



bobNET

**무선 AP 진단 스크립트
사용 안내서**

Team - 234567

목차

1. bobNET 설치

2. bobNET 실행

3. 동작

[0] Help(Usage introduction)

[1] Rescan

[2] Fake AP

[3] ARP Pollution

[4] Beacon Flooding

[5] Deauth Attack & Checking

[6] Disasso Attack & Checking

[7] Exit

1. bobNET 설치

```
git clone https://github.com/team-234567/bobNET
```

2. bobNET 실행

1. 설치된 폴더로 이동한다.

```
cd bobNET
```

2. 설치된 폴더경로에서 다음 명령어를 수행한다.

- ① `g++ -o bobNET main.cpp dot11.cpp -lpcap -pthread`
- ② `./bobNET <interface>`

직접 컴파일(①)을 하여 실행 파일을 생성한 뒤 위와 같은 방법으로 실행(②)시킨다. 단, 실행시키기 전에 무선랜 어댑터와 연결이 되어야 한다.

컴파일(①) 없이 바로 실행 파일(②)을 실행시켜 사용할 수도 있다. 실행 파일을 실행하면 무선 패킷을 캡처하여 사용자 주변 AP 정보를 제공한다.

bobNET Run screen

```

BSSID      PWR    Beacons  #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
[1] 00:07:00:00:00:00 -1      2          0    0   WPA   TKIP    KT_GiGA_2G_Wave2_F674
[2] 00:23:00:00:00:00 -1      3          0    0   WPA   TKIP    SK_WiFiGIGA2E78
[3] 00:27:00:00:00:00 -1      2          0    0   WPA   TKIP    SK_WiFi907E
[4] 02:27:00:00:00:00 -1      2          0    0  WPA2   CCMP    SK_WiFiGIGA0808
[5] 04:09:00:00:00:00 -1      2          0    0  WPA2   CCMP    지점's WIFI
[6] 04:8d:00:00:00:00 -1      2          0    0  WPA2   CCMP
[7] 12:09:00:00:00:00 -1      2          0    0  WPA2   CCMP
[8] 12:23:00:00:00:00 -1      2          0    0  WPA2   CCMP
[9] 40:31:00:00:00:00 -1      2          0    0   WPA   TKIP    Xiaomi_20B5
[10] 42:09:00:00:00:00 -1      2          0    0   WPA   TKIP    SK_WiFiGIGA0808_2.4G
[11] 42:23:00:00:00:00 -1      2          0    0   WPA   TKIP    SK_WiFiGIGA2E78_2.4G
[12] 54:d1:00:00:00:00 -1      1          0    0   WPA   TKIP    t-broadB975
[13] 54:d1:00:00:00:00 -1      1          0    0   WPA   TKIP
[14] 70:5d:00:00:00:00 -1      3          0    0  WPA2   CCMP    yeonheeseong
[15] 72:5d:00:00:00:00 -1      2          0    0   OPN    -      kendinghuizuo
[16] 86:25:00:00:00:00 -1      1          0    0  WPA2   CCMP    DIRECT-g2C43x Series
[17] 88:36:00:00:00:00 -1      1          0    0  WPA2   CCMP    iptime_kite
[18] 88:36:00:00:00:00 -1      1          0    0   WPA   TKIP    큰방 2.4G
[19] 88:36:00:00:00:00 -1      2          0    0  WPA2   CCMP    iptime
[20] 88:3c:00:00:00:00 -1      1          0    0   WPA   TKIP    KT_WiFi_2G_F5A1
[21] 88:3c:00:00:00:00 -1      1          0    0   WPA   TKIP    SK_WiFiGIGA4C7A
[22] 88:3c:00:00:00:00 -1      1          0    0   WPA   TKIP    KT_GiGA_2G_Wave2_69B9
[23] 8a:3c:00:00:00:00 -1      2          0    0  WPA2   CCMP
[24] 90:9f:00:00:00:00 -1      2          0    0  WPA2   CCMP    iptime
[25] 90:9f:00:00:00:00 -1      3          0    0  WPA2   CCMP    iptime_JJJ
[26] ac:84:00:00:00:00 -1      2          0    0  WPA2   CCMP    TP-Link_758A
[27] b4:a9:00:00:00:00 -1      1          0    0   WPA   TKIP    8st
[28] b4:a9:00:00:00:00 -1      2          0    0   WPA   TKIP    KT_GiGA_2G_Wave2_ED1B

Dangerous AP List
BSSID      PWR    Beacons  #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
[15] 72:5d:00:00:00:00 -1      2          0    0   OPN    -      kendinghuizuo

select AP Number (research:0) : █
```

위와 같이 AP 스캔 후 사용자가 진단할 AP를 선택하여 진행된다.

