virtual machine should display the metasploitable logo (Note: Your mouse pointer may disappear. Press the Ctrl+Alt keys together to get your mouse back). Log into the virtual machine with username “msfadmin”, and password “msfadmin”. After login, you will see the screen on the right.



- You can set up the GUI on Metasploitable 2 by using the following commends. Switch back to command line using Ctrl+ALT+FN+F2/F3; and return to GUI with Ctrl+Alt+F7.
  msfadmin@metasploitable:~$:sudo rm /tmp/.X0-lock
  msfadmin@metasploitable:~$:startx

Finding the IP address of the target

This lab uses Metasploitable 2 VM as the attacking target.

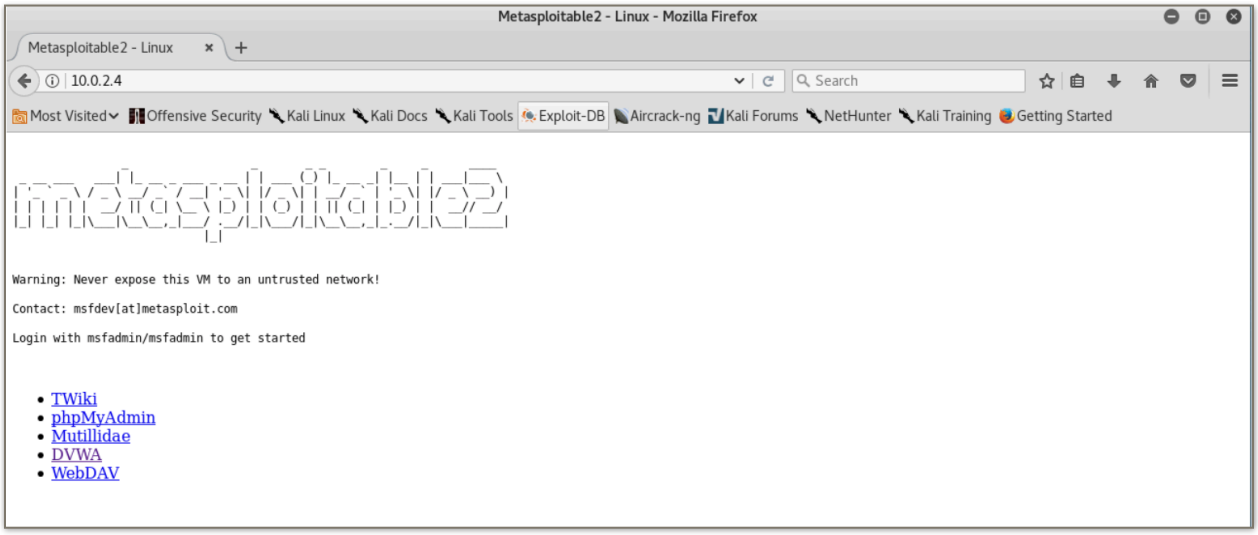
- Find the host IP address of the target to launch a scanning.
- Use the command “ifconfig” or “ip a”. This command allows you to find all the connected interfaces and network cards. Go to the Metasploitable 2 VM, and execute the following command
  $ ifconfig

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1c:19:d3
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1c:19d3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:34 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5261 (5.1 KB)  TX bytes:7443 (7.2 KB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$ _
```

From the screenshot above, we can see that the IP address of the network interface, eth0, is 10.0.2.4 under an inet addr for the 'eth' (Ethernet) portion of the output. This is the IP address for the target. **Note that you will get a different IP address for your Metasploitable 2 VM**. This is not a public IP but we can access it within the subset. Now open the Kali Linux web browser. Type the IP address that you obtained from Metasploitable's ifconfig output into the URL bar. You should see the page as shown below.

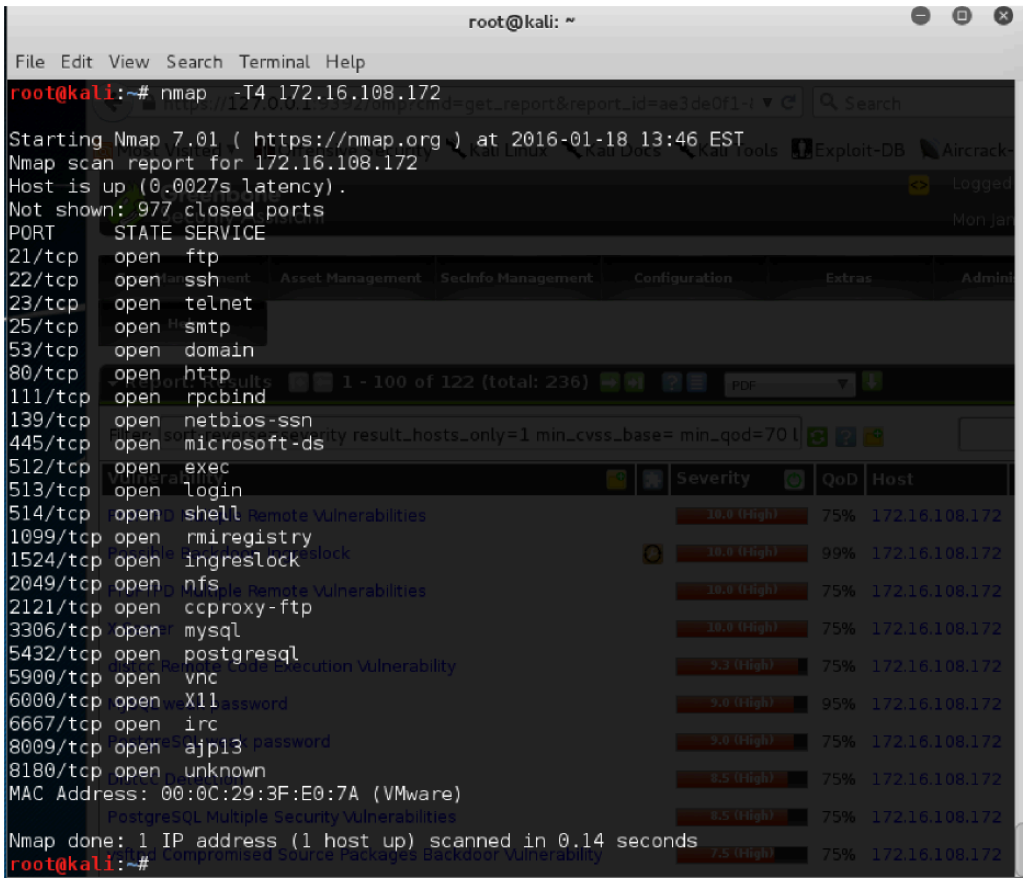


Task 1: Scanning the target using `nmap`

- Go to the Kali Linux (unlocking by Ctrl+ALT+L), and open up a terminal by clicking the icon 
- Launch the scanning in the terminal by typing the command:

  $ nmap –T4 *172.16.108.172 [replace with your own IP address]*

  where nmap is the execution command; option -**T4** means faster execution; and 172.16.108.172 is the IP address of the target which will be replaced with your own IP address.



