Lab – CTF Walkthrough for HA: Forensics Flag #1

Overview

In this lab, you will complete the walkthrough for the CTF, HA: Forensics. This is a Capture the Flag type of challenge. It contains FOUR flags that are accessible as the solving of the lab progresses based on hints. It is a Forensics focused machine.

In this first lab, you will be tasked with capturing the first flag of the 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.

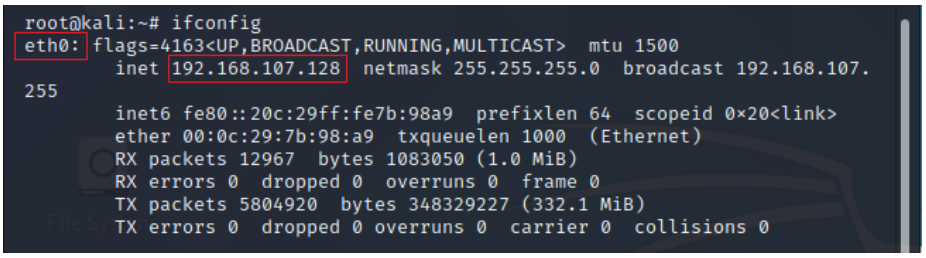
- Install of **VMware Workstation Player**
- Once virtual install of **Kali Linux for VMWare**.
- The OVA image file for HA: Forensics Target downloaded from **Vulnhub**

Begin the Lab!

Reconnaissance

From your Kali desktop, open a terminal, and at the prompt, type ifconfig. Find the IP address assigned to your Kali Linux eth0 adapter. If both your Kali and the target have their networking configured for host-only, they will both have joined the same network meaning they will share the network portion of the IP address assigned to your Kali's eth0 adapter.

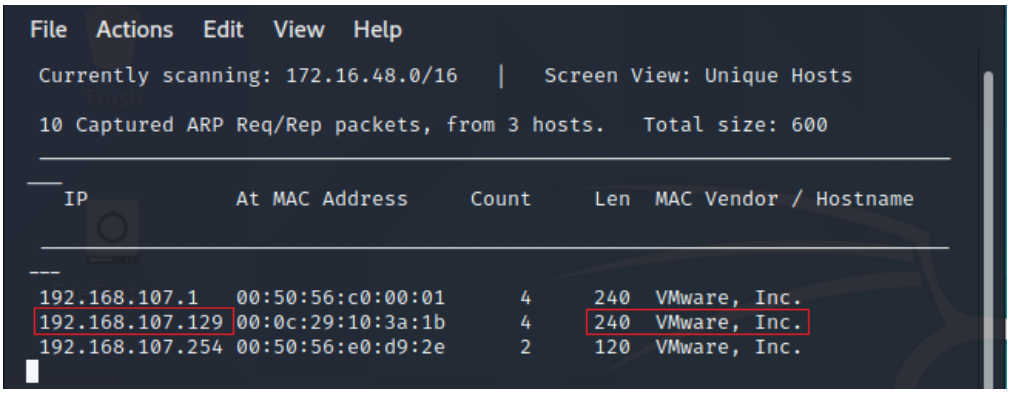
This is my IP address; yours may differ.



With the above information, we can find any target on the same network using netdiscover. Netdiscover uses ARP requests to find devices on the network.

At the prompt, type **`netdiscover -i eth0.`** This will send the ARP request out the same network adapter that Kali is using. The **`-i`** switch assigns the interface to use. Be patient; the scan takes a few minutes.

Press enter.