3. 동작

진단할 AP를 선택하면 Menu창이 나온다.

```
select AP Number (research:0) : 1

[0] Help (Usage Introduction)
[1] Rescan
[2] Fake AP
[3] ARP Pollution
[4] Beacon Flooding
[5] Deauth Attack & Checking
[6] Disasso Attack & Checking
[7] Exit

select Menu Number : █
```

사용자는 0부터 7까지 숫자로 기능을 선택할 수 있으며, 0은 메뉴에 있는 각 기능에 대한 설명을 볼 수 있다.

[0] Help(Usage introduction)

bobNET이 제공하는 각 기능을 설명한다.

```
Wireless AP diagnostic tool - Version 1.0 (2020)
Team - 234567.

usage : bobNET <interface>

First, select ap to diagnose and proceed.
Second, select the attack menu to be diagnosed.

Options - Number selection
[0] Help(Usage introduction) : Describes the attack menu to be diagnosed.
[1] Rescan : rescan and reselect ap
[2] Fake AP : The probability that the selected ap is a fake ap is judged as a risk rating.
               * Whether to judge - password, ESSID name, ESSID duplicate
[3] ARP Pollution : Among the stations connected to the selected ap, Find a station where arp spoofing can proceed.
               * ARP Spoofing - arp spoofing is a man-in-the-middle attack technique that uses
               messages to intercept data packets from other parties.
[4] Beacon Flooding : A beacon packet is transmitted by generating a random MAC address including
               the same SSID and channel number as the selected AP. It is possible to determine
               whether the selected AP can be attacked by Beacon Flooding.
[5] Deauth Attack & Checking : Diagnose by checking if deauth attack is possible against the selected AP.
[6] Disasso Attack & Checking : Diagnose by checking if deauth attack is possible against the selected AP.
[7] Resasso Attack & Checking : Diagnose by checking if deauth attack is possible against the selected AP.
[8] Exit : Exit the diagnostic program
```

