CCCCO CySA+ Lab Series

Lab 1: Vulnerability Scanning

Document Version: 2019-09-06

Contents

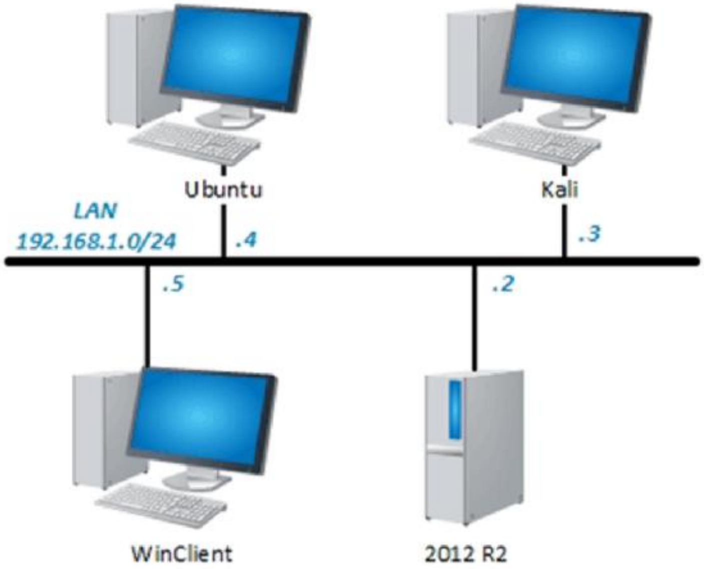
Introduction

In this lab, you will explore various network discovery methods and use them to perform a vulnerability scan on your network.

Objectives

- Perform port scans with netstat
- Perform network scans with nmap
- Use OpenVAS to perform a vulnerability scan

Lab Topology



Lab Settings

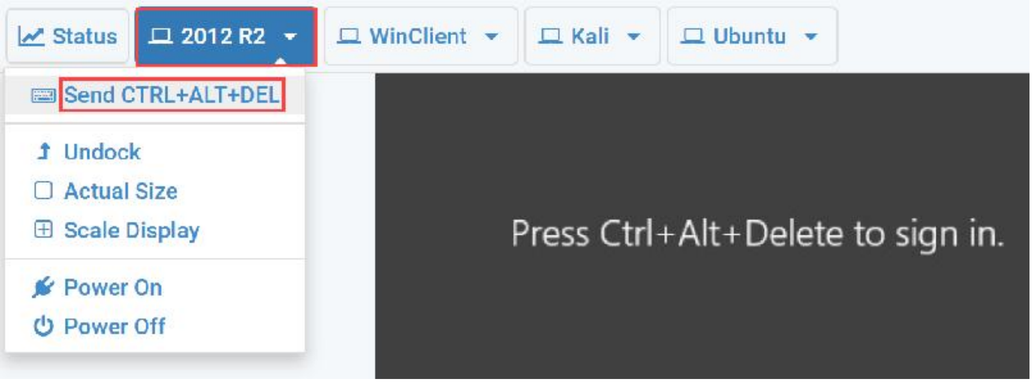
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account	Password
2012 R2	192.168.1.2	Administrator	Password123
WinClient	192.168.1.5	student	Password123
Kali	192.168.1.3	root	toor
Ubuntu	192.168.1.4	sysadmin	Password123

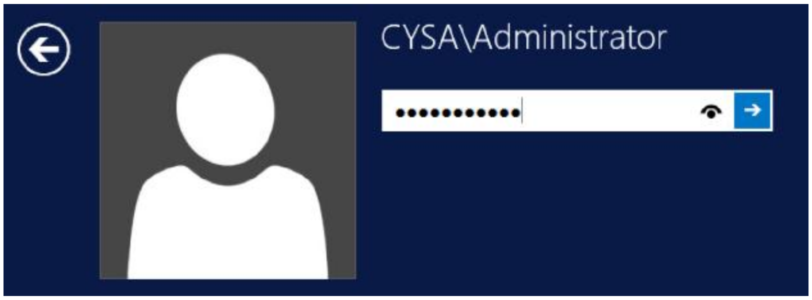
1 Utilizing Netstat to Perform System Scans

In this task, you will use netstat to scan your machine to discover which ports are open, and which processes and their PIDs are listening on those ports.

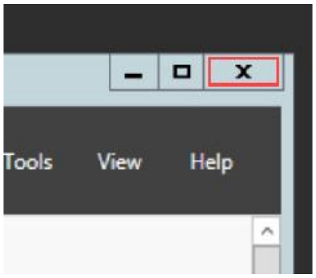
1. Launch the **2012 R2** virtual machine to access the graphical login screen.
2. Bring up the login window by sending a **Ctrl + Alt + Delete**. To do this, click the **2012 R2** drop-down menu and click **Send CTRL+ALT+DEL**.



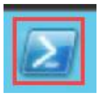
3. Log in as `CySA\Administrator` using the password `Password123`.



4. Once logged into the virtual machine, close the **Server Manager** by clicking the **x** button in the upper-right.

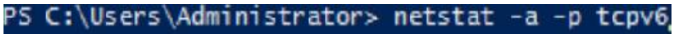


5. Click on the **PowerShell** icon on the taskbar to bring up a **Terminal** window.

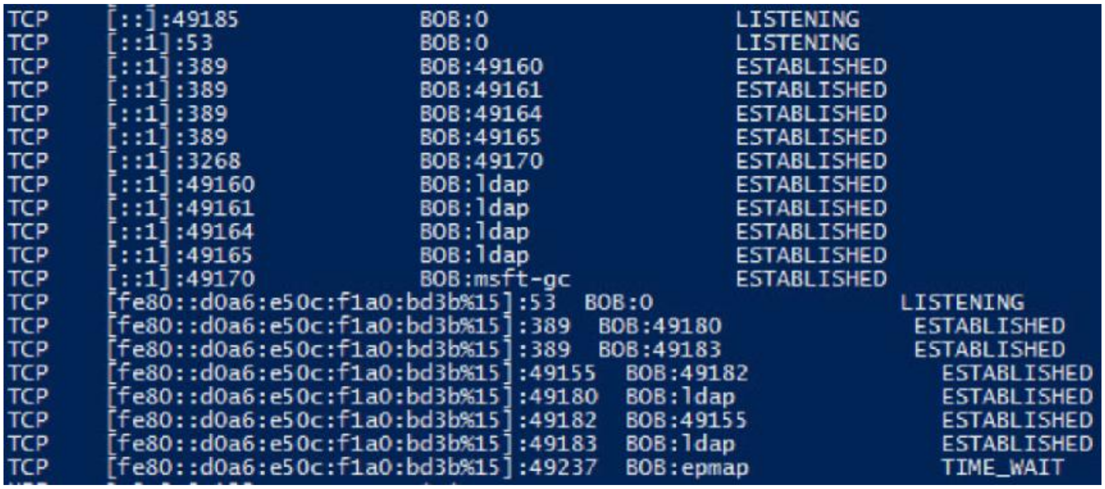


6. In **PowerShell**, enter the following command to check which ports are open. As you can see by the results, there are several ports listening and several with an ESTABLISHED status.

```
PS C:\Users\Administrator> netstat -a -p tcpv6
```



```
PS C:\Users\Administrator> netstat -a -p tcpv6
```

