Cybersecurity 701

RAT Removal Lab

Please Note: It is highly recommended to have completed the Backdoor Removal Lab prior to this lab.

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

RAT Removal Materials

- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine

- Software tool used (from Kali Linux)
  - Metasploit Framework

- Note: This lab will attempt to remove a persistence script that is already running on the Windows 7 machine

Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 2.4 - Given a scenario, analyze indicators of malicious activity.
    - Malware attacks

What is a RAT?

- A Remote Access Trojan (RAT) is a tool that allows malicious users to connect remotely to a system
  - Sometime referred to as a Remote Administration Tool
  - An ultimate backdoor

- It is recommended to use the same RAT installed by the RAT/Bot Lab

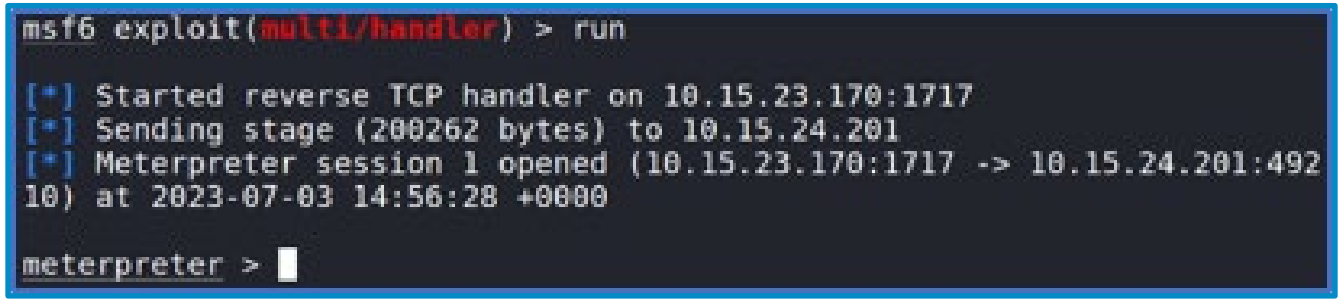
RAT Removal Lab Overview

1. Connect to the RAT
2. Shut Down the Current Session
3. Re-open the Backdoor
4. Locate the RAT
5. Locate all the RATs
6. Delete the RATs and Reboot
7. Try to Reconnect

Please Note: It is highly recommended to connect to the RAT by following along with the RAT/Bot Lab!

Connect to the RAT

- Connect with the RAT from the Kali Linux machine
  - Have a backdoor session open on the Kali machine
  - Windows 7 machine is being controlled

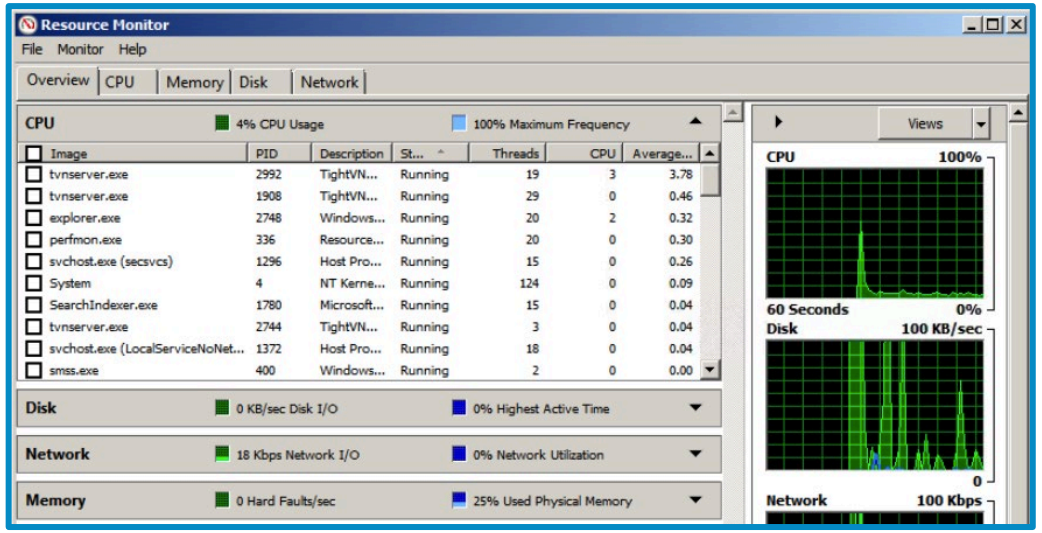


Open backdoor session, connected via a RAT

  - It is highly recommended to have the persistence scripts from the RAT/Bot lab used for this RAT

