CS 3339 Cyber Security Lab

Lab 5: Scanning and Reconnaissance

Introduction

The key to successfully exploit or intrude a remote system is about the information you have. The first step for penetration is the scanning and reconnaissance. In this lab, you will learn how to use tools to scan and retrieve information from a targeting system. You will be using *nmap* and *OpenVAS* to scan a vulnerable machine and identify exploits that can be used to attack it. We will use two Linux virtual machines: One is a Kali Linux with *nmap* and *OpenVAS*; and the other one is intentionally vulnerable Linux. We will use the *nmap* and *OpenVAS* on Kali Linux to scan the vulnerable Linux machine.

Software Requirements

- VirtualBox
  https://www.virtualbox.org/wiki/Downloads

- The Kali Linux, Penetration Testing Distribution from LAB 1

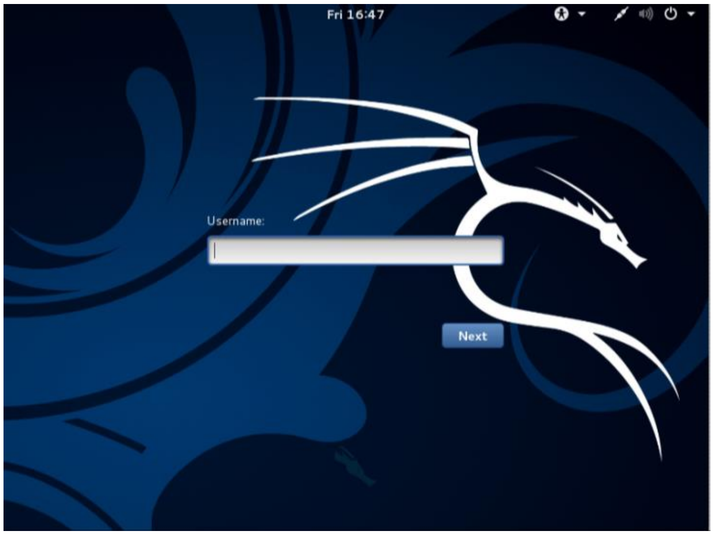
- Metasploitable2: Vulnerable Linux Platform
  https://s2.smu.edu/~rtumac/cs3339/Lab3/Metasploitable2-Linux.ova
  http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

- nmap: the Network Mapper - Free Security Scanner
  https://nmap.org/

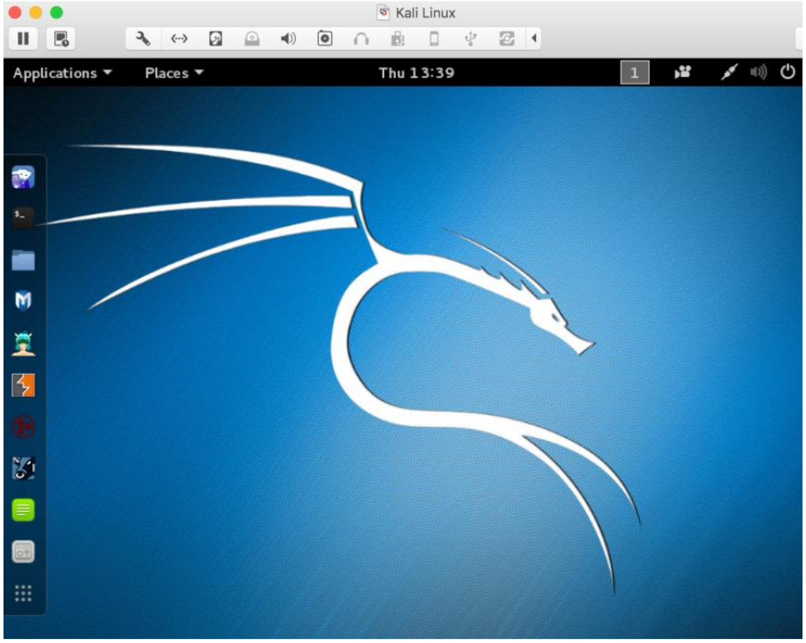
- OpenVAS: Open Vulnerability Assessment System
  http://www.openvas.org/index.htm

Starting the Lab 3 Virtual Machines

We need to use two VMs for this lab: the Kali Linux and the Metasploitable2-Linux. First, import the new Kali Linux VM and start the machine.

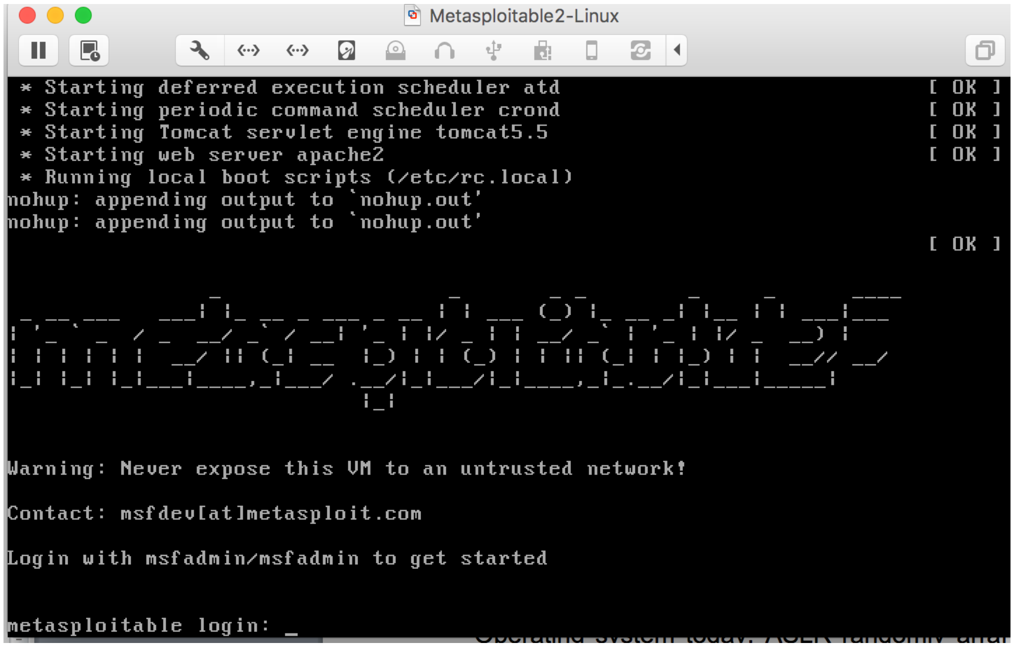


Login the Kali Linux with username root, and password CS3339. Below is the screen snapshot after login



