



计算机科学与工程系

Department of Computer Science and Engineering

CS 315 Computer Security Course

Lab 4 Part1: 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

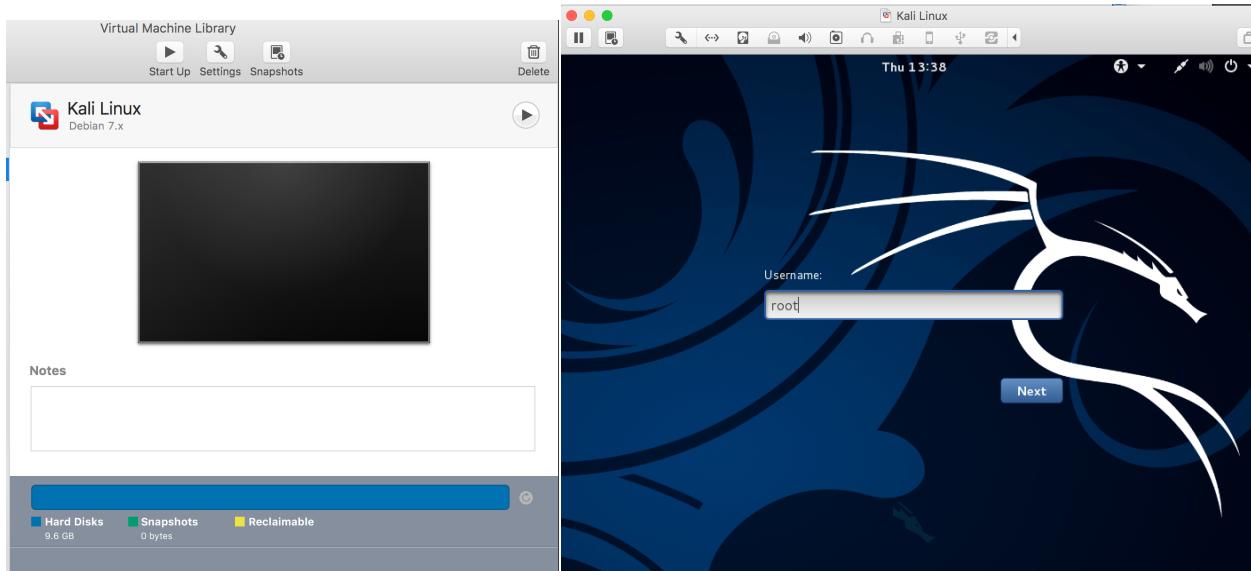
- The VMWare Software
 - <https://www.vmware.com/>
- The VirtualBox Software
 - <https://www.virtualbox.org/wiki/Downloads>
 - <https://www.vmware.com/support/developer/ovf/>
 - <https://www.mylearning.be/2017/12/convert-a-vmware-fusion-virtual-machine-to-virtualbox-on-mac/>
- The Kali Linux, Penetration 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 4 Part 1 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



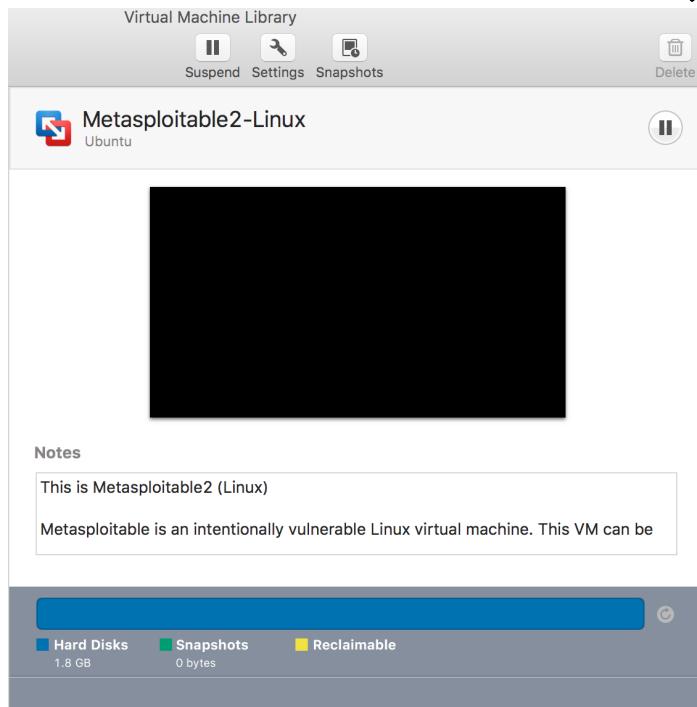
Login the Kali Linux with username root and password [TBA in the class]. Below is the screen snapshot after login.