The screenshot above shows a quick scan of the target machine using `nmap`. We can see that there are many open ports and services on the target system including FTP, SSH, HTTP, and MySQL. These services may contain vulnerabilities that you can exploit.

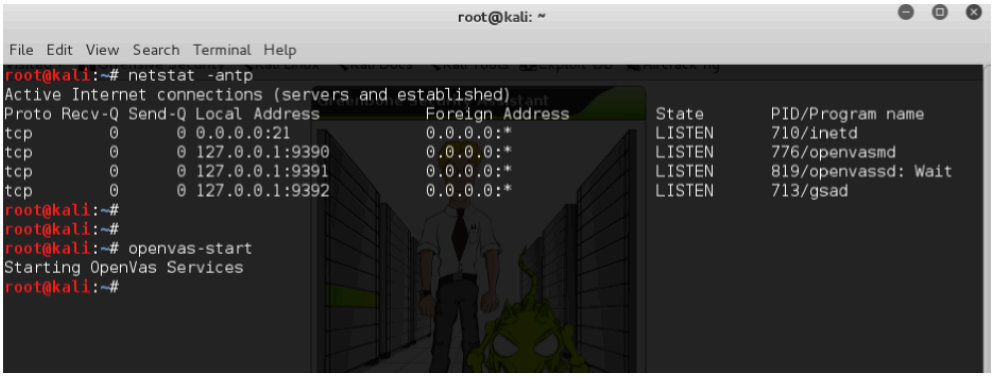
`nmap` provides many useful functions that we can use. You can find more information from the man page of `nmap` by executing the command or refer to the nmap manual page:

$man nmap

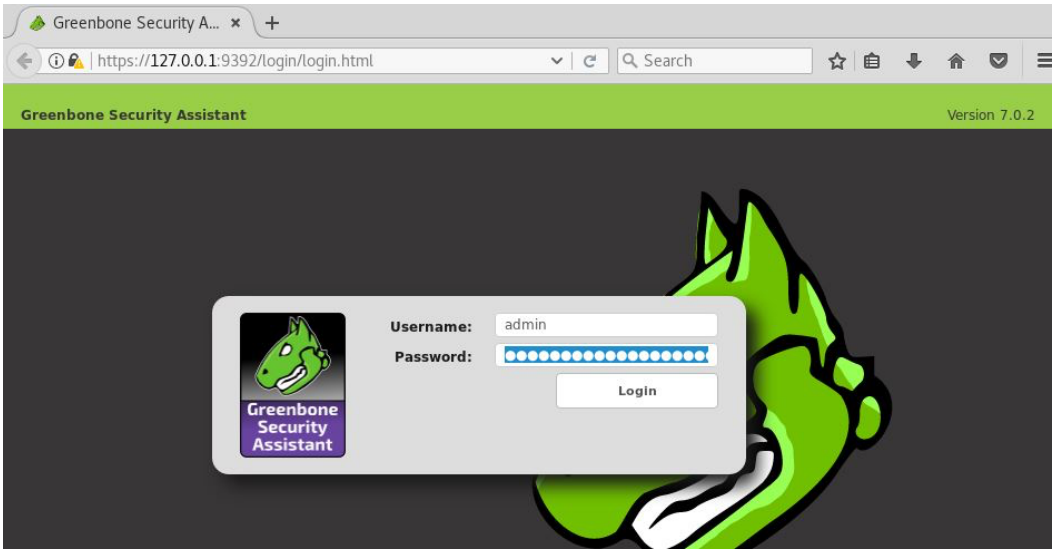
Task 2: Vulnerability scanning using `OpenVAS`

- OpenVAS has been installed and configured. You may check if the OpenVAS manager, scanner, and GSAD services are listening by running the following command:

  root@kali:~# netstat –antp

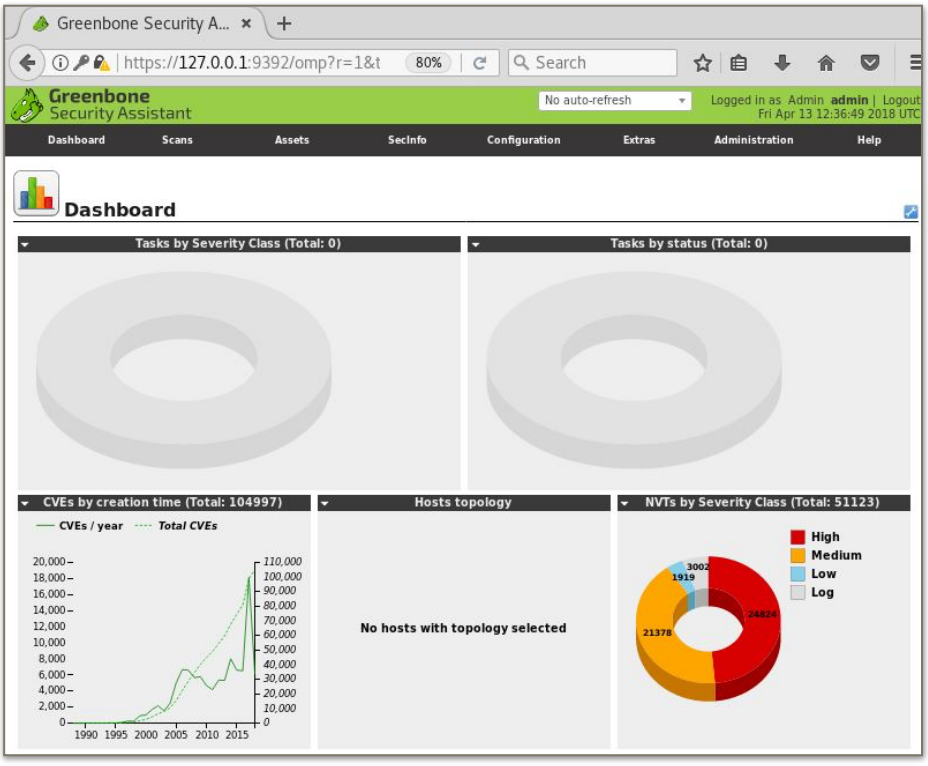


- Start the services by executing the command.
  root@kali:~# openvas-start