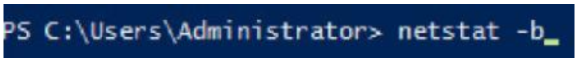


```
TCP    [::]:49185                BOB:0                 LISTENING
TCP    [::1]:53                  BOB:0                 LISTENING
TCP    [::1]:389                 BOB:49160             ESTABLISHED
TCP    [::1]:389                 BOB:49161             ESTABLISHED
TCP    [::1]:389                 BOB:49164             ESTABLISHED
TCP    [::1]:389                 BOB:49165             ESTABLISHED
TCP    [::1]:3268                BOB:49170             ESTABLISHED
TCP    [::1]:49160               BOB:ldap              ESTABLISHED
TCP    [::1]:49161               BOB:ldap              ESTABLISHED
TCP    [::1]:49164               BOB:ldap              ESTABLISHED
TCP    [::1]:49165               BOB:ldap              ESTABLISHED
TCP    [::1]:49170               BOB:msft-gc           ESTABLISHED
TCP    [fe80::d0a6:e50c:f1a0:bd3b%15]:53  BOB:0            LISTENING
TCP    [fe80::d0a6:e50c:f1a0:bd3b%15]:389  BOB:49180        ESTABLISHED
TCP    [fe80::d0a6:e50c:f1a0:bd3b%15]:389  BOB:49183        ESTABLISHED
TCP    [fe80::d0a6:e50c:f1a0:bd3b%15]:49155  BOB:49182        ESTABLISHED
TCP    [fe80::d0a6:e50c:f1a0:bd3b%15]:49180  BOB:ldap         ESTABLISHED
TCP    [fe80::d0a6:e50c:f1a0:bd3b%15]:49182  BOB:49155        ESTABLISHED
TCP    [fe80::d0a6:e50c:f1a0:bd3b%15]:49183  BOB:ldap         ESTABLISHED
TCP    [fe80::d0a6:e50c:f1a0:bd3b%15]:49237  BOB:epmap        TIME_WAIT
```

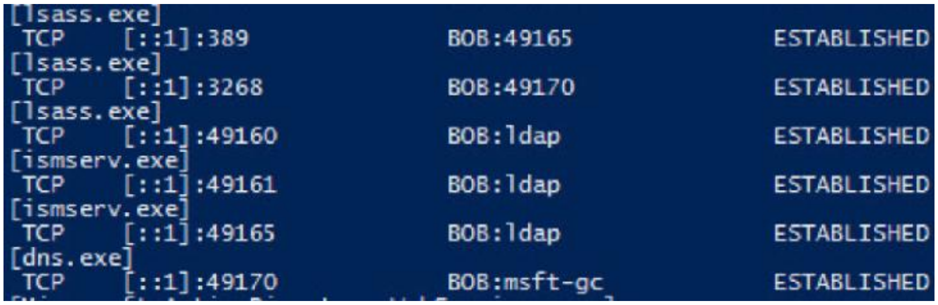
The *-a* option displays all connections and listening ports. In order to prevent every UDP port from being scanned (which will cause so much information that the relevant information will be scrolled off your screen) you will also use the *-p tcpv6* option to specify that you are only interested in TCP ports.

7. Enter the following command to examine which processes are utilizing certain ports. Note that the service name is listed on the left-hand side for each port with an *ESTABLISHED* status.

```
PS C:\Users\Administrator> netstat -b
```



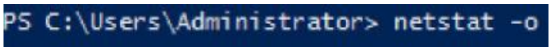
```
PS C:\Users\Administrator> netstat -b
```



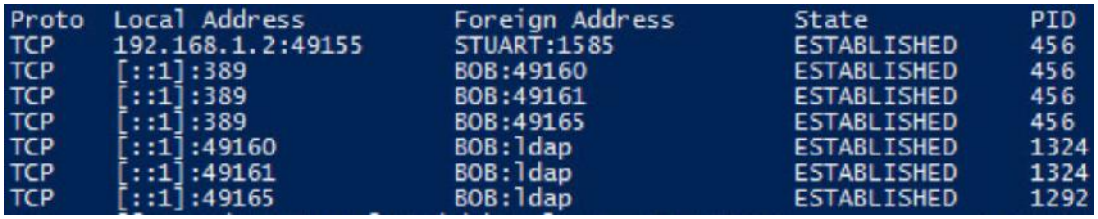
```
[lsass.exe]
 TCP    [::1]:389              BOB:49165              ESTABLISHED
[lsass.exe]
 TCP    [::1]:3268             BOB:49170              ESTABLISHED
[lsass.exe]
 TCP    [::1]:49160            BOB:ldap               ESTABLISHED
[ismserv.exe]
 TCP    [::1]:49161            BOB:ldap               ESTABLISHED
[ismserv.exe]
 TCP    [::1]:49165            BOB:ldap               ESTABLISHED
[dns.exe]
 TCP    [::1]:49170            BOB:msft-gc            ESTABLISHED
```

8. Enter the following command to see what process IDs are given to the processes listed in the previous scan. Notice you are provided with the process ID for each *ESTABLISHED* port on the right-hand side.

```
PS C:\Users\Administrator> netstat -o
```



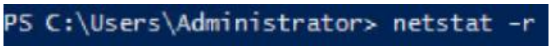
```
PS C:\Users\Administrator> netstat -o
```



