

Samuel Oates
 Lab Assignment #5
 3/22/2019

Tftpd64 Directory

The screenshot shows a virtual machine environment with a FileZilla client window and a Tftpd64 directory listing window. The FileZilla window shows a successful transfer of a file. The Tftpd64 directory listing window shows the following files:

file	start time	progress
peer		
desktop.ini	1/10/2017 282	
putty.exe	1/13/2017 531 368	
SamuelOates_tftp.bt	3/22/2019 22	
Tftpd64.lnk	3/2/2017 1699	

The FileZilla window shows the following transfer details:

Server/Local file	Direction	Remote file
Selected 1 file. Total size: 22 bytes		
Queued files	Failed transfers	Successful transfers (1)

FileZilla Window displaying the successful file transfer

The screenshot shows a FileZilla client window displaying the successful transfer of a file. The window shows the local site view and the transfer details.

Transfer Details:

Server/Local file	Direction	Remote file	Size	Priority	Time
student@172.30.0.10	<<<	/SamuelOates_tftp.bt	22	Normal	3/22/2019 2:12:35 PM

Local Site View:

Filename	Filesize	Filetype	Last modified
connections		File folder	2/7/2017 10:35:27 ...
desktop.ini	282	Configuration ...	1/10/2017 5:04:55 ...
File Transfer.lnk	2,453	Shortcut	2/22/2017 12:40:09...
SamuelOates_tft...	22	Text Document	3/22/2019 2:12:35 ...
Tftpd64.lnk	1,699	Shortcut	1/16/2017 12:45:53...

Captured file transfer in the entire Wireshark window

LAB GUIDE

- 2. Introduction
- 3. Section 1: Hands-On Demonstration
 - Part 1: Generate Network Traffic
 - Part 2: Analyze Traffic using Wireshark
 - Part 3: Analyze Traffic using NetWitness Investigator
- Part 2: Analyze Traffic using Wireshark**

17. Use the **down arrow** to locate the name of the file transferred during the FTP session.

While Wireshark could not capture the contents of the transferred file, almost everything else was easily visible in clear text. Despite this lack of security, FTP is still an extremely popular method of sharing and transferring files over the Internet.

```

0000  00 50 56 a6 e7 08 00 50 56 a6 f8 42 08 00 41 02  ..PV..P.V..E..
0010  00 48 5f a7 08 00 00 00 42 05 6c 18 00 00 00 18  ..@..S.....
0020  00 0a c2 26 00 15 05 e7 08 49 07 70 01 50 58 18  ..@..@..@..@..
0030  00 15 f9 c3 08 00 52 05 50 52 0a 04 0f 05 74 0a  ..@..@..@..@..
0040  61 65 65 5f 74 66 74 70 24 74 70 74 0a 0a  ..mFTP.txt...
    
```

Captured file transfer

```

0000  00 50 56 a6 7b 61 00 50 56 a6 50 44 08 00 45 02  ..PV..a.P.V.PD..E..
0010  00 5e 7c 23 40 00 00 06 26 2c ac 1e 00 0a ac 1e  ..^|@#...&.....
0020  00 02 00 15 c2 33 34 cd 14 44 01 49 6d 92 50 18  ....34..D.Im.P..
0030  20 14 1e 59 00 00 32 32 36 20 53 75 63 63 65 73  ..Y..22 6 Succes
0040  73 66 75 6e 6e 79 20 74 72 61 5e 73 66 65 72 72  sfully E transferr
0050  65 64 20 22 2f 53 61 6d 75 65 6c 6f 61 74 65 73  ed "/SamuelOates
0060  5f 74 66 74 70 2e 74 78 74 22 0d 0a  .._tftp.tx t"...
    
```

File Transfer Protocol (FTP): Protocol | Packets: 333 | Displayed: 43 (12.9%) | Dropped: 0 (0.0%) | Profile: Default

Password information for the yourname_collection

LAB GUIDE

- Part 1: Generate Network Traffic
- Part 2: Analyze Traffic using Wireshark
- Part 3: Analyze Traffic using NetWitness Investigator

4. Section 2: Applied Learning

5. Section 3: Lab Challenge and Analysis

Part 3: Analyze Traffic using NetWitness Investigator

9. Under the Password category, click the **[open]** link to open the report.

10. Under the Password category, click the **(2)** link to view the session details related to password captures.

11. Make a screen capture showing the password information for the **yourname_collection** and paste it into your Lab Report file.