- If you need to troubleshoot any issues, you can identity the problem by using the commend
  root@kali:~# openvas-check-setup
- You may stop the services by the following command
  root@kali:~# openvas-stop
- You may also connect to the OpenVAS web interface by opening the browser in Kali Linux. Then go to https://127.0.0.1:9392 and accept the self-signed SSL certificate.
- Start OpenVAS. Input the username as “admin”, and the password “ccser”. You will enter the Greenbone Security Assistant which is a web application that connects to the OpenVAS Manager and Administrator to provide a full-featured user interface for vulnerability management.



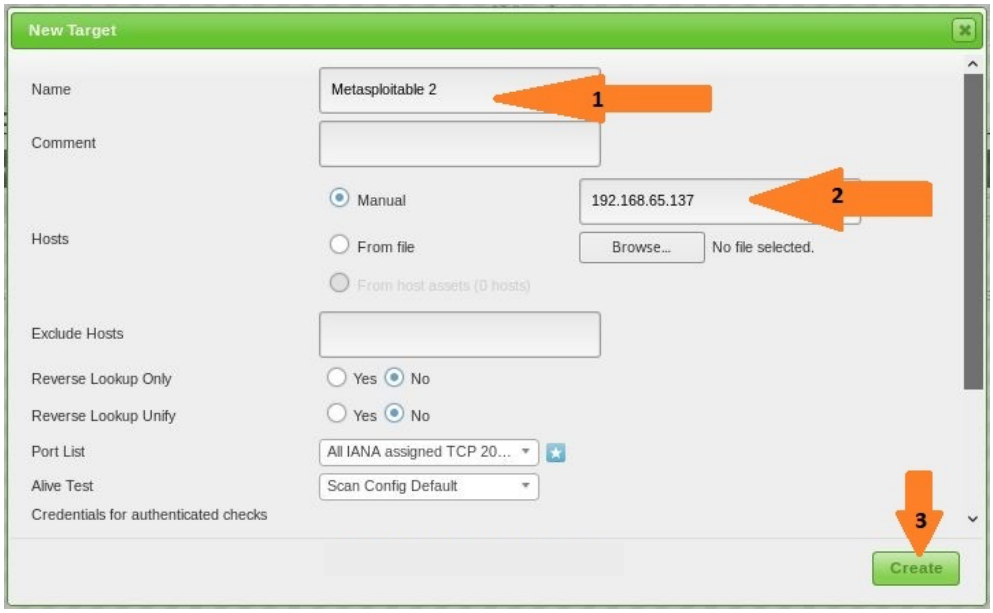
- You can change the admin password using the following command:
  root@kali:~# openvasmd –-user=admin –-new-password=[password]

- After logging in on the web interface we’ve redirected to the **Dashboard** from where we can configure and run vulnerability scans.

