**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.

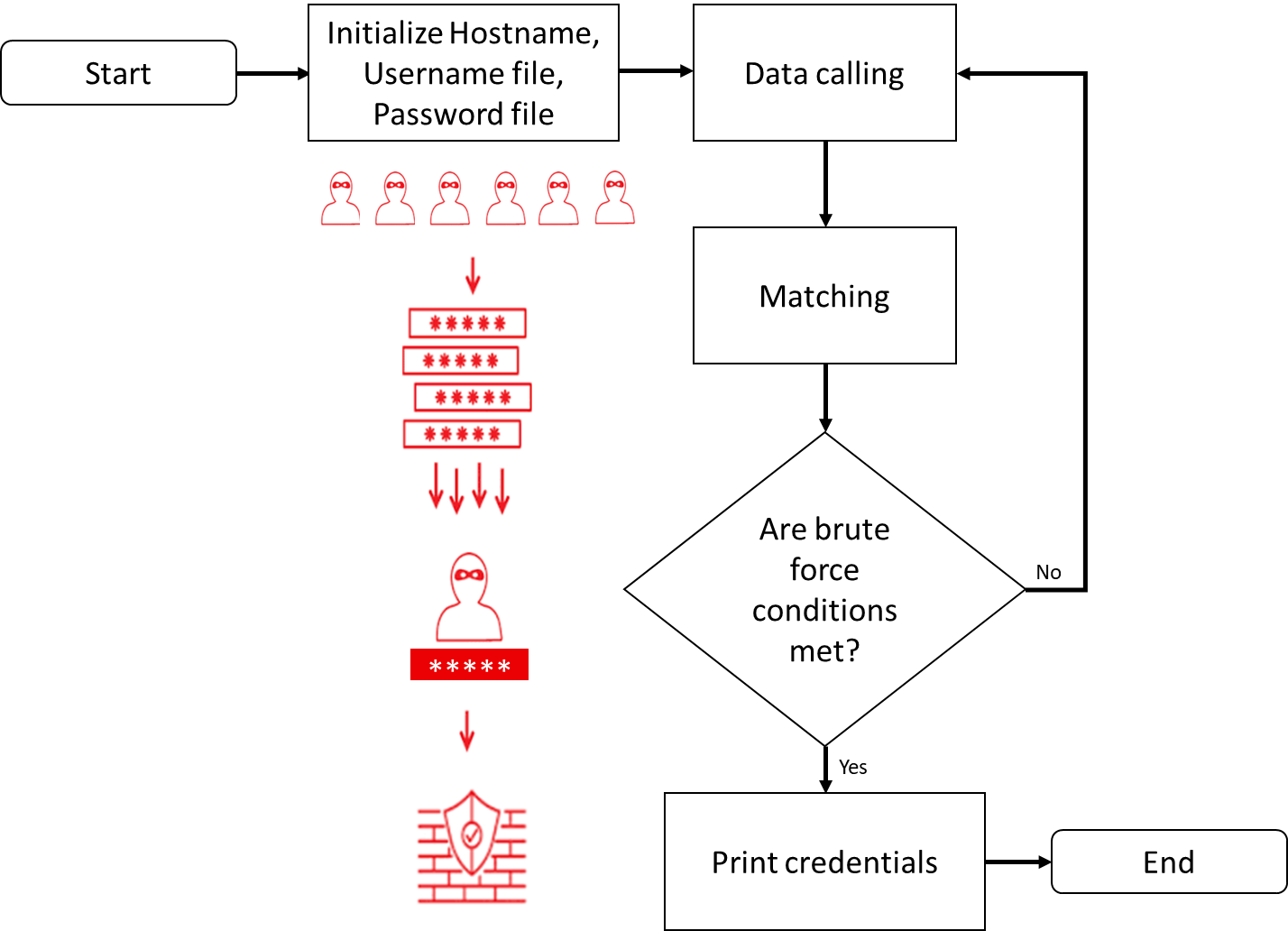
**Aim:**

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