12. Close the NetWitness Investigator window.

NetWitness Investigator 10.6

Collection: SamuelOates_S1_Collection > Password EXISTS > Sessions for "p@ssw0rd"

Time	Service	Size	Events
2019-Mar-22 14:10:26	IP / TCP / FTP	2.45 KB	<ul style="list-style-type: none"> 00:50:56:A6:7B:61 -> 00:50:56:A6:50:44 172.30.0.2 -> 172.30.0.10 49713 -> 21 (ftp) payload: 738 medium: Ethernet tcp.flags: 219 streams: 2 packets: 32 lifetime: 120 action: login username: student password: P@ssw0rd! 1 linked session
2019-Mar-22 14:12:15	IP / TCP / FTP	2.28 KB	<ul style="list-style-type: none"> 00:50:56:A6:7B:61 -> 00:50:56:A6:50:44 172.30.0.2 -> 172.30.0.10 49715 -> 21 (ftp) payload: 658 medium: Ethernet tcp.flags: 219 streams: 2 packets: 30 lifetime: 80 action: login username: student password: P@ssw0rd! action: get filename: SamuelOates_tftp.txt

My name S2 TFTPd64 directory

Performing Packet Capture and Traffic Analysis
Samuel Oates
2 hours remaining

LAB GUIDE

3. Section 1: Hands-On Demonstration

4. Section 2: Applied Learning

- Part 1: Generate Network Traffic
- Part 2: Analyze Traffic using Wireshark
- Part 3: Analyze Traffic using NetWitness Investigator

Part 1: Generate Network Traffic

20. At the command prompt, **execute the command** to transfer `yourname_S2_tftp.txt` to TargetWindows02 using `tftp`, then **close the command prompt window**.

You will see a successful TFTP file transfer of `yourname_S2_tftp.txt` from the vWorkstation desktop to TargetWindows02.

21. **Restore the remote TargetWindows02 connection**.

22. In the Tftp64 window, **click the Show Dir button** to confirm the file transfer was successful.

23. **Make a screen capture** showing `yourname_S2_tftp.txt` in the Tftp64 directory and **paste it** into your Lab Report file.

24. **Close the directory window** and the Tftp64 window.

25. **Launch FileZilla Server**, then minimize the remote TargetWindows02 connection.

Tftp64 by Ph. Jouin

Current Directory: C:\Program Files\Tftp64

Server interfaces: 172.30.0.10 vrnnet3 Ethernet Adapter

Tftp Server Log view

Tftp64: directory

peer			total	timeo...
EUPLE_N.pdf	3/24/2009	34312		
SamuelOates_S2_tftp.txt	3/22/2019	33		
tlp32.chm	5/6/2015	337218		
tlp32.exe	11/29/2013	664		
Tftp64.exe	5/6/2015	343040		
uninstall.exe	3/2/2017	36850		

FileZilla window displaying the successful transfer

Performing Packet Capture and Traffic Analysis
Samuel Oates
2 hours remaining

LAB GUIDE

3. Section 1: Hands-On Demonstration

4. Section 2: Applied Learning

- Part 1: Generate Network Traffic
- Part 2: Analyze Traffic using Wireshark
- Part 3: Analyze Traffic using NetWitness Investigator

Part 1: Generate Network Traffic

29. **Transfer the yourname_S2_tftp.txt file** from the TargetWindows02 desktop to the vWorkstation desktop, **overwriting the existing file**.

When a file is successfully transferred, FileZilla will display a blue success pop-up and the bottom of the FileZilla window will indicate the transfer has taken place.

30. **Make a screen capture** showing the FileZilla window displaying the successful file transfer and **paste it** into your Lab Report file.

31. **Close the FileZilla Client window** and restore the remote TargetWindows02 connection.

student@172.30.0.10 - FileZilla

File Edit View Transfer Server Bookmarks Help

Host: 172.30.0.10 Username: student Password: ***** Port: Quickconnect

Status: Insecure server, it does not support FTP over TLS.
Status: Logged in
Status: Starting upload of C:\Users\Administrator\Desktop\SamuelOates_S2_tftp.txt
Status: File transfer successful, transferred 33 bytes in 1 second
Status: Retrieving directory listing of "/"...
Status: Directory listing of "/" successful

Local site: C:\Users\Administrator\Desktop\ Remote site: /

Filename	Filesize	Filetype	Last modified	Permissions	Owner
Connections		File folder	2/7/2017 10:35:27 ...		
desktop.ini	282	Configuration ...	1/10/2017 5:04:55 ...		
File Transfer.link	2,453	Shortcut	2/22/2017 12:40:09...		
SamuelOates_S2...	33	Text Document	3/22/2019 3:11:31 ...		
Tftp64.link	1,699	Shortcut	1/16/2017 12:45:53...		