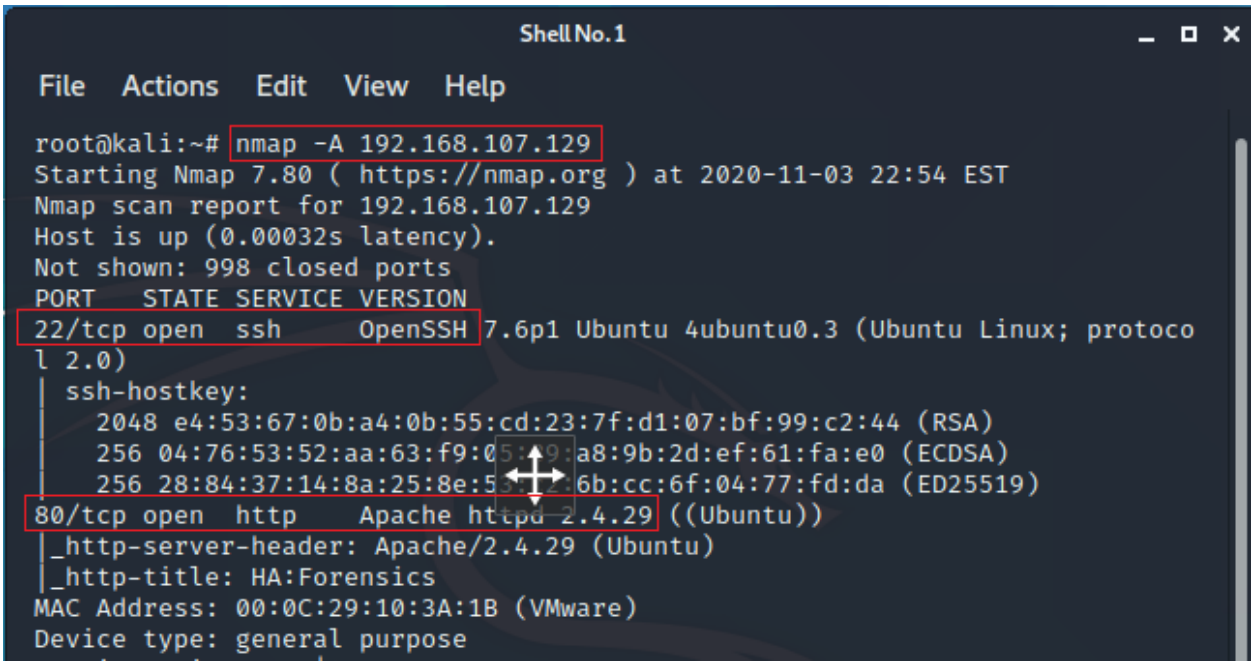


Our results come back relatively quickly. I can assume that the host IP of 129 belongs to my target.

We next need to run a nmap scan against our target, looking for any services that may be running.

`nmap -A 192.168.107.129`

The results show that we have port 22 running SSH and port 80 running a web service.

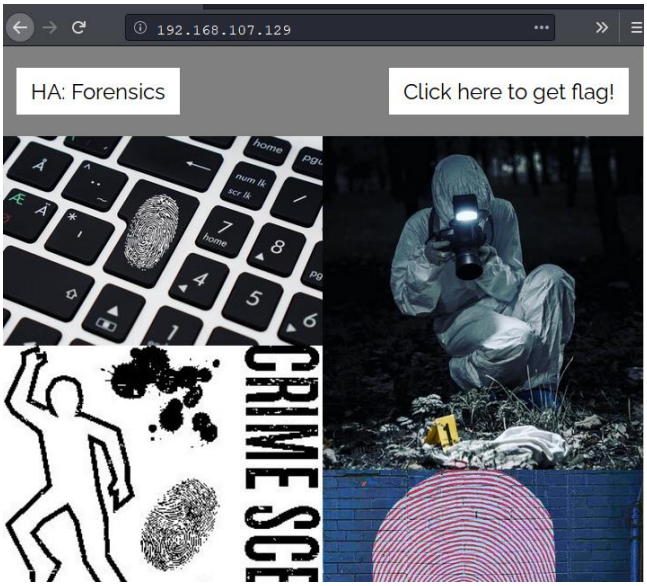


As always, we attend to the low hanging fruit first, which will be the HTTP service that is running on our target.

Open a browser and in the address bar, type the IP address of your target.

http://192.168.107.129

We see a button that says, “Click here to get flag!”



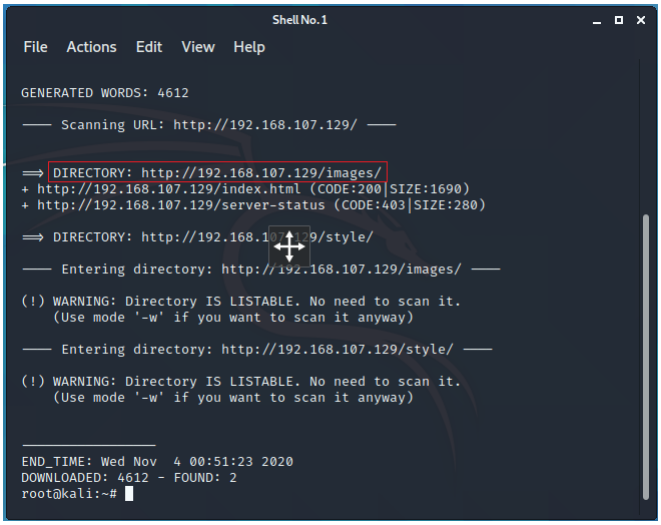
This is just a rabbit hole that goes nowhere.

We can close out our browser.

The webpage has some forensics images. Nothing unusual, so we can move on. Next, we need to brute force our way through the web server's directory. For this task, we will use dirb.