**Problem Statement:**

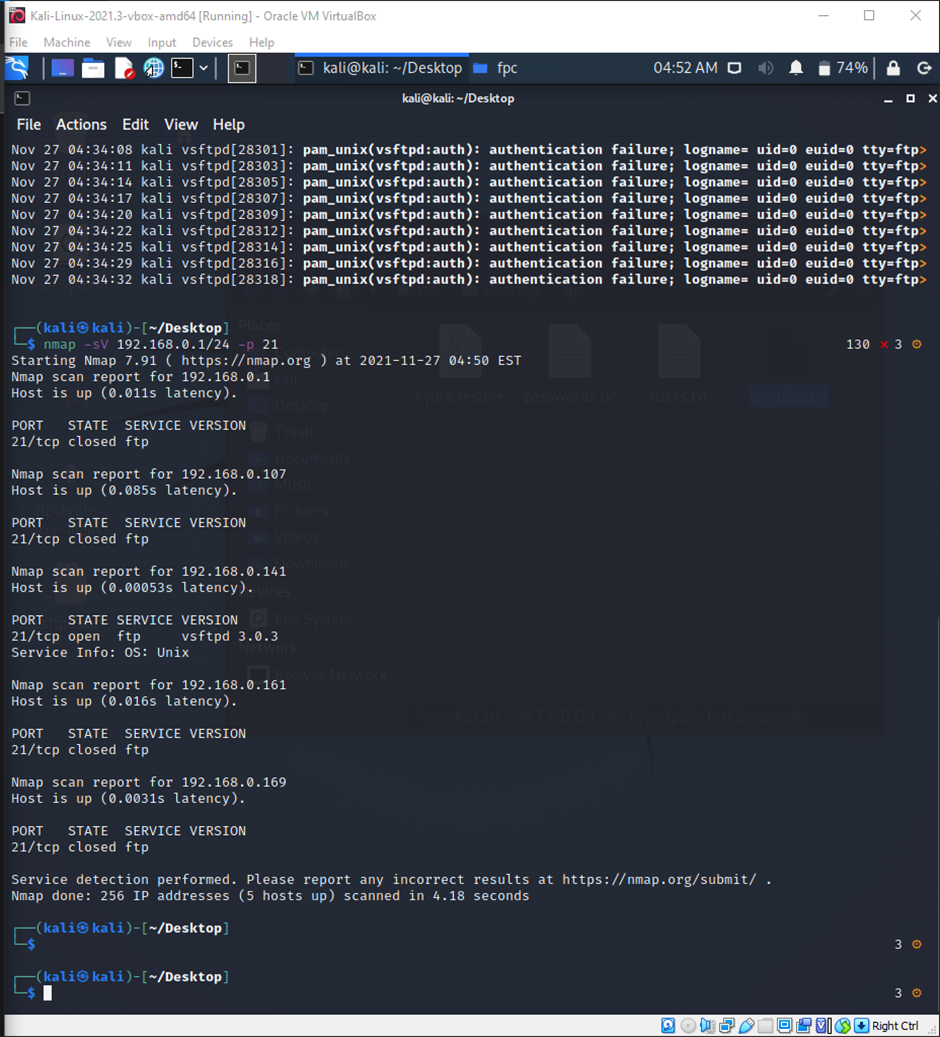
Hack FTP server credentials using **‘Dictionary attack’** (bruteforcing with a wordlist) and access its content files.

