



计算机科学与工程系

Department of Computer Science and Engineering

CS 315 Computer Security Course

Lab 3: 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* installed; and the other one is intentionally vulnerable Linux. We will use the *nmap* and *OpenVAS* on Kali Linux to scan the vulnerable Linux machine.

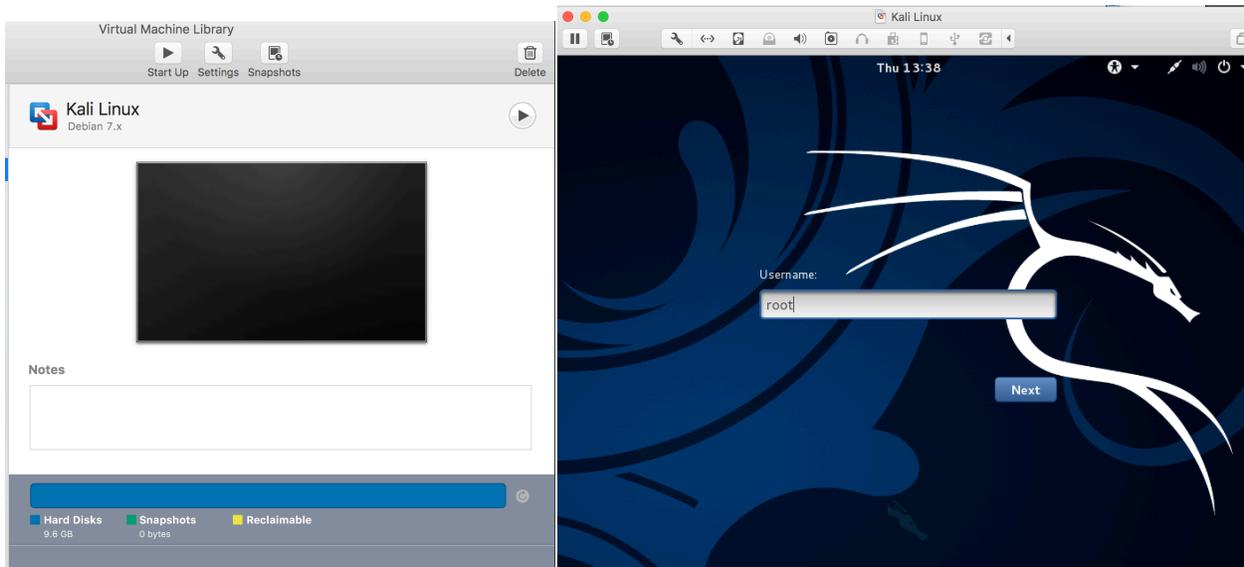
Software Requirements

- The VMWare Software
 - <https://www.vmware.com/>
- The VirtualBox Software
 - <https://www.virtualbox.org/wiki/Downloads>
 - <https://www.vmware.com/support/developer/ovf/>
 - <https://www.mylearning.be/2017/12/convert-a-vmware-fusion-virtual-machine-to-virtualbox-on-mac/>
- The Kali Linux, Penetration Testing Distribution
 - <https://www.kali.org/downloads/>
- Metasploitable2: Vulnerable Linux Platform
 - <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.html>

