개인 공부

2020.12.01 김현진

airodump-ng

모니터링 모드를 통해 네트워크 정보를 출력해주는 프로그램

Aircrack-ng

aircrack-ng , airdecap-ng , airmon-ng
aireplay-ng , airodump-ng

airodump-ng

Monitor Mode

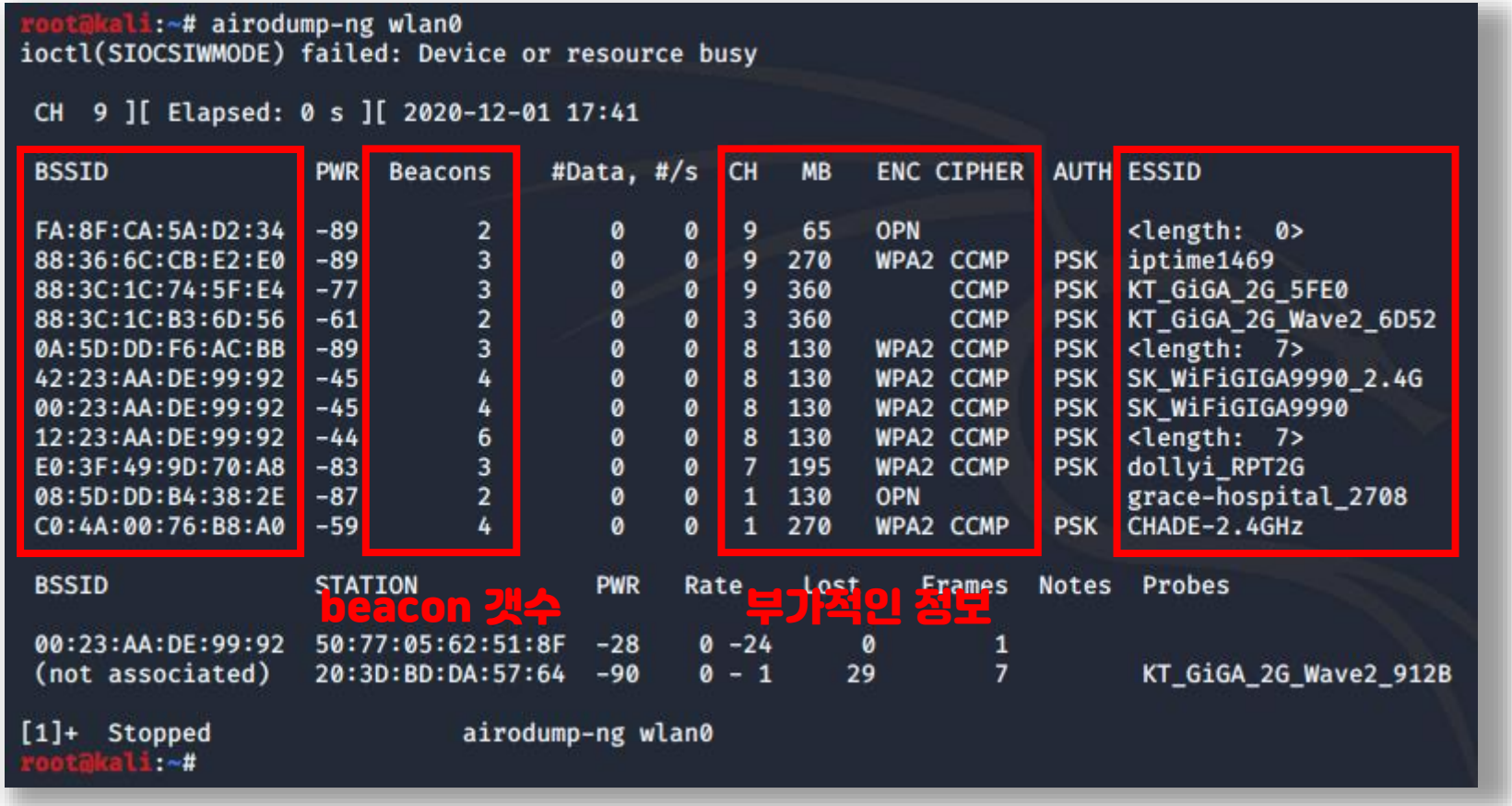
공기 주변에 뿌려지는 모든 패킷을 볼 수 있는 모드

* Managed 모드 : 나에게 오는 패킷만 볼 수 있는 모드

airodump-ng

AP 의 MAC

AP의 이름



Beacon packet

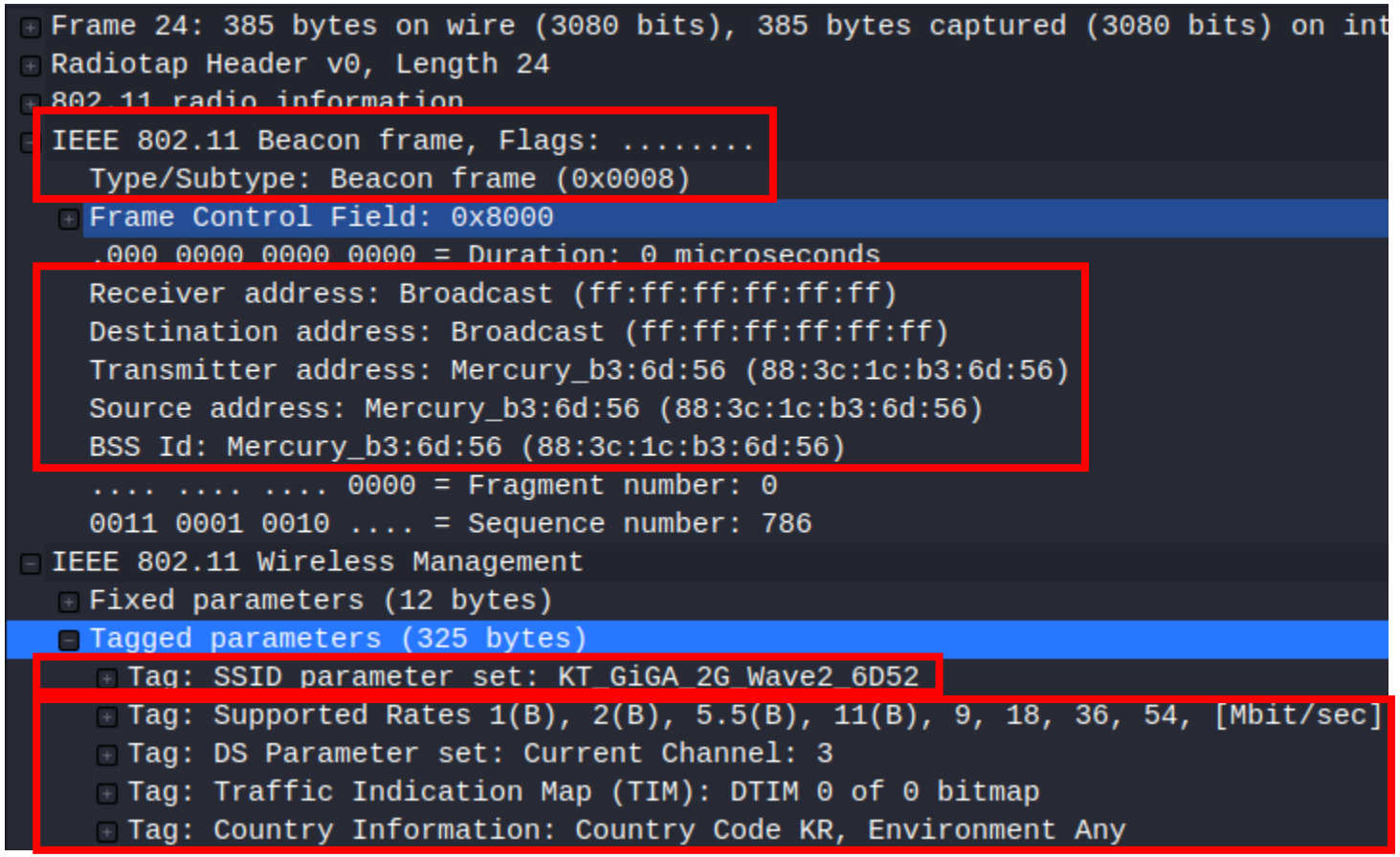
AP가 보내는 방송 프레임

프레임 타입

MAC 주소

SSID

부가적인 정보



프로그램

```
Input Your Interface !!

sample: wlan0
Input : wlan0
Interface : wlan0

****  What Choice?  ****
*  1.Scanning         *
*  2.Stop Scanning    *
************************
```

```
no    BSSID              Ch    SSID
-----------------------------------------------
1     8a:3c:1c:8f:36:21  4
2     ba:3c:1c:8f:36:21  4     SK_WiFiGIGA361E_2.4G
3     88:3c:1c:b3:6d:56  3     KT_GiGA_2G_Wave2_6D52
4     c0:4a:00:76:b8:a0  1     CHADE-2.4GHz
5     08:5d:dd:b4:38:2d  1
6     18:c5:01:80:29:3a  1     U+Net293B
7     70:2c:1f:5f:5c:26  1     [refrigerator] Samsung
8     88:3c:1c:35:ee:37  1     KT_GiGA_2G_EE33
9     08:5d:dd:50:b2:35  1
10    08:5d:dd:50:b2:36  1     grace-hospital_2805
11    08:5d:dd:b4:13:52  1     grace-hospital_2608
12    42:23:aa:de:99:92  8     SK_WiFiGIGA9990_2.4G
13    00:23:aa:de:99:92  8     SK_WiFiGIGA9990
14    12:23:aa:de:99:92  8
15    70:5d:cc:6e:bc:ae  2     kiss
```