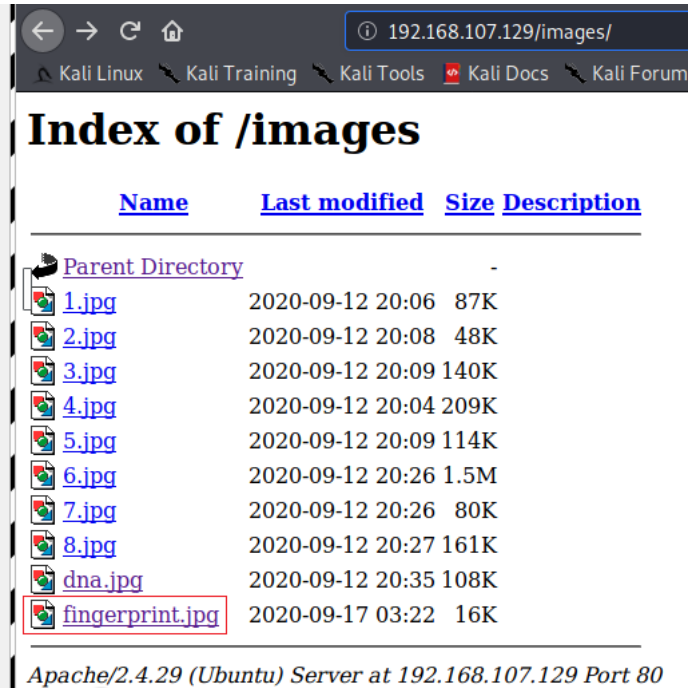
`dirb http://192.168.107.129`

We learn there is an image directory on the webserver.



We can view the contents of the images directory by using our web browser and appending the directory's name to the front of our IP address like so.

http://192.168.107.129/images/



Open the fingerprint.jpg image. Right-click on the image and save it to your Downloads directory. Close your browser.

Saving the image places a copy of the image in the Downloads directory.

Next, we need to examine the EXIF metadata of the image.

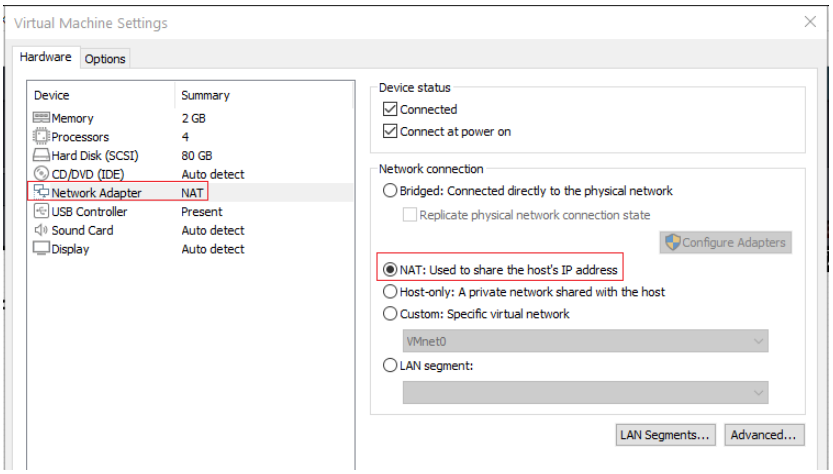
EXIF is short for Exchangeable Image File, a format that is a standard for storing interchange information in digital photography image files using JPEG compression. Almost all new digital cameras use the EXIF annotation, storing data on the image such as shutter speed, exposure compensation, F-number, what metering system was used, if a flash was used, ISO number, date and time the image was taken, white balance, auxiliary lenses that were used and resolution.

Some images may even store GPS information so you can easily see where the photos were taken!

There are different ways to view the EXIF data for the image, but not every way will work. For this lab, I attempted to use the Exiftool but without any luck. The thing about the Exiftool is that it is also an editor allowing you to modify the EXIF data.

If one tool does not work, there are others.

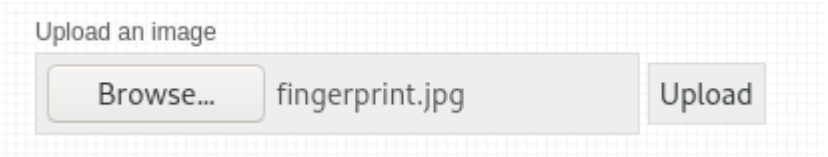
The easiest way to view the EXIF data is to use an online website. To access the Internet, access your VMware settings, and change your Kali network connection type from host-only to NAT.



Open your browser. Ensure you have Internet access. In the address bar, point your browser to

http://exifdata.com/exif.php

On the site's main page, upload your saved image file.



Once the image loads, you will be able to see a summary and detailed view of the EXIF data for the image. Click on the Detailed option.

Under the comment, you will see the hash for the first flag. Well done!

Change your Kali networking back to Host-only.

Congratulations! You have captured the first flag—time to move on to flag #2.

End of the lab!