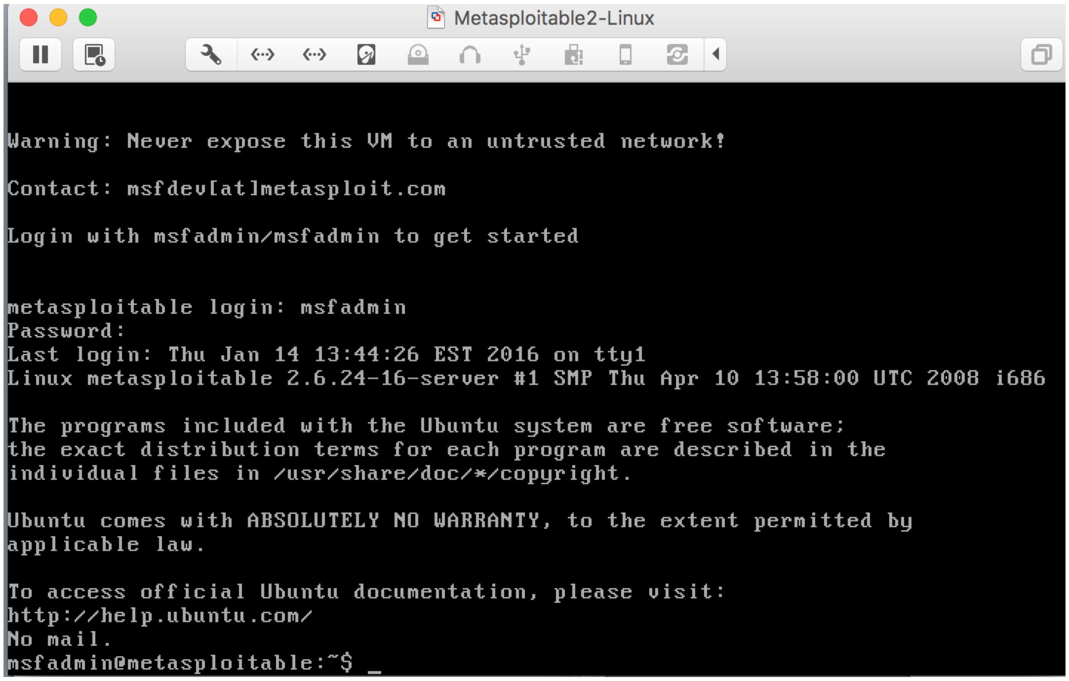
Then, import and start up the **Metasploitble2-Linux** virtual machine. This is an intentionally vulnerable Linux VM that you will attack against.

Log into the virtual machine with username, msfadmin, and password msfperunaadmin.



```
 * Starting deferred execution scheduler atd                            [ OK ]
 * Starting periodic command scheduler crond                            [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                             [ OK ]
 * Starting web server apache2                                          [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                        [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: _
```

After you log into the VM, you will see the screen below.



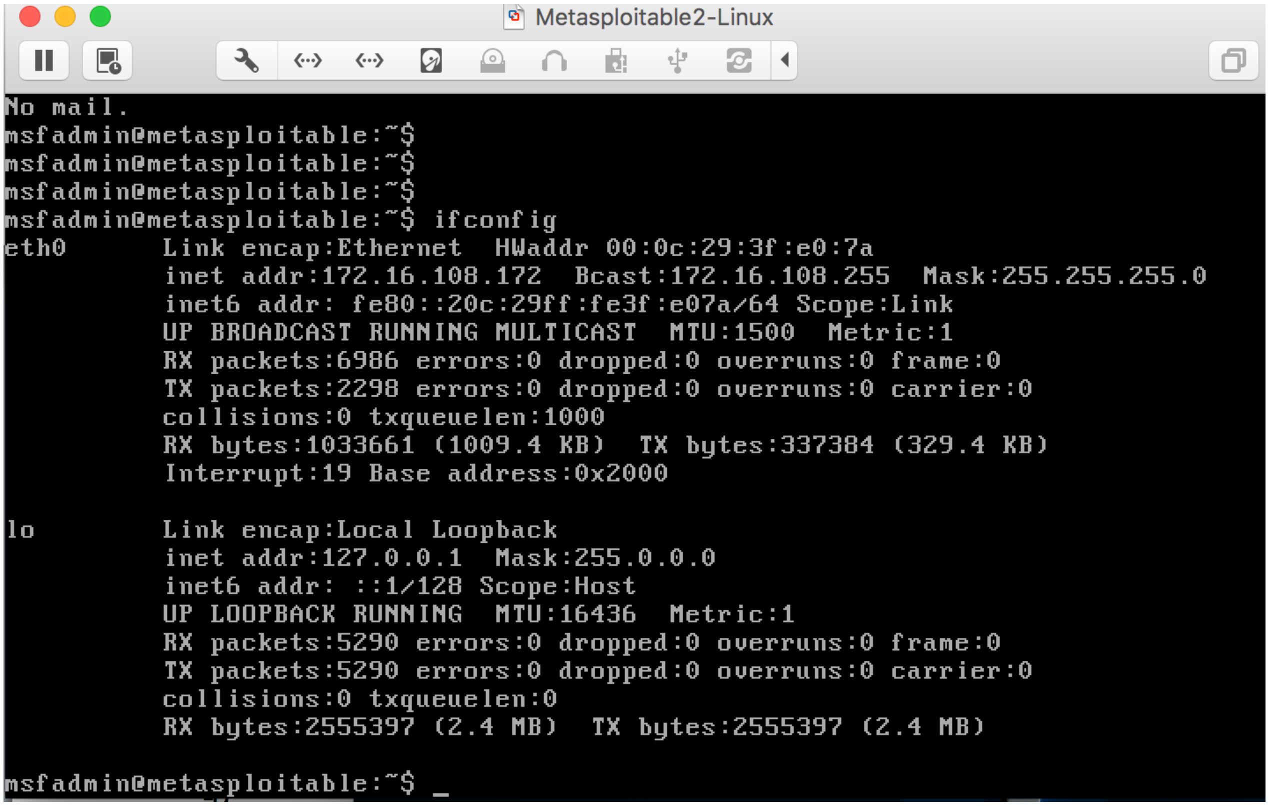
```

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Thu Jan 14 13:44:26 EST 2016 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _
```

Finding the IP Address of the Attacking Target

For the purpose of this lab, it uses Metasploitable2-Linux as the attacking target. First, we need to find the host IP address of the target to launch a scan. You can use the command "ifconfig" (ipconfig is the windows equivalent). This command allows you to find all the connected interfaces and network cards.

