

Faculty of Business, IT, and Management
Hacking & Exploits – HACK2200
Final Test

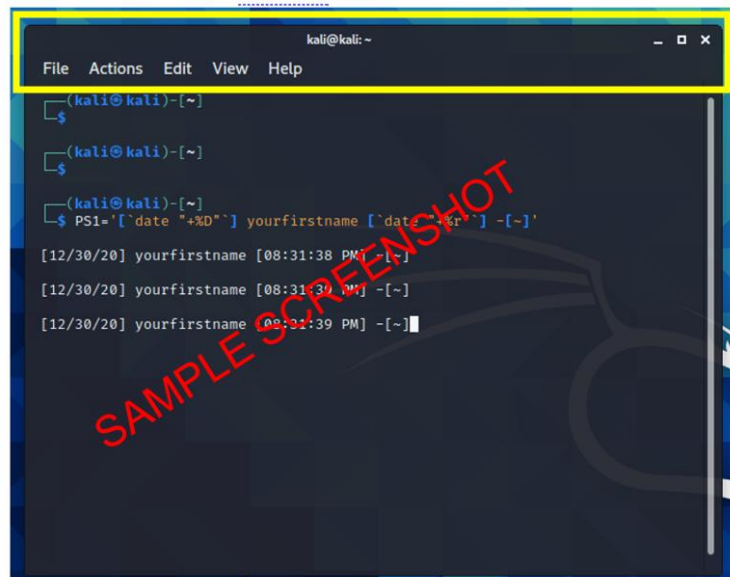
By proceeding with this test, I promise that I will not lie, cheat, or use any unauthorized aids or assistance to complete this test. Further, I promise that I will not offer any unauthorized assistance to any of my fellow students, and I promise that I will not ask any of my fellow students for unauthorized assistance.

I promise that the work I submit is my own, and that I will not share this test material with any students.

I have read the above statement and express my agreement by proceeding to write this test.

Instructions

- This is an open-book test. You can use the labs, slides, and the internet to search for help.
- 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.**
- When taking a screenshot of a terminal, include the full terminal, with the menu bar showing as shown in the yellow box below. Don't crop any part of your terminal when you are taking screenshots. **Cropped terminals, and terminals without your name in the prompt will receive zero credit.**



- 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.
- If you believe a question is ambiguous or confusing, state in writing what you believe is wrong, make and state in writing any reasonable assumptions you think are necessary, and proceed to answer the question.
- Arbitrarily assign values that are not specified.

Important Note: be mindful of time, once the test due time has passed, the dropbox will close. Make sure you submit your answer file by the due time.

Submission: Submit only the answer file through DC Connect by the Due Time of this test.

Question#1 – Using Kali Linux Metasploit Framework (msf), exploit Rejetto HTTP File Server (HFS) 2.3.b that is installed on a Metasploitable 3 Windows Server 2008 box.

