네트워크 포렌식 스터디

CERT-IS

양윤지

19.11.04.월요일

5장 FTP 패킷 분석

Telnet(Telecommunication Network Protocol): 자신이 사용권한 가짐, 다른 사람의 호스트 컴퓨터를 원격지에서 액세스 할 수 있는 기능 🡪 원격지 컴퓨터 액세스 명령, TCP/IP

\*\*wireshark 설정) 포트 번호를 프로토콜 이름으로: [Capture]-[Options]-[Resolve]

(1) 패킷 수집 프로그램에서 서버 배너정보 확인

(2) 접속 계정 요구하는 login: 프롬프트 확인

(3) Telnet 접속계정 입력(문자 입력 시 문자열 서버 전송🡪화면에 문자열 표시: echo 현상)

(4) 패스워드 요구 Password: 프롬프트 확인

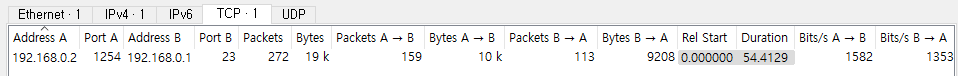
(5) 패스워드 입력(echo 현상 x)

(6) 인증 성공 시, 접속시간과 함께 프롬프트 확인

0. Telnet 패킷 분석

Chapter\_5.pcap 파일 사용

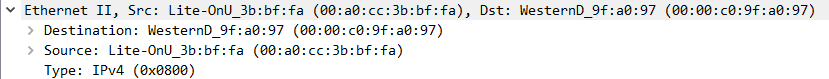
-프로토콜 확인: [Statistics]-[Conversations]



Port B가 23인데 이게 Telnet 인가보다.

\*\*wireshark 설정 변경

1. 이더넷 헤더



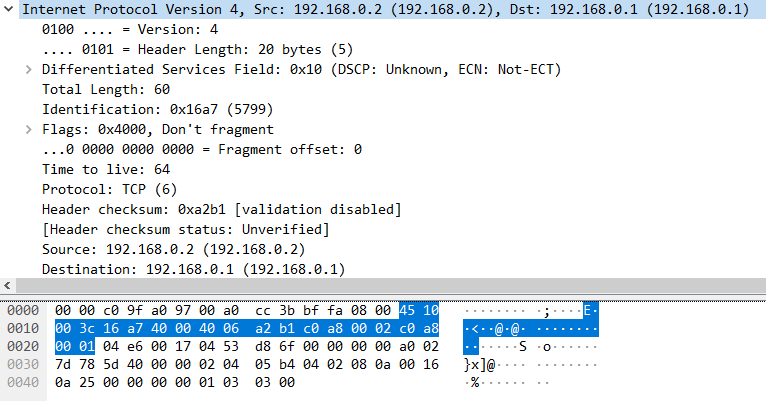
\*필드

-Destination(목적지 MAC 주소): 00:00:c0:9f:a0:97

-Source(송신지 MAC 주소): 00:a0:cc:3b:bf:fa

-Type(이더넷 다음 헤더): 0x0800(=IP)

2. IP 헤더



\*필드

-Version: 4

-Header Length: 5 (=20byte)

--

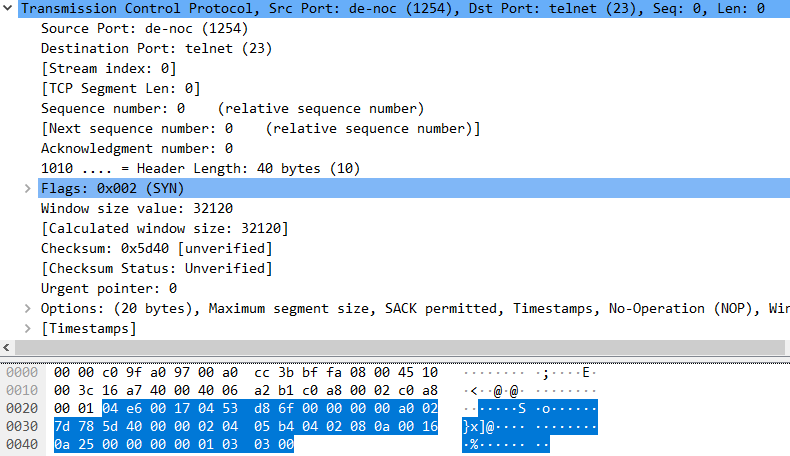
-Time to live(패킷수명 최대 홉수): 40(=64)

-Protocol(IPv4다음 프로토콜): 06(=TCP)

-Source: c0 a8 00 02(=192.168.0.2)