Go to the Metasploitable2-Linux VM, and execute the following command

$ ifconfig



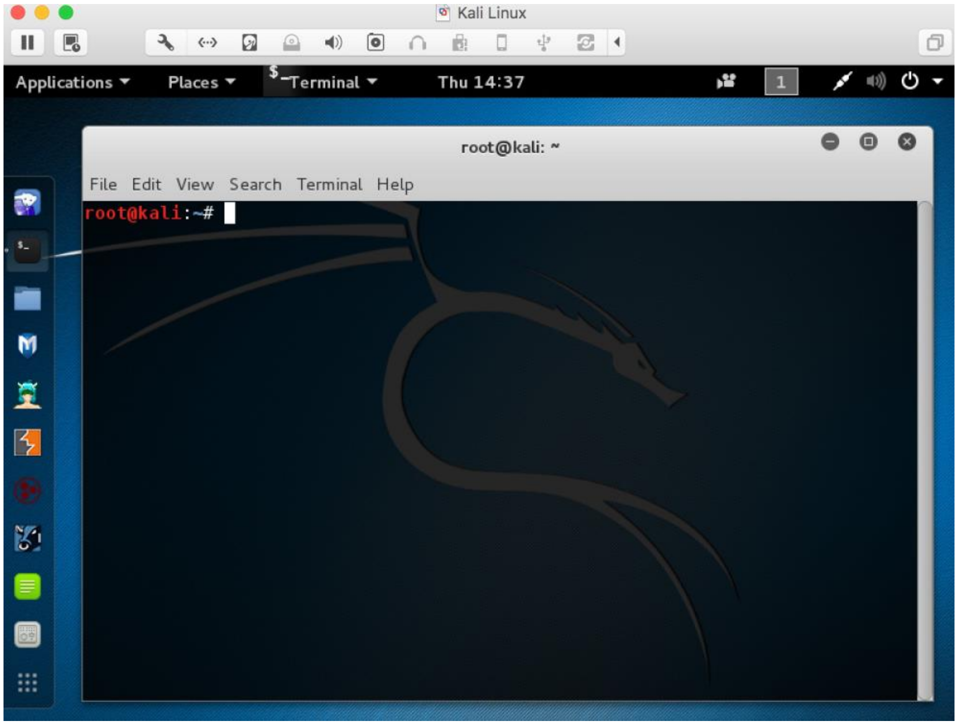
```
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:3f:e0:7a
          inet addr:172.16.108.172  Bcast:172.16.108.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe3f:e07a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6986 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2298 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1033661 (1009.4 KB)  TX bytes:337384 (329.4 KB)
          Interrupt:19 Base address:0x2000

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:5290 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5290 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2555397 (2.4 MB)  TX bytes:2555397 (2.4 MB)

msfadmin@metasploitable:~$ _
```

From the screenshot above, we can see that the IP address of the network interface, eth0, is **172.16.108.172**. This is the IP address for the target that you will use later in this lab. When you work on the lab in the classroom, you will get a different IP address for your Metaploitable2-Linux VM. Note that this is not a public IP but we can access it within the subset.

Scanning the Target Using nmap

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 for scanning the target host in this lab.

Go to the Kali Linux, and open up a terminal by clicking the icon .