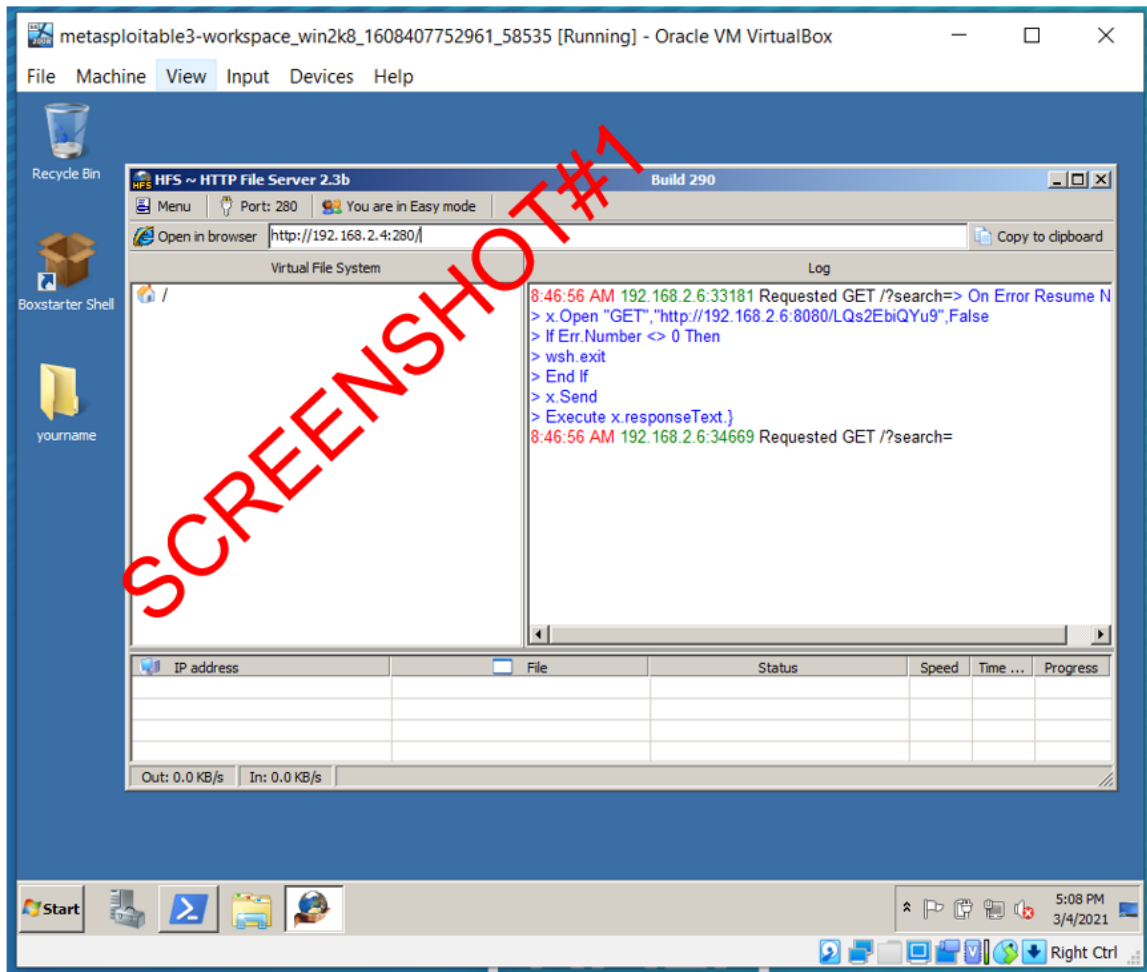
Note that exploiting HFS 2.3b using any tool other than Kali msf and on any box other than Metasploitable 3 Windows Server 2008 will receive zero marks for this question. Note also that exploiting any other version of HFS (i.e., 2.3m) will receive zero marks.

HFS vulnerability information can be found here: <https://www.exploit-db.com/exploits/39161>

To guide you exploit this service follow the steps below:

- 1- Download HFS 2.3b from DC Connect final exam assignment. If you have trouble downloading the file from DC Connect, the file is also available here: <https://sourceforge.net/projects/hfs/files/HFS/2.3b/>
- 2- On your Metasploitable3 Windows Server 2008, do the following:
 - Login as the administrator to the Metasploitable3 Windows Server 2008.
 - Create a new folder with your name, and place it on the desktop.
 - Inside the folder create a file and name it as `yourfirstname-confidential.txt`. Open the text file you just created and type anything you want in the text file. Add your first and last names in the text file. Save and close the file.
 - Unzip and install/run the downloaded hfs2.3b.zip file.
- 3- Take a screenshot similar to the one below, and place it in the answer file under **SCREENSHOT#1**.





- 4- Switch back to Kali Linux, launch Metasploitable framework (msfconsole), and set the prompt by issuing the following commands:

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

- 5- Choose and set an exploit that is available for HFS.
- 6- Pick a payload from the options available to your exploit that allows you to gain a meterpreter terminal on a Windows machine.
- 7- Set all the options needed the exploit and payload you chose.
- 8- Run the following command:

```
show options
```

- 9- Take a screenshot of your full msfconsole terminal. Your terminal should show the correct terminal prompt, and the issuance and the results of the `show`



options command you issued in the previous step. Place the screenshot under **SCREENSHOT#2** in the answer file.

10- Answer the following questions in your answer file:

Question#1.1: What exploit did you use?