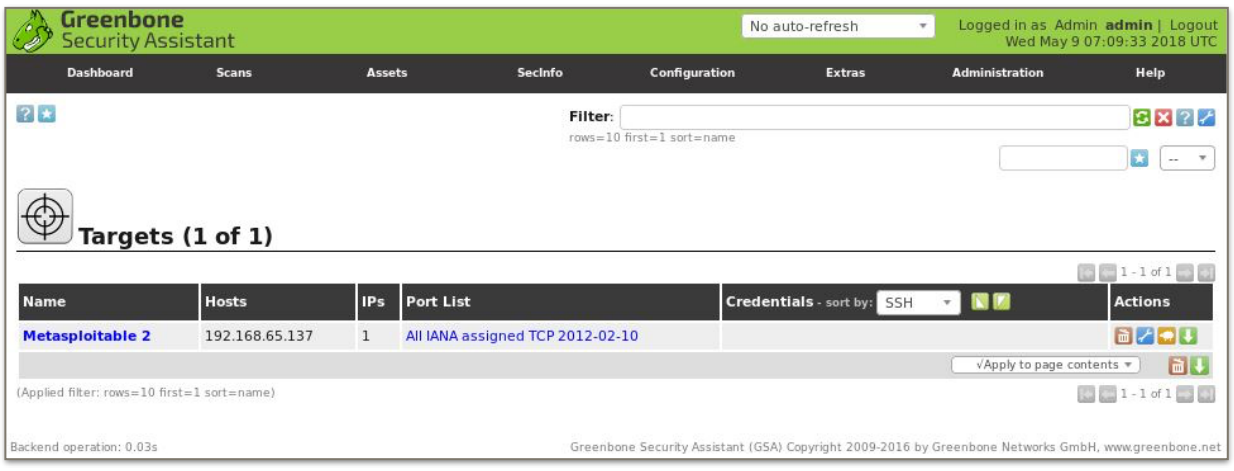


- **Create and configure a target** using the OpenVAS/Greenbone Security Assistant web interface. Go to 'Configuration' in the top menu and select 'Targets'. Click the blue star icon in the top left corner to create a new target.

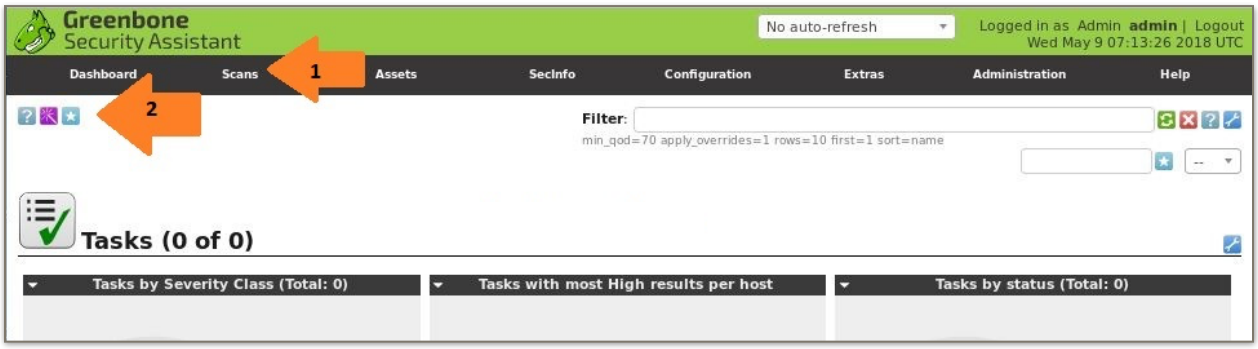
- After hitting the new target button, a dialog screen appears. Enter the following information:
  1. Target name -> Metasploitable2
  2. The target IP host -> *192.168.65.137 [replace with your own IP address]*
  3. Keep all other settings default and click the 'Create' button.



The newly created target will appear in the list of available targets:

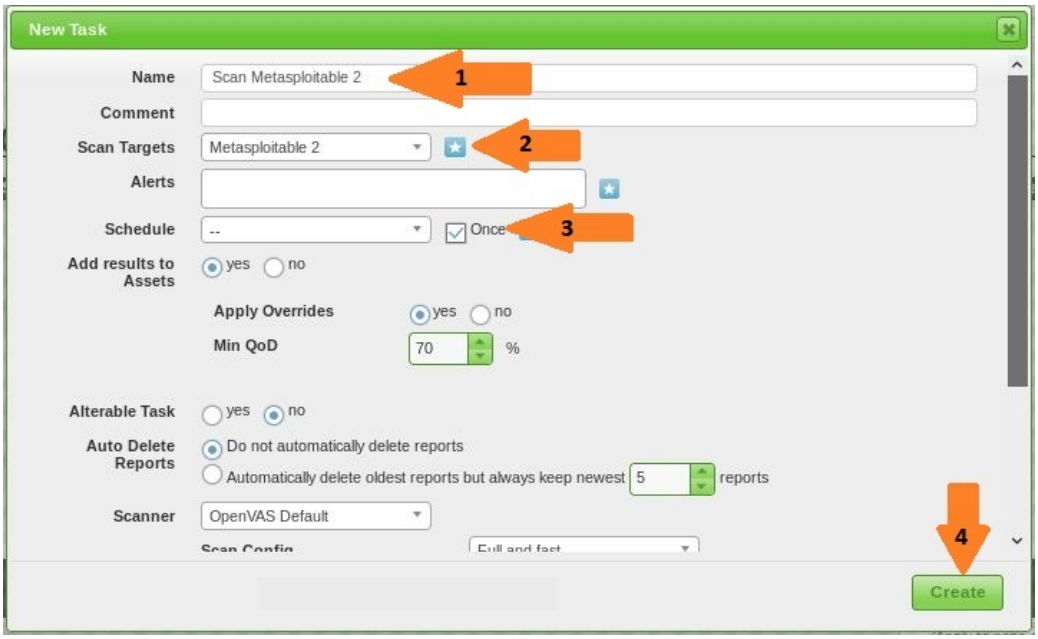


- **Create a new scanning task** which defines which targets will be scanned and also the scanning options such as a schedule, scanning configuration and concurrently scanned targets and Network Vulnerability Tests (NVTs) per host. In this lab we will just create a scan task and use default scan configurations. Click ‘Scans -> Tasks’. Point to the blue star icon

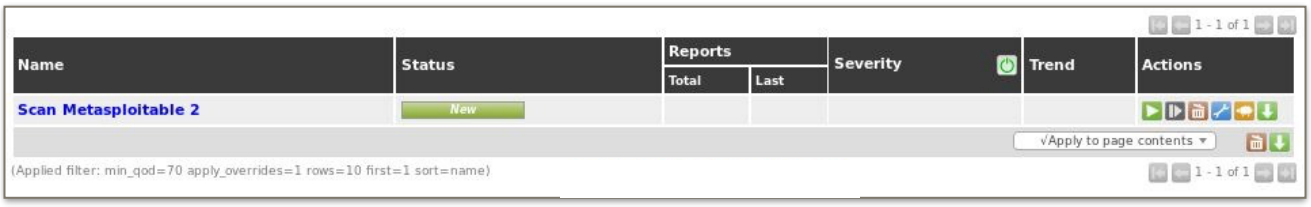


in the top left corner and select ‘New Task’.