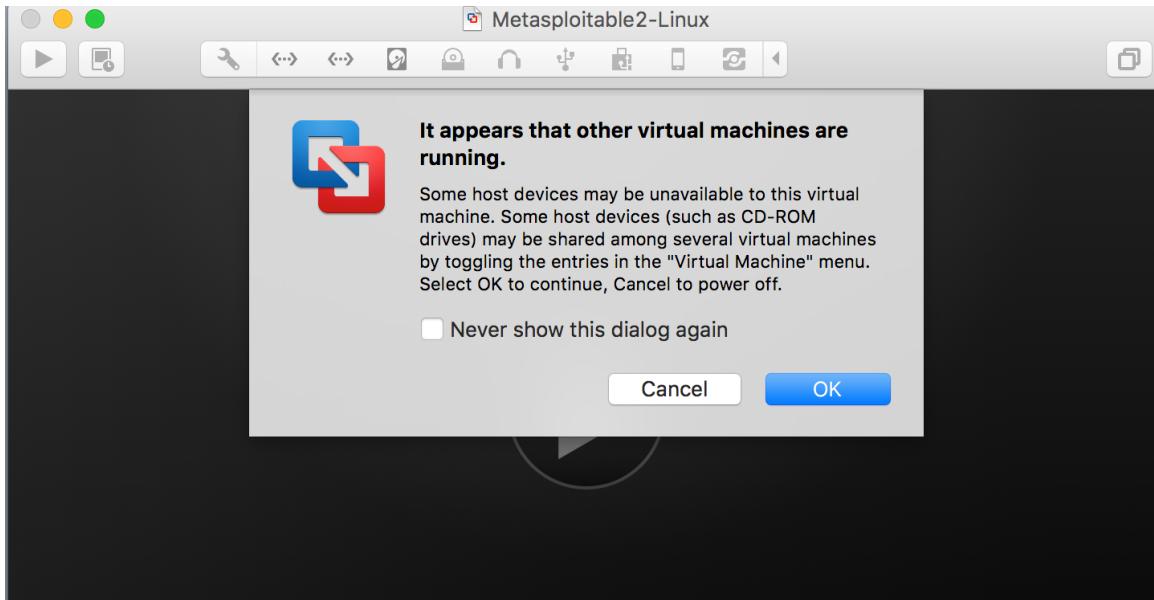


Then, you select **Metasploitable2-Linux**, and press Start up. This is an intentionally vulnerable Linux VM that you will attack against.