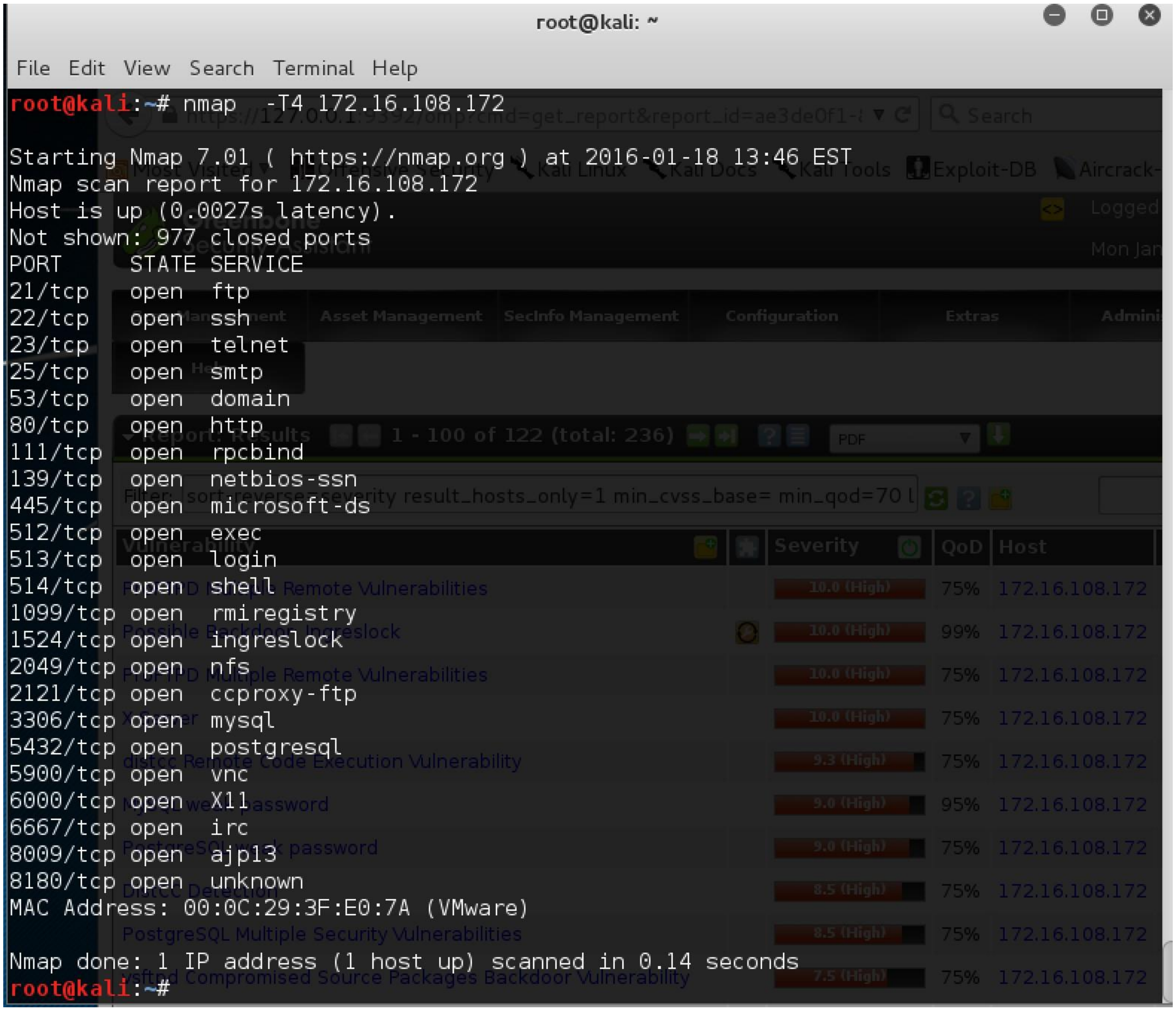


```
root@kali:~#
```

Since nmap has been installed on the Kali Linux, we can just launch the scanning in the terminal by typing the following command:

```
$ nmap -T4 172.16.108.172
```

nmap is the execution command; option **-T4** means faster execution; and **172.16.108.172** is the IP address of the target. As mentioned, you will have a different IP address when working on this with the VMs in the classroom.



```
root@kali:~# nmap  -T4 172.16.108.172

Starting Nmap 7.01 ( https://nmap.org ) at 2016-01-18 13:46 EST
Nmap scan report for 172.16.108.172
Host is up (0.0027s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:3F:E0:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
root@kali:~#
```

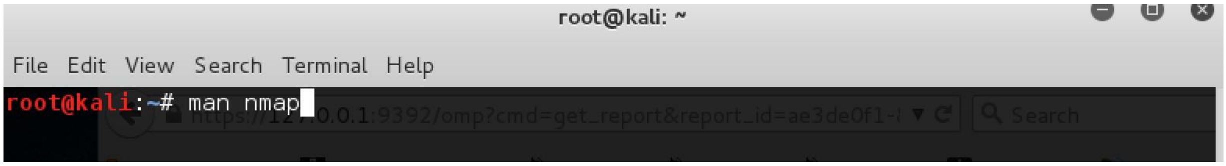
The screenshot above shows a quick scan of the target machine using **nmap**. We can see that there are many open ports and services on the target system including FTP, SSH, HTTP, and MySQL. These services may contain vulnerabilities that you can exploit.

nmap provides many useful functions that we can use. You can find more information from the man page of **nmap**

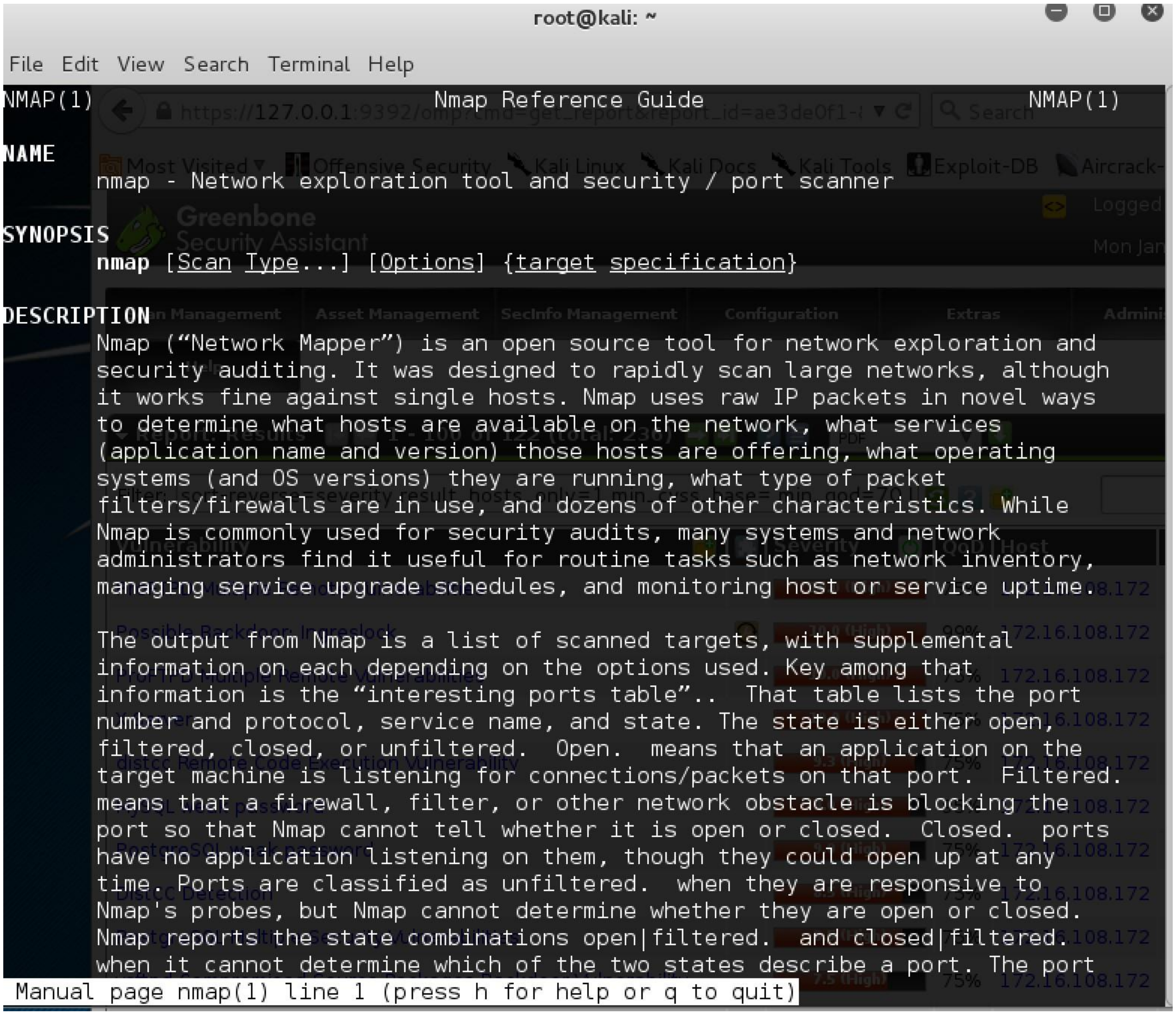
From this link: http://linux.die.net/man/1/nmap