interface 입력 : wlan0

네트워크 정보 : BSSID / CH / SSID

BSSID : 공유기 MAC 주소을 알기 위함

CH : 채널을 알기 위함

SSID : WiFi 이름을 알기 위함

프로그램 코드

패킷 구조체

```
#pragma pack(push, 1)
struct IEEE80211_radiotap_header
        u_int8_t        it_versio
        u_int8_t        it_pad;
        u_int16_t       it_len;
        u_int32_t       it_presen
} __attribute__((__packed__));
#pragma pack(pop)

#pragma pack(push, 1)
struct Beacon_Frame {
    uint16_t  Type;
    uint16_t  Dur;
    u_char    dst_mac[6];
    u_char    src_mac[6];
    u_char    bssid[6];
    uint16_t  number;
};
#pragma pack(pop)

#pragma pack(push, 1)
struct Fixed {
    uint8_t   Time[8];
    uint16_t  Interval;
    uint16_t  capabilities;
};
#pragma pack(pop)
```

패킷 스캔

```
printf("\nno   BSSID                Ch
printf("-----------------------------------

while(my_th_info->th_ex) {
    struct pcap_pkthdr* header;
    const u_char* packet;

    int res = pcap_next_ex(handle, &header
    if (res == 0) continue;
    if (res == -1 || res == -2) {
        printf(" pcap_next_ex error \n");
        exit (0);
    }

    struct IEEE80211_radiotap_header * rad
    radiotab = (struct IEEE80211_radiotap_
    packet += radiotab->it_len;

    struct Beacon * beacon_frame;
    beacon_frame = (struct Beacon *)packet
    u_short b_type = ntohs(beacon_frame->b

    if (b_type != Beacon_type) continue;

    memcpy(&ssid_size,&beacon_frame->tag.l
```

프로그램 동작

```
int Num,Num2,res,status;
pthread_t p_thread[2];
struct Thr_info * th_info;
th_info = (Thr_info *)malloc(sizeof(Thr_info));

memcpy(th_info->Dev,Dev,sizeof(Dev));

while(true) {

    printf("Choice : ");
    scanf("%d",&Num);

    sleep(1);

    if (Num == 1) {
        th_info->th_ex=1;
        res = pthread_create(&p_thread[0], NULL, scan, (void
        if (res < 0) {
            perror("thread create error : ");
            exit (0);
        }
    }
    if (Num == 2) {
        printf("\nStop Scanning....\n\n");
        th_info->th_ex=0;
        pthread_join(p_thread[0], (void **)&status);
    }
```

프로그램 코드

```
Input Your Interface !!

sample: wlan0
Input : wlan0
Interface : wlan0

****  What Choice?  ****
*  1.Scanning          *
*  2.Stop Scanning     *
**************************
```

기능

1. 패킷 스캔
2. 패킷 길이 읽기
3. 패킷 정보 출력
4. 중복된 패킷 처리
5. 스캔하고 나서 중지

...

프로그램 코드

```
Input Your Interface !!

sample: wlan0
Input : wlan0
Interface : wlan0

****  What Choice?  ****
*  1.Scanning          *
*  2.Stop Scanning     *
**************************
```

기능

1. 패킷 스캔
2. 패킷 길이 읽기
3. 패킷 정보 출력
4. 중복된 패킷 처리
5. 스캔하고 나서 중지

...

MAP

Key , value 가 쌍으로 저장되는 함수

#include <map>

생성 > map<std:string , int> m;

key : string 자료형 / value : int 자료형

삽입 > m.insert({key,value});

key : string 자료형 / value : int 자료형

MAP

```
5   map<std::string, std::string> m;
6   //map<std::string, std::string> :: iterator it;
7
8   bool dump(u_char BSSID[],std::string ss) {  //}, u_char *SSID) {
9
10      char bssid[] = "";
11      sprintf(bssid,"%02x%02x%02x%02x%02x%02x",BSSID[0],BSSID[1],BSSID[2],BSSID[3],BSSID[4],BSSID[5]);
12
13      std::string bs(bssid);
14
15  /* print key, value
16      for (it=m.begin();it !=m.end();it++) {
17          cout << "\nkey : " << it->first << "Value : " << it->second ;
18      }
19  */
20      if (m.find(bs) != m.end()) {    //find
21          return true;
22      }
23      else {                          // not find
24          m.insert(pair<std::string,std::string>(bs,ss));
25          return false;
26      }
27  }
```

map 생성

키가 존재하는지 확인 : find(key)