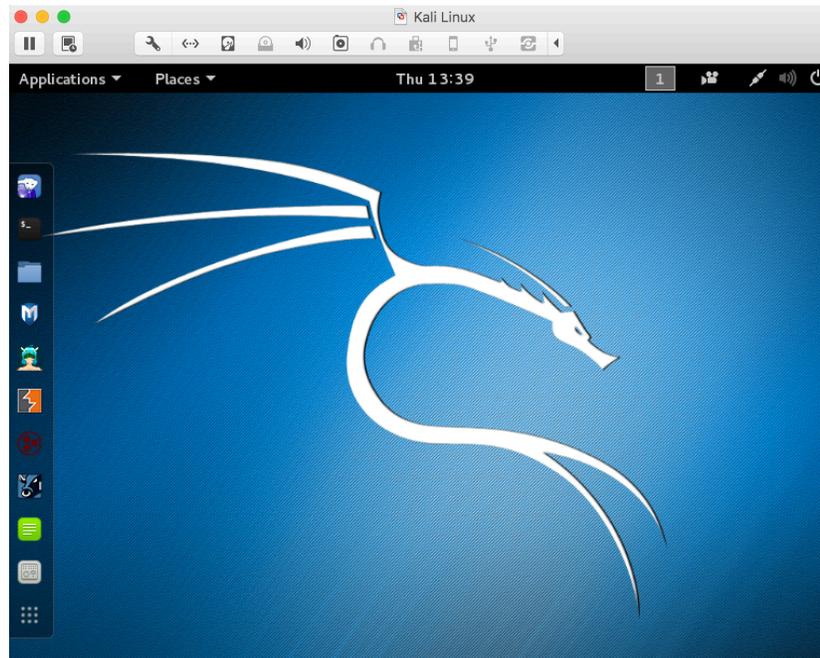
Starting the Lab 3 Virtual Machines

We need to use two VMs for this lab: the Kali Linux and the Metasploitable2-Linux.

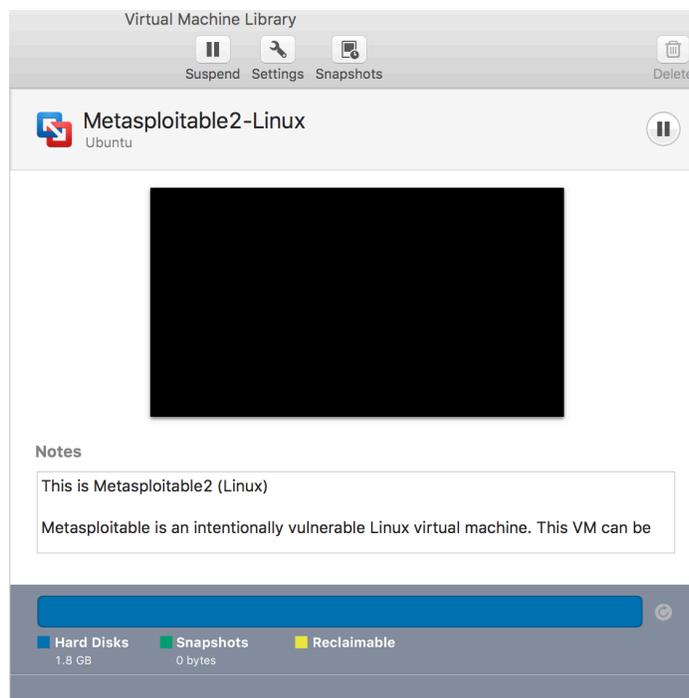
First, select the Kali Linux and press Start up



