**The Code Caper**

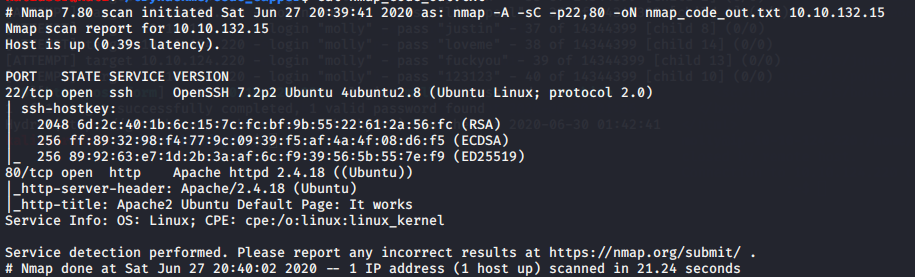
This was an interesting room covering web enumeration, reverse shell, command execution, and buffer overflow concepts. It is a guided room, so it is more like a tutorial.

**Task 1 : Intro**

Deploy the machine

**Task 2 : Host Enumeration**

Run the Nmap

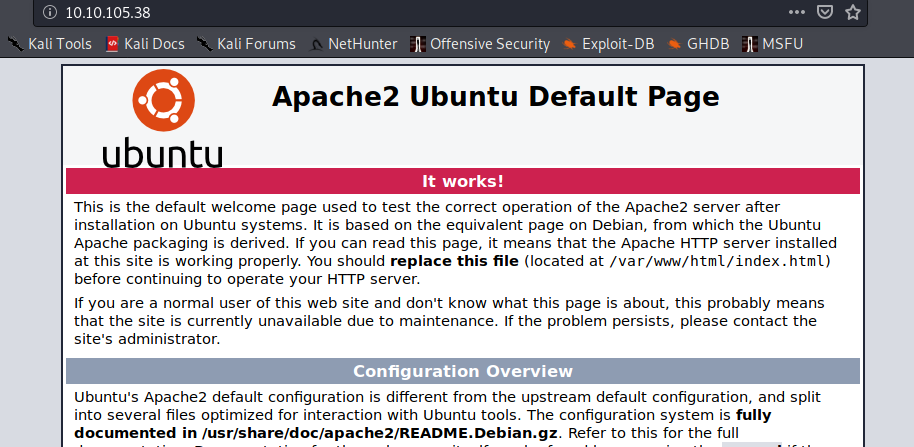


From the Nmap output we gat :

**2.1 :** 2

**2.3 :** OpenSSH 7.2p2 Ubuntu 4ubuntu2.8

**2.4 :** Apache/2.4.18



And opening the web page we get

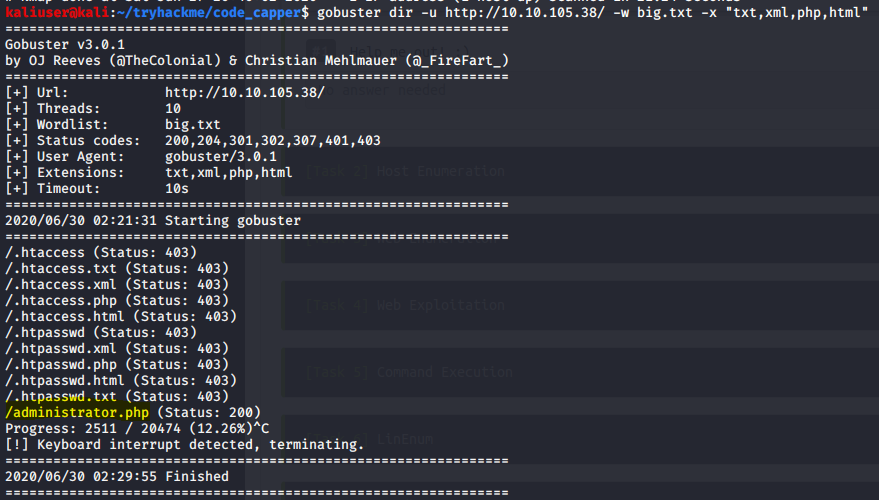
**2.2 :** "Apache2 Ubuntu Default Page: It works"

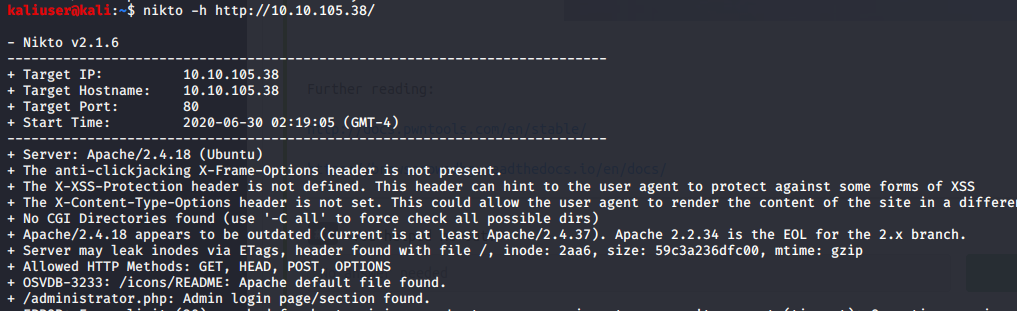
**Task 3 : Web Enumeration**

As given in the intro I ran gobuster command with suggested wordlist.