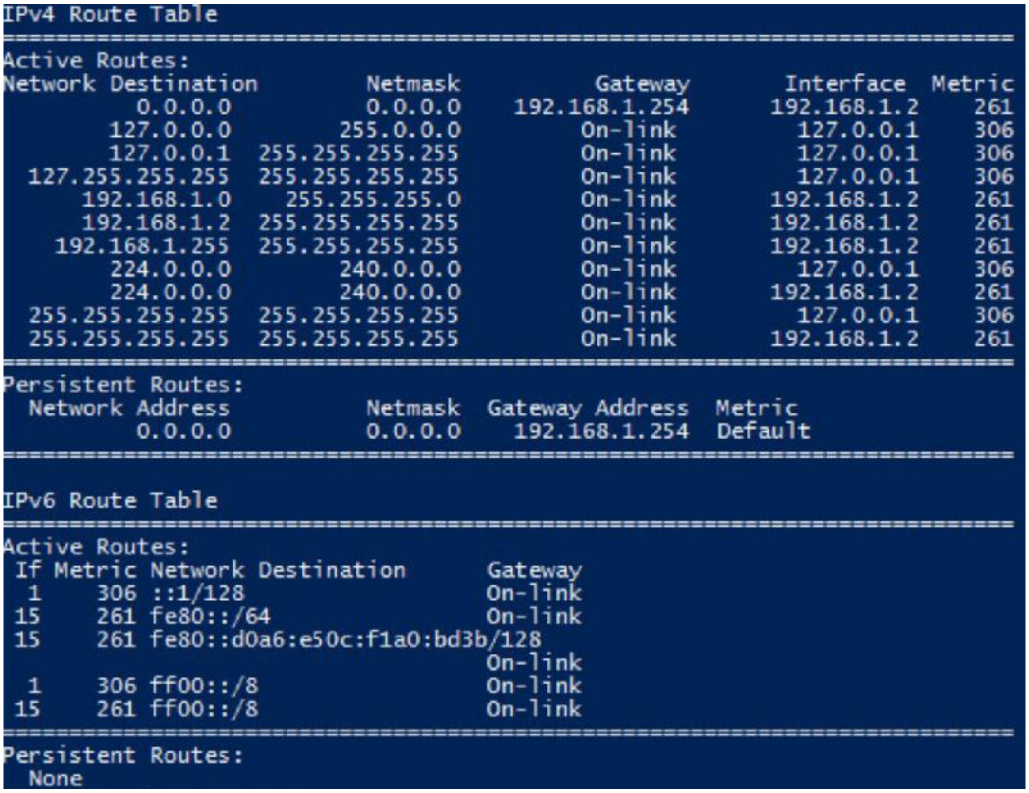
```
Proto  Local Address          Foreign Address        State           PID
TCP    192.168.1.2:49155      STUART:1585            ESTABLISHED     456
TCP    [::1]:389              BOB:49160              ESTABLISHED     456
TCP    [::1]:389              BOB:49161              ESTABLISHED     456
TCP    [::1]:389              BOB:49165              ESTABLISHED     456
TCP    [::1]:49160            BOB:ldap               ESTABLISHED     1324
TCP    [::1]:49161            BOB:ldap               ESTABLISHED     1324
TCP    [::1]:49165            BOB:ldap               ESTABLISHED     1292
```

9. Finally, the following command can be used to check the routing table with netstat. The routing table will tell you which destination traffic is being directed through which interface, along with metric for that destination. You will also see that the default route for this device is listed as 192.168.1.254.

```
PS C:\Users\Administrator> netstat -r
```



```
PS C:\Users\Administrator> netstat -r
```

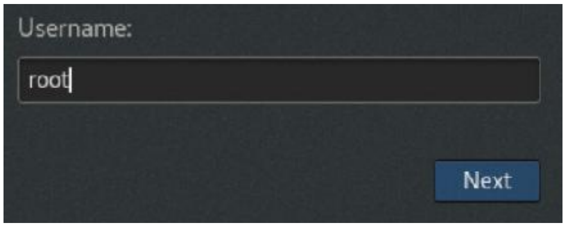


```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.1.254     192.168.1.2    261
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.1.0    255.255.255.0         On-link       192.168.1.2    261
      192.168.1.2  255.255.255.255         On-link       192.168.1.2    261
    192.168.1.255  255.255.255.255         On-link       192.168.1.2    261
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link       192.168.1.2    261
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link       192.168.1.2    261
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0    192.168.1.254  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    306 ::1/128                  On-link
 15    261 fe80::/64                On-link
 15    261 fe80::d0a6:e50c:f1a0:bd3b/128
                                    On-link
  1    306 ff00::/8                 On-link
 15    261 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

2 Performing Network Scans with Nmap

In this task, you will use nmap to scan your network and discover which hosts are available, what ports they have open and listening, what OS they are running, and other details that an intruder may be able to detect with a rogue device.

1. Launch the **Kali** virtual machine to access the graphical login screen.
2. Press **ENTER** to bring up the log in screen. Log in as `root` using the password `toor`.



Username:
root

3. Open a **Terminal** window.

4. Enter the following command to view the help page for nmap. You will need to scroll up to view the entire nmap help page content.

```
root@kali:~# nmap -h
```

```
root@kali:~# nmap -h
```

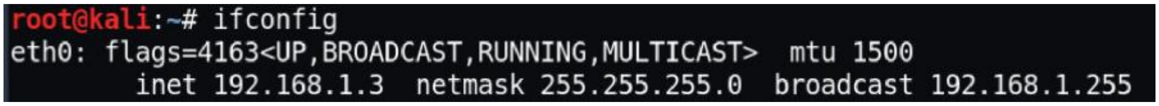
5. Enter the following command to view the man pages for nmap. Spend a few minutes reading the options for nmap and press **q** when you are finished.

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

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

6. Run the **ifconfig** command to get the host's current ip address. Note that the current IP address is *192.168.1.3* and the subnet mask is *255.255.255.0*

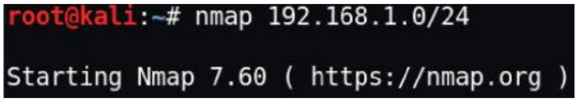
```
root@kali:~# ifconfig
```



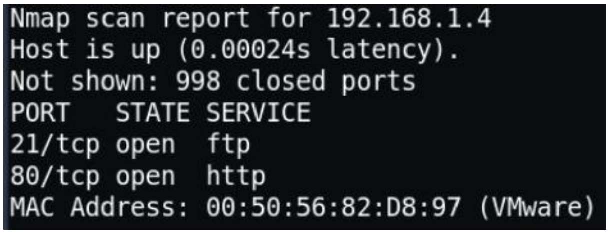
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.3  netmask 255.255.255.0  broadcast 192.168.1.255
```

7. Now that you know the network address, you can begin probing the 192.168.1.0 network with nmap. Enter the following command to display a listing of other devices on the network. Each device will have its IP and MAC address displayed, along with a listing of its open ports.

```
root@kali:~# nmap 192.168.1.0/24
```



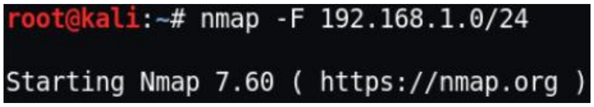
```
root@kali:~# nmap 192.168.1.0/24

Starting Nmap 7.60 ( https://nmap.org )
```



```
Nmap scan report for 192.168.1.4
Host is up (0.00024s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
MAC Address: 00:50:56:82:D8:97 (VMware)
```

8. To do a quick scan of the 192.168.1.0 network, with fewer ports tested, enter the following command:

```
root@kali:~# nmap -F 192.168.1.0/24
```