Question#1.2: What payload did you use?

11- Run the exploit, and take a screenshot of your terminal, showing the `exploit` command and the gained `meterpreter` shell in the **same** terminal. Place the screenshot under **SCREENSHOT#3** in the answer file.

12- Using your gained meterpreter, copy your `yourfirstname-confidential.txt` file you created on the victim machine to the attacker machine. You can use the below command to copy the file from the victim machine. (Note that the below command is only a suggestion, you need to ensure the command runs successfully or find another command(s) to copy the file from the victim machine using the gained interpreter):

```
Meterpreter > run post/windows/gather/enum_files
SEARCH_FROM=C:\\Users\\Administrator\\Desktop\\yourname\\
FILE_GLOBS=*.*
```

13- Take a screenshot of your full `meterpreter` terminal showing the results of running the `exploit` command and the command in the previous step. Place the screenshot under **SCREENSHOT#4** in the answer file.

14- On Kali linux machine, browse to where `meterpreter` saved your `yourfirstname-confidential.txt` file, and open the file. Take a screenshot of the full terminal of the opened file. Place the screenshot under **SCREENSHOT#5** in the answer file. Include the full-text editor in your screenshot showing the location of the file in the file name.

15- Back in your `meterpreter`, grab a screenshot of the victim machine.

16- This is the end of Question#1. You can shut down your KaliVM and Metasploitable3 Windows Server 2008 VMs now. You will not need them for the rest of this test.

Question#2 – Using a SEED VM, exploit the buffer overflow vulnerability based on the Labsetup.zip file attached to this test.

- 1- Using the attached `Labsetup.zip` files, exploit the buffer overflow vulnerability using your SEED VM and containers.
- 2- Note that the `Labsetup.zip` file attached has a **different** buffer size configured. It is **not** the same buffer size you exploited in the lab, and will result in different `ret` and `offset` values.

3- Change the SEED VM prompt to be:

```
$ PS1='[\`date "+%D"`] yourname [\`date "+%r"`] -[~] '
```

4- When you exploit the buffer overflow, modify the shell code to list the folders and display your name and a random number of your choice, by replacing the following line in the shellcode:

```
"/bin/ls -l; echo Hello 32; /bin/tail -n 2 /etc/passwd *"
```



with this line:

```
"/bin/ls -l; Hello yourname @insert random number here      *"
```

Remember to align the * at the end of the line with your guiding * in the shellcode file

- 5- Once you exploit the attached Labsetup.zip buffer overflow, answer the following questions. All your answers should be in hexadecimal format.

Question#2.3: What is the Frame Pointer (ebp) inside bof() address in hexadecimal?

Question#2.4: What is the Buffer's address inside bof() in hexadecimal?

Question#2.5: What is the value of the ret address in hexadecimal?