Shut Down the Current Session

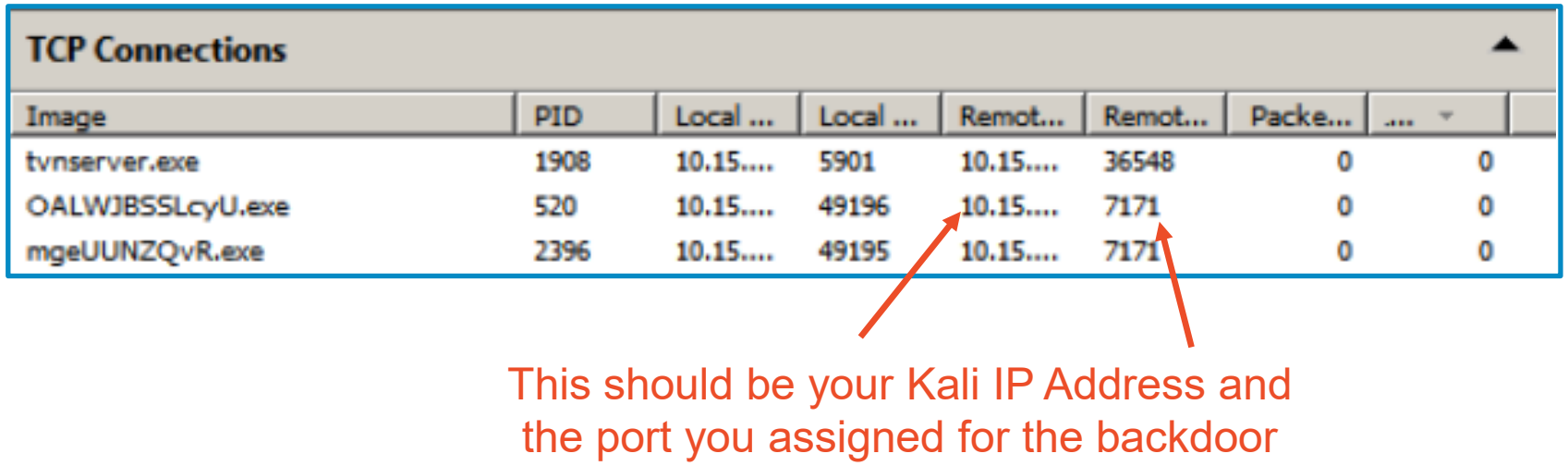
- In Windows, the user can search and try to kill a backdoor session just like in the Backdoor Removal Lab.
- In Windows, open the Resource Monitor.
  - Press the **Windows Start** button
  - Search for "*Resource Monitor*"
  - Open the *Resource Monitor application*



Windows 7 Resource Monitor

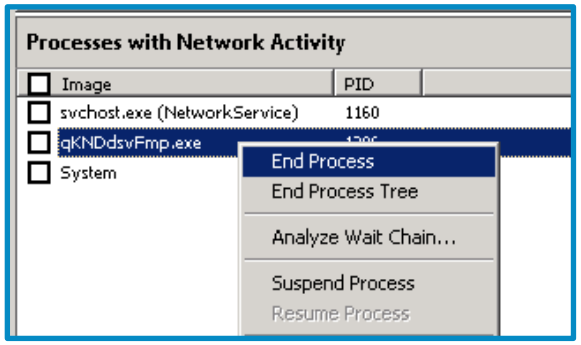
Shut Down the Current Session

- In the Resource Monitor, select the *Network* tab
- Open the *TCP Connections* tab
- Locate the backdoor session
  - It should be using the remote address of the Kali machine

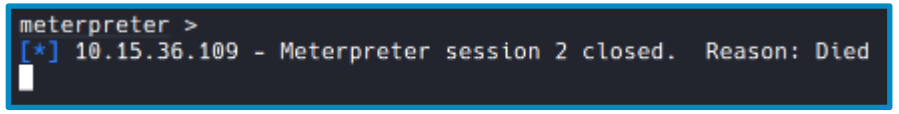


Shut Down the Current Session

- Once you have the backdoor session, shut it down
- Up in *Processes with Network Activity*
  - Right click on the session
  - Select *End Process* to terminate the session
- You should notice on the Kali machine the session has been closed