**Block Diagram:**



**Procedure:**

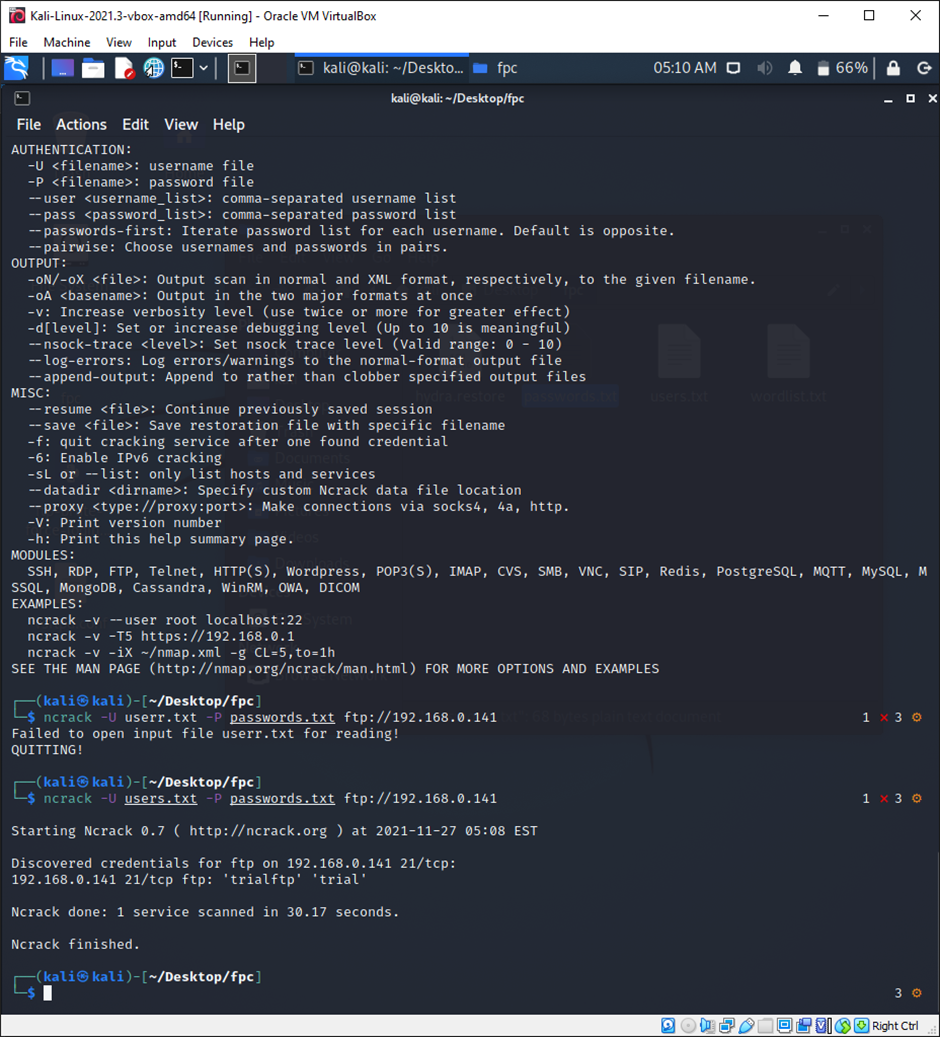
1. Perform an nmap scan in the command prompt. It gives a list of available ftp servers. Look for state- ‘open’.