-Destination: c0 a8 00 01(=192.168.0.1)

3. TCP 헤더



\*필드

-Source port: 04 e6(=1254)

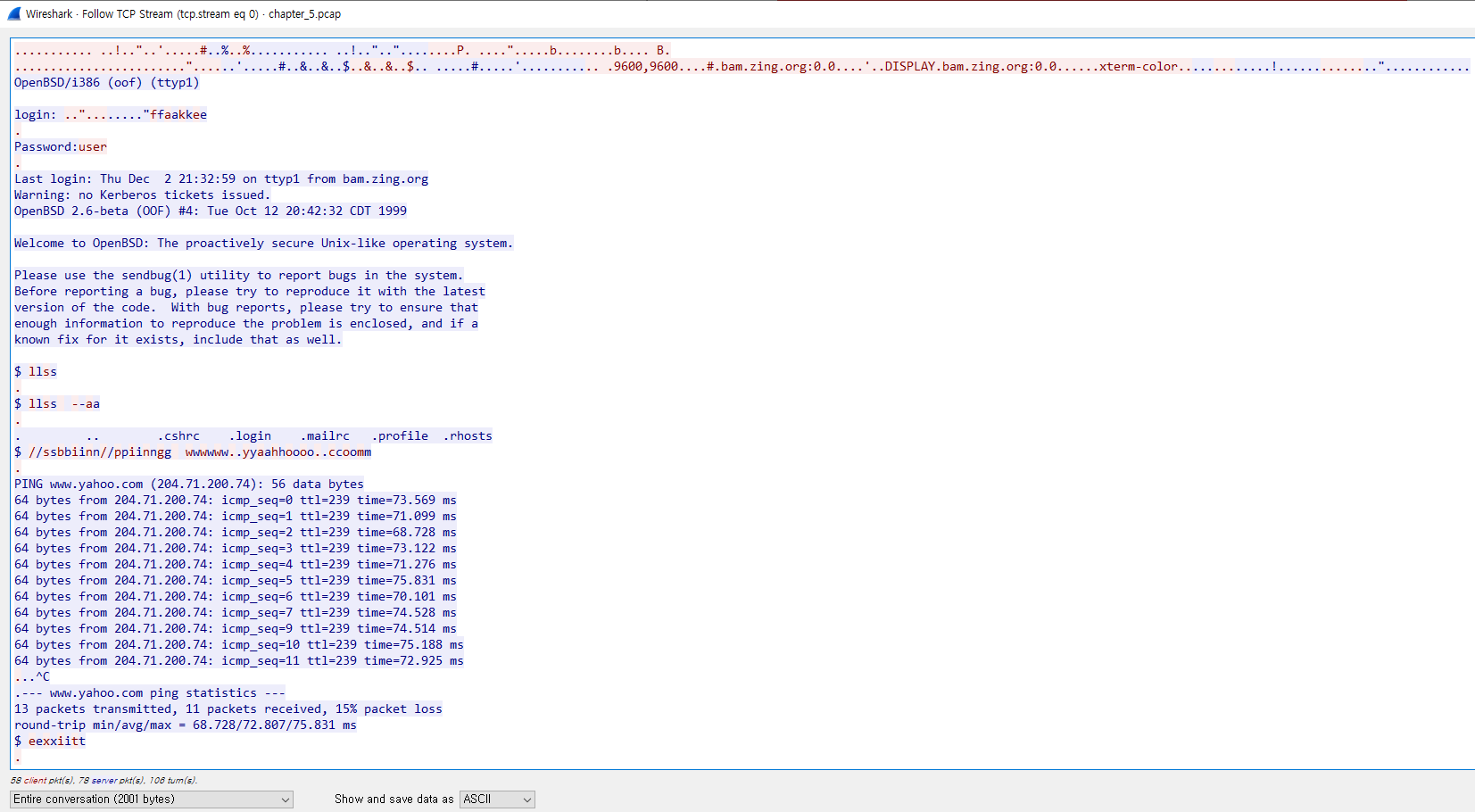
-Destination port: 0017(=23)

--

-Header length: a0(=40 bytes) //a0은 10진수로 160인데 왜 40byte인가요

-

4. Telnet 데이터 패킷 조합 [Statistics]-[Conversations]-[Follow stream]



\*명령어

login: ..”……..”ffaakkee echo현상:홍홍진진호호

Password:User

Welcome to OpenBSD: 서버 배너정보

$ llss

$ llss --aa 명령어 ls 입력

5. 정리

텔넷의 포트번호는 23번인거같다

입력 시 echo현상이 발생한다.