Point to note -x flag with specific extensions is very important as I ran it without the flag and after very long I found 0 files :P

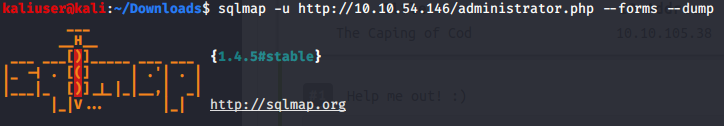
But I had also run Nikto tool so it had also found administrator.php file

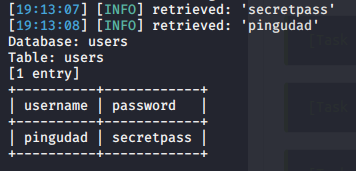




**3.1** administrator.php

**Task 4 : Web Exploitation**





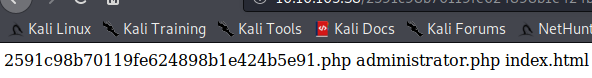
**4.1 :** pingudad

**4.2 :** secretpass

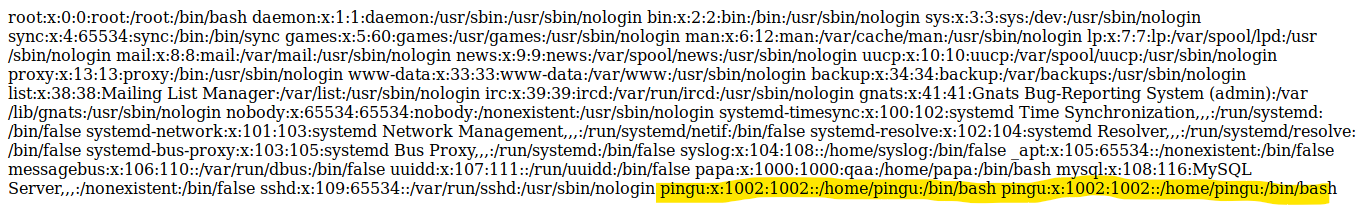
**4.4 :** 3 (from the sqlmap verbose prompt)

**Task 5 : Command Execution**

**5.1 :** 3

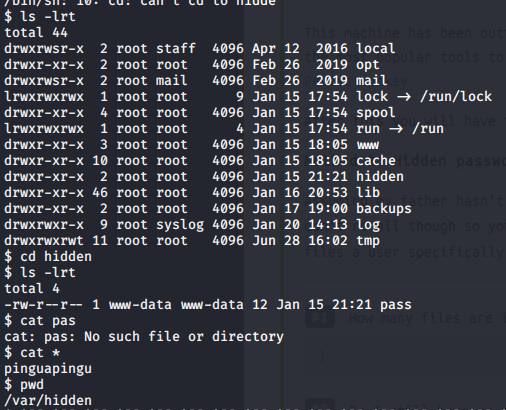


**5.2 :** yes



For pingu's password I opened a reverse shell, Although it is mentioned that nc is installed none of the nc shells worked for me. I got the reverse shell using perl.

after getting the reverse shell I was just navigating through systems and I found a "hidden" directory which had a file called pass contain the required password



**Task 6 : Linenum**

Downloaded the Linenum file and used scp to transfer it to machine ran it and checked the output

**6.1 :** /opt/secret/root

Task 7 : pwndgb

**7.1 :** read :)

Task 8 : Binary Exploitation : manually

**8.1 :** followed the instructions

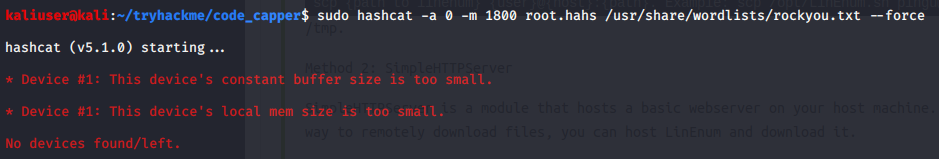
**Task 9 : Binary Exploitation: The pwntools way**

**9.1** Wrote the python script and ran

**Task 10 :** Finishing the job

From analysing the hash and referring to link given we could infer it is a 512sha hash

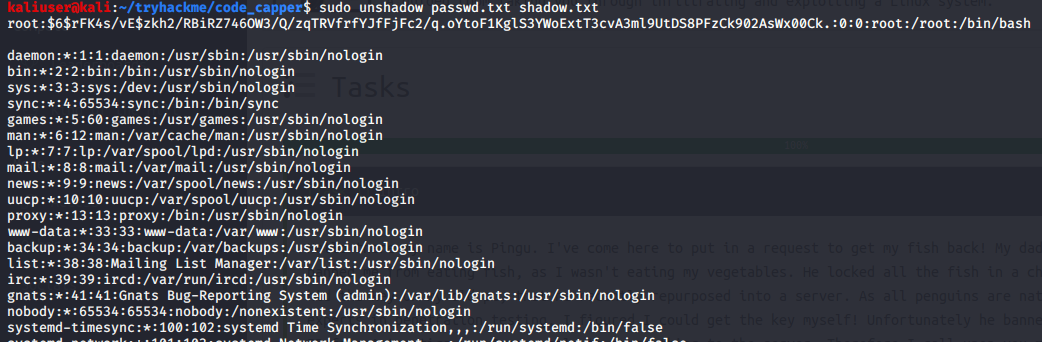
I have Kali VM and hashcat is not work saying no devices found



So I cracked the password using John

First I copied /etc/passwd and /etc/shadow file in my local machine

And used unshadow utility



|  |  |
| --- | --- |
| Here unshadow step was not necessary |  |

And then ran John