Or execute the following command in a terminal:

$ man nmap



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



```
NMAP(1)                      Nmap Reference Guide                      NMAP(1)

NAME
       nmap - Network exploration tool and security / port scanner

SYNOPSIS
       nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
       Nmap (“Network Mapper”) is an open source tool for network exploration and
       security auditing. It was designed to rapidly scan large networks, although
       it works fine against single hosts. Nmap uses raw IP packets in novel ways
       to determine what hosts are available on the network, what services
       (application name and version) those hosts are offering, what operating
       systems (and OS versions) they are running, what type of packet
       filters/firewalls are in use, and dozens of other characteristics. While
       Nmap is commonly used for security audits, many systems and network
       administrators find it useful for routine tasks such as network inventory,
       managing service upgrade schedules, and monitoring host or service uptime.

       The output from Nmap is a list of scanned targets, with supplemental
       information on each depending on the options used. Key among that
       information is the “interesting ports table”..  That table lists the port
       number and protocol, service name, and state. The state is either open,
       filtered, closed, or unfiltered.  Open.  means that an application on the
       target machine is listening for connections/packets on that port.  Filtered.
       means that a firewall, filter, or other network obstacle is blocking the
       port so that Nmap cannot tell whether it is open or closed.  Closed.  ports
       have no application listening on them, though they could open up at any
       time. Ports are classified as unfiltered.  when they are responsive to
       Nmap's probes, but Nmap cannot determine whether they are open or closed.
       Nmap reports the state combinations open|filtered.  and closed|filtered.
       when it cannot determine which of the two states describe a port. The port
 Manual page nmap(1) line 1 (press h for help or q to quit)
```

The screenshot above shows the man page of **nmap**.

Vulnerability Scanning Using OpenVAS

OpenVAS is an open-source framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. If OpenVAS is not already installed, you can follow these steps:

root@kali:~# apt update

root@kali:~# apt install openvas

root@kali:~# openvas-setup

REMEMBER THE PASSWORD given to you when you run openvas-setup. If you don't remember the password, you can reset it by running the following command:

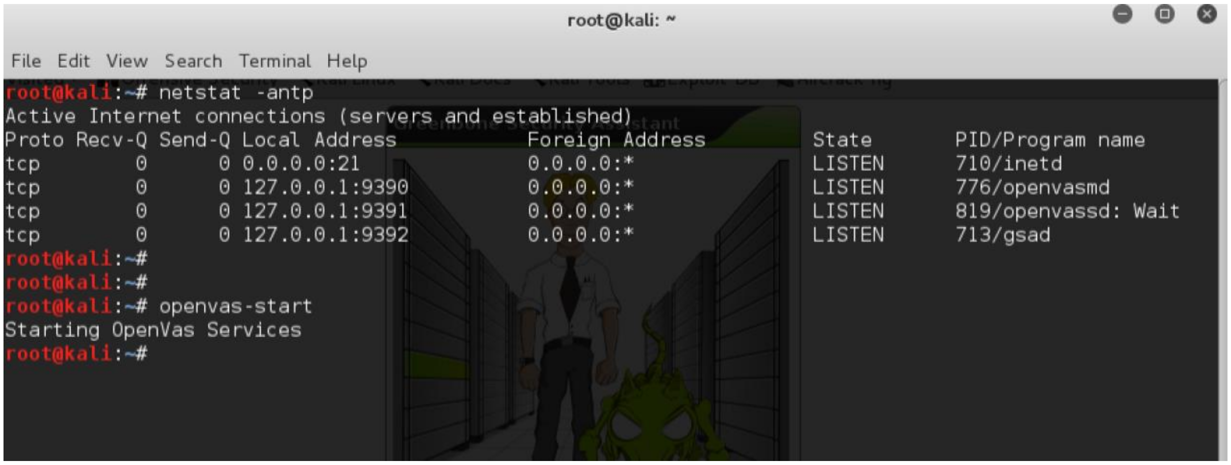
root@kali:~# openvasmd --user=admin --new-password=new-super-secure-pass

You can run the following command to check if the OpenVAS manager, scanner, and GSAD services are listening:

