9/1 공부내용_공재호

Asignee	
Joined	@Sep 1, 2020 1:32 PM
Location	공재호
Title	

1. monitor 모드 패킷 5000개 이상

- 듀얼 부팅 오류 해결
- 시간 동기화 문제 해결 후 apt-get update && apt-get upgrade 해줘야함
- 5G 잡는 명령어를 모르겠음.. 2G는 잘 잡히지만 엄청 많이 잡히지 않음
- fast.com 계속 실행하면 패킷 수가 꾸준 히 오르긴하지만 5000개까지 수집하는데 시간이 꽤 걸렸음

2. dummy interface

매번 똑같은 패턴의 패킷이 수신되면 디버깅
https://gilgil.gitlab.io/2020/07/23/1.html

- sudo ./pcap-test eth0 → 수많은 패킷
- sudo wireshark → eth0 → tcp.stream eq 3 → File - Export Specified Packets - 저장형식 pcap
- sudo ip link add dum0 type dummy
- sudo ./pcap-test dum0
- 터미널 하나 더 열어서 tcpreplay -i dum0 저장파일명.pcap

3. PCAP 코드 수정