네트워크 포렌식 스터디

CERT-IS

양윤지

19.11.10.일요일

9장 포트스캔 패킷분석: 포트스캔 툴🡪 포트정보

-TCP 스캔: 3-웨이 핸드쉐이킹🡪포트 오픈여부 확인

TCP는 세션 연결 필수, 정확한 데이터 전송

-통신 요청

1) [SYN] : 통신 요청

2) [SYN], [ACK] : 포트 오픈

[RST], [ACK] : 포트 닫힘

3) [ACK] : ㅇㅋ

-통신 종료

1) [ACK], [FIN]: 종료 요청

2) [ACK]: 확인

3) [ACK], [FIN]: 그래종료하자

4) [ACK]: ㅇㅇ

-UDP: 오픈시 무응답일수도, 닫혀있을 시 ICMP unreachable 메시지 전송

UDP와 ICMP가 동시에 포함된 경우: 접속 실패

\*\* Expression 을 통해 필터링 가능