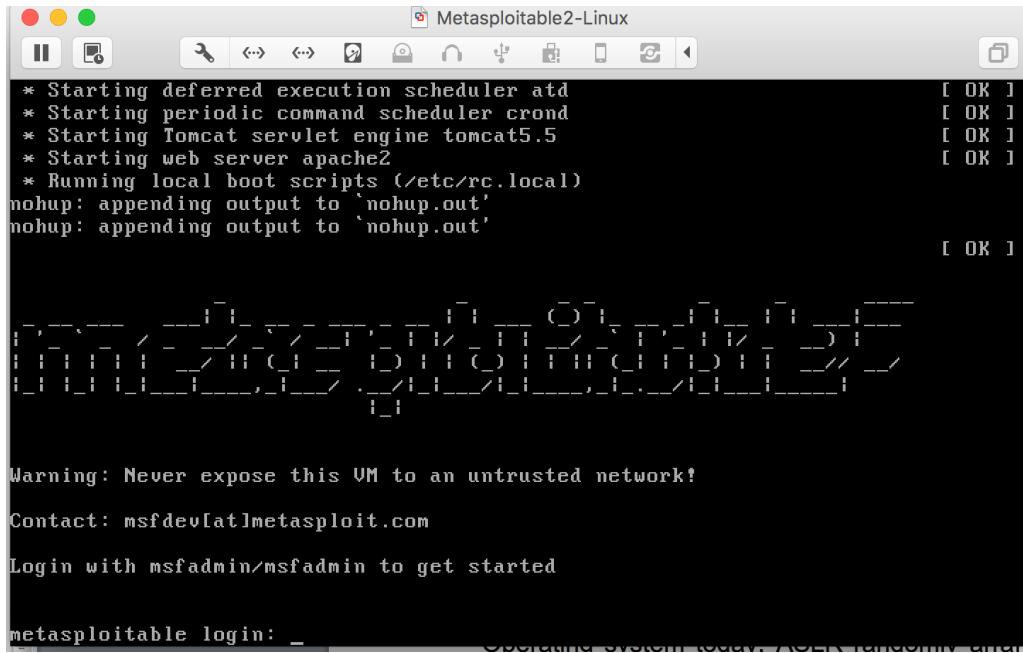
ifconfig



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].



```
* 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 ]

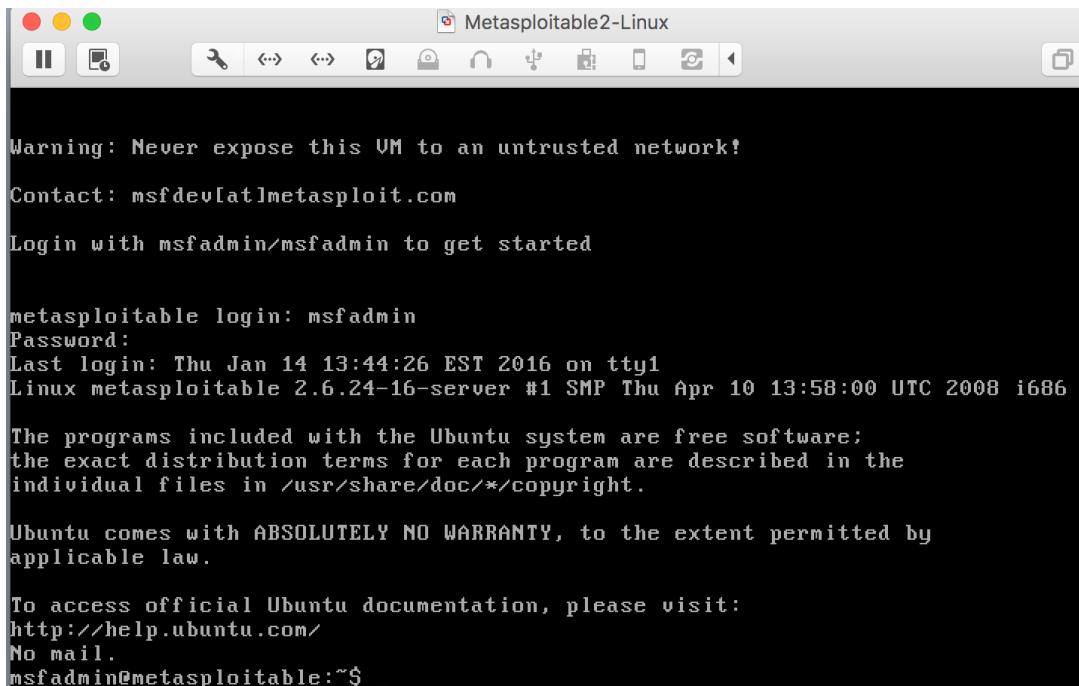
[----]
[----]
[----]
[----]
[----]
[----]
[----]
[----]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: _
```

Operating System: Ubuntu 10.04 LTS (64-bit) - 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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 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

assign a public IP will make it easy to be attacked.

```
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:~$ _
```