[1] Rescan

AP 스캔을 재진행하며 사용자는 AP 선택을 다시 할 수 있다.

```

BSSID      PWR    Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
[1] 00:07:00:00:00:00 -1      2          0    0   WPA   TKIP   KT_GiGA_2G_Wave2_F674
[2] 00:23:00:00:00:00 -1      3          0    0   WPA   TKIP   SK_WiFiGIGA2E78
[3] 00:27:00:00:00:00 -1      2          0    0   WPA   TKIP   SK_WiFi907E
[4] 02:27:00:00:00:00 -1      2          0    0  WPA2   CCMP
[5] 04:09:00:00:00:00 -1      2          0    0   WPA   TKIP   SK_WiFiGIGA0808
[6] 04:8d:00:00:00:00 -1      2          0    0  WPA2   CCMP   지 섬 's WIFI
[7] 12:09:00:00:00:00 -1      2          0    0  WPA2   CCMP
[8] 12:23:00:00:00:00 -1      2          0    0  WPA2   CCMP
[9] 40:31:00:00:00:00 -1      2          0    0   WPA   TKIP   Xiaomi_20B5
[10] 42:09:00:00:00:00 -1      2          0    0   WPA   TKIP   SK_WiFiGIGA0808_2.4G
[11] 42:23:00:00:00:00 -1      2          0    0   WPA   TKIP   SK_WiFiGIGA2E78_2.4G
[12] 54:d1:00:00:00:00 -1      1          0    0   WPA   TKIP   t-broadB975
[13] 54:d1:00:00:00:00 -1      1          0    0   WPA   TKIP
[14] 70:5d:00:00:00:00 -1      3          0    0  WPA2   CCMP   yeonheeseong
[15] 72:5d:00:00:00:00 -1      2          0    0   OPN    -      kendinghuizuo
[16] 86:25:00:00:00:00 -1      1          0    0  WPA2   CCMP   DIRECT-g2C43x Series
[17] 88:36:00:00:00:00 -1      1          0    0  WPA2   CCMP   iptime_kite
[18] 88:36:00:00:00:00 -1      1          0    0   WPA   TKIP   큰 방 2.4G
[19] 88:36:00:00:00:00 -1      2          0    0  WPA2   CCMP   iptime
[20] 88:3c:00:00:00:00 -1      1          0    0   WPA   TKIP   KT_WiFi_2G_F5A1
[21] 88:3c:00:00:00:00 -1      1          0    0   WPA   TKIP   SK_WiFiGIGA4C7A
[22] 88:3c:00:00:00:00 -1      1          0    0   WPA   TKIP   KT_GiGA_2G_Wave2_69B9
[23] 8a:3c:00:00:00:00 -1      2          0    0  WPA2   CCMP
[24] 90:9f:00:00:00:00 -1      2          0    0  WPA2   CCMP   iptime
[25] 90:9f:00:00:00:00 -1      3          0    0  WPA2   CCMP   iptime_JJJ
[26] ac:84:00:00:00:00 -1      2          0    0  WPA2   CCMP   TP-Link_758A
[27] b4:a9:00:00:00:00 -1      1          0    0   WPA   TKIP   8st
[28] b4:a9:00:00:00:00 -1      2          0    0   WPA   TKIP   KT_GiGA_2G_Wave2_ED1B

Dangerous AP List
BSSID      PWR    Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
[15] 72:5d:00:00:00:00 -1      2          0    0   OPN    -      kendinghuizuo

select AP Number (research:0) : █
```

스캔 된 AP들의 정보를 볼 수 있다.

- BSSID : MAC 주소
- Beacons : 스캔하는 동안 AP에서 보낸 beacon frame의 수
- CH : 사용하는 채널
- ENC : 사용하는 암호화 방식(OPN, WEP, WPA, WPA2) *OPN=개방형
- CIPHER : 사용하는 key 전달 방식 (WEP-40, WEP-104, TKIP, CCMP)
- ESSID : Wi-fi 이름

Dangerous AP List는 취약한 보안을 사용하여 사용하지 않도록 권장하는 위험한 AP들이다. 각 AP들에 부여된 번호를 입력하면 선택이 된다. 이때, 0을 입력하면 다시 AP들을 스캔해준다.

[2] Fake AP

해당 AP가 Fake AP일 가능성이 있는지에 대해 판단하여 사용자에게 위험등급으로 알려준다.



```
BOBNET
-----Select-----
b4:a9:15:15:2c:4f
-----Menu-----
[0] Help (Usage Introduction)
[1] Rescan
[2] Fake AP
[3] ARP Pollution
[4] Beacon Flooding
[5] Deauth Attack & Checking
[6] Disasso Attack & Checking
[7] Exit

select Menu Number : 2
Risk Name : KT_GiGA
-----List of Duplicate Names-----
KT_GiGA_2G_Wave2_F674
KT_GiGA_2G_Wave2_2C4B
KT_GiGA_2G_Wave2_5B64
KT_GiGA_2G_Wave2_ED1B
KT_GiGA_2G_Wave2_E97C

Risk Level testing ...
Fake AP Risk Score : 5
Fake AP Risk Rating : Medium
```

진단 기준은 3가지 이며 다음과 같다.

