패킷 분석 보고서

ftp.pcap

i-Keeper

2018 May 9

저자: 최홍준

목차

1. 개요

파일 전송 프로토콜로 알려진 FTP(20, 21)를 사용하여 통신하는 과정을 캡쳐 해 놓은 ftp.pcap 파일을 분석했다.

2. 패킷 분석

2.1 분석 환경

OS	Wireshark
Window 10	version 2.4.5

[표 1] 분석 환경

2.2 ftp.pcap

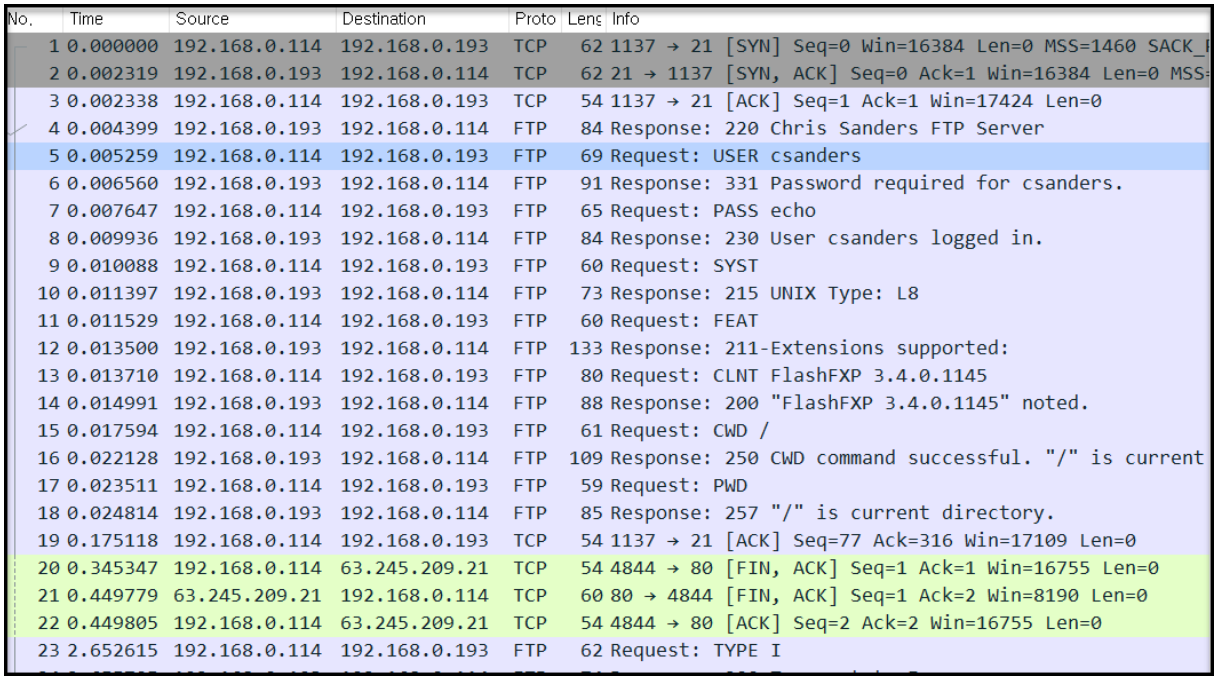
FTP 프로토콜을 이용하여 통신을 맺고 사용자가 하는 행동을 캡처한 파일이다. 취약한 21 번 포트를 사용하여 내용이 평문 전송 됨을 확인할 수 있다. 확인된 내용은 아래와 같다.

