8/30 공부 내용

Joined	@Aug 30, 2020 5:39 PM
Location	공재호
Property	
Title	

1. 무선랜 보안가이드(2010)

2. LG그램에 Kali 설치 - 멀티 부팅 가능하도록(설치완료)

모니터 모드

ip link set wlan0 down
iwconfig wlan0 mode monitor
ip link set wlan0 up
airodump-ng wlan0

3. 놀리팝 영상 시청

1. 와이파이 암호화 원리와 실제 해킹 실습[WIFI해킹/모의해킹]

무선랜 종류 : WEP, WPA, WPA2

1) WEP : 1999 표준

- 암호화 알고리즘 : RC4 : stream 암호화 알고리즘

  암호화

  - IV초기화벡터(24bit) + 키(40bit) → key stream(64bit)

- IV초기화벡터로 같은 단어가 인코딩되어도 다른 값이 나옴
- **KEY stream(64bit)** XOR **Plain Text = CipherText**
- 전송은 다음을 전송함 : [IV] [CipherText]

복호화

- IV + KEY = KEY stream
- **KEY stream(64bit)** XOR **CipherText = Plain Text**

크랙

- IV 값은 24bit, 즉 3byte
- weakness IV 값 많이 수집하면 KEY Stream을 알 수 있고 key을 알 수 있다.

2) WPA : WEP를 개선 (2003)

- KEY가 특정 시간마다 변함
- 해커가 가로챈 후 변경하였는지에 대한 여부를 아는 무결성 검사도 함
- 4 WAY handshake

크랙

- 공유키 : 4 WAY handshake에서 key를 가져갈 수 있음

키 크랙

- Brute Force : 모든 경우의 수
- Dictionary Attack : 할만한 것

3) WPA2 : RC4 대신 AES사용 (2004)

크랙

- 여전히 4 WAY handshake에서 key를 가져갈 수 있음

4) WPA3 (2018)

크랙

- Dragon Blood (CVE-2019-9494)

AirCrack : kali, 모니터모드 지원해야 함

모니터 모드 실습!

2. 그림으로 배우는 네트워크 이야기 [OSI 7 Layer/네트워크]

OSI : Open System interconnection

- 7 : Application
- 6 : Presentation : Encoding, Encryption, Compress
- 5 : Session
- 4 : Transport : port
- 3 : Network : Address (IP)
- 2 : DataLink : MAC (호수)
- 1 : Physical

3. 모의해킹 칼리리눅스와 ARP Spoofing 해킹실습 [칼리리눅스 / 모의해킹]

: 칼리는 모의해킹을 하기위해 만들어짐(600가지 도구 제공)

- 호환성
- 기본적으로 설치됨
- 환경설정 용이

ARP Spoofing 실습

칼리 : arpspoof -t ip ip

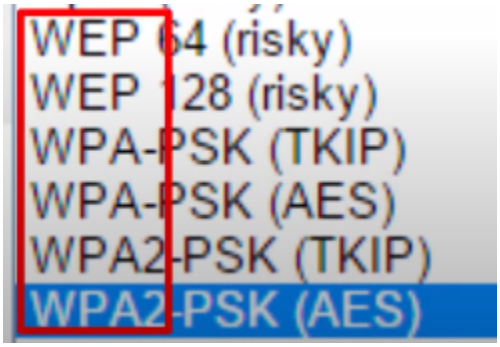
인터넷 안될때 : fragrouter -B1

4. 네트워크로 전송한 파일을 해커가 훔치는 방법

Network Packet을 통한 File carving

- 파일 구조 : meta data, DATA
- meta data는 data 복구
- DATA는 file carving
- 파일 시그니처(확장자...)