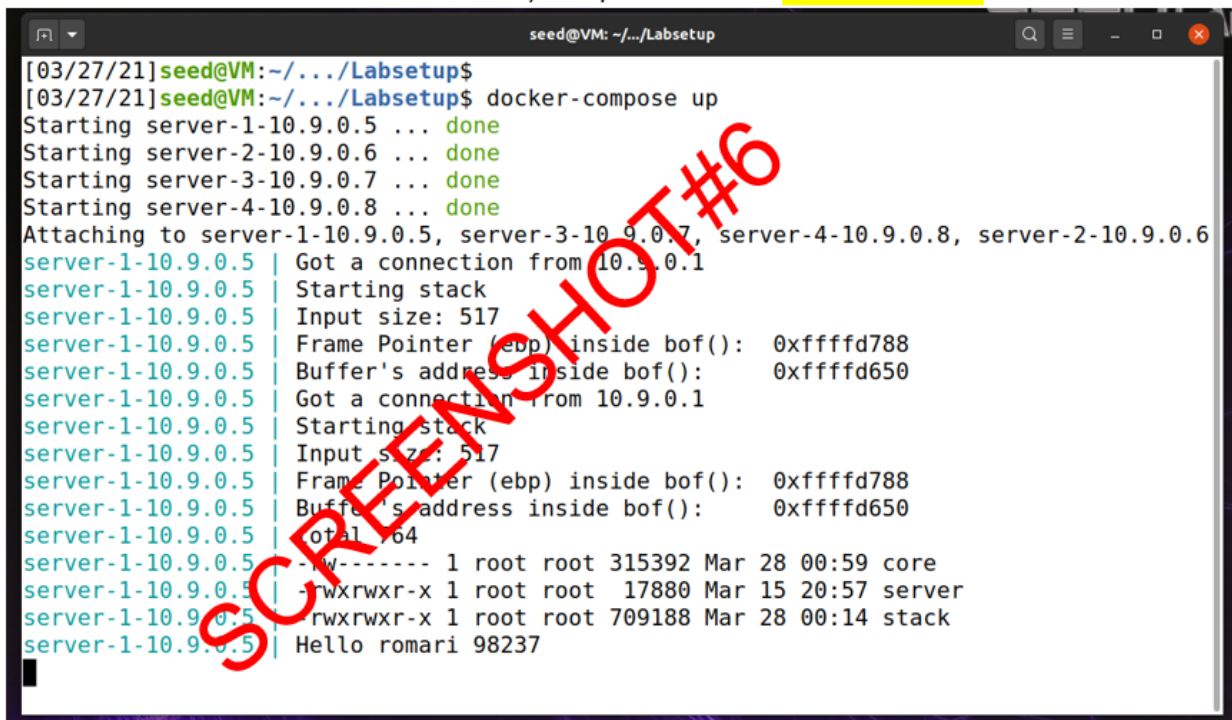
Question#2.6: What is the value of the offset in hexadecimal?

- 6- Run the exploit file, and send the badfile to the victim machine.

```
$ ./exploit.py
$ cat badfile | nc 10.9.0.5 9090
```

- 7- Observe the output on the server container (victim machine).

- 8- Take a screenshot of the terminal, and place it under **SCREENSHOT#6** in the answer file.



```
seed@VM: ~/.../Labsetup
[03/27/21]seed@VM:~/.../Labsetup$
[03/27/21]seed@VM:~/.../Labsetup$ docker-compose up
Starting server-1-10.9.0.5 ... done
Starting server-2-10.9.0.6 ... done
Starting server-3-10.9.0.7 ... done
Starting server-4-10.9.0.8 ... done
Attaching to server-1-10.9.0.5, server-3-10.9.0.7, server-4-10.9.0.8, server-2-10.9.0.6
server-1-10.9.0.5 | Got a connection from 10.9.0.1
server-1-10.9.0.5 | Starting stack
server-1-10.9.0.5 | Input size: 517
server-1-10.9.0.5 | Frame Pointer (ebp) inside bof(): 0xffffd788
server-1-10.9.0.5 | Buffer's address inside bof(): 0xffffd650
server-1-10.9.0.5 | Got a connection from 10.9.0.1
server-1-10.9.0.5 | Starting stack
server-1-10.9.0.5 | Input size: 517
server-1-10.9.0.5 | Frame Pointer (ebp) inside bof(): 0xffffd788
server-1-10.9.0.5 | Buffer's address inside bof(): 0xffffd650
server-1-10.9.0.5 | total 64
server-1-10.9.0.5 | -rw-r--r-- 1 root root 315392 Mar 28 00:59 core
server-1-10.9.0.5 | -rwxrwxr-x 1 root root 17880 Mar 15 20:57 server
server-1-10.9.0.5 | -rwxrwxr-x 1 root root 709188 Mar 28 00:14 stack
server-1-10.9.0.5 | Hello romari 98237
```

- 9- This is the end of Question 2. You can shut down your SEED VM now. You will not need it for the rest of this test.

Question 3 – Write a simple virus (10 Marks).

Write a simple virus to exploit a victim machine running a Windows operating system. The virus should perform the tasks listed below. Write the command(s) that should be issued to perform each of these tasks:



1. Force the deletion of all the files on the D, E, and F drives. (2.5 Marks)
2. Delete all entries in the HKCR registry key. (2.5 Marks)
3. Encrypt the files in a c:\data folder. (2.5 Marks)
4. Shutdown the victim machine with the message "Own3d!". (2.5 Marks)

End of Final Test.

Good luck!