- Enter the following information in the dialog screen appeared.
  1. task name -> Scan Metasploitable2
  2. Select Scan Targets -> Metasploitable2
  3. Click the schedule once checkbox
  4. Keep all other settings default and click the ‘Create’ button to create the new task.

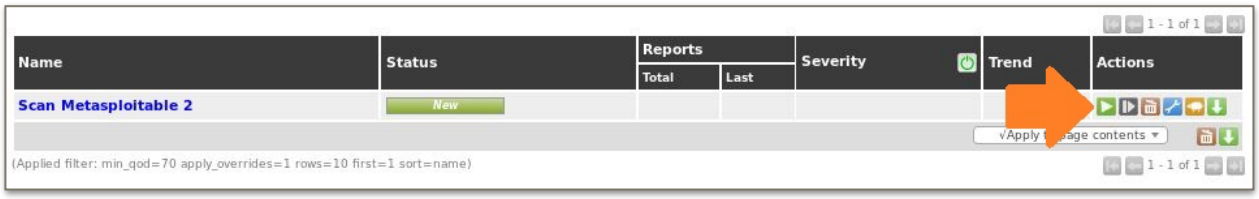


The newly created task will appear in the task list as follows:

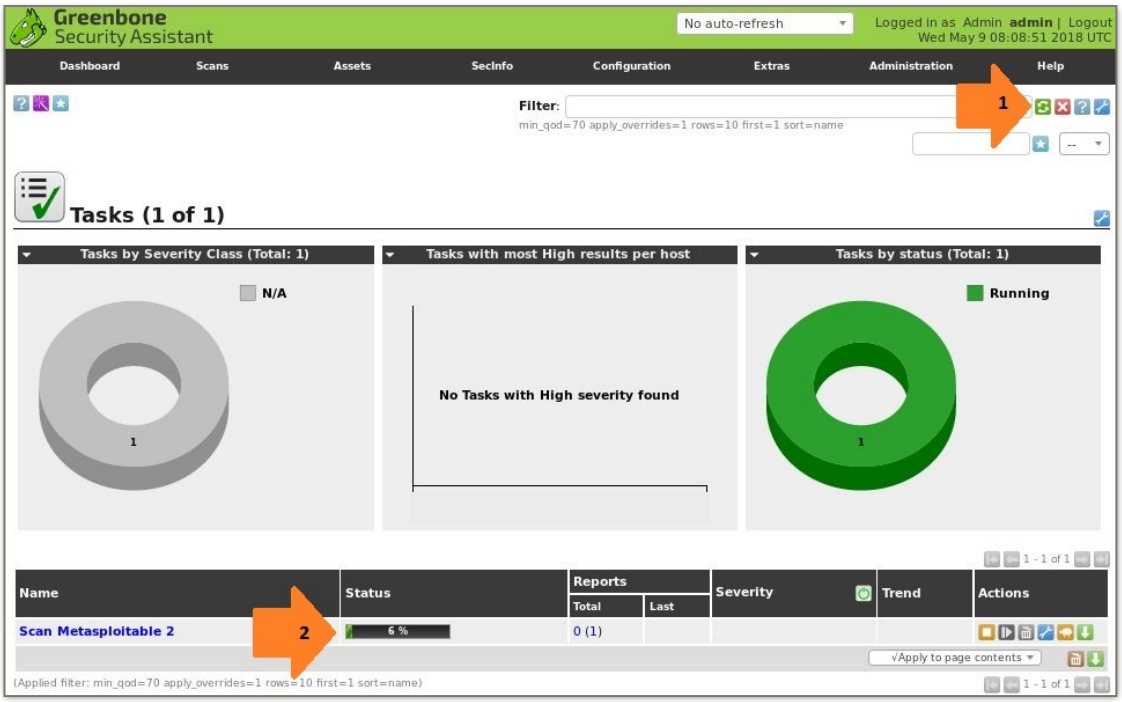


There's other options to create scan tasks. We can use the 'Scan Task Wizard' to instantly scan a target and also the 'Advanced Scan Task Wizard' which gives a few more options to configure. For this lab we'll stick with the task we've just created.

