RV UNIVERSITY

School of Computer Science and Engineering

Bengaluru – 560059

ETHICAL HACKING ESSENTIALS

COURSE CODE: CS3432

VI Semester B.Sc/B.Tech (HONS.)

Name	**Aditya Kushal**
USN	**1RVU22CSE008**
Title	**Task 2 (a) Capture and Analyze Network Traffic Using Wireshark**

LIST OF CONTENTS

Introduction

This project focuses on capturing and analyzing both insecure (FTP) and secure (FTPS) file transfer traffic using Wireshark. It demonstrates the risks of unencrypted protocols and the value of secure communication.

Basic Working of FTP

FTP (File Transfer Protocol) is a standard network protocol used to transfer files between a client and a server over a TCP-based network. It operates in two modes:

- **Command Channel**: Transmits commands and responses
- **Data Channel**: Transfers files

A typical session involves:

1. Client connects to the server on port 21
2. Client sends login credentials (often in plaintext)
3. Client uploads or downloads files using commands like STOR or RETR

Basic Working of TLS

TLS (Transport Layer Security) is a cryptographic protocol that ensures privacy and data integrity between applications. It works by:

1. Performing a **handshake** to establish a secure session
2. Generating **session keys** using asymmetric encryption (public/private keys)
3. Encrypting all subsequent data using symmetric encryption

FTPS is FTP secured with TLS, where:

- The control and data channels are encrypted
- It prevents eavesdropping and tampering

This lab setup helps visualize how FTP transmits data in plaintext while FTPS protects it with encryption.

Tools Used

- **Operating System**: Arch Linux (or any Linux distribution)

- **Python 3**
- **vsftpd** – Very Secure FTP Daemon
- **OpenSSL** – for generating SSL certificates
- **Wireshark** – network traffic analyzer

Step-by-Step Execution

1. Install vsftpd

sudo pacman -S vsftpd

2. Set Up Insecure FTP Server

sudo python3 setup_ftp.py

- Configures /etc/vsftpd.conf
- Enables anonymous login
- Creates directories: ftp/ and uploads/
- Starts vsftpd server

3. Set Up Secure FTPS Server

sudo python3 setup_ftps.py

- Generates SSL cert at /etc/ssl/private/vsftpd.pem
- Enables TLS encryption
- Configures secure vsftpd settings
- Waits for user input STOP to shutdown

4. Create a Test File

echo "This is confidential data for Wireshark demo." > secret.txt

5. Run FTP Client Script

python3 demo_ftp.py

- Logs in as anonymous
- Uploads and downloads secret.txt using ftp module

6. Run FTPS Client Script

python3 demo_ftps.py

- Uses FTP_TLS
- Secures data transfer with prot_p()

7. Capture with Wireshark

- Start Wireshark on lo interface
- Apply filters:
    - FTP: ftp || ftp-data
    - FTPS: tls
- Observe transmission behavior in both protocols

Findings & Analysis

- **FTP**:
    - Sends usernames, passwords, and file contents in **plaintext**
    - Easily viewable in Wireshark, exposing sensitive data like:
        - USER anonymous
        - PASS 12345
        - File content during upload/download
- **FTPS**:
    - All data encrypted via TLS
    - FTP commands and file contents are **not readable**
    - Traffic seen as TLS packets in Wireshark

These findings emphasize how insecure FTP is unsuitable for any sensitive or production use, and highlight the effectiveness of TLS encryption in FTPS.

Recommendations

- Avoid using FTP in production environments
- Use **SFTP** or **FTPS** for secure file transfer
- Employ **firewalls** and **VPNs** to isolate FTP/FTPS services
- Regularly **audit** network services and ports
- Always test network protocols using tools like Wireshark to identify vulnerabilities

Conclusion

The project successfully demonstrates how network traffic varies between insecure (FTP) and secure (FTPS) transfers. Using Wireshark, students can observe critical security flaws in FTP and the protection provided by FTPS. Such practical analysis is essential for ethical hackers and security professionals to identify and mitigate real-world vulnerabilities.

Screenshots

setup_ftp.py

```
(ethical_hacking) [arch@arch wireshark_ftp_traffic_analysis]$ sudo python setup_ftp.py
[sudo] password for arch:
[*] Writing config...
[*] Restarting vsftpd service...
[+] vsftpd started with demo config.

📡 FTP server running with demo config.
🛑 Type 'STOP' and press Enter to stop the server and delete the config :
```

Wireshark

Username and Password Leaked

```
 82 Request: USER anonymous
 66 21 → 42666 [ACK] Seq=21 Ack=17 Win=65536 Len=0 TSval=3635043420 TSecr=3635043420
100 Response: 331 Please specify the password.
 78 Request: PASS 12345
 89 Response: 230 Login successful.
```

Data Leaked

```
112 FTP Data: 46 bytes (PASV) (STOR uploads/secret.txt)
 66 13567 → 33816 [ACK] Seq=1 Ack=47 Win=65536 Len=0 TSval=3635043424 TSecr=3635043424
 66 33816 → 13567 [FIN, ACK] Seq=47 Ack=1 Win=65536 Len=0 TSval=3635043424 TSecr=3635043424
```

```
e lo, id 0
00:00:00:00:00:00)

Len: 46
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E·
0010  00 62 5a 1e 40 00 40 06  e2 75 7f 00 00 01 7f 00   ·bZ·@·@· ·u·····
0020  00 01 84 18 34 ff 16 8a  d8 33 60 f2 e0 28 80 18   ····4··· ·3`··(··
0030  02 00 fe 56 00 00 01 01  08 0a d8 aa 5c 60 d8 aa   ···V···· ····\`··
0040  5c 60 54 68 69 73 20 69  73 20 63 6f 6e 66 69 64   \`This i s confid
0050  65 6e 74 69 61 6c 20 64  61 74 61 20 66 6f 72 20   ential d ata for
0060  57 69 72 65 73 68 61 72  6b 20 64 65 6d 6f 2e 0a   Wireshar k demo.·
```