Shutting the backdoor session down



Metasploit showing the session closed

Re-open the Backdoor

- In Kali, press **CTRL+C** to bring back up meterpreter
- Use **`exit`** to quit the session
- Use **`run`** to re-connect with the session

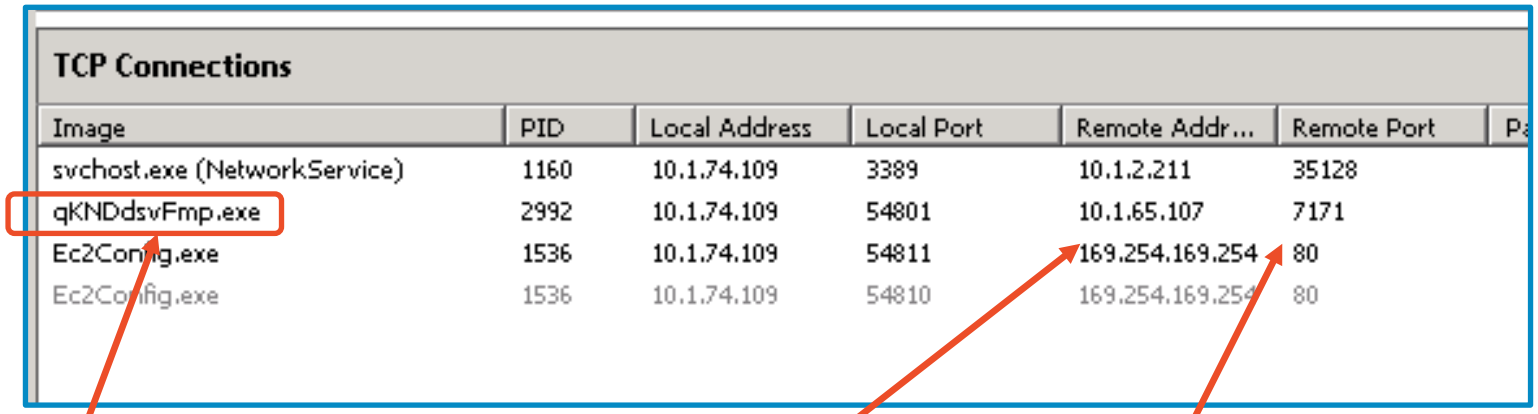
```
meterpreter >
[*] 10.15.36.109 - Meterpreter session 2 closed.  Reason: Died
Interrupt: use the 'exit' command to quit
meterpreter > exit
[*] Shutting down Meterpreter...
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.15.25.197:7171
[*] Sending stage (175686 bytes) to 10.15.36.109
[*] Meterpreter session 3 opened (10.15.25.197:7171 -> 10.15.36.109:49202)
0000

meterpreter >
```

Re-connected to the backdoor

Please Note: Although the session was shut down, it was very easy for the malicious user to re-connect to the RAT

Locate the RAT

- In Windows, stay in the Resource Monitor app
- Locate the name of the RAT application