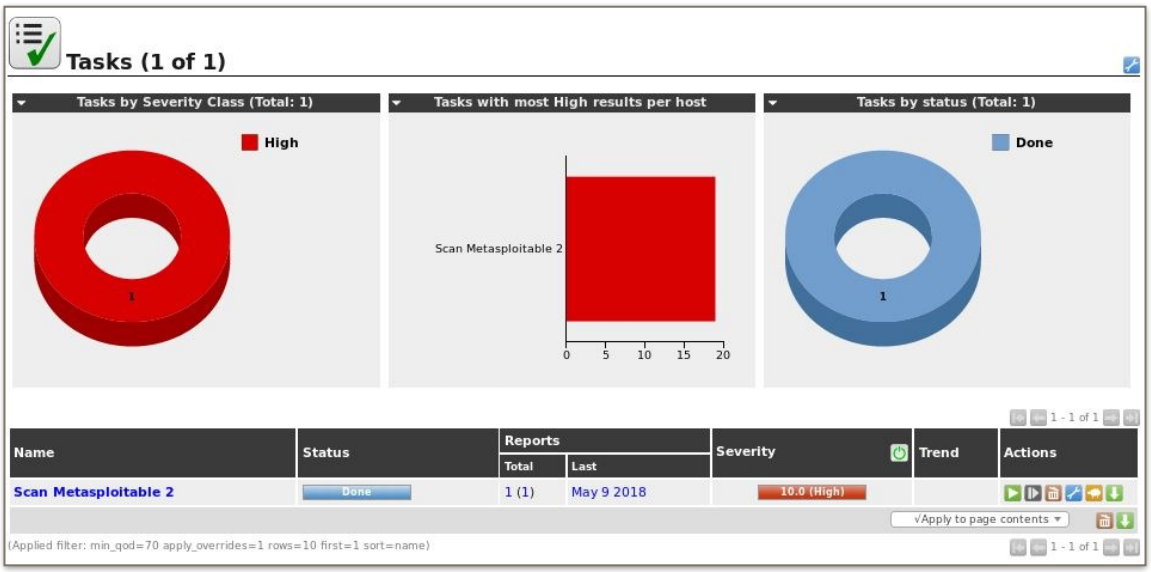
- **Run the scan task** by clicking the green start button. The scan task will execute against the selected target. Note that full scan may take a while to complete.



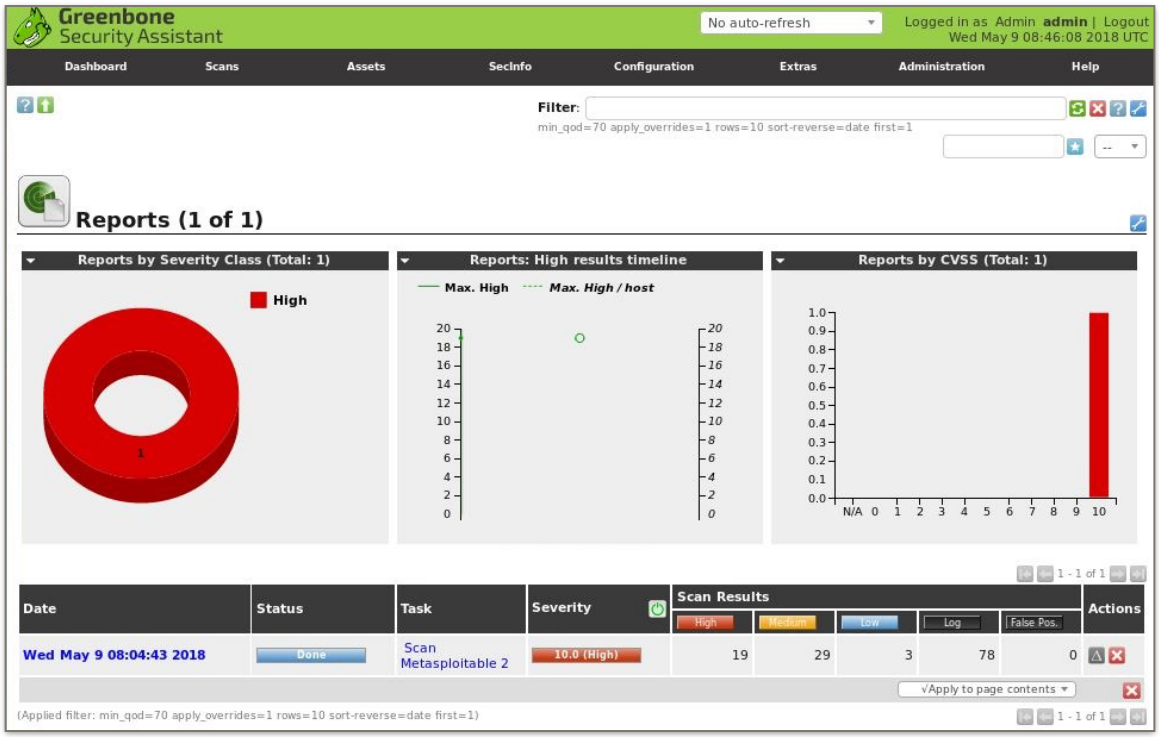
- Refresh the tasks page to check the progress for the executed task