root@kali:~# netstat –antp

Otherwise, just start the services by executing the following command

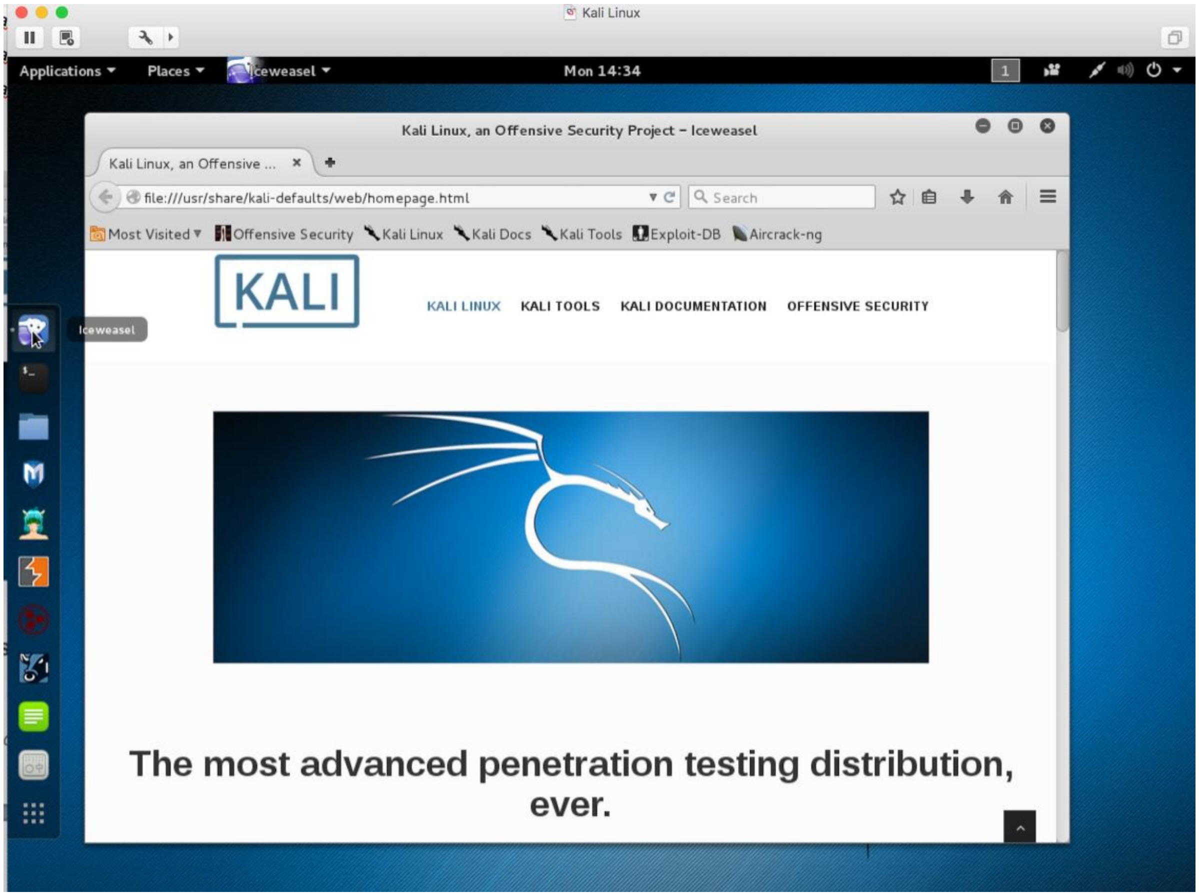
root@kali:~# openvas-start



```
root@kali:~# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      710/inetd
tcp        0      0 127.0.0.1:9390          0.0.0.0:*               LISTEN      776/openvasmd
tcp        0      0 127.0.0.1:9391          0.0.0.0:*               LISTEN      819/openvassd: Wait
tcp        0      0 127.0.0.1:9392          0.0.0.0:*               LISTEN      713/gsad
root@kali:~#
root@kali:~#
root@kali:~# openvas-start
Starting OpenVas Services
root@kali:~#
```

Connecting to the OpenVAS Web Interface

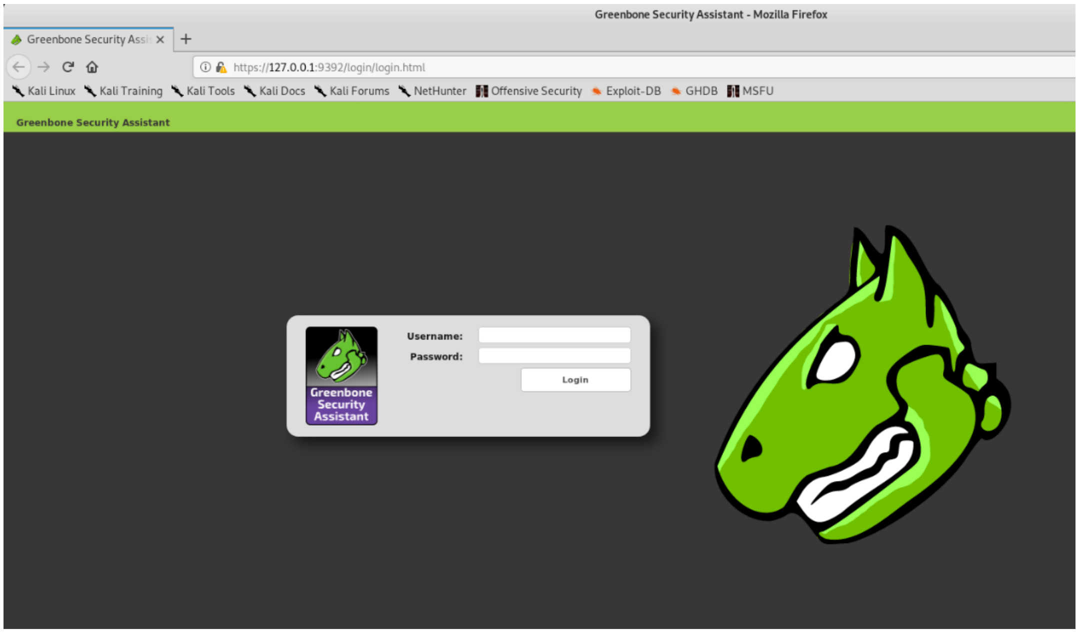
Go to the Kali Linux, and open the browser



file:///usr/share/kali-defaults/web/homepage.html

The most advanced penetration testing distribution, ever.