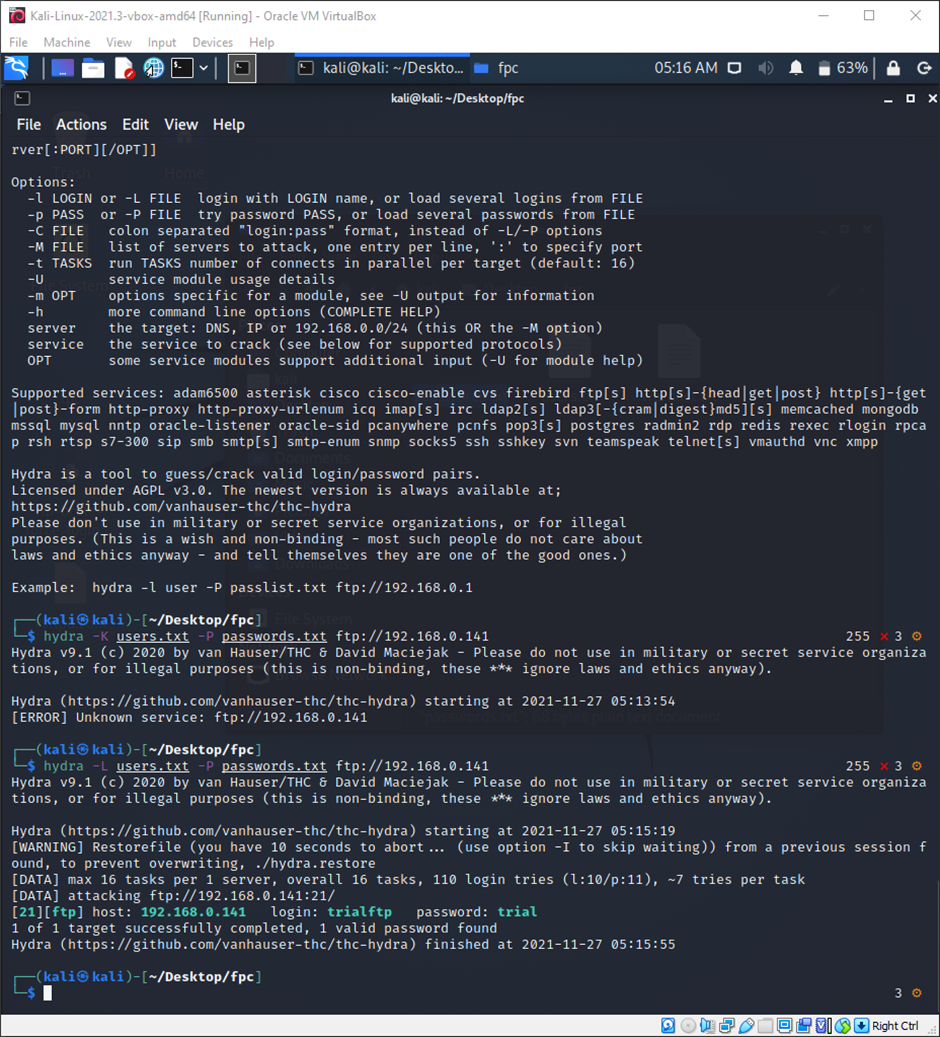
****

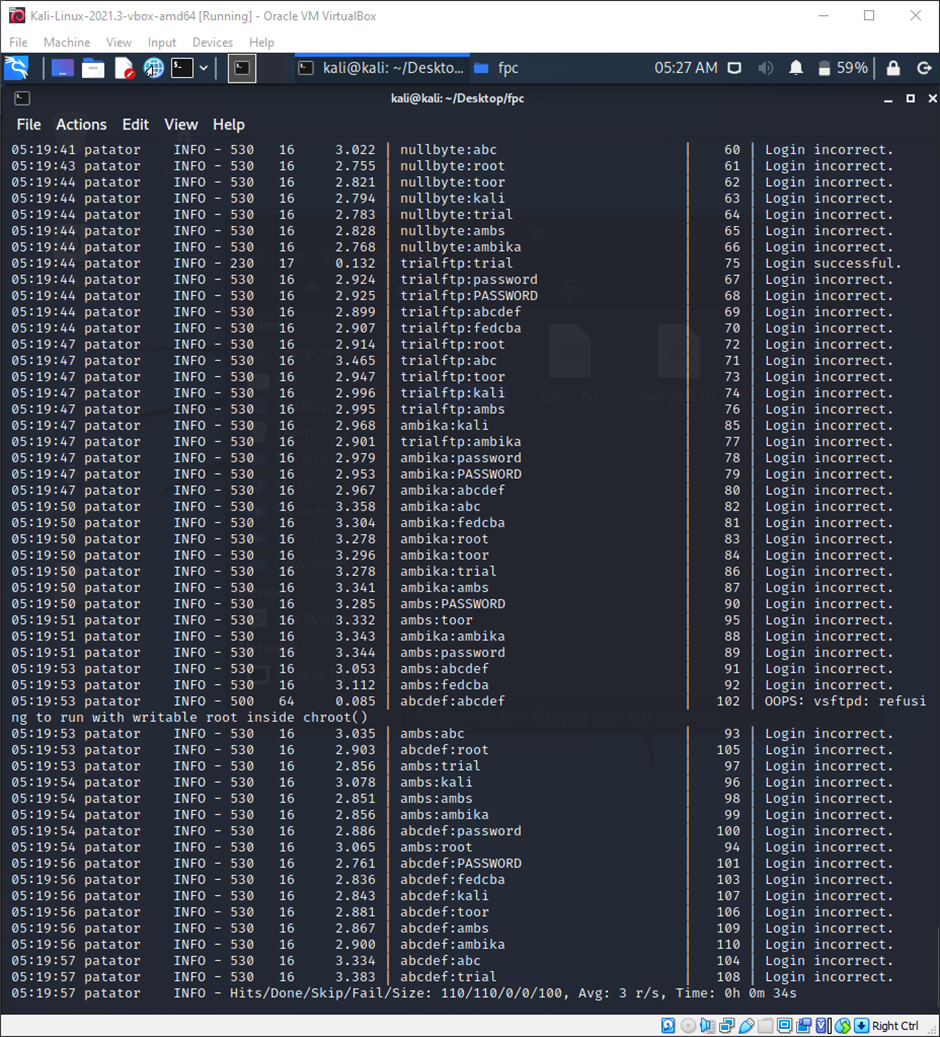
1. Once you obtain an active ftp server, you can begin brute-forcing. Start wireshark capture and run the .py file containing the ftplib module. If the credentials match, they are displayed in the terminal.