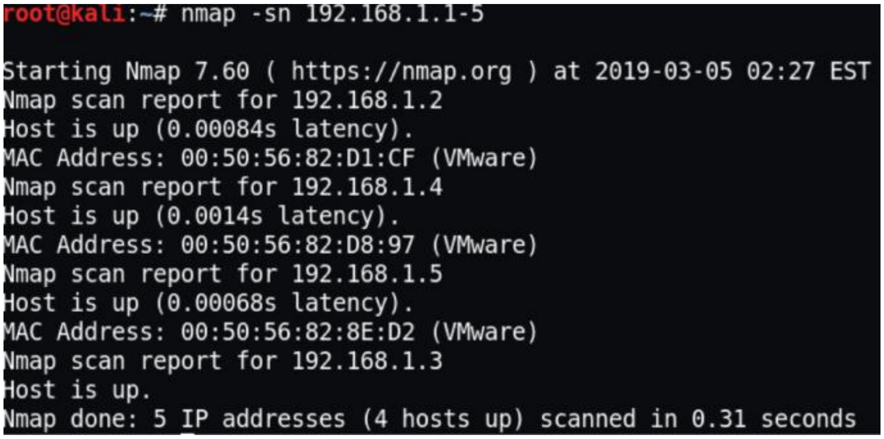


```
root@kali:~# nmap -F 192.168.1.0/24

Starting Nmap 7.60 ( https://nmap.org )
```

While the *-F* option contains much the same information that was gathered without it, the scan was much faster. This is because the *-F* option only tests the most common 100 ports. By default, Nmap scans the top 1,000 most common ports.

9. Note that only 4 hosts appeared in either of the previous two scans. With this information, you can narrow the scanning criteria to 192.168.1.1-5, as no hosts were utilizing an address higher than 192.168.1.5. Using a range will prevent the nmap scan from trying to probe every possible device on the network, potentially saving time and resources. Enter the following command to get a simple overview of which hosts are up within this range:

```
root@kali:~# nmap -sn 192.168.1.1-5
```

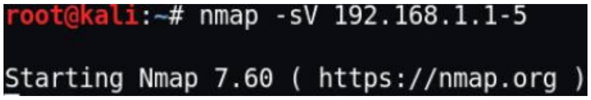


```
root@kali:~# nmap -sn 192.168.1.1-5

Starting Nmap 7.60 ( https://nmap.org ) at 2019-03-05 02:27 EST
Nmap scan report for 192.168.1.2
Host is up (0.00084s latency).
MAC Address: 00:50:56:82:D1:CF (VMware)
Nmap scan report for 192.168.1.4
Host is up (0.0014s latency).
MAC Address: 00:50:56:82:D8:97 (VMware)
Nmap scan report for 192.168.1.5
Host is up (0.00068s latency).
MAC Address: 00:50:56:82:8E:D2 (VMware)
Nmap scan report for 192.168.1.3
Host is up.
Nmap done: 5 IP addresses (4 hosts up) scanned in 0.31 seconds
```

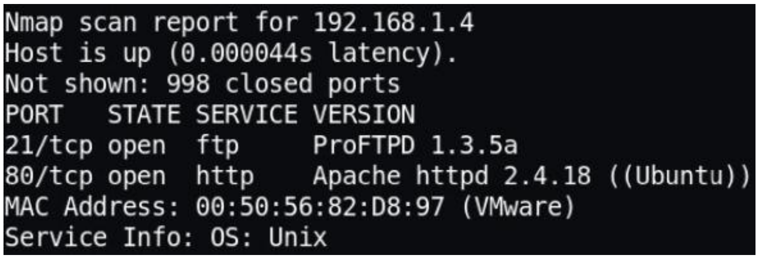
The *-sn* option performs host discovery only. Notice that the only information given is which devices are active on the network, along with their IP and MAC address. This is helpful to simply map out connected hosts.

10. When a port is open, it is being utilized by an application or service. The -sV option displays the services that are utilizing each port. It also displays information about the version for each running service, as well as OS information for each host. Enter the following command to perform a scan utilizing the -sV option:

```
root@kali:~# nmap -sV 192.168.1.1-5
```



```
root@kali:~# nmap -sV 192.168.1.1-5

Starting Nmap 7.60 ( https://nmap.org )
```

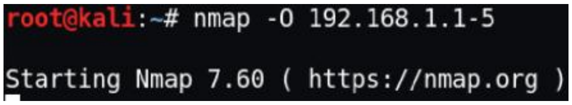


```
Nmap scan report for 192.168.1.4
Host is up (0.000044s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5a
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 00:50:56:82:D8:97 (VMware)
Service Info: OS: Unix
```

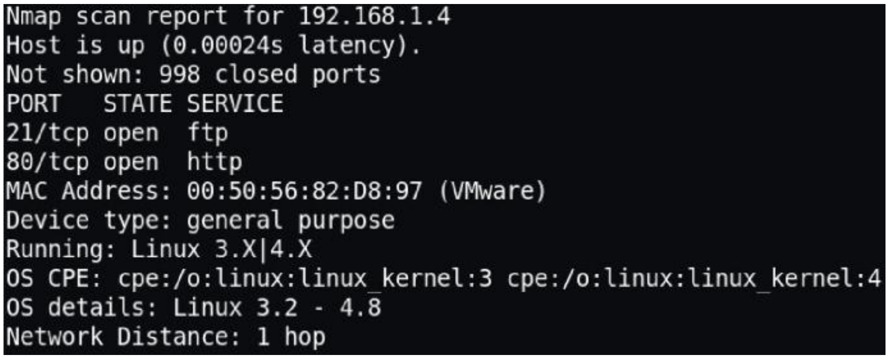
Note that this scan may take 1-2 minutes to complete.

11. To gain more detailed information about the OS being run by devices on the 192.168.1.0 network, use the following command. Note that this provides more information about the OS, as well as the number of hops away that the host is from your current network position.

```
root@kali:~# nmap -O 192.168.1.1-5
```



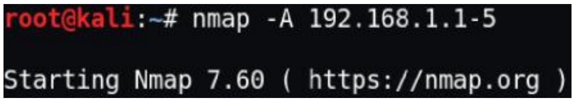
```
root@kali:~# nmap -O 192.168.1.1-5

Starting Nmap 7.60 ( https://nmap.org )
```