TCP Connections

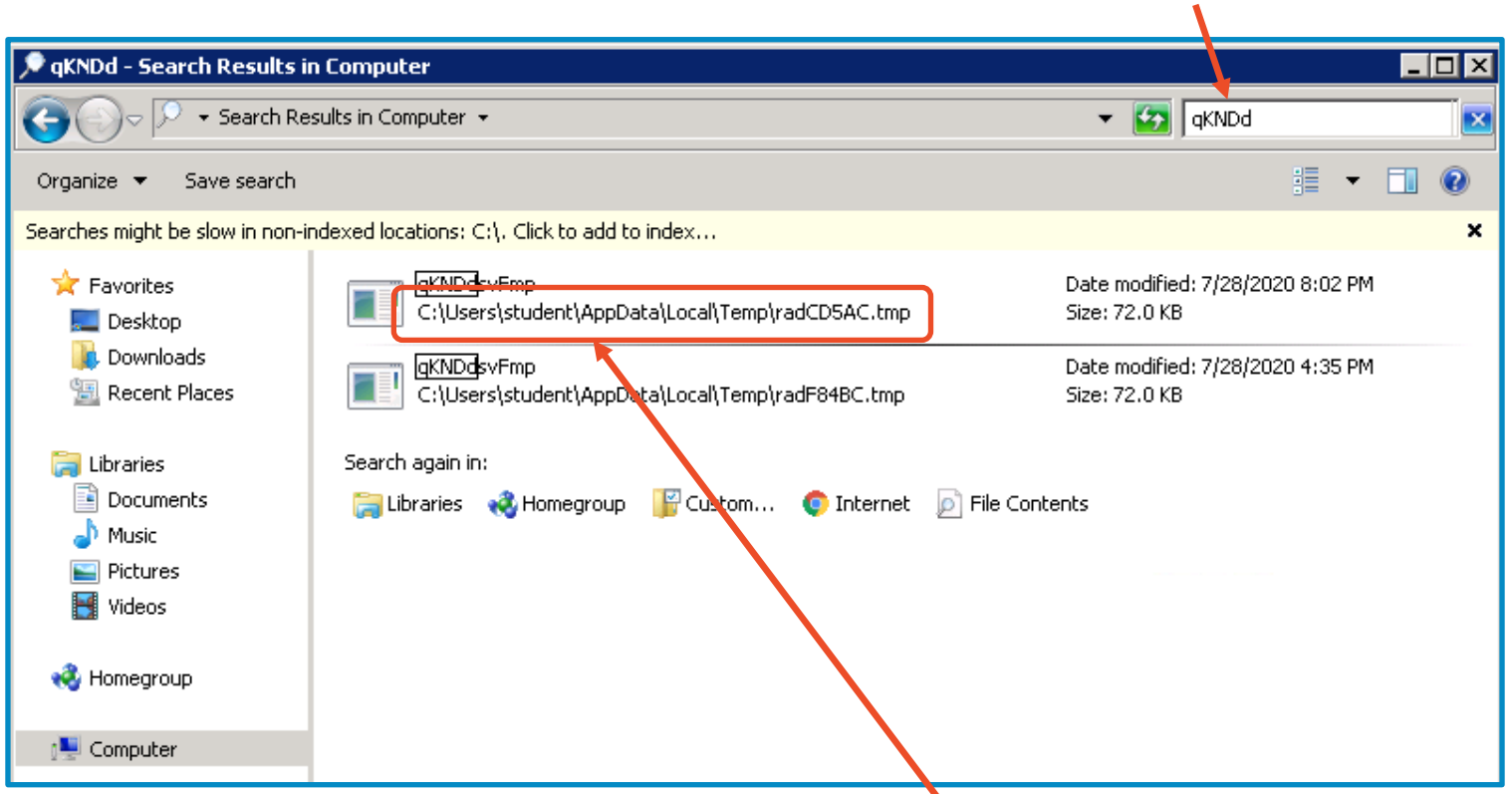
Image	PID	Local Address	Local Port	Remote Addr...	Remote Port	P
svchost.exe (NetworkService)	1160	10.1.74.109	3389	10.1.2.211	35128	
qKNDdsvFmp.exe	2992	10.1.74.109	54801	10.1.65.107	7171	
Ec2Config.exe	1536	10.1.74.109	54811	169.254.169.254	80	
Ec2Config.exe	1536	10.1.74.109	54810	169.254.169.254	80	

Locate the RAT

- Open Windows Explorer
  - Press the **Windows Start** button
  - Search for "*Windows Explorer*"
  - Open *Windows Explorer*
- Click on **Computer** button
- In the search bar, search for the first 5 letters of the backdoor program
- You should see the location of the RAT