Next Page

setup_ftps.py

```
(ethical_hacking) [arch@arch wireshark_ftp_traffic_analysis]$ sudo python setup_ftps.py
[*] Cleaning up config, cert, and FTP root...
[+] Cleanup complete.
[*] Generating self-signed SSL certificate...
...+.....+......+.+..................+.........+.....+.+..+...+....+..+.+..+......+.......
...+....+..+++++++++++++++++++++++++++++++++++++++*.+.............+.........+.......+..+.
......+.........+..+......+.+.....................+.+.....+....+......+........+.+......+.
.+...+.......++++++++++++++++++++++++++++++++++++++*.+......+......+.++++++++++++++++++++
.....+...+.....+.........+...+..+......+.........+.....+.......+.....+...+....++++++
-----
[+] SSL certificate created at /etc/ssl/private/vsftpd.pem
[*] Writing vsftpd config...
[*] Restarting vsftpd service...
[+] FTPS server started.

📡 FTPS server running with demo config.
🛑 Type 'STOP' to stop server and clean up:
```

Wireshark

Data is Encrypted

```
  1629 Server Hello, Application Data, Application Data, Application Data, Application Data, Application Data
   170 Application Data, Application Data
   321 Application Data
   104 Application Data
   321 Application Data
   122 Application Data
   100 Application Data
   111 Application Data
    96 Application Data
   108 Application Data
    96 Application Data
   111 Application Data
    96 Application Data
   119 Application Data
    94 Application Data
   136 Application Data
   113 Application Data
   110 Application Data
   583 Client Hello
```

```
nterface lo, id 0
 (00:00:00:00:00:00)

51, Len: 1563
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ···· ···· ···· ··E·
0010  06 4f bd cb 40 00 40 06  78 db 7f 00 00 01 7f 00   ·O·· @·@· x··· ····
0020  00 01 00 15 91 12 eb f2  13 41 b0 11 1f 81 80 18   ···· ···· ·A·· ····
0030  02 00 04 44 00 00 01 01  08 0a d8 b0 61 76 d8 b0   ···D ···· ···· av··
0040  61 74 16 03 03 00 9b 02  00 00 97 03 03 f2 42 f5   at·· ···· ···· ··B·
0050  5d 83 0c ee 07 64 4e c2  67 f3 69 62 e1 2d 5a ea   ]···· dN· g·ib ·-Z·
0060  bf a0 dc ad e4 ce e9 45  f5 96 a0 e1 e2 20 e6 1d   ···· ···E ···· ·· ··
0070  c8 87 02 18 aa 57 b4 ca  1d 9f 23 10 7c 53 0e 2f   ···· ·W·· ··#· |S·/
0080  10 c9 e0 95 31 b4 de 66  8b 33 33 6f 21 e7 13 02   ···· 1··f ·33o! ····
0090  00 00 4f 00 2b 00 02 03  04 00 33 00 45 00 17 00   ··O· +··· ··3· E···
00a0  41 04 1e d2 77 20 71 66  48 e5 5c de 51 a6 24 45   A··· w qf H·\· Q·$E
00b0  b9 27 1a 4e 5e c4 7a f7  72 c5 3e 6e 25 41 7a 0b   ·'·N ^·z· r·>n %Az·
00c0  6a e6 70 2e 68 64 7e 05  28 5e d2 ab 9a 2e 1f 91   j·p· hd~· (^·· ····
00d0  88 0b c7 35 2f c5 a5 86  3d a9 c5 de 6c a5 a4 e1   ···5 /··· =··· l···
00e0  ec 88 17 03 03 00 17 1e  a9 24 c6 00 45 ad c6 ae   ···· ···· ·$·· E···
00f0  47 6e 99 24 82 11 8a 70  d7 5b ea d0 4c fe 17 03   Gn·$ ···p ·[·· L···
0100  03 00 44 ef bc eb b0 61  26 c4 e0 fd a7 4a 86 2c   ··D· ···a &··· ·J·,
0110  28 9a 3e e6 c8 5d 1f 20  32 d5 70 a3 23 35 c6 c8   (·>· ·]· 2·p· #5··
0120  94 1f 67 7b de ec fb 42  a7 3d 8b 7c 1c 1d 26 55   ··g{ ···B ·=·| ··&U
0130  d5 40 35 f1 0d d0 ca 82  9b d8 99 93 74 c7 15 8d   ·@5· ···· ···· t···
0140  e3 57 e3 33 53 d4 2a 17  03 03 03 a9 f9 fd f1 f0   ·W·3 S·*· ···· ····
0150  f1 62 cc dc 12 e6 ef 4e  25 68 0b 3d 64 e1 2a 0b   ·b·· ···N %h·=d·*·
0160  a7 54 87 42 15 61 0f 12  df bb af 7e 54 ca 10 f8   ·T·B ·a·· ···~T···
0170  5a 4d 4c 73 0f 8b 9f 3c  5d 0b 56 3e aa b9 e9 25   ZMLs ···< ]·V> ···%
```