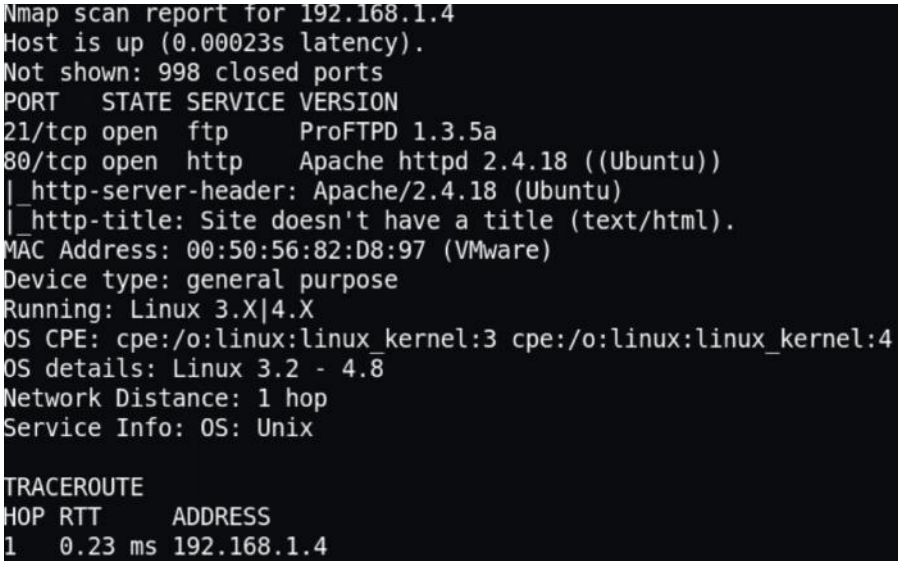
```
Nmap scan report for 192.168.1.4
Host is up (0.00024s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
MAC Address: 00:50:56:82:D8:97 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
Network Distance: 1 hop
```

12. To perform a detailed scan of the network, enter the following command. You may close the **Terminal** window when you are finished examining the results.

```
root@kali:~# nmap -A 192.168.1.1-5
```



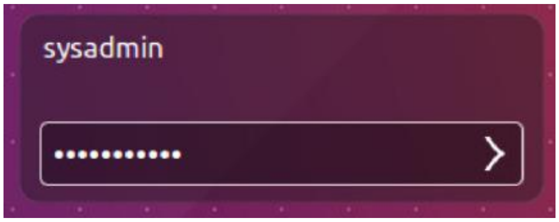
```
root@kali:~# nmap -A 192.168.1.1-5

Starting Nmap 7.60 ( https://nmap.org )
```



```
Nmap scan report for 192.168.1.4
Host is up (0.00023s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5a
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:50:56:82:D8:97 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
Network Distance: 1 hop
Service Info: OS: Unix

TRACEROUTE
HOP RTT     ADDRESS
1   0.23 ms 192.168.1.4
```

> Note that this scan will take 2-3 minutes to complete. This is because the *-A* option provides more information than any of the other options you have explored. This information includes OS detection, version detection, script scanning, and a traceroute. Using this option on a network with many hosts can cause a significant delay.

13. Launch the **Ubuntu** virtual machine to access the graphical login screen.
14. Log in as `sysadmin` using the password `Password123`.



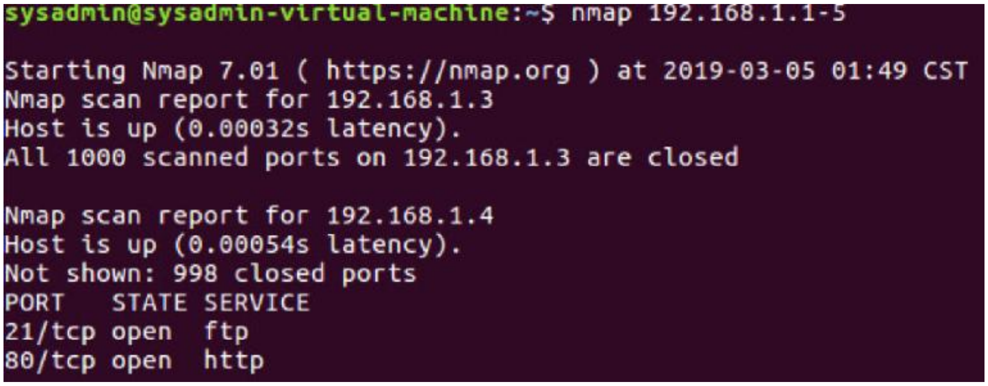
sysadmin

••••••••••••

15. Open a **Terminal** window.

16. Scan the 192.168.1.0 network from this host by entering the following command. Note the differences between the scan made from the Kali VM in step 7. Specifically, that 192.168.1.2 is not displayed at all, and that the Kali VM (192.168.1.3) is. Also, note that the Kali VM has all of its ports closed. Despite 192.168.1.2 not showing up on this probe, you know from probes on the Kali machine that there is a host with this IP address on the 192.168.1.0 network.

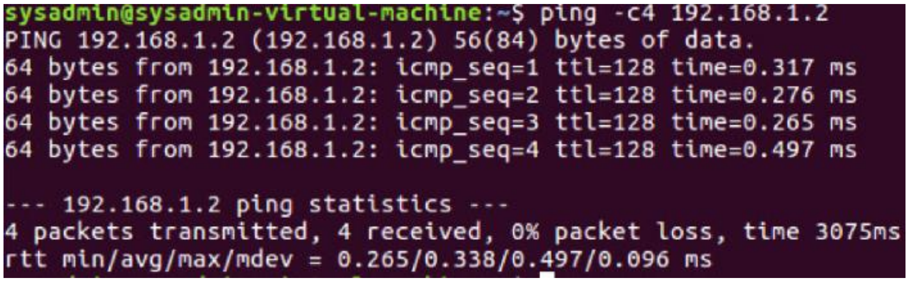
```
sysadmin@sysadmin-virtual-machine:~$ nmap 192.168.1.1-5
```



```
sysadmin@sysadmin-virtual-machine:~$ nmap 192.168.1.1-5

Starting Nmap 7.01 ( https://nmap.org ) at 2019-03-05 01:49 CST
Nmap scan report for 192.168.1.3
Host is up (0.00032s latency).
All 1000 scanned ports on 192.168.1.3 are closed

Nmap scan report for 192.168.1.4
Host is up (0.00054s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
21/tcp open  ftp
80/tcp open  http
```

17. Test to see if you can communicate with 192.168.1.2 with an icmp request using the following command. In this command, the -c option specifies the count or number of ping requests sent. Without using this option, your ping would continue on until manually cancelled. Notice that responses are received for each packet with a 0% packet loss, demonstrating that a host is responding to your ping requests.