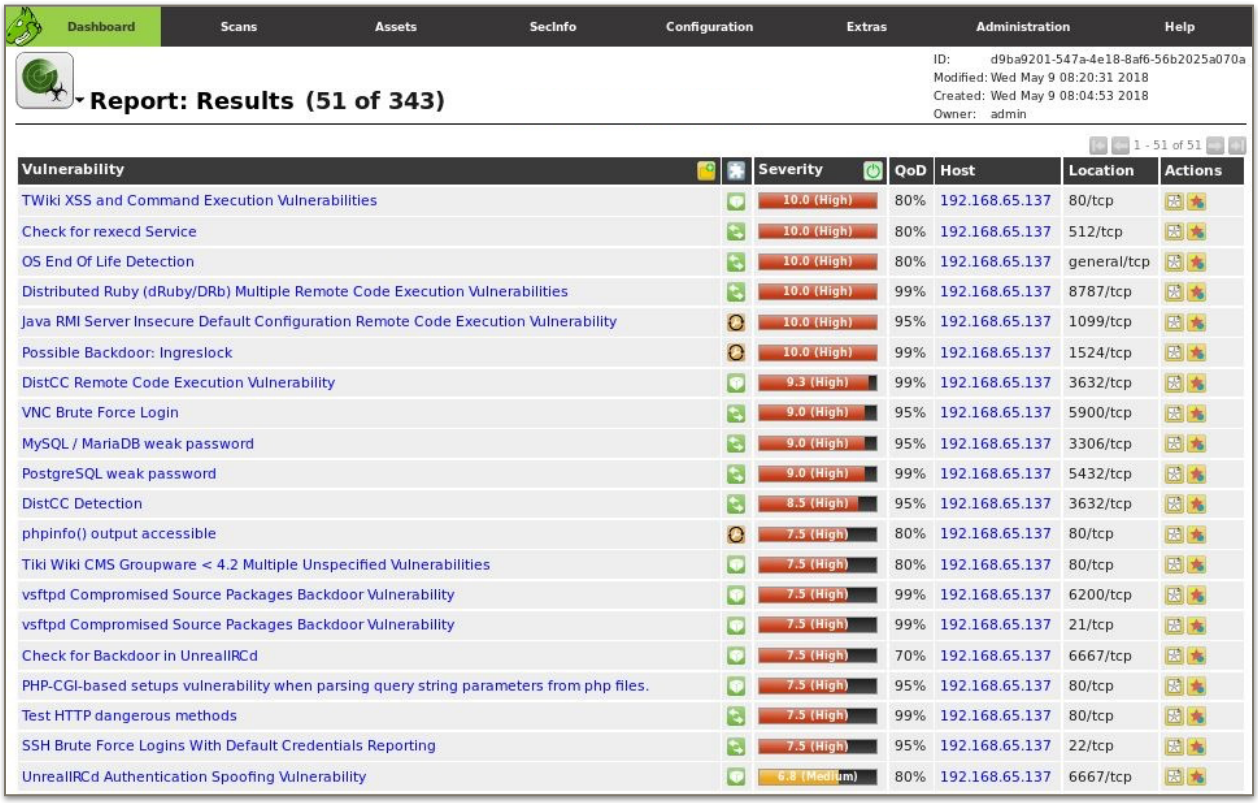
- Once the scan task is finished and the status changes to 'Done'



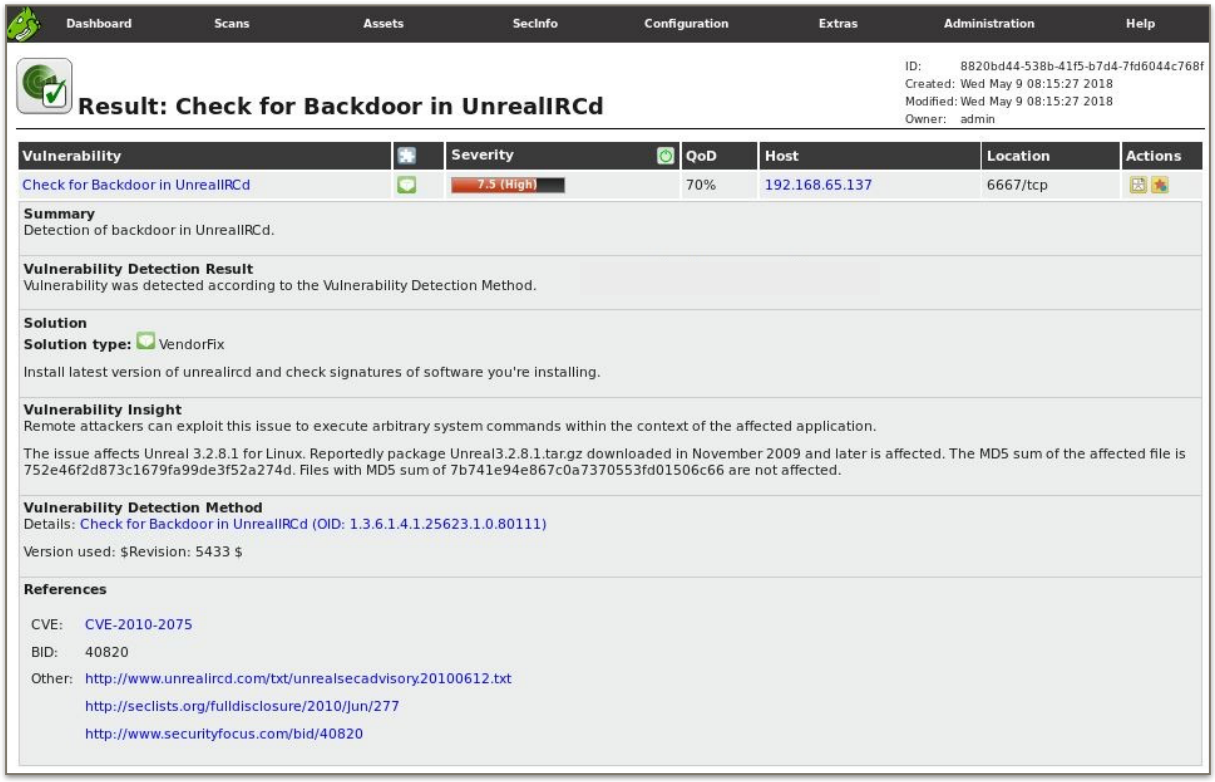
- Browse to ‘Scans -> Reports’ in the top menu. On the reports page we can find the report for the completed scanning task and **interpret the scan results**.