Selected 1 file. Total size: 33 bytes

3 files. Total size: 533,349 bytes

Server/Local file	Direction	Remote file	Size	Priority	Status

Captured file transfer in the entire Wireshark window

LAB GUIDE

- Section 1: Hands-On Demonstration
- Section 2: Applied Learning
 - Part 1: Generate Network Traffic
 - Part 2: Analyze Traffic using Wireshark
 - Part 3: Analyze Traffic using NetWitness Investigator

Part 2: Analyze Traffic using Wireshark

While Wireshark could not capture the contents of the transferred file, almost everything else was easily visible in clear text. Despite this lack of security, FTP is still an extremely popular method of sharing and transferring files over the Internet.

```

0000  00 50 56 a6 c0 56 00 50 56 a6 d3 f6 00 00 45 02  .PV...V.P V.....E.
0001  00 61 7c 84 40 00 80 06 25 c8 ac 1e 00 0a 0c 1e  .l.!.%.....%.....
0002  00 02 00 15 c 2 17 63 92 a0 2e 2e 7e 23 96 50 18  .....c.....#P.
0003  04 02 7a 08 00 00 32 32 36 20 53 75 63 63 65 73  ..z...22 6 Succes
0004  79 66 75 6c 79 20 74 72 61 6e 73 66 65 72 72  fully t ransferr
0005  65 64 20 22 2f 53 61 6d 75 65 6c 4f 61 74 65 73  ed "/samuelOates
0006  5f 53 32 5f 74 66 74 70 2e 74 78 74 22 0d 0a  _s2_tftp.txt"...
    
```

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
219	483.114885	172.30.0.2	172.30.0.10	FTP	62	Request: TYPE A
220	483.115376	172.30.0.10	172.30.0.2	FTP	73	Response: 200 Type set to A
221	483.116871	172.30.0.2	172.30.0.10	FTP	60	Request: PASV
222	483.117792	172.30.0.10	172.30.0.2	FTP	103	Response: 227 Entering Passive Mode (172,30,0,10,165,...
223	483.118673	172.30.0.2	172.30.0.10	FTP	84	Request: STOR SamuelOates_s2_tftp.txt
228	483.120590	172.30.0.10	172.30.0.2	FTP	136	Response: 150 Opening data channel for file upload to...
233	483.123214	172.30.0.10	172.30.0.2	FTP	111	Response: 226 Successfully transferred "/samuelOates_...
235	483.162807	172.30.0.2	172.30.0.10	FTP	62	Request: TYPE I
236	483.163306	172.30.0.2	172.30.0.10	FTP	73	Response: 200 Type set to I

Packet Details:

- Frame 233: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface 1
- Ethernet II, Src: Vmware_a6:d3:f6 (00:50:56:a6:d3:f6), Dst: Vmware_a6:c0:56 (00:50:56:a6:c0:56)
- Internet Protocol Version 4, Src: 172.30.0.10, Dst: 172.30.0.2
- Transmission Control Protocol, Src Port: 21, Dst Port: 49687, Seq: 512, Ack: 107, Len: 57
- File Transfer Protocol (FTP)

Session detail for the file transfer

LAB GUIDE

- Section 1: Hands-On Demonstration
- Section 2: Applied Learning
 - Part 1: Generate Network Traffic
 - Part 2: Analyze Traffic using Wireshark
 - Part 3: Analyze Traffic using NetWitness Investigator

Part 3: Analyze Traffic using NetWitness Investigator

Password	Clear text passwords seen on the network. Click [open] to view.
----------	---

- Locate the `yourname_s2_tftp.txt` file that was transferred earlier in this lab and display the session detail related to the file.
- Make a screen capture showing the session detail for the `yourname_s2_tftp.txt` file transfer and paste it into your Lab Report file.
- Close the `yourname` Collection tab and select **Collection > Export Collection** from the NetWitness Investigator menu.
- Export the file to the desktop as `yourname_s2_collection.xml`.
- Close NetWitness Investigator.

NetWitness Investigator 10.6

All Data

SamuelOates_S2_Collection > Sessions for "samueloates_s2_tftp.txt"

Time	Service	Size	Events
2019-Mar-22 20:43:57	IP / TCP / FTP	2.89 KB	<ul style="list-style-type: none"> 00:50:56:A6:C0:56 -> 00:50:56:A6:D3:F6 172.30.0.2 -> 172.30.0.10 49687 -> 21 (ftp) payload: 850 medium: Ethernet tcp.flags: 219 streams: 2 packets: 38 lifetime: 22 action: login username: student password: P@ssw0rd! action: put filename: SamuelOates_s2_tftp.txt extension: txt 2 linked sessions