- Password
- ESSID name
- ESSID duplicate

[3] ARP Pollution

선택한 AP를 사용하는 Station들 중 하나를 골라 해당 station이 ARP Table이 감염될 수 있는지 진단해주는 기능이다. 이 기능의 작동을 위해서 진단 툴을 사용하는 PC가 선택한 AP에 접속되어 있어야 한다.

```
select Menu Number : 3
      BSSID                IP
[1] 4c:56:9d:59:52:d7      11.11.11.11
total station : 1
select station Number (research:0) : █
```

해당 기능을 실행시키면 AP를 사용하는 Station 목록들을 스캔해준다. 이때, IP 정보는 가져오지 못하므로 초기값 17.17.17.17로 초기화되어있다.

```
select Menu Number : 3
      BSSID                IP
[1] dc:52:85:f0:40:ea      17.17.17.17
total station : 1
select station Number (research:0) : 0
```

다시 스캔하고 싶으면 0을, 원하는 station이 있는 경우 번호를 입력해주면 된다.

```
select station Number (research:0) : 2 █
      AP
      70:5d:cc:7d:19:d0
      17.17.17.17
      Station
      dc:52:85:f0:40:ea
      17.17.17.17
      Menu
      [1] Rescan
      [2] ARP Pollution
      [3] Find IP
      [4] Set IP
      [5] Exit
select Menu Number : █
```

Station을 선택하면 ARP Pollution 메뉴가 나타난다.

[3] ARP Pollution - (1) Rescan

Station 스캔 및 선택을 다시 할 수 있다.

```
select station Number (research:0) : 2
AP
70:5d:cc:7c:18:de
17.17.17.17
Station
dc:52:cc:7c:18:de
17.17.17.17
Menu
[1] Rescan
[2] ARP Pollution
[3] Find IP
[4] Set IP
[5] Exit
select Menu Number : 1
BSSID          IP
[1] 4c:56:cc:7c:18:de 17.17.17.17
[2] 5c:c1:cc:7c:18:de 17.17.17.17
[3] dc:52:cc:7c:18:de 17.17.17.17
total station : 3
select station Number (research:0) : █
```

[3] ARP Pollution - (2) ARP Pollution

ARP Pollution 실행 및 진단 기능이다.

만약, IP 값을 설정하지 않아 초기 값을 가지면 실행되지 않는다.

```
select Menu Number : 2
you should find IP first
AP
70:5d:cc:7c:18:de
17.17.17.17
Station
dc:52:cc:7c:18:de
17.17.17.17
Menu
[1] Rescan
[2] ARP Pollution
[3] Find IP
[4] Set IP
[5] Exit
select Menu Number : █
```

IP주소를 설정한 후 실행을 시키면

```
Result
ARP defense : not defensive
AP
70:5d:01:01:01:01
192.168.0.1
Station
dc:52:00:11:11:11
192.168.0.35
Menu
[1] Rescan
[2] ARP Pollution
[3] Find IP
[4] Set IP
[5] Exit
select Menu Number : 1
```

ARP Pollution에 관한 결과가 나타난다. 이때, 정확한 진단을 위해서 station이 슬립모드가 아닌 활성화 상태에 있게 하도록 권장한다. 위 사진은 ARP Pollution에 취약한 station에 관한 결과이다.

[3] ARP Pollution - (3) Find IP

station 및 AP의 IP주소를 모르는 경우 IP주소를 찾아주는 기능이다. 비교적 많은 시간이 필요하다.

[3] ARP Pollution - (4) Set IP

AP와 station의 IP를 직접 입력할 수 있다.

```
select Menu Number : 4
AP IP(xx.xx.xx.xx): 192.168.0.1
Station IP(xx.xx.xx.xx): 192.168.0.35

-----AP-----
70:5d:cc:00:00:00
192.168.0.1
-----Station-----
dc:52:00:00:00:00
192.168.0.35
-----Menu-----
[1] Rescan
[2] ARP Pollution
[3] Find IP
[4] Set IP
[5] Exit

select Menu Number : █
```

[3] ARP Pollution - (5) Exit

ARP Pollution 메뉴를 나가서 메인 메뉴로 갈 수 있다.

```
-----AP-----
70:5d:cc:00:00:00
192.168.0.1
-----Station-----
dc:52:00:00:00:00
192.168.0.35
-----Menu-----
[1] Rescan
[2] ARP Pollution
[3] Find IP
[4] Set IP
[5] Exit

select Menu Number : 5

-----Select-----
70:5d:cc:00:00:00
-----Menu-----
[0] Help (Usage Introduction)
[1] Rescan
[2] Fake AP
[3] ARP Pollution
[4] Beacon Flooding
[5] Deauth Attack & Checking
[6] Disasso Attack & Checking
[7] Resasso Attack & Checking
[8] Exit

select Menu Number : █
```

[4] Beacon Flooding



해당 기능을 실행시키면 선택한 AP와 유사한 이름의 와이파이 목록에 뜨도록 한다.