5. 와이파이 해킹 2탄! 와이파이 비밀번호 취약점과 실습 [무선랜보안/WPA2] WPA2 와이파이 크랙



WPA : 어떻게 주고받을 것인지

PSK : Pre-Shared Key : 암호키 공유 방식

() : 암호화 방식

- TKIP : RC4 stream 방식 + key Mixing :: 여전히 취약
- AES : 더욱 강력해짐

크랙

4 Way Handshake : PSK 와 5개의 변수 주고받음 → 암호 알아냄

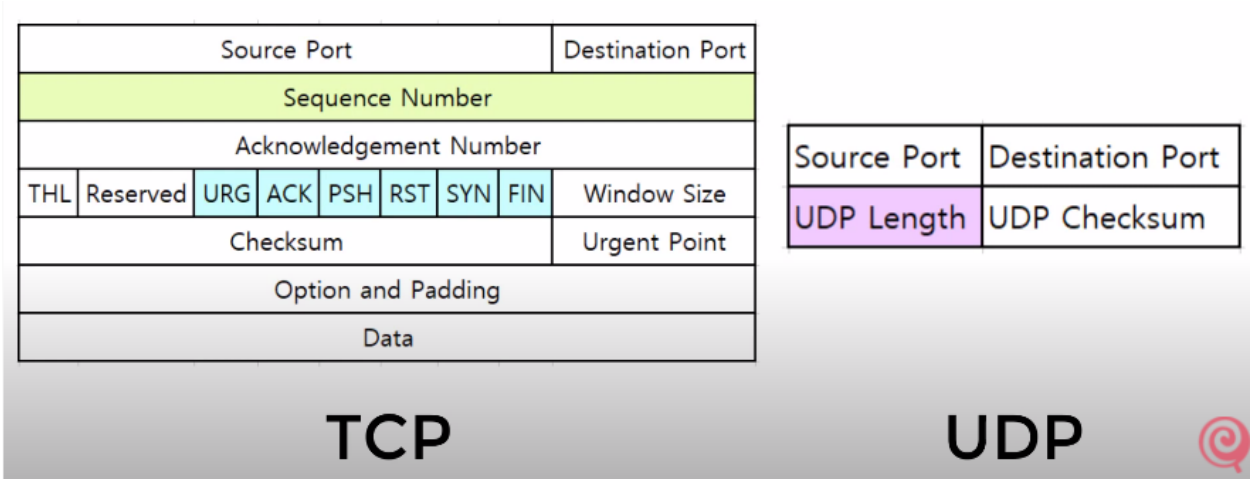
6. WPA WiFi Security in Kali Linux [Tutorial] → 위의 WPA 내용 같음!

7. Principle of WiFi Security in Kali Linux [Tutorial]
→ 위의 내용 같음!

8. 통신할 때 꼭 지켜야 하는 약속, 프로토콜

서로 데이터를 주고받을 때 같은 프로토콜로 주고받음

- **정하는 요소 : Syntax(데이터 포맷), Semantic(제어정보), Timing**
- 전송 시 Fragmentation으로 전송
- 캡슐화
- OSI 7 계층과 TCP/IP로 전송
- TCP와 UDP(실시간)의 차이



9. 네트워크 공격으로 인공지능 스피커 먹통만들기 [DoS & DDoS]

DoS와 DDoS로 인공지능 스피커의 네트워크 연결을 끊을 수 있음

DoS

- Ping of Death : 패킷이 나누어져 보내짐 (이것을 이용) : 핑 요청을 매우 큰 양을 보냄 (이제는 잘안됨)

- SYN Flooding : SYN 만 계속 보냄. ACK는 안받음

DDoS : 분산해서 동시 공격(좀비PC)

