네트워크 포렌식 스터디

CERT-IS

양윤지

19.11.05.화요일

6장 파일 Magic Number

File Magic Number(앞에서 D4 C3 B2 A1이라고 했었는데)로 메신저 내용, 전송된 파일 분석

\*\*플래그

[SYN] : 통신 요청

[ACK]

[SYN, ACK]

[FIN, ACK]

\*\*포트

Port 22: TCP 22번은 암호화 처리하는 프로토콜(Telnet 등의 평문데이터를 보호하기 위해)

0. CHAPTER\_6.PCAP 파일 분석

[Statistics]-[Conversations] 전체내용 파악

[Follow stream] 통신내용 분석

[Apply as filter]-[Selected]-[A <-> B] 상세분석

\*\*OFT2 packet: AOL Instant Messenger

구조: OFT2 OFT2 PK OFT2 …

🡪 PK: Magic number, 파일 포맷마다 고유의 magicnumber 가짐

🡪 패킷 내의 파일종류 확인, 추출

🡪[Follow strean]에서 [Raw] 형식으로 recipe.docx 저장

🡪 HxD로 편집

🡪OFT2 블록 제거