Locate the RAT

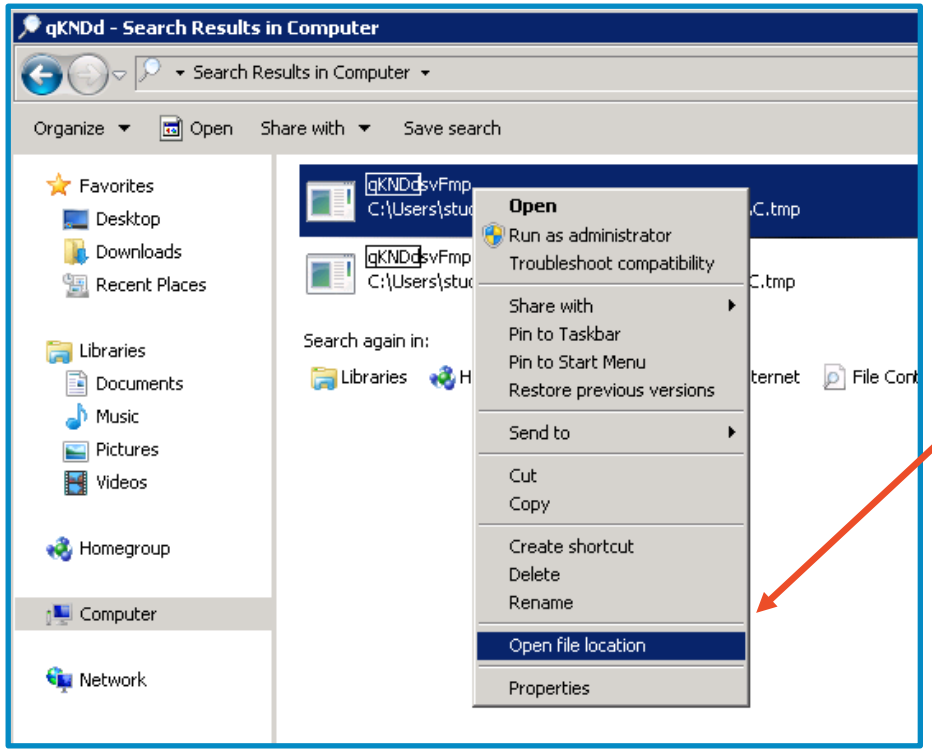
Searching for first 5 letters of the backdoor program



Location of the backdoor program

Locate the RAT

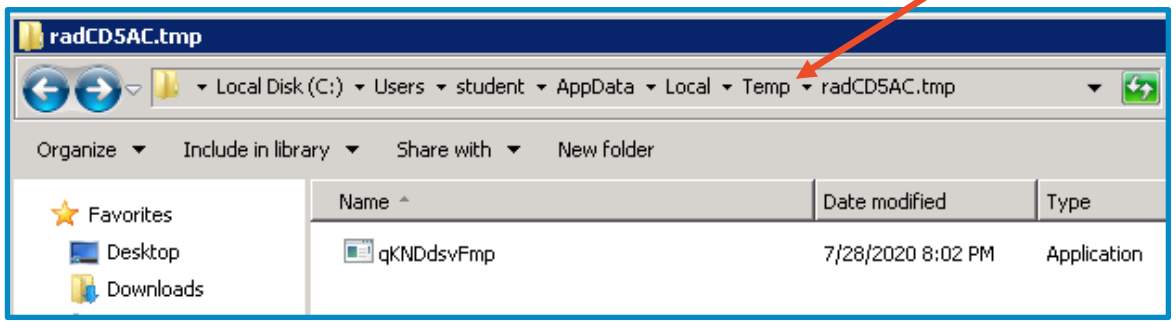
- Right-click on the RAT
- Select the Open file location option
  - This will open up the RAT's file location



