<Chapter 04. FTP 패킷분석>

FTP : File Transfer Protocol

: 21번 포트번호 사용 (TCP 21, 20번)
- 21번: 사용자 인증 및 명령어전달
- 20번: 사용자의 명령처리 결과전달

FTP
- 패킷분석

(윈도우)

- 이더넷헤더
  - Destination : 목적지 MAC주소
  - Source : 송신지 MAC주소
  - Type : 이더넷헤더 다음에 오는 헤더
    - ex) IP

- IPV4헤더
  - Version
  - Header Length
  - Differentiated Services Field
    - ex) 0x00 (서비스종류없음)
  - Total Length
  - Identification
    - ex) 0xa8c5 (패킷순서 구분번호)
  - Flags
    - ex) 0x00 (패킷분할안됨)
  - Fragment offset
    - ex) 0 (첫번째로 해당됨 0)
  - Time to live
    - ex) 128 (패킷수명 홉개수)
  - Protocol
    - ex) IPv6 (IPv4헤더 다음에 오는 프로토콜)
  - Header Checksum
    - ex) 0xd95b (헤더오류검출체크)
  - Source
  - Destination

- IPV6헤더
  - Version
  - Traffic
    - ex) 0x00000000
    - ↳ IPv4의 Differentiated Services Field와 유사한 기능
  - Flow label
    - ex) 0x00000000
    - ↳ 실시간데이터(음성, 화상) 서비스 품질제공
  - Payload Length (IP데이터길이)
  - Next header
    - ex) TCP (IPv6 다음 데이터는 프로토콜)
  - Hop Limit
    - ex) 128 (IPv4의 Time to live와 동일기능)
  - Source
  - Destination
  - Flags ex) 0x02 (SYN만있을경우 송신을 처리완료하라는 단계)
  - Window size (한번에 수신할수 있는 패킷사이즈)
  - Checksum
  - Options

- FTP데이터
  - ↳ FTP 인증및 데이터전송등의 정보포함
  - 방법) Follow TCP Stream 명령어사용

(명령어)
- USER anonymous : Annoymous 계정을 입력함
- PASS IEUser@ : IEUser@ 암호를 입력함
- Opts utf8 on : 자동완성 명령어를 입력한상태
- Syst : 시스템타입을 리턴함
- Site help : Site명령어는 Site다음의 명령어를 시행함

< Chapter 05. Telnet 패킷분석 >

텔넷

Telnet → Telecommunication Network Protocol

: 원격지 컴퓨터를 액세스하기 위한 사용자 명령들과 TCP/IP 기반의 프로토콜.

- Telnet 통신방식

① 패킷수집 프로그램에서 서버배너정보가 확인된다.

② 접속계정을 요구하는 login: 프롬프트가 확인된다.

③ Telnet 접속계정을 입력한다.

ex) test 인경우,

계정의 첫번째 문자열 t 입력 → t문자열이 서버로 전송됨

→ 다시 서버에서 동일한 문자 t 리턴

→ 화면에 입력한 t 문자열이 보여짐

⇨ echo 현상 !!

④ 패스워드를 요구하는 Password: 프롬프트가 떨어짐.

⑤ 패스워드를 입력한다.

↳ echo 현상 x.

사용자가 입력한 문자열의 1개씩 전송됨

⑥ 인증에 성공하면 접속시간과 함께 프롬프트가 보여진다.

- Telnet 패킷분석

처음 1, 2, 3번라인 ⇝ TCP의 세션연결과정인 3way Handshaking [SYN], [SYN, ACK], [Ack] 보여줌.

4~268라인 ⇝ 로그인 및 명령어 등을 사용한 내역

269~272라인 ⇝ [FIN, Ack]보내서 통신종료요청.

[Ack]로 응답

[FIN, Ack] 전송

[Ack] ↑ 응답

· 이더넷헤더 (필드)
- Destination
- Source
- Type

· IP헤더 (필드)
- Version
- Header Length
- ⋮

⇝ 보는건 FTP패킷 분석이랑 동일

· TCP헤더 (필드)
- Source Port (송신자의포트번호)
- Destination Port (수신자의포트번호)
- Sequence Number
  ex) 1 (데이터순서를나타내는번호)
- Acknowledge Number
  ex) 1 (다음에 수신할번호)
- Header Length
- Flags
  ex) 0x10 (ACK)
- Window size
- Checksum
- Options

· Telnet 데이터

[Statistics] - [Conversations] 에서 라인선택

→ 하단의 Follow stream 버튼 클릭

→ 패킷을 조합해서 볼 수 있음

(명령어)

- login: "...." ffaakkee : fake계정을 입력함
  ↳ echo현상으로 1개 문자열이 2개로보임
- Password: user : 암호 user을 입력함
- Welcome to OpenBSD: : 서버배너정보가보임
- $ llss / $ llss --aa : ls 및 ls -al 명령어를 입력함
- $ //ssbbiinn//ppiinngg wwwwww.yyaahhoooo..ccoomm.PING www.yahoo.com (204.71.200.74): 56 date bytes
  : /sbin/ping www.yahoo.com 명령어를 입력하여 ↑에 ping을 전송함
- eexxiitt : exit 명령어를 입력함

< Chapter 06. 파일 Magic Number >

↳ 와이어샤크를 통해 메신저 내용을 분석하거나
메신저를 통해 전송된 파일들을 File Magic Number를
통해 추출하는 방법.

순서) ① [Conversations]를 통한 전체내용 파악

② 세션별 [Follow Stream]을 통해
통신내용분석

③ 세션별 [Follow Stream]으로 확인되지
않은정보는 필터링을 통해 상세분석

(여섯번째 세션)

· OFT2 packet ⇝ AOL Instant Messenger

↳ 메신저프로그램을 이용한 통신임을 가정해볼수있음

구조
OFT2 ···
OFT2 ···
PK ···
OFT2 ···

"PK"라는 문자열을 ⇝ Magic Number 라는값

(파일포맷마다 고유의 Magic Number를 가지고 있어,
이를 통해 패킷내에 포함된 파일 종류를 확인하고
추출해낼 수 있다)

↳ http://www.garykessler.net/library/file_sigs.html 에서
찾아볼수 있음

→ docx 파일만들고
헥사에디터에서 PK부분 앞,뒤 (OFT2) 삭제한후
파일 열어보면 워드문서 확인가능.

< Chapter 07. HTTP 컨텐츠 분석 >

↳ HTTP 패킷내에 포함된 그림파일을 추출하는방법.
(80)

- 와이어샤크의 HTTP 파일추출기능
[File] - [Export Objects] - [HTTP...]

- NetworkMiner 툴을 이용한 파일추출기능