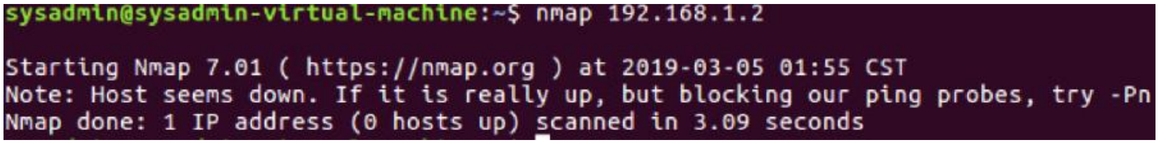
```
sysadmin@sysadmin-virtual-machine:~$ ping -c4 192.168.1.2
```



```
sysadmin@sysadmin-virtual-machine:~$ ping -c4 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=128 time=0.317 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=128 time=0.276 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=128 time=0.265 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=128 time=0.497 ms

--- 192.168.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3075ms
rtt min/avg/max/mdev = 0.265/0.338/0.497/0.096 ms
```

18. To better understand 192.168.1.2’s absence in the nmap scan performed in step 16, attempt an nmap scan on 192.168.1.2 specifically. Note the error message that nmap gives you, denoting that a firewall may be stopping nmap from working correctly. Enter the following command:

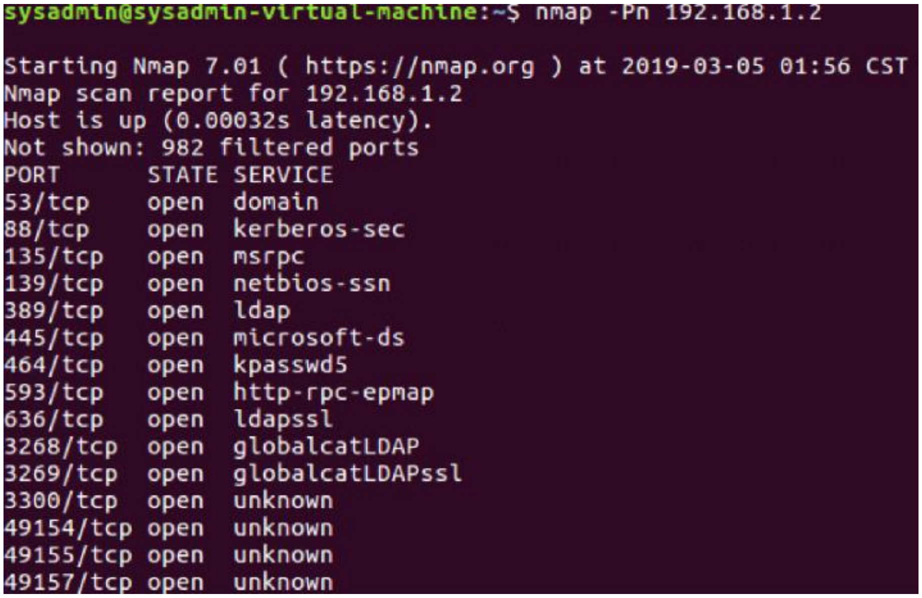
```
sysadmin@sysadmin-virtual-machine:~$ nmap 192.168.1.2
```



```
sysadmin@sysadmin-virtual-machine:~$ nmap 192.168.1.2

Starting Nmap 7.01 ( https://nmap.org ) at 2019-03-05 01:55 CST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds
```

19. Following nmap's recommendation, scan 192.168.1.2 once more with the -Pn option. Once you have finished examining the results, you may close the **Terminal** window.

```
sysadmin@sysadmin-virtual-machine:~$ nmap -Pn 192.168.1.2
```



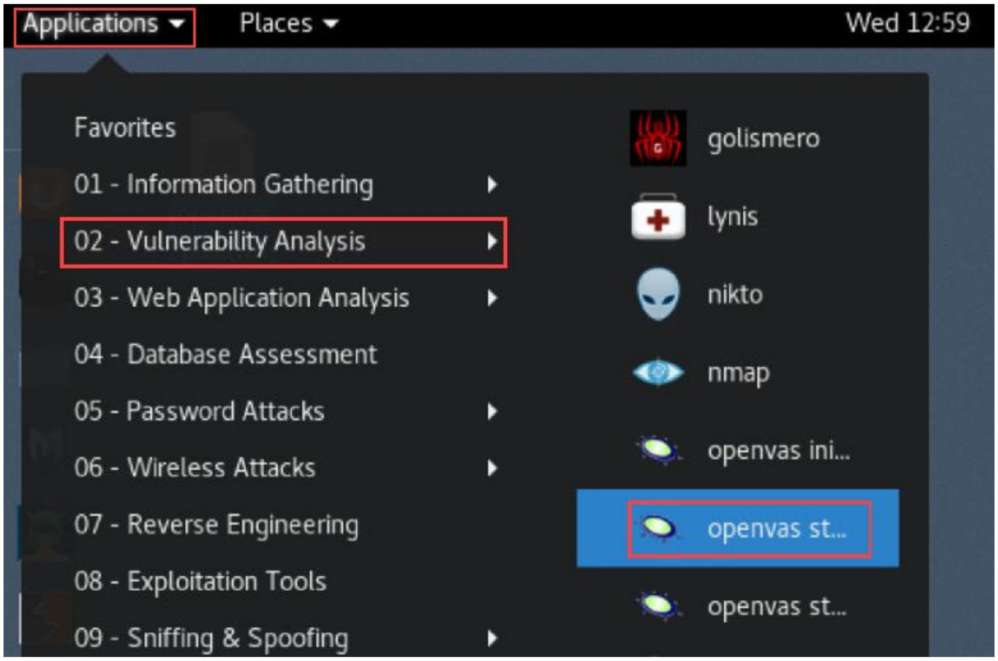
```
sysadmin@sysadmin-virtual-machine:~$ nmap -Pn 192.168.1.2

Starting Nmap 7.01 ( https://nmap.org ) at 2019-03-05 01:56 CST
Nmap scan report for 192.168.1.2
Host is up (0.00032s latency).
Not shown: 982 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3300/tcp  open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
```

This scan returns a successful probe of 192.168.1.2's open ports. This is because the *-Pn* option for nmap skips the host discovery portion of the process and continues to probe for open ports as if the device had responded to the icmp request.

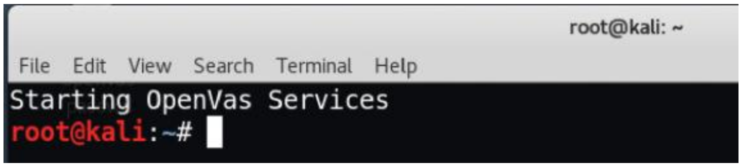
3 Performing a Vulnerability Scan with OpenVAS

In this task, you will use OpenVAS to perform a vulnerability scan with a GUI and analyze the vulnerability results.

1. Return to the **Kali VM**.
2. Start OpenVAS by clicking on **Application**-> **Vulnerability Analysis**-> **OpenVAS start**.