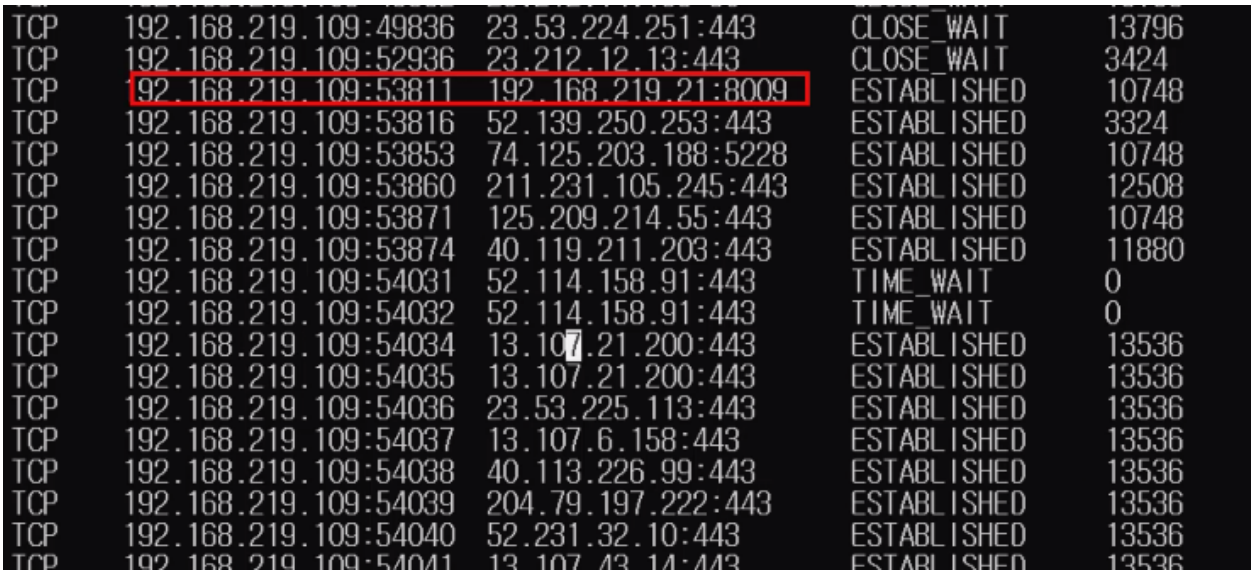
인공지능 스피커 공격

1. 타겟 IP찾기
2. DoS 공격
3. 타겟 테스트

10. 해킹을 위한 사전준비, Port Scan

Port : usb, HDMI

- 포트는 0~65536



TCP	192.168.219.109:49836	23.53.224.251:443	CLOSE_WAIT	13796
TCP	192.168.219.109:52936	23.212.12.13:443	CLOSE_WAIT	3424
TCP	192.168.219.109:53811	192.168.219.21:8009	ESTABLISHED	10748
TCP	192.168.219.109:53816	52.139.250.253:443	ESTABLISHED	3324
TCP	192.168.219.109:53853	74.125.203.188:5228	ESTABLISHED	10748
TCP	192.168.219.109:53860	211.231.105.245:443	ESTABLISHED	12508
TCP	192.168.219.109:53871	125.209.214.55:443	ESTABLISHED	10748
TCP	192.168.219.109:53874	40.119.211.203:443	ESTABLISHED	11880
TCP	192.168.219.109:54031	52.114.158.91:443	TIME_WAIT	0
TCP	192.168.219.109:54032	52.114.158.91:443	TIME_WAIT	0
TCP	192.168.219.109:54034	13.107.21.200:443	ESTABLISHED	13536
TCP	192.168.219.109:54035	13.107.21.200:443	ESTABLISHED	13536
TCP	192.168.219.109:54036	23.53.225.113:443	ESTABLISHED	13536
TCP	192.168.219.109:54037	13.107.6.158:443	ESTABLISHED	13536
TCP	192.168.219.109:54038	40.113.226.99:443	ESTABLISHED	13536
TCP	192.168.219.109:54039	204.79.197.222:443	ESTABLISHED	13536
TCP	192.168.219.109:54040	52.231.32.10:443	ESTABLISHED	13536

포트는 53811

Port Scan : TCP Scan, UDP Scan, SYN Scan

- **TCP Scan : 3 Way Handshake**