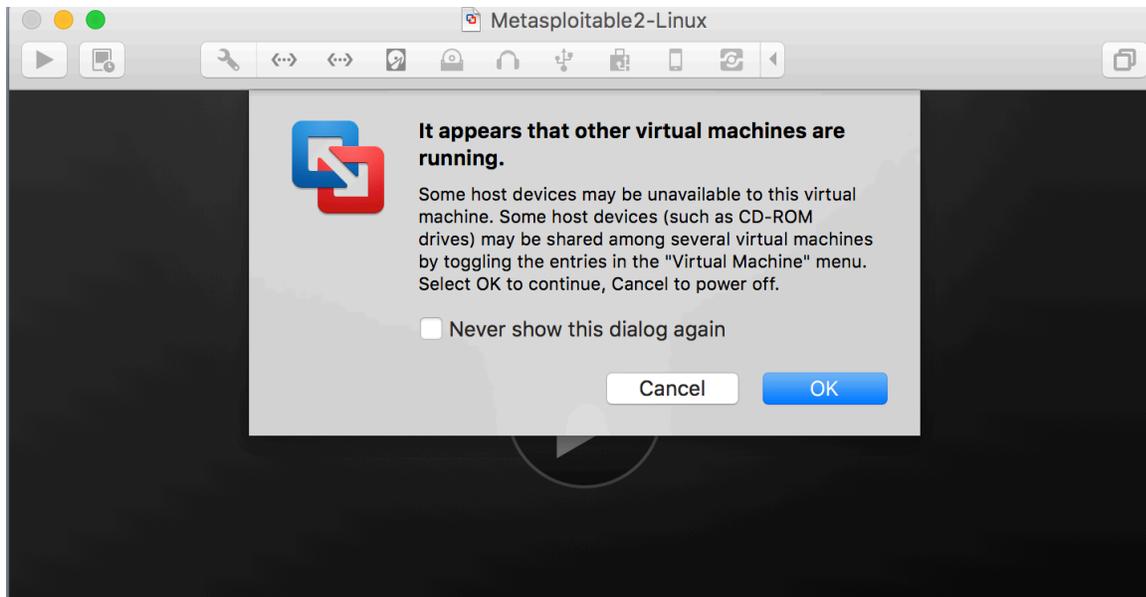
Login the Kali Linux with username root, and password [TBA in the class]. Below is the screen snapshot after login.



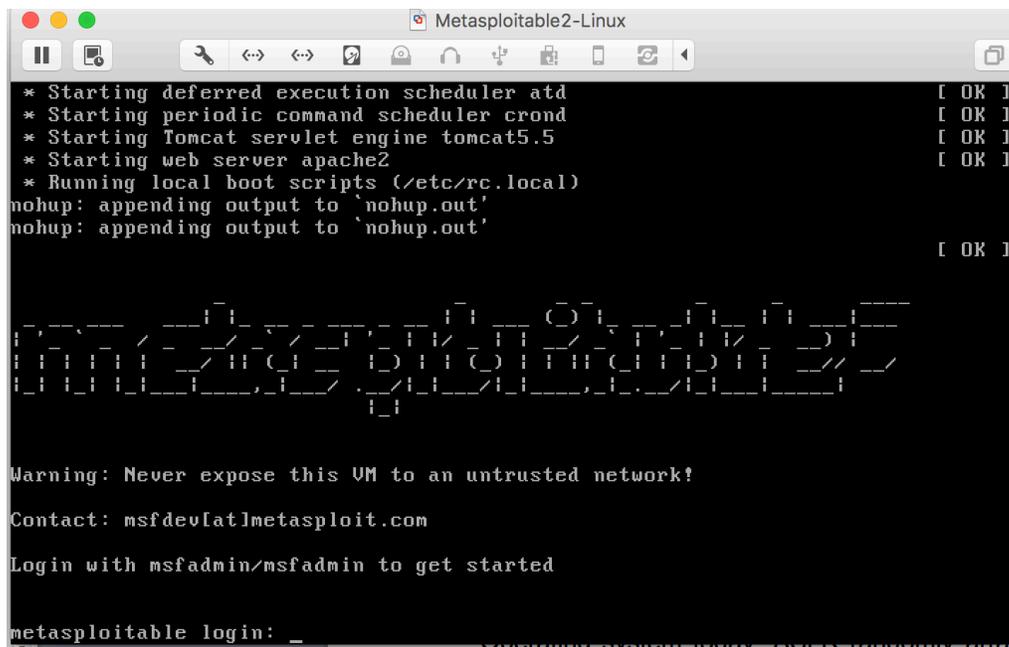
Then, you select **Metasploitable2-Linux**, and press Start up. This is an intentionally vulnerable Linux VM that you will attack against.



If you see the window below, just click OK. This is due to running two VM at the same time.



Log into the virtual machine with username, msfadmin, and password [TBA in Class, Same password to login Kali Linux].