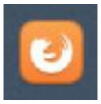


3. Wait until you see a prompt appear after the *Starting OpenVas Services* message.

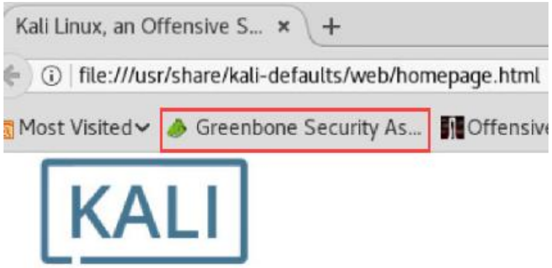


```
Starting OpenVas Services
root@kali:~#
```

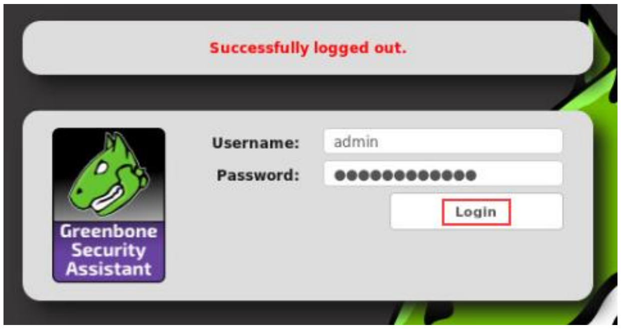
4. Click on the **Firefox** icon.



5. In the Bookmarks toolbar, click on **Greenbone Security Assistant**.


Kali Linux, an Offensive S...
file:///usr/share/kali-defaults/web/homepage.html
Most Visited
Greenbone Security As...
Offensive
KALI

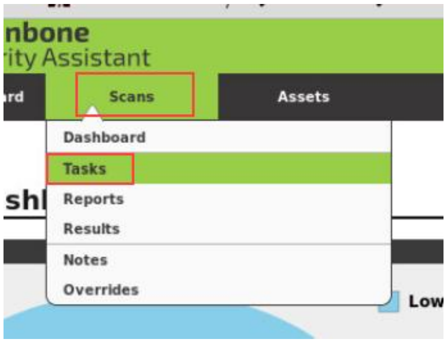
6. Click on **login**. If the credentials aren't saved, the username is **admin,** and the password is **greenbonendg**.


Successfully logged out.

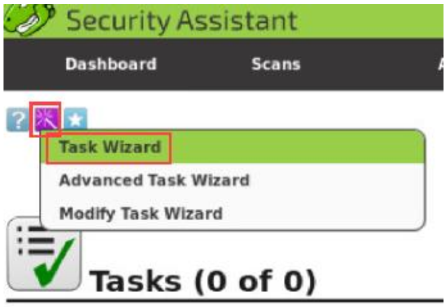
Username: admin

Password: ●●●●●●●●●●●●

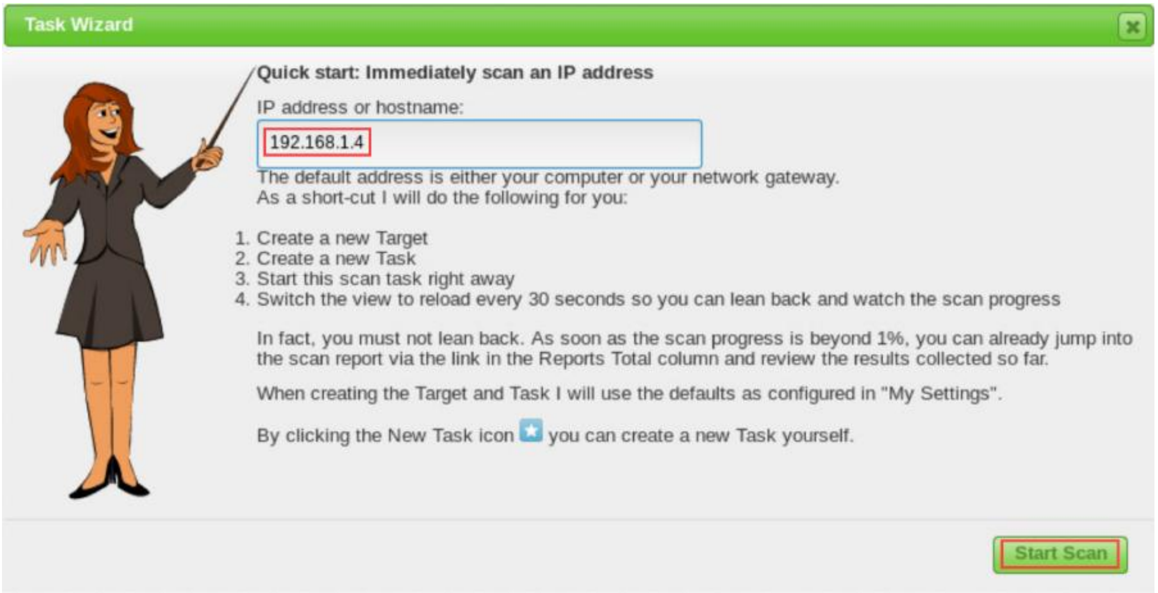
7. Once logged in, in the menu bar at the top of the screen, navigate to **Scans**-> **Tasks.**



8. Hover over the **Task Wizard** icon in the upper-left of the screen and select **Task Wizard**.



9. In the wizard, enter the IP address for the **Ubuntu** machine. In this case, it is **192.168.1.4**. Click **Start Scan**.



Quick start: Immediately scan an IP address

IP address or hostname:

192.168.1.4

The default address is either your computer or your network gateway.
As a short-cut I will do the following for you:

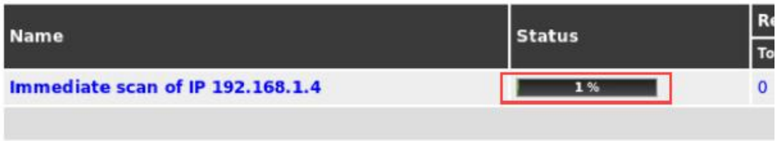
1. Create a new Target
2. Create a new Task
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

When creating the Target and Task I will use the defaults as configured in "My Settings".

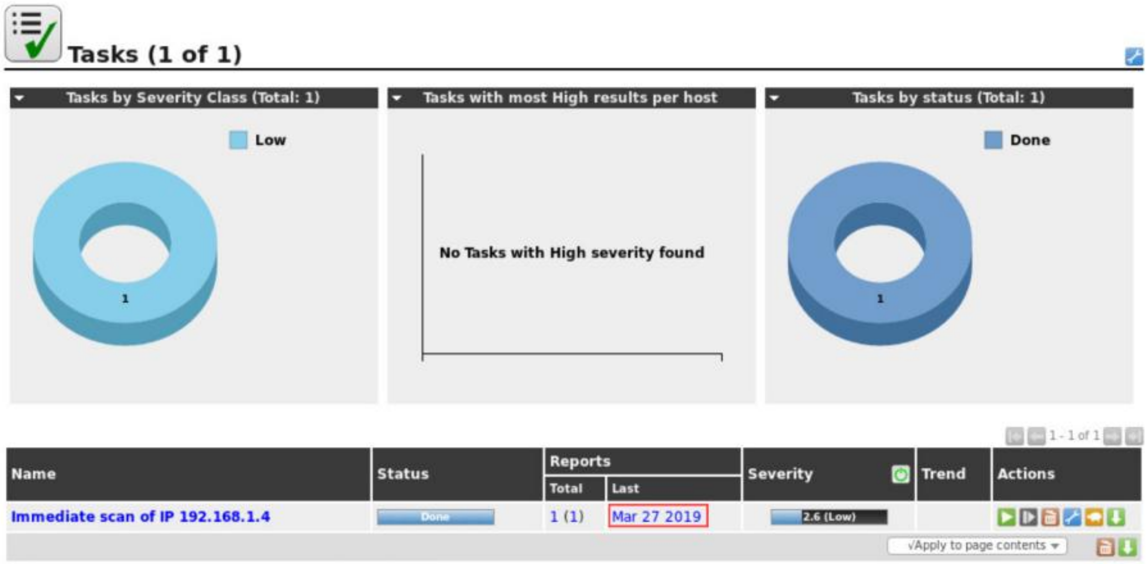
By clicking the New Task icon you can create a new Task yourself.