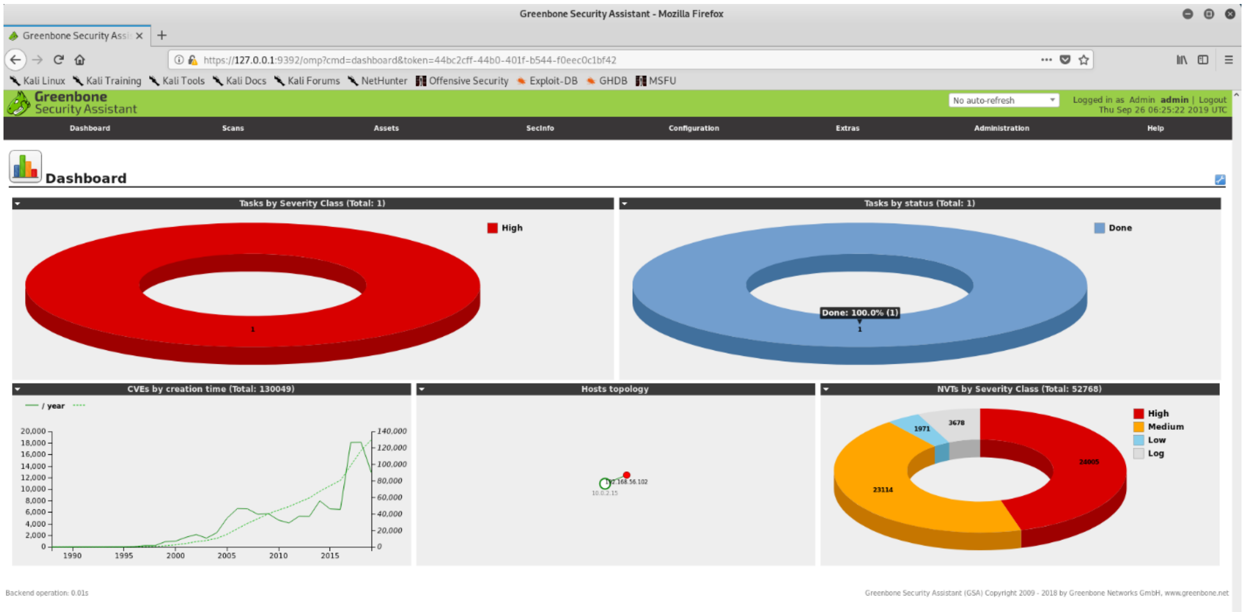
Then, go to https://127.0.0.1:9392 and accept the self-signed SSL certificate.

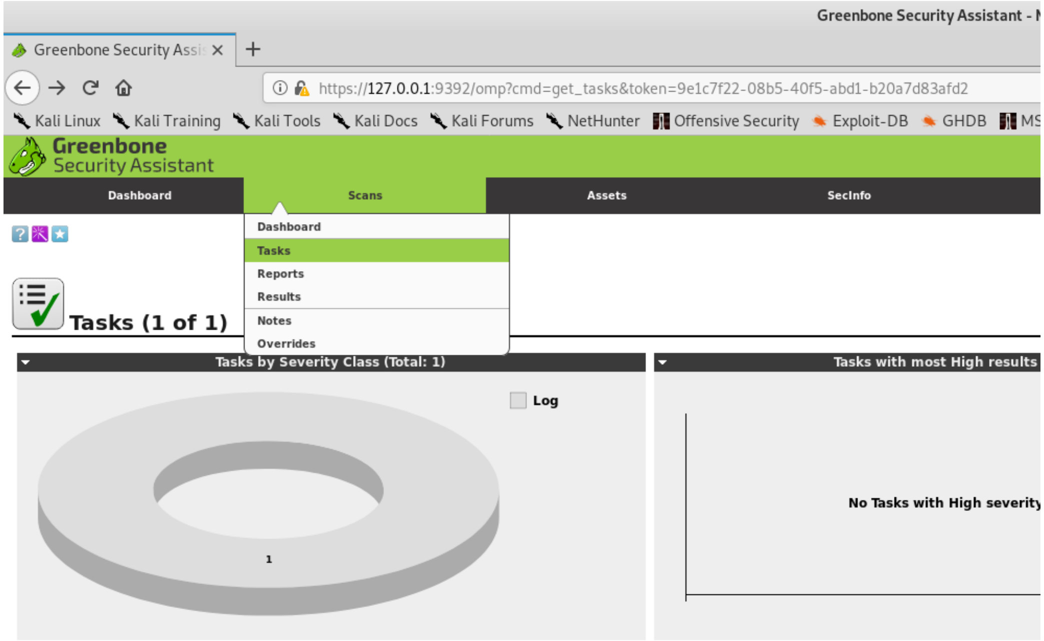


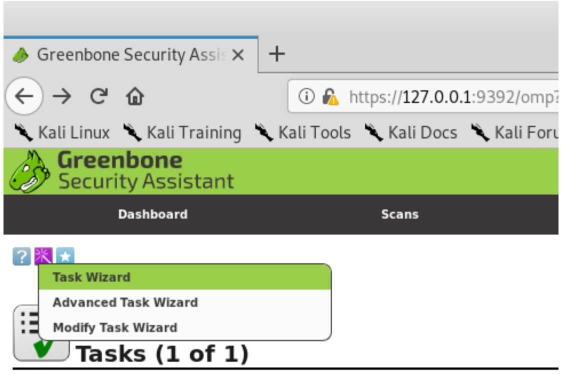
Input the username as admin, and the password given to you when you ran **openvas-setup**

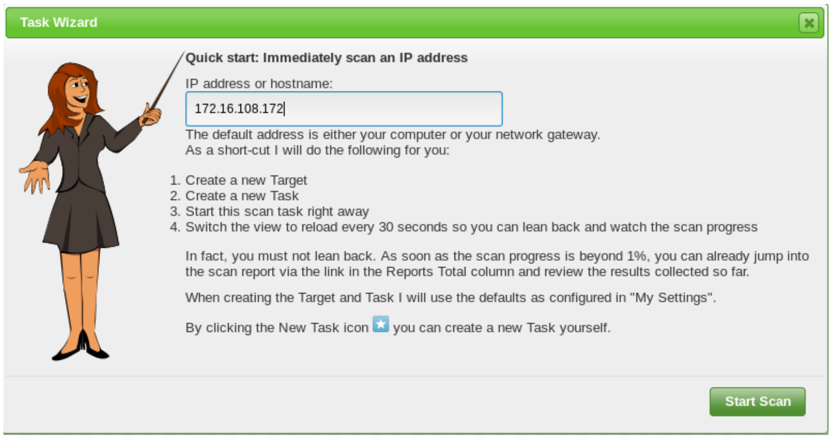
The following screenshot is the homepage of OpenVAS. Navigate to Scans -> Tasks. Then, open the Task Wizard (screenshot on next page). Type the IP address of the target in the Task Wizard, and press “Start Scan”. It will do the following for you:

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 30 seconds so you can lean back and watch the scan progress




Greenbone Security Assistant - M
Greenbone Security Assi
https://127.0.0.1:9392/omp?cmd=get_tasks&token=9e1c7f22-08b5-40f5-abd1-b20a7d83afd2
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MS
Greenbone Security Assistant
Dashboard
Scans
Assets
SecInfo
Dashboard
Tasks
Reports
Results
Notes
Overrides
Tasks (1 of 1)
Tasks by Severity Class (Total: 1)
Log
1
Tasks with most High results
No Tasks with High severity