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



```
Metasploitable2-Linux

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 scanning. 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
```



```
Metasploitable2-Linux
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)

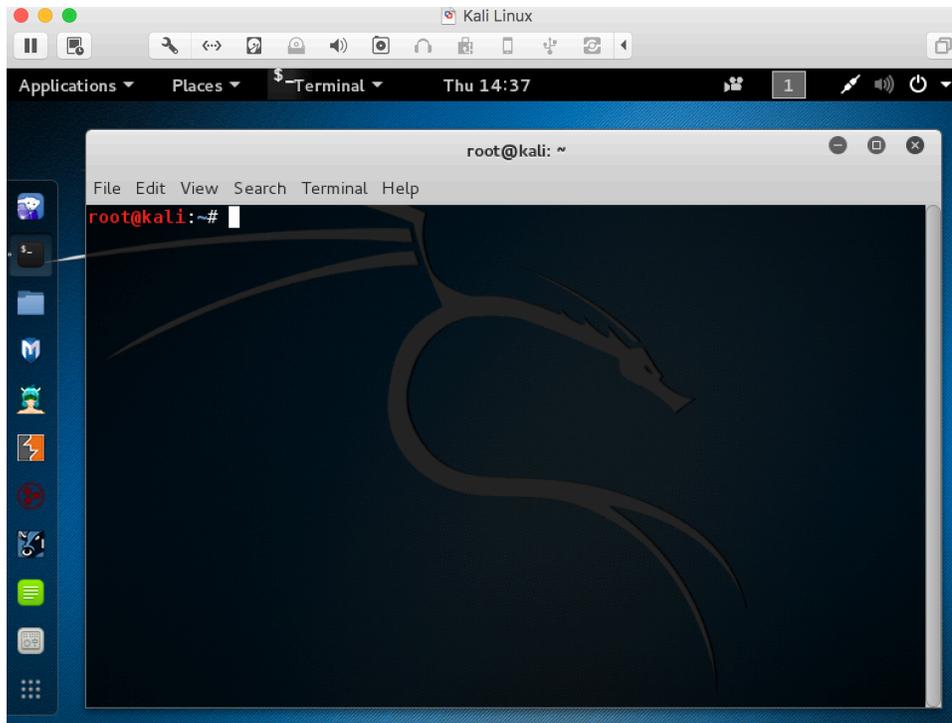
msfadmin@metasploitable:~$ _
```

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 .



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: ~
File Edit View Search Terminal Help
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 Remote Vulnerabilities
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs file Remote Vulnerabilities
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11 password
6667/tcp  open  irc
8009/tcp  open  ajp13 password
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: ~
File Edit View Search Terminal Help
root@kali:~# man nmap
```



```
root@kali: ~
File Edit View Search Terminal Help
NMAP(1) https://127.0.0.1:9392/nmap.html#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. In our Kali Linux image, OpenVAS has been installed and setup for you.

If you want to setup OpenVAS in your own machine, you can follow the steps below.

```
root@kali:~# apt-get update
```

```
root@kali:~# apt-get dist-upgrade
```

```
root@kali:~# apt-get install openvas
```