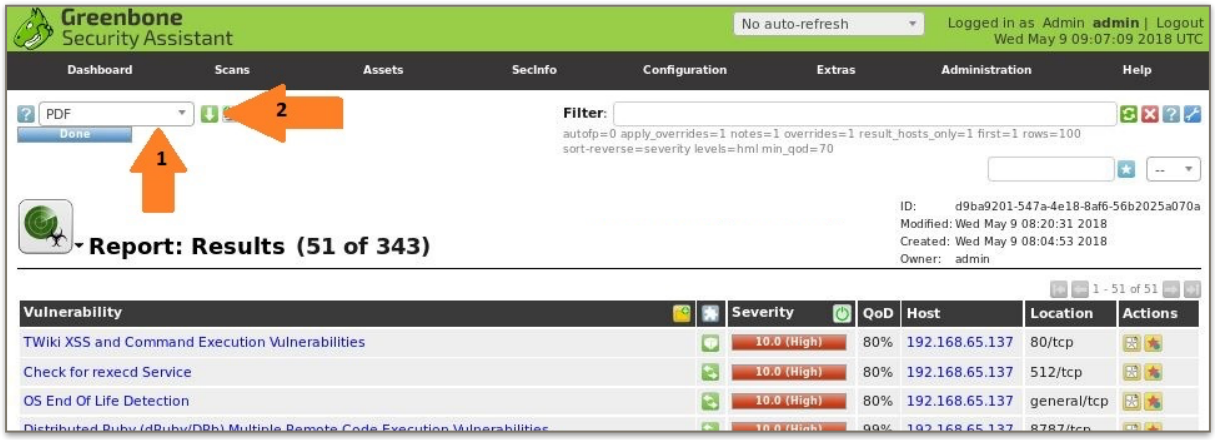
- Clicking the report name and get an overview of all discovered vulnerabilities on the Metasploitable2 machine. The results are ordered on severity rate by default.



- Click on the vulnerability name to get an overview of the details regarding the vulnerability. The following details apply to a backdoor vulnerability in Unreal IRCD:

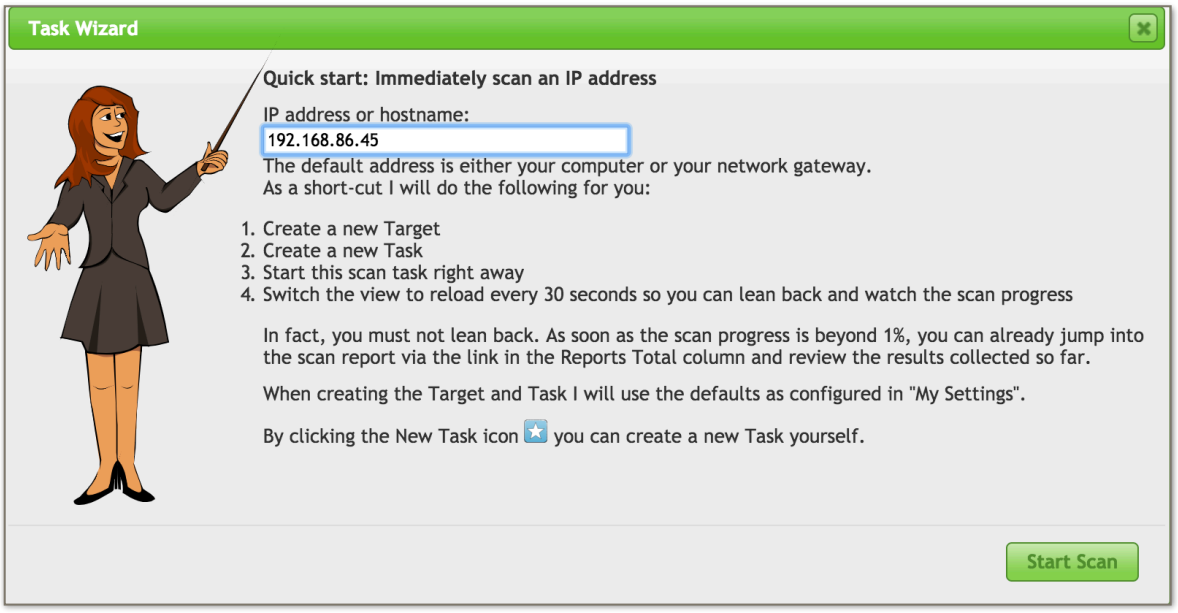


- We can also export the report in a variety of formats, such as: XML, HTML and PDF. Select the desired format from the drop-down menu and click the green export icon



- If you only scan one target IP, you may run it in a '**Quick start**' Box by clicking 'Scans -> Tasks' and then click the purple fireworks icon for 'Task Wizard'
- Type the IP address of the target, e.g., 172.16.108.172 in the "Quick start" box, and press "Start Scan". It will do the following for you:
  1. Create a new Target with default Port List
  2. Create a new Task using this target with default Scan Configuration
  3. Start this scan task right away

4. Switch the view to reload every 30s so you can lean back and watch the scan progress



Reconnaissance Lab Report

Scanning Manifest

Penetration Tester	Your name
Scanning periods	Record all time periods when you perform scanning
Tools	Tool name and version
Scope	Briefly describe the scope of the scanning tasks
Description	Briefly describe the purpose and impact of this reconnaissance lab

Executive Summary

Scope:

Describe in detail the scope of the scanning tasks.

Approach:

Describe in detail the scanning methods and techniques you apply to fulfill the tasks. Use snapshots to help illustrate your approaches.

You will receive a BONUS point if any optimization techniques are applied to improve scanning performance interns of scanning time and accuracy. Analyze and compare the results.

Findings:

Analyze the scanning reports and summarize your findings. Scanning reports are attached as supporting document.