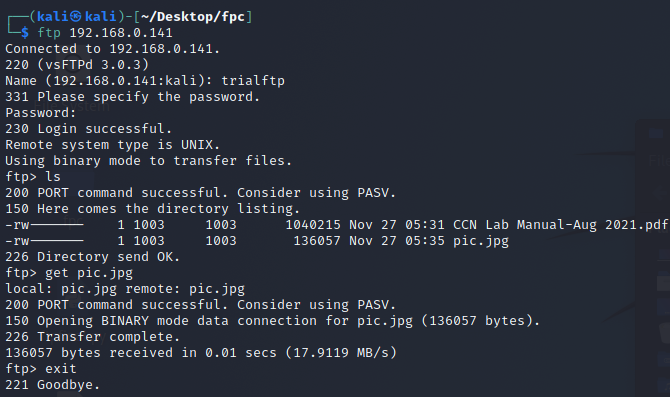
1. Similarly, brute-forcing can be done using tools like NCRACK and HYDRA in LINUX. They take in wordlist files for both usernames and passwords and try to get the right combination. PATATOR, another tool in Linux, lists out all the possible combinations, stating if they are correct or not.







1. 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.

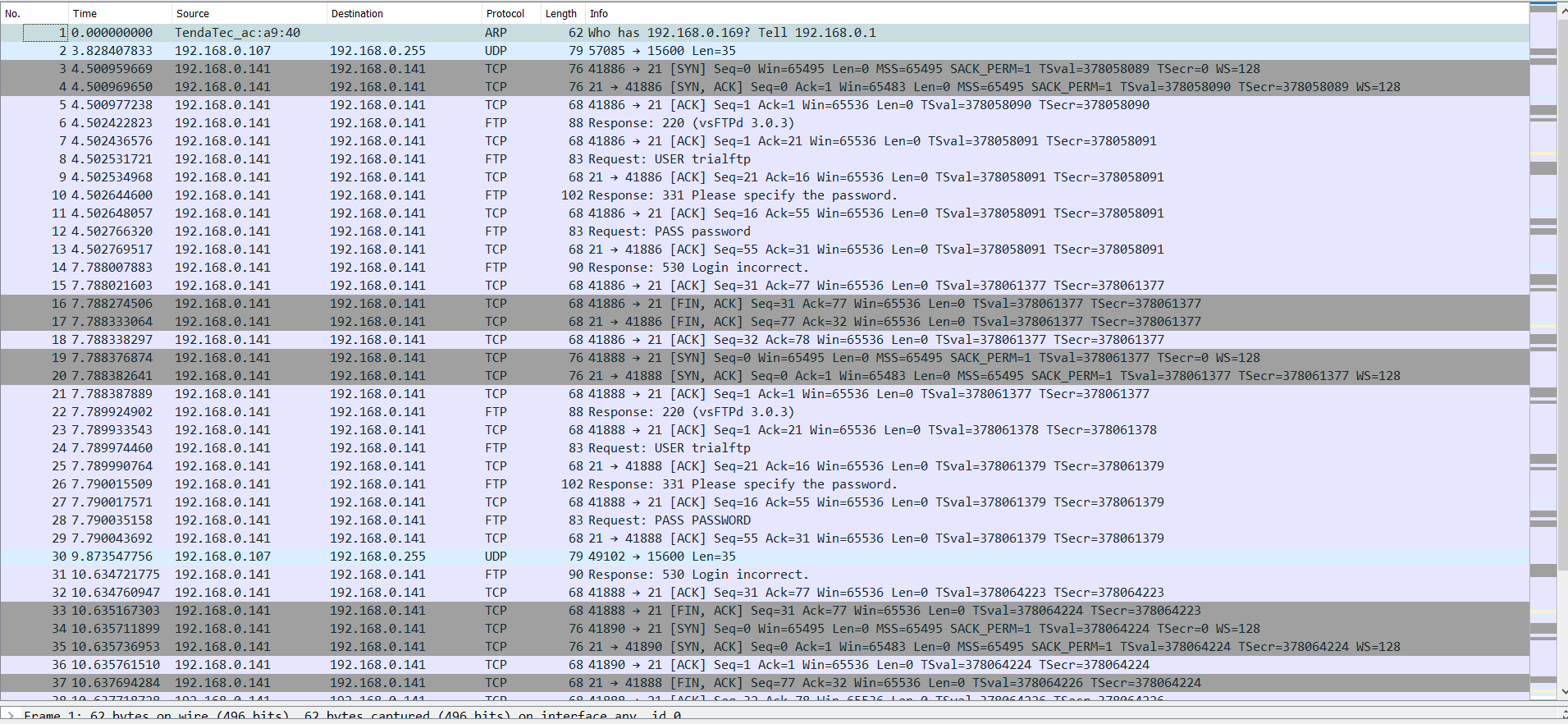


**Concepts Used:**

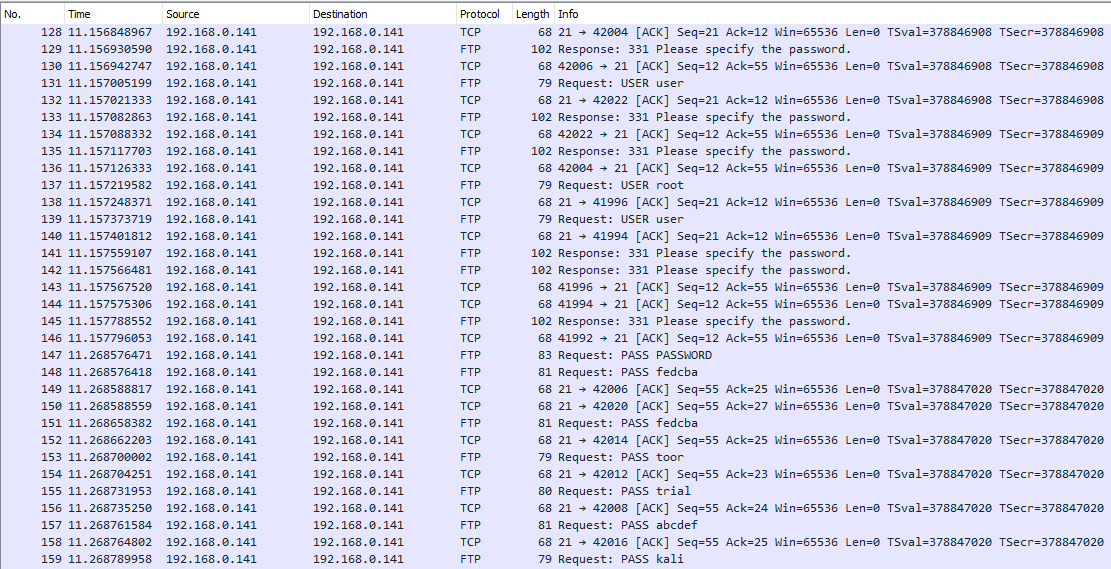
1. .py file: modules- ftblib, sys, ArpParse
2. Wireshark for packet sniffing
3. nmap, ncrack, hydra, patator.