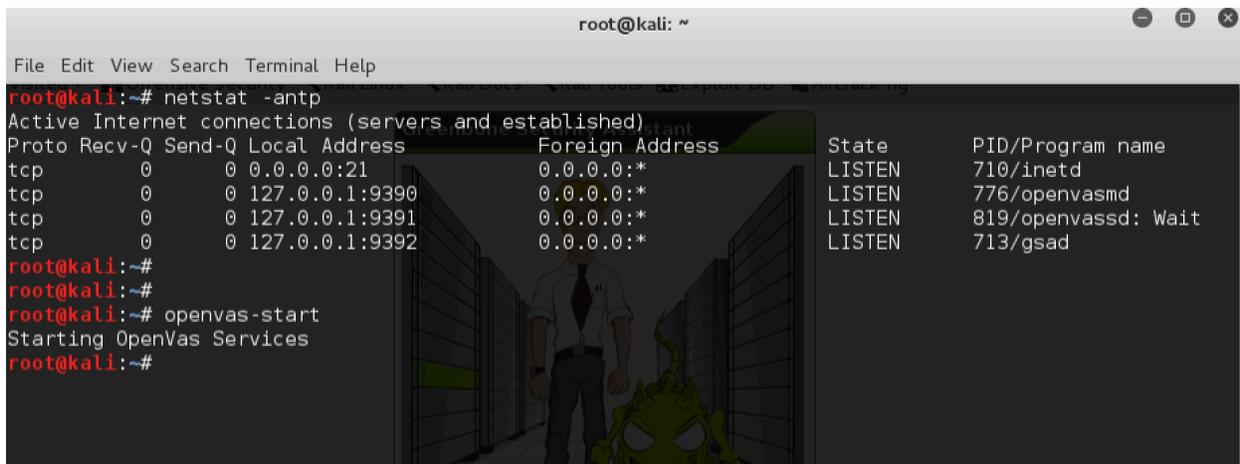
```
root@kali:~# openvas-setup
```

Since the Kali Linux image has everything setup for you, you don't need to run the setup commands. 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
```

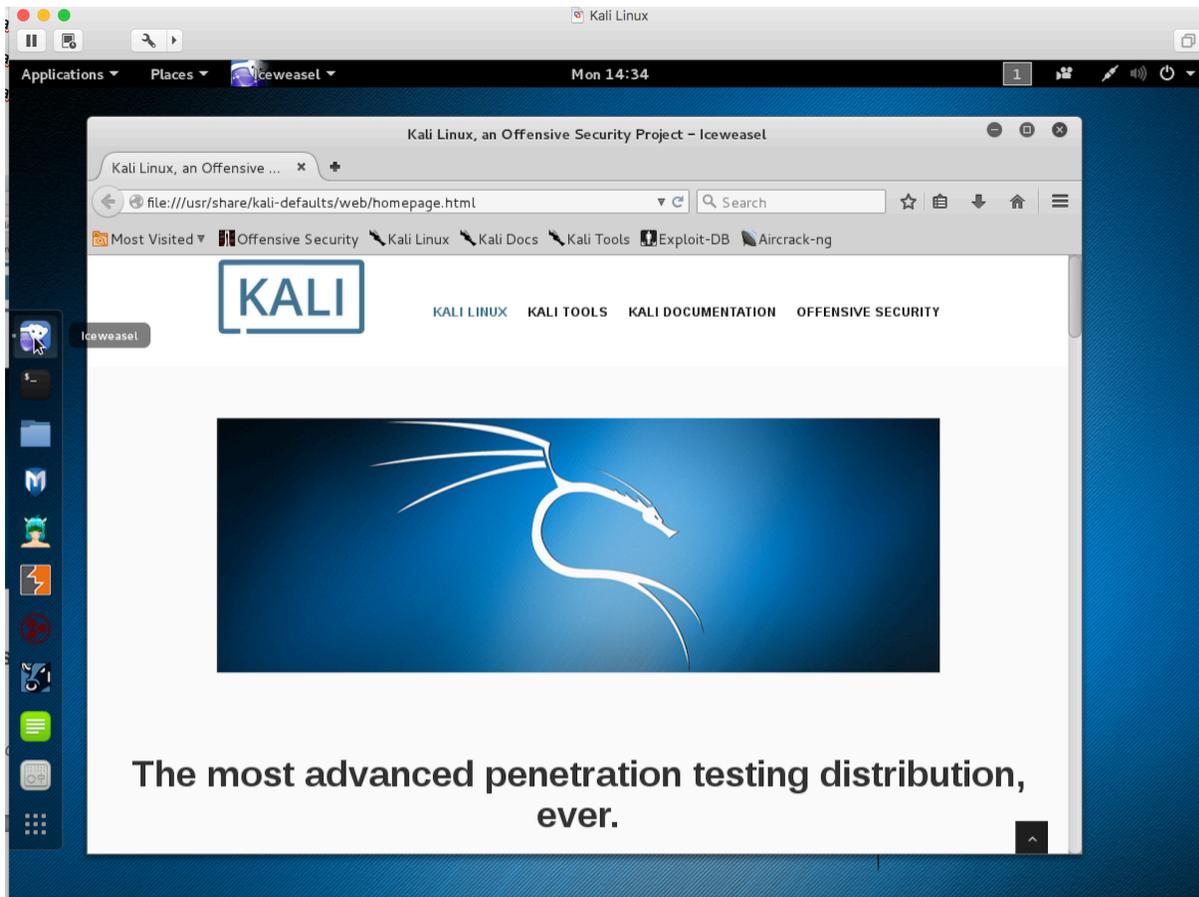