Quick start: Immediately scan an IP address

IP address or hostname: 172.16.108.172

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

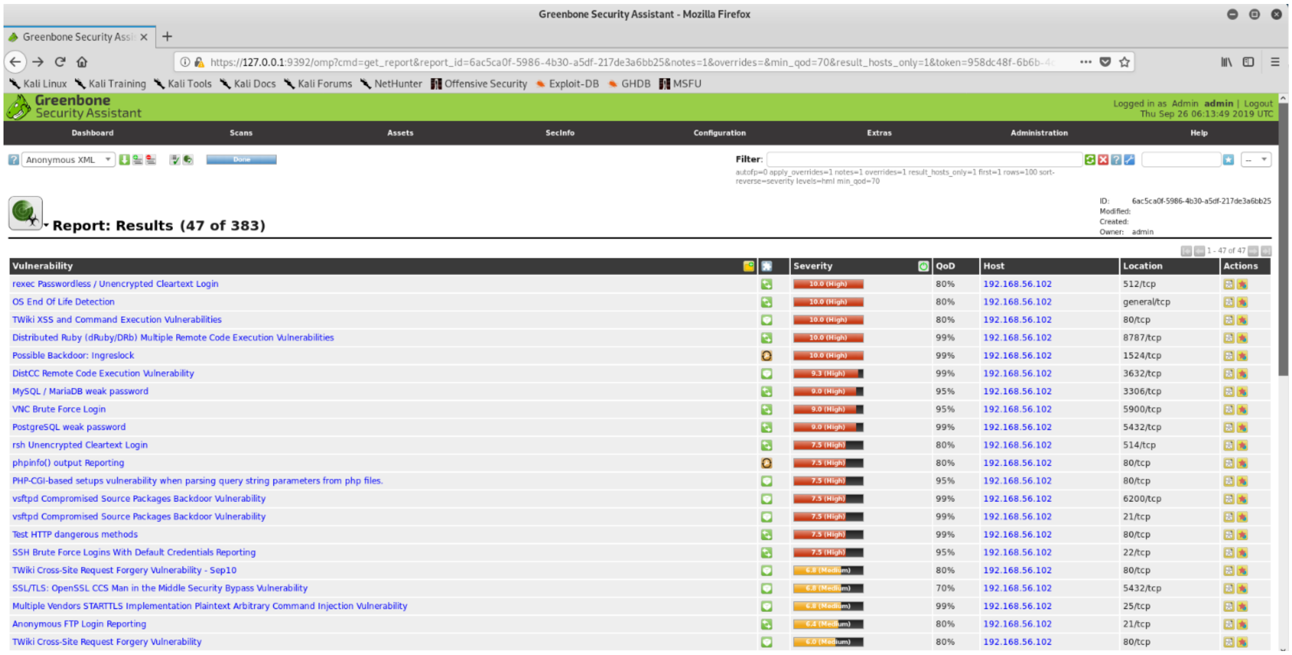
1. Create a new Target
2. Create a new Task
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

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.

After finishing the scanning, you can look at the reports (Scans -> Reports) as shown in the screenshot below.


Greenbone Security Assistant - Mozilla Firefox
Greenbone Security Assi
https://127.0.0.1:9392/omp?cmd=get_report&report_id=6ac5ca0f-5986-4b30-a5df-217de3a6bb25&notes=1&overrides=&min_qod=70&result_hosts_only=1&token=958dc48f-6b6b-4
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Greenbone Security Assistant
Logged in as Admin admin | Logout
Thu Sep 26 06:13:49 2019 UTC
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Anonymous XML
Done
Filter:
1 - 47 of 47

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 (47 of 383)

ID: 6ac5ca0f-5986-4b30-a5df-217de3a6bb25
Modified:
Created:
Owner: admin

Vulnerability		Severity	QoD	Host	Location	Actions
rexec Passwordless / Unencrypted Cleartext Login		10.0 (High)	80%	192.168.56.102	512/tcp	
OS End Of Life Detection		10.0 (High)	80%	192.168.56.102	general/tcp	
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80%	192.168.56.102	80/tcp	
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities		10.0 (High)	99%	192.168.56.102	8787/tcp	
Possible Backdoor: Ingreslock		10.0 (High)	99%	192.168.56.102	1524/tcp	
DistCC Remote Code Execution Vulnerability		9.3 (High)	99%	192.168.56.102	3632/tcp	
MySQL / MariaDB weak password		9.0 (High)	95%	192.168.56.102	3306/tcp	
VNC Brute Force Login		9.0 (High)	95%	192.168.56.102	5900/tcp	
PostgreSQL weak password		9.0 (High)	99%	192.168.56.102	5432/tcp	
rsh Unencrypted Cleartext Login		7.5 (High)	80%	192.168.56.102	514/tcp	
phpinfo() output Reporting		7.5 (High)	80%	192.168.56.102	80/tcp	
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.		7.5 (High)	95%	192.168.56.102	80/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	99%	192.168.56.102	6200/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	99%	192.168.56.102	21/tcp	
Test HTTP dangerous methods		7.5 (High)	99%	192.168.56.102	80/tcp	
SSH Brute Force Logins With Default Credentials Reporting		7.5 (High)	95%	192.168.56.102	22/tcp	
TWiki Cross-Site Request Forgery Vulnerability - Sep10		6.8 (Medium)	80%	192.168.56.102	80/tcp	
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability		6.8 (Medium)	70%	192.168.56.102	5432/tcp	
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability		6.8 (Medium)	99%	192.168.56.102	25/tcp	
Anonymous FTP Login Reporting		6.4 (Medium)	80%	192.168.56.102	21/tcp	
TWiki Cross-Site Request Forgery Vulnerability		6.0 (Medium)	80%	192.168.56.102	80/tcp	

Assignments for the Lab 3

1. Read the lab instructions above and finish all the tasks.
2. Use nmap to scan the target and find the software version of the OS and the running services (post a screenshot).
3. Use OpenVAS to find two vulnerabilities of the target, and briefly describe them. Post a screenshot with the list of vulnerabilities found by OpenVAS.

Happy Scanning