① Client, Server IP

② Src, Dst Port

③ FTP 계정

④ 각종 명령어 사용



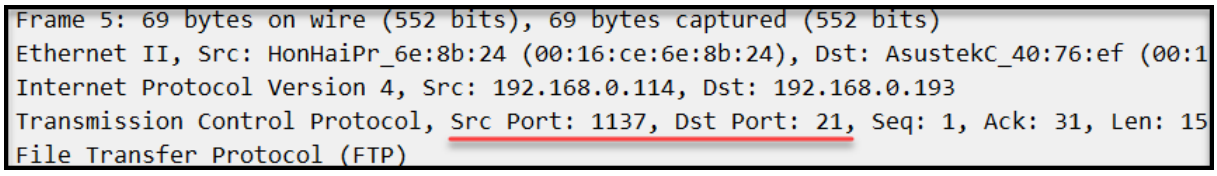
No.	Time	Source	Destination	Proto	Leng	Info
1	0.000000	192.168.0.114	192.168.0.193	TCP	62	1137 → 21 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_
2	0.002319	192.168.0.193	192.168.0.114	TCP	62	21 → 1137 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=
3	0.002338	192.168.0.114	192.168.0.193	TCP	54	1137 → 21 [ACK] Seq=1 Ack=1 Win=17424 Len=0
4	0.004399	192.168.0.193	192.168.0.114	FTP	84	Response: 220 Chris Sanders FTP Server
5	0.005259	192.168.0.114	192.168.0.193	FTP	69	Request: USER csanders
6	0.006560	192.168.0.193	192.168.0.114	FTP	91	Response: 331 Password required for csanders.
7	0.007647	192.168.0.114	192.168.0.193	FTP	65	Request: PASS echo
8	0.009936	192.168.0.193	192.168.0.114	FTP	84	Response: 230 User csanders logged in.
9	0.010088	192.168.0.114	192.168.0.193	FTP	60	Request: SYST
10	0.011397	192.168.0.193	192.168.0.114	FTP	73	Response: 215 UNIX Type: L8
11	0.011529	192.168.0.114	192.168.0.193	FTP	60	Request: FEAT
12	0.013500	192.168.0.193	192.168.0.114	FTP	133	Response: 211-Extensions supported:
13	0.013710	192.168.0.114	192.168.0.193	FTP	80	Request: CLNT FlashFXP 3.4.0.1145
14	0.014991	192.168.0.193	192.168.0.114	FTP	88	Response: 200 "FlashFXP 3.4.0.1145" noted.
15	0.017594	192.168.0.114	192.168.0.193	FTP	61	Request: CWD /
16	0.022128	192.168.0.193	192.168.0.114	FTP	109	Response: 250 CWD command successful. "/" is current
17	0.023511	192.168.0.114	192.168.0.193	FTP	59	Request: PWD
18	0.024814	192.168.0.193	192.168.0.114	FTP	85	Response: 257 "/" is current directory.
19	0.175118	192.168.0.114	192.168.0.193	TCP	54	1137 → 21 [ACK] Seq=77 Ack=316 Win=17109 Len=0
20	0.345347	192.168.0.114	63.245.209.21	TCP	54	4844 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16755 Len=0
21	0.449779	63.245.209.21	192.168.0.114	TCP	60	80 → 4844 [FIN, ACK] Seq=1 Ack=2 Win=8190 Len=0
22	0.449805	192.168.0.114	63.245.209.21	TCP	54	4844 → 80 [ACK] Seq=2 Ack=2 Win=16755 Len=0
23	2.652615	192.168.0.114	192.168.0.193	FTP	62	Request: TYPE I

[그림 1] ftp.pcap

패킷을 열어보면 그림 1과 같다. 기본적인 TCP 3-Way Handshake 통신부터 FTP 프로토콜을 이용하여 클라이언트가 서버와 통신을 맺고 각종 명령어를 사용하고 있다. 그림 1에서 분석한 내용은 아래 표 2와 같다.

Client IP	Server IP
192.168.0.114	192.168.0.193

[표 2] Client, Server IP



```
Frame 5: 69 bytes on wire (552 bits), 69 bytes captured (552 bits)
Ethernet II, Src: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24), Dst: AsustekC_40:76:ef (00:1
Internet Protocol Version 4, Src: 192.168.0.114, Dst: 192.168.0.193
Transmission Control Protocol, Src Port: 1137, Dst Port: 21, Seq: 1, Ack: 31, Len: 15
File Transfer Protocol (FTP)
```

[그림 2] No.5 패킷 정보

Request: USER csanders 정보를 가진 패킷의 하단을 보면 그림 2와 같다. 여기서 얻을 수 있는 정보들이 많지만 그 중 Src, Dst Port를 살펴보면 아래 표 3과 같다.

Src Port	Dst Port
1137	21

[표 3] Src, Dst Port

```
220 Chris Sanders FTP Server
USER csanders
331 Password required for csanders.
PASS echo
230 User csanders logged in.
SYST
215 UNIX Type: L8
FEAT
211-Extensions supported:
 CLNT
 MDTM
 PASV
 REST STREAM
 SIZE
211 End.
CLNT FlashFXP 3.4.0.1145
200 "FlashFXP 3.4.0.1145" noted.
CWD /
250 CWD command successful. "/" is current directory.
PWD
257 "/" is current directory.
TYPE I
200 Type set to I.
SIZE Music.mp3
213 4980924
PASV
227 Entering Passive Mode (192,168,0,193,28,86)
RETR Music.mp3
150 Data connection accepted from 192.168.0.114:1140; transfer starting for
Music.mp3 (4980924 bytes).
```

[그림 3] Follow TCP Stream

패킷을 분석하는데 있어 유용한 기능인 Follow TCP Stream 이다. 빨간색 부분이 클라이언트, 파란색 부분이 서버측이다. 그림 3 에서 분석한 내용은 아래 표 4, 표 5 와 같다.

ID	PW
csanders	echo

[표 4] FTP 계정

명령어	해석
SYST	시스템 유형 반환
FEAT	서버가 추가한 기능 목록 보기
CLNT FlashFXP 3.4.0.1145	FlashFXP 3.4.0.1145 소프트웨어 식별
CWD /	루트 디렉터리로 변경
PWD	현재 디렉터리 반환
TYPE I	이미지(바이너리 데이터)로 전송 모드 설정
SIZE Music.mp3	Music.mp3 파일 크기 반환
PASV	수동 모드 들어가기
RETR Music.mp3	Music.mp3 파일 전송

[표 5] 명령어 정리

3. 대응방안

① 취약 FTP 서비스 구동 중지

② SFTP(22) 프로토콜 사용

4. 참고문헌

http://www.nsftools.com/tips/RawFTP.htm - Raw FTP Command List