```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      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:~#
```

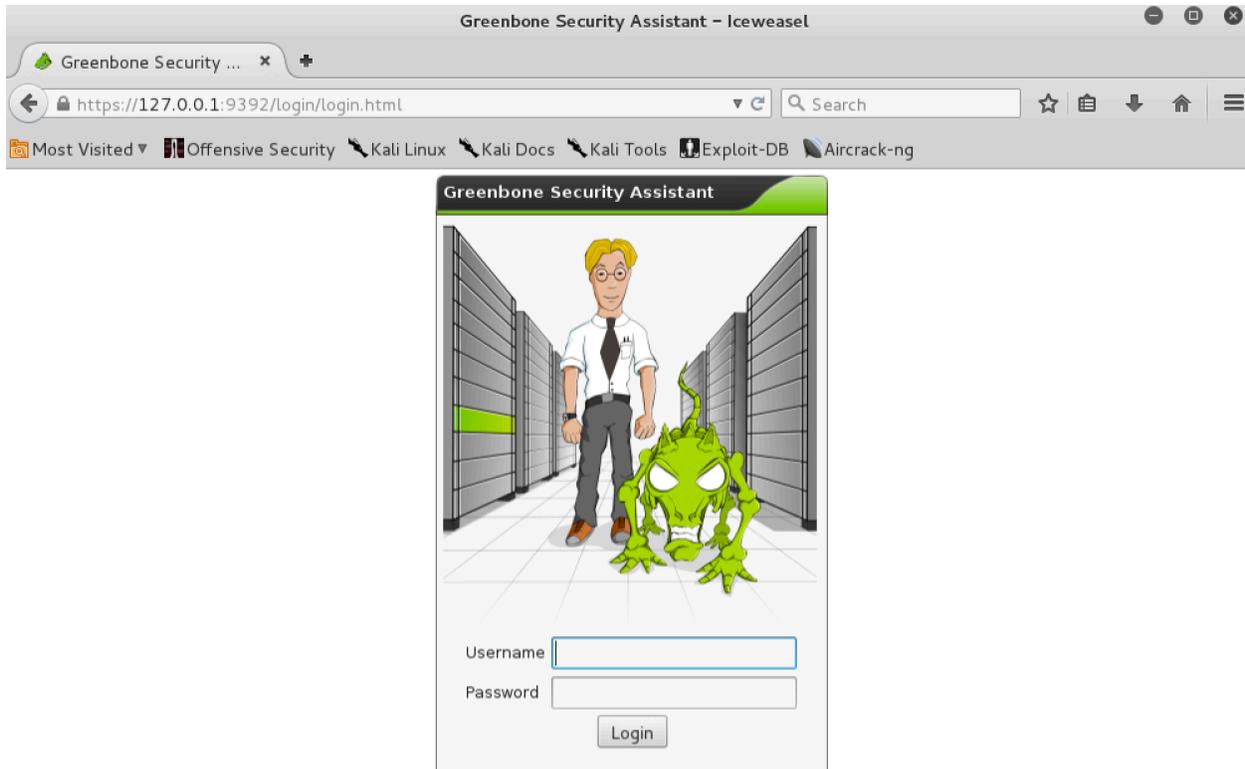


Connecting to the OpenVAS Web Interface

Go to the Kali Linux, and open the browser, Iceweasel, by clicking the icon 



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



Input the username as admin, and the password [TAB in the classroom, same password as Kali Linux Login].

The screenshot on next page is the homepage of OpenVAS. Type the IP address of the target 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 30 seconds so you can lean back and watch the scan progress



Greenbone Security Assistant – Iceweasel

Greenbone Security Assistant | Logged in as Admin admin | Logout
Mon Jan 18 19:50:46 2016 UTC

Scan Management | Asset Management | Secinfo Management | Configuration | Extras | Administration | Help

Tasks 1 - 1 of 1 (total: 1) Refresh every 30 Sec.

Filter: apply_overrides=1 rows=10 first=1 sort=name

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 172.16.108.172	Done	1 (1)	Jan 18 2016	10.0 (High)		

Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.
I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.
If you want help creating new scan tasks but also more options, you can select "Advanced Task Wizard" from the wizard selection menu at the top of this window where it currently says "Task Wizard" marked with a small arrow.
For more detailed information on functionality, please try the integrated help system. It is always available as a

Quick start: Immediately scan an IP address
IP address or hostname:
 Start Scan
172.16.108.172
For this short-cut you 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
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 default Port List, Alert, OpenVAS Scan Config, Credentials, OpenVAS Scanner and Slave configured in "My Settings".

After finishing the scanning, you can look at the reports as shown in the screenshot below.



