네트워크 포렌식 스터디

CERT-IS

양윤지

19.11.11.월요일

11장 백도어 패킷분석

-백도어: 인증을 거친 후, 원격접속을 보장하여 시스템에 악의적인 행동을 하는 프로그램

\*\*[Analyze]-[Expert Information]: 해당 접속했던 모든 웹 페이지 확인

여기서 해당 패킷을 follow stream 하는 방법을 모르겠어서

[Apply as filter]-[Selected] 한 다음

[Analyze]-[Follow]-[TCP Stream] 해줌

\*맞는지 모르겠다🡪아닌거같다..

??????????????