This step will take approximately 5 minutes to complete. While you wait, you can monitor the status of the scan:



Name	Status	Re To
Immediate scan of IP 192.168.1.4	1 %	0

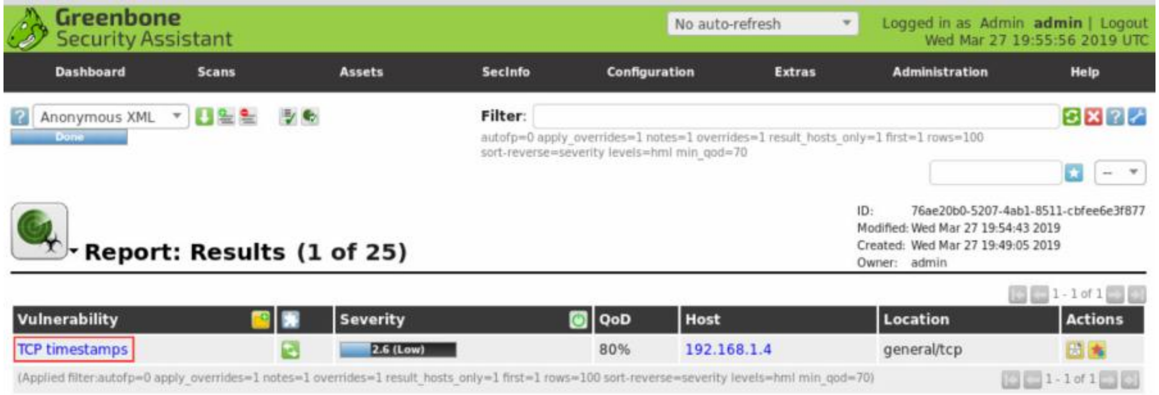
10. Once the scan finishes, the status will change to *Done*. View the scan report by clicking on the date of the last report under the **Reports** category.


Tasks (1 of 1)

Tasks by Severity Class (Total: 1)
Low
1
Tasks with most High results per host
No Tasks with High severity found
Tasks by status (Total: 1)
Done
1
1 - 1 of 1

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 192.168.1.4	Done	1 (1)	Mar 27 2019	2.6 (Low)		

11. Here, you can view the vulnerabilities detected. To see the details for a vulnerability, click on the name of the vulnerability. In this instance, it is **TCP timestamps**.



autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

Report: Results (1 of 25)

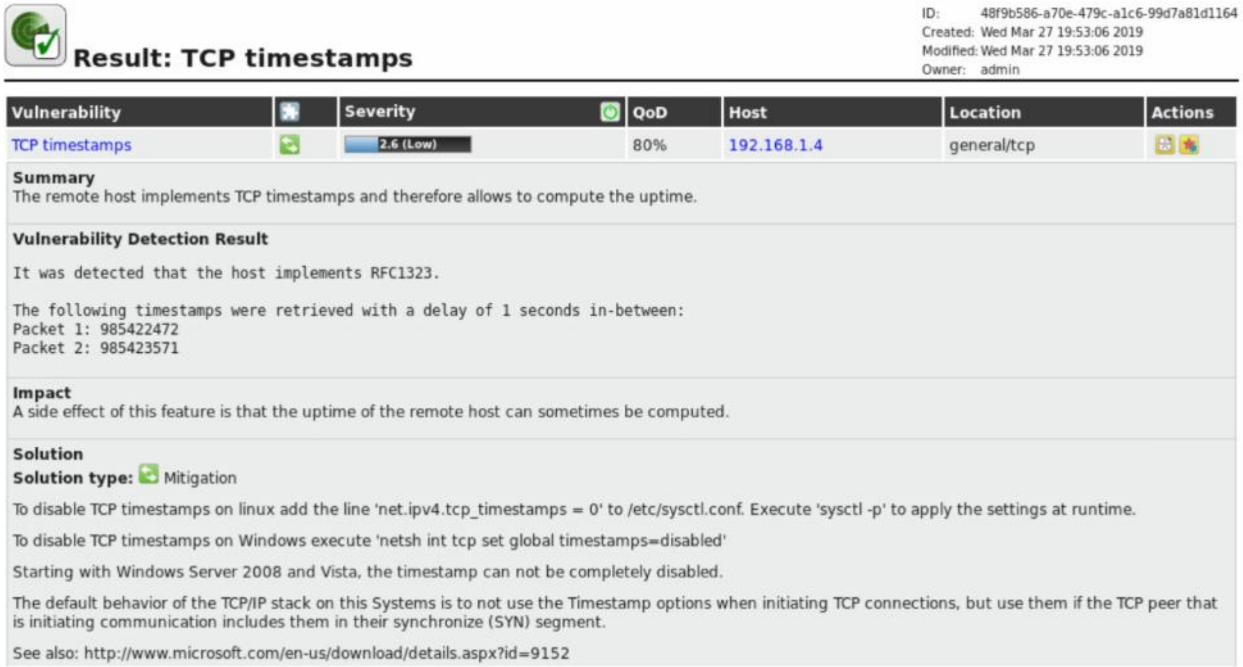
ID: 76ae20b0-5207-4ab1-8511-cbfee6e3f877
Modified: Wed Mar 27 19:54:43 2019
Created: Wed Mar 27 19:49:05 2019
Owner: admin

1 - 1 of 1

Vulnerability		Severity	QoD	Host	Location	Actions
TCP timestamps		2.6 (Low)	80%	192.168.1.4	general/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70) 1 - 1 of 1

12. Click on **TCP timestamps** to view the details pertaining to this specific vulnerability.



Result: TCP timestamps

ID: 48f9b586-a70e-479c-a1c6-99d7a81d1164
Created: Wed Mar 27 19:53:06 2019
Modified: Wed Mar 27 19:53:06 2019
Owner: admin

Vulnerability		Severity	QoD	Host	Location	Actions
TCP timestamps		2.6 (Low)	80%	192.168.1.4	general/tcp	

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 985422472
Packet 2: 985423571
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

13. This concludes the lab. You may now end the reservation.