일정 시간이 지난 후 다시 메뉴 목록으로 돌아온다.

[5] Deauth Attack & Checking

Deauth Attack에 관한 진단을 할 수 있다. 이때, 정확한 진단을 위해 선택한 AP에 연결된 Station들이 슬립모드가 아니라 활성화시켜 놓는 것을 권장한다.

```
select AP Number (research:0) : 2
[0] Rescan
[1] Fake AP
[2] ARP Pollution
[3] Beacon Flooding
[4] Deauth Attack & Checking
[5] Disasso Attack & Checking
[6] Exit

NETWORK
[0] Rescan
[1] Fake AP
[2] ARP Pollution
[3] Beacon Flooding
[4] Deauth Attack & Checking
[5] Disasso Attack & Checking
[6] Exit

select Menu Number : 5
Deauth testing..(for 30s)
```

실행시키면 Deauth testing...(for 30s)이 뜬다. 이 과정에 AP와 연결된 station들의 네트워크 상태가 불안정해질 수 있다.

```
Result
Total time : 27.000000
Deauth defense : not defensive

[0] Rescan
[1] Fake AP
[2] ARP Pollution
[3] Beacon Flooding
[4] Deauth Attack & Checking
[5] Disasso Attack & Checking
[6] Exit

select Menu Number :
```

약 30초 후 결과가 나온다. Deauth Attack에 방어기능이 없다면 not defensive라는 결과가 도출된다.

만약 Deauth Attack의 방어기능이 있다면 다음과 같이 나온다.



해당 AP의 PMF 기능이 활성화 되어 있다면 'The AP's PMF function is activated.' 라는 문구가 화면에 출력되며 defensive라는 결과가 도출된다.

[6] Disasso Attack & Checking

Disassociation Attack에 관한 진단을 할 수 있다. 이때, 정확한 진단을 위해 선택한 AP에 연결된 Station들이 슬립모드가 아니라 활성화시켜 놓는 것을 권장한다.

```
select AP Number (research:0) : 10
[0] Help
[1] Rescan
[2] Fake AP
[3] ARP Pollution
[4] Beacon Flooding
[5] Deauth Attack & Checking
[6] Disasso Attack & Checking
[7] Exit

[0] Help (Usage Introduction)
[1] Rescan
[2] Fake AP
[3] ARP Pollution
[4] Beacon Flooding
[5] Deauth Attack & Checking
[6] Disasso Attack & Checking
[7] Exit

select Menu Number : 6
Disassociation testing..(for 30s)
```

실행시키면 Disassociation testing...(for 30s)이 뜬다. 이 과정에 AP와 연결된 station들의 네트워크 상태가 불안정해질 수 있다.

```
Result
Total time : 26.000000
Disasso defense : not defensive

[0] Help (Usage Introduction)
[1] Rescan
[2] Fake AP
[3] ARP Pollution
[4] Beacon Flooding
[5] Deauth Attack & Checking
[6] Disasso Attack & Checking
[7] Exit

select Menu Number :
```

약 30초 후 결과가 나온다. Disasso Attack에 방어기능이 없다면 not defensive라는 결과가 도출된다.

만약 Disasso Attack의 방어기능이 있다면 다음과 같이 나온다.

```
The AP's PMF function is activated.

Result
Total time : 26.000000
Disasso defense : defensive

BOBNET

Select
04:8d:23:c1:c1:c1
Menu
[0] Help (Usage Introduction)
[1] Rescan
[2] Fake AP
[3] ARP Pollution
[4] Beacon Flooding
[5] Deauth Attack & Checking
[6] Disasso Attack & Checking
[7] Exit

select Menu Number : 
```

해당 AP의 PMF 기능이 활성화 되어 있다면 'The AP's PMF function is activated.' 라는 문구가 화면에 출력되며 defensive라는 결과가 도출된다.

[7] Exit

bobNET 사용을 종료한다.