**VulnHub – Empire LupinOne**

1. A screenshot of a computer screen

   Description automatically generatedThe first task is to obtain the ip-address of the victim machine. This involves using netdiscover command to scan the network.

Kali: 192.168.56.101 (eth1)

Victim: 192.168.56.107

1. A screen shot of a computer

   Description automatically generatedNext, perform a nmap scan to determine what ports and services are available.

* There are two ports open for ssh and http. This could mean an apache server.

1. Using nikto to find any vulnerabilities.

* A screen shot of a computer

  Description automatically generatedThis scan reveals apache 2.4.48.

1. Manual viewing of the website.

* A screenshot of a computer

  Description automatically generatedA thing that I immediately noticed was that the tab title is the ip and then a forward slash. This could indicate directory. Maybe a vulnerability is there, in the way this page has been set up. The site itself is just an image.

1. A screenshot of a computer

   Description automatically generatedExploring a vulnerability that nikto may have found was robots.txt.

* This could mean what we can manipulate the useragent or do some kind of URL injection.

1. My next thought is to use gobuster to try and brute force possible directories.

* A computer screen shot of a program

  Description automatically generatedthis only showed that robots.txt is the only available directory we can find.

1. A screenshot of a computer

   Description automatically generatedGoing into FFUF I was able to find secret. The reason why the FUZZ has the tilde is because if you look at the Disallow: /~myfile, this gives a hint that there may be something that starts with this symbol.
2. <http://192.168.56.107/~secret/> is the url used.

A screenshot of a computer

Description automatically generated

* A screenshot of a computer

  Description automatically generatedTo find this file we can re-use fuzzing on the url to determine the possible directory.
* The output of this discovers a secret file mysecret.txt.
* A screenshot of a computer

  Description automatically generatedfollowing this url will lead you to the encrypted SSH private key. This is however, in base 58.

1. Download the file using wget.

* A computer screen shot of a computer code

  Description automatically generatedThe file when it is downloaded with be using the period symbol at the beginning of the file which indicates it will be hidden.
* Change this to see it.

1. Once you have converted to file from base58 to text, then you need to obtain the hash for john.



1. A screenshot of a computer program

   Description automatically generatedNow it is time to crack the password.

* To check the password run the following:

A screen shot of a computer code

Description automatically generated

* Now we have his username: icex64 and password: P@55w0rd!

1. I was unable to get past this point because the OPENSSH private key was apparently in bad format. The password I kept trying also didn’t work. I googled multiple times and found the password, username and ssh command to be correct. I wasn’t able to get in but I obtain all the information to get in.