Select the Open file location

Locate all the RATs

- Select back one folder

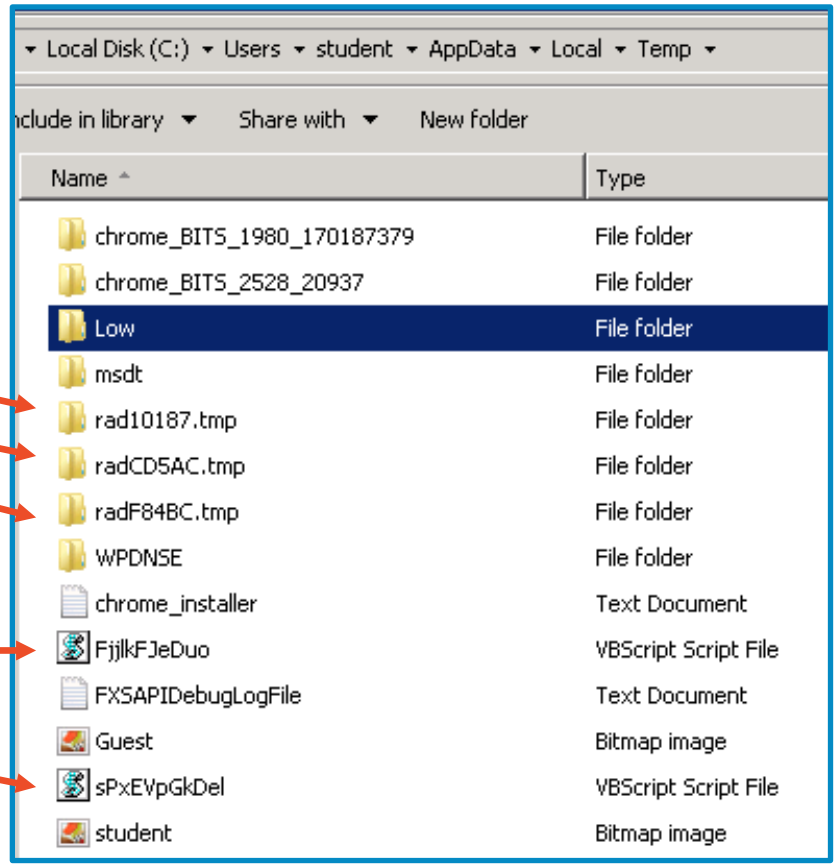


- This will open up the location of the RATs
- Try to locate programs that look like they don't belong, they'll be random strings of letters

Locate all the RATs

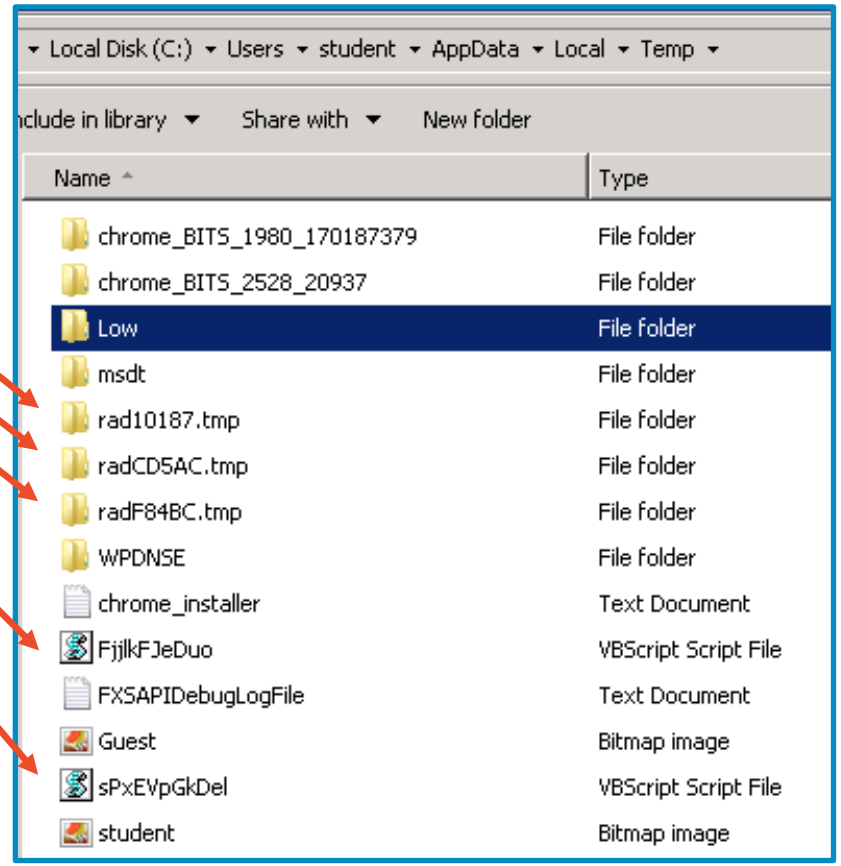
These are the location of the backdoor scripts

These are the RATs that create the backdoor scripts. Notice they are VBScript files.