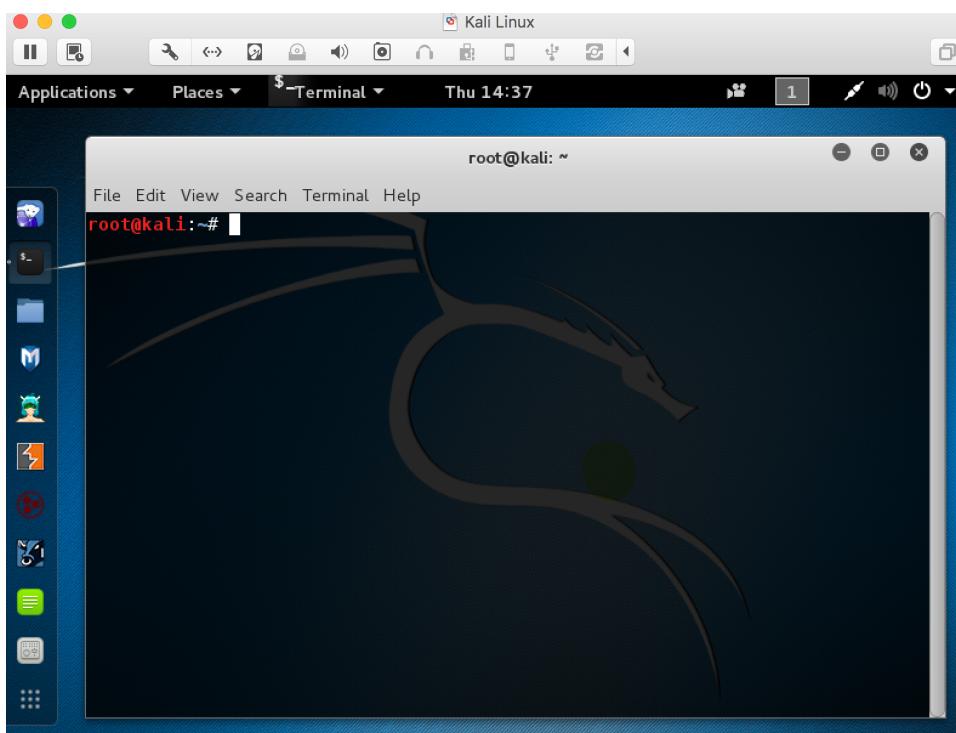
From the screenshot above, we can see that the IP address of the network interface, eth0, is 172.16.108.172. This is the IP address for the target that you will use later in this lab. When you work on the lab in the classroom, you will get a different IP address for your Metasploitable2-Linux VM. Note 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.



The screenshot shows a terminal window titled "root@kali: ~". The user has run the command `nmap -T4 172.16.108.172`. The output indicates that the host is up with 0.0027s latency. A table lists various open ports and services:

PORT	STATE	SERVICE	Severity	QoD	Host	
21/tcp	open	ftp	10.0 (High)	75%	172.16.108.172	
22/tcp	open	ssh	10.0 (High)	99%	172.16.108.172	
23/tcp	open	telnet	10.0 (High)	75%	172.16.108.172	
25/tcp	open	smtp	10.0 (High)	75%	172.16.108.172	
53/tcp	open	domain	10.0 (High)	75%	172.16.108.172	
80/tcp	open	http	10.0 (High)	75%	172.16.108.172	
111/tcp	open	rpcbind	10.0 (High)	75%	172.16.108.172	
139/tcp	open	netbios-ssn	10.0 (High)	75%	172.16.108.172	
445/tcp	open	microsoft-ds	10.0 (High)	75%	172.16.108.172	
512/tcp	open	exec	10.0 (High)	75%	172.16.108.172	
513/tcp	open	login	10.0 (High)	75%	172.16.108.172	
514/tcp	open	shell	Remote Vulnerabilities	10.0 (High)	75%	172.16.108.172
1099/tcp	open	rmiregistry	10.0 (High)	75%	172.16.108.172	
1524/tcp	open	ingreslock	10.0 (High)	99%	172.16.108.172	
2049/tcp	open	nfs	10.0 (High)	75%	172.16.108.172	
2121/tcp	open	ccproxy-ftp	10.0 (High)	75%	172.16.108.172	
3306/tcp	open	mysql	10.0 (High)	75%	172.16.108.172	
5432/tcp	open	postgresql	10.0 (High)	75%	172.16.108.172	
5900/tcp	open	vnc	9.3 (High)	75%	172.16.108.172	
6000/tcp	open	X11	9.0 (High)	95%	172.16.108.172	
6667/tcp	open	irc	9.0 (High)	75%	172.16.108.172	
8009/tcp	open	ajp13	password	9.0 (High)	75%	172.16.108.172
8180/tcp	open	unknown	8.5 (High)	75%	172.16.108.172	
MAC Address:	00:0C:29:3F:E0:7A	(VMware)	PostgreSQL Multiple Security Vulnerabilities	8.5 (High)	75%	172.16.108.172
			Compromised Source Packages Backdoor Vulnerability	7.5 (High)	75%	172.16.108.172

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

The screenshot shows a terminal window titled "root@kali: ~". The user has run the command `man nmap`. The output is displayed in the terminal, showing the manual page for the nmap command.



```
File Edit View Search Terminal Help
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 upgrades, 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 these 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**.



Assignments for the Lab 4 Part I

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)?
-

Happy Scanning!