The screenshot shows the Greenbone Security Assistant web interface. The browser address bar displays the URL: `https://127.0.0.1:9392/omp?cmd=get_report&report_id=ae3de0f1-8d74-488b-...`. The interface is logged in as 'Admin admin' and shows the date 'Mon Jan 18 20:00:23 2016 UTC'. The main content area displays a report titled 'Report: Results' with 122 items out of a total of 236. A filter is applied: `sort-reverse=severity result_hosts_only=1 min_cvss_base= min_qod=70`. Below the filter is a table of vulnerabilities.

Vulnerability	Severity	QoD	Host	Location	Actions
ProFTPD Multiple Remote Vulnerabilities	10.0 (High)	75%	172.16.108.172	21/tcp	[Icons]
Possible Backdoor: Ingreslock	10.0 (High)	99%	172.16.108.172	1524/tcp	[Icons]
ProFTPD Multiple Remote Vulnerabilities	10.0 (High)	75%	172.16.108.172	2121/tcp	[Icons]
X Server	10.0 (High)	75%	172.16.108.172	6000/tcp	[Icons]
distcc Remote Code Execution Vulnerability	9.3 (High)	75%	172.16.108.172	3632/tcp	[Icons]
MySQL weak password	9.0 (High)	95%	172.16.108.172	3306/tcp	[Icons]
PostgreSQL weak password	9.0 (High)	75%	172.16.108.172	5432/tcp	[Icons]
DistCC Detection	8.5 (High)	75%	172.16.108.172	3632/tcp	[Icons]
PostgreSQL Multiple Security Vulnerabilities	8.5 (High)	75%	172.16.108.172	5432/tcp	[Icons]
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	75%	172.16.108.172	21/tcp	[Icons]
ProFTPD Server SQL Injection Vulnerability	7.5 (High)	75%	172.16.108.172	21/tcp	[Icons]
phpMyAdmin Code Injection and XSS Vulnerability	7.5 (High)	75%	172.16.108.172	80/tcp	[Icons]
phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities	7.5 (High)	75%	172.16.108.172	80/tcp	[Icons]
phpMyAdmin Configuration File PHP Code Injection Vulnerability	7.5 (High)	75%	172.16.108.172	80/tcp	[Icons]
TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	75%	172.16.108.172	80/tcp	[Icons]

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 (list at least 3 of the running services). What are the differences if we use T1, T2, T3 flags? How to avoid detection from an intrusion detection system (e.g., stealthy scanning)?
3. Use OpenVAS to find two vulnerabilities of the target, and briefly describe them.

Happy Scanning!