Delete the RATs and Reboot

Delete all of these files, especially the VBScripts files

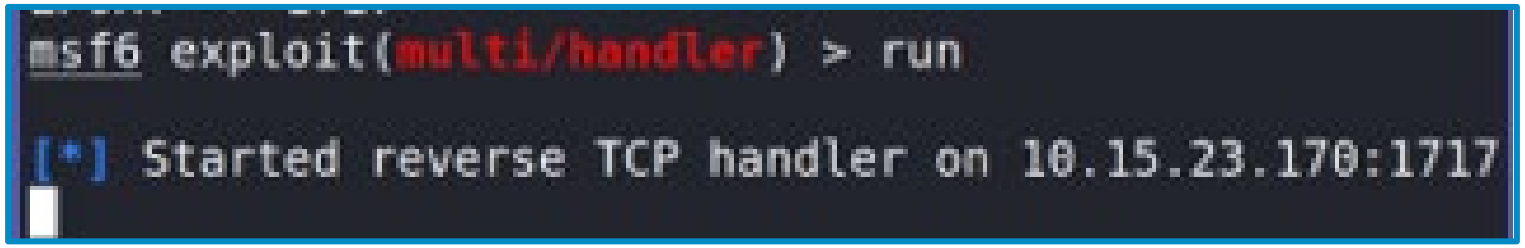


- After they are deleted, restart the Windows machine
  - Depending on your range, this also might require Kali to be rebooted

Please Note: You might not be able to delete a .tmp folder since there is an active backdoor inside that folder. This will erase when we restart the system.

Try to Reconnect

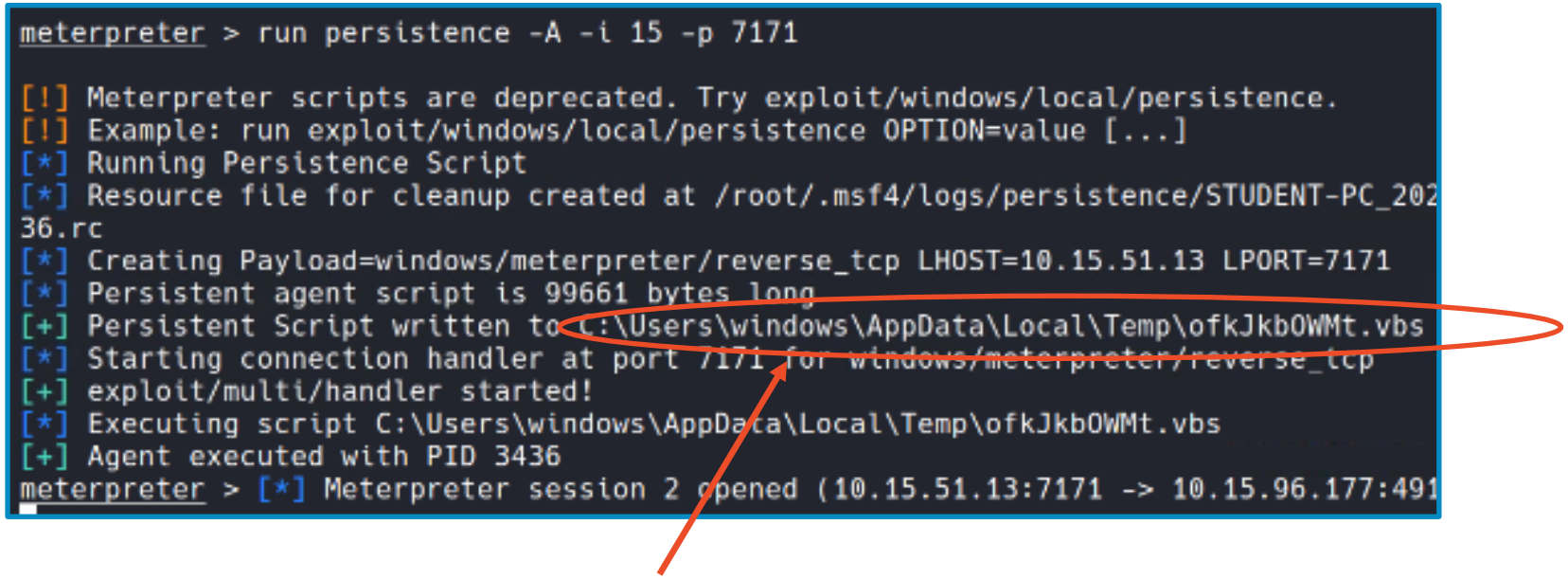
- Once Windows has restarted, try to reconnect to the RAT from the Kali Linux machine



Notice that the Kali machine is not able to create a backdoor session into the Windows machine

Please Note!

- This is what meterpreter reads when running the persistence script from the Kali machine



Notice, it shows where it is installing the RAT