**Wireshark Snapshots:**

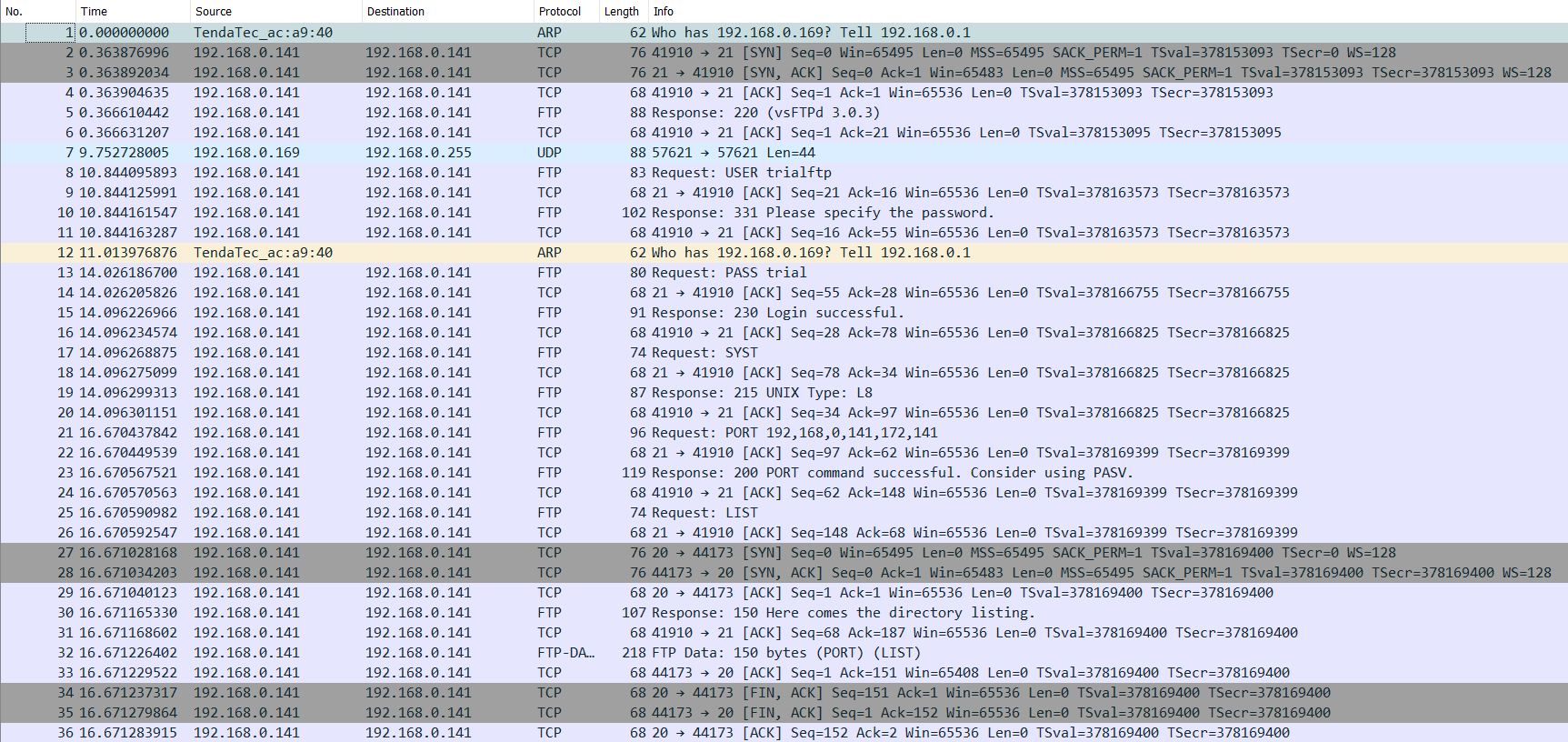
1. Sniffing of the python attack



1. Sniffing hydra attack



1. Sniffing the GET command



**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>