map에 key, value를 삽입

MAP

map 생성

```
5   map<std::string, std::string> m;
6   //map<std::string, std::string> :: iterator it;
7
8   bool dump(u_char BSSID[],std::string ss) {  //},
9
10      char bssid[] = "";
11      sprintf(bssid,"%02x%02x%02x%02x%02x%02x",BSSI
12
13      std::string bs(bssid);
14
15  /* print key, value
16      for (it=m.begin();it !=m.end();it++) {
17          cout << "\nkey : " << it->first << "Value : " << it->second ;
18      }
19  */
20      if (m.find(bs) != m.end()) {    //find
21          return true;
22      }
23      else {                          // not find
24          m.insert(pair<std::string,std::string>(bs,ss));
25          return false;
26      }
27  }
```

```
78          if (dump(BSSID,ssid)!=false) continue;
79
80
81          // print
82          printf("%d   ",k);
83          if (k<10) printf(" ");
84          for (i=0;i <6;i++) {
85              printf("%02x",beacon_frame->b_frame.bssid[i]);
86              if(i<5) {
87                  printf(":");
88              }
89          }
```

키가 존재하는지 확인 : find(key)

map에 key, value를 삽입

Tread

하나의 프로그램에서 여러가지 기능을 동시에 작업 할 수 있게 하는 함수

```
#include <pthread.h>
```

생성

```
int pthread_create( pthread_t *th_id, const pthread_attr_t *attr, void* 함수명,
void *arg );
```

```
void pthread_exit( void* ret_value );
```

종료

```
int pthread_join( pthread_t th_id, void** thread_return );
```

종료시 자원해제

Tread

현재 스레드의 식별자 정보를 담고 있음

```
20  pthread_t p_thread[2];
21  struct Thr_info * th_info;
22  th_info = (Thr_info *)malloc(sizeof(Thr_info));
23
24  memcpy(th_info->Dev,Dev,sizeof(Dev));
25
26  while(true) {
27
28      printf("Choice : ");
29      scanf("%d",&Num);
30
31      sleep(1);
32
33      if (Num == 1) {
34          th_info->th_ex=1;
35          res = pthread_create(&p_thread[0], NULL, scan, (void *)th_info);
36          if (res < 0) {
37              perror("thread create error : ");
38              exit (0);
39          }
40      }
41      if (Num == 2) {
42          printf("\nStop Scanning....\n\n");
43          th_info->th_ex=0;
44          pthread_join(p_thread[0], (void **)&status);
45      }
```

Tread

```
20  pthread_t p_thread[2];
21  struct Thr_info * th_info;
22  th_info = (Thr_info *)malloc(sizeof(Thr_info));
23
24  memcpy(th_info->Dev,Dev,sizeof(Dev));
25
26  while(true) {
27
28      printf("Choice : ");
29      scanf("%d",&Num);
30
31      sleep(1);
32
33      if (Num == 1) {
34          th_info->th_ex=1;
35          res = pthread_create(&p_thread[0], NULL, scan, (void *)th_info);
36          if (res < 0) {
37              perror("thread create error : ");
38              exit (0);
39          }
40      }
41      if (Num == 2) {
42          printf("\nStop Scanning....\n\n");
43          th_info->th_ex=0;
44          pthread_join(p_thread[0], (void **)&status);
45      }
```

현재 스레드의 식별자 정보를 담고 있음

scan 함수

```
8   void * scan(void *th_info) {
9
10      char errbuf [PCAP_ERRBUF_SIZE];
11      int i,k=1;
12
13      struct Thr_info * my_th_info = (Thr_info *)th_info;
14      char dev[50] ;
15      memcpy(dev,my_th_info->Dev,sizeof(my_th_info));
```

Tread

```
20  pthread_t p_thread[2];
21  struct Thr_info * th_info;
22  th_info = (Thr_info *)malloc(sizeof(Thr_info));
23
24  memcpy(th_info->Dev,Dev,sizeof(Dev));
25
26  while(true) {
27
28      printf("Choice : ");
29      scanf("%d",&Num);
30
31      sleep(1);
32
33      if (Num == 1) {
34          th_info->th_ex=1;
35          res = pthread_create(&p_thread[0], NULL, scan, (void *)th_info);
36          if (res < 0) {
37              perror("thread create error : ");
38              exit (0);
39          }
40      }
41      if (Num == 2) {
42          printf("\nStop Scanning....\n\n");
43          th_info->th_ex=0;
44          pthread_join(p_thread[0], (void **)&status);
45      }
```

현재 스레드의 식별자 정보를 담고 있음

scan 함수

```
129         pcap_close(handle);
130         pthread_exit((void *)0);
131 }
```

Tread

```
20  pthread_t p_thread[2];
21  struct Thr_info * th_info;
22  th_info = (Thr_info *)malloc(sizeof(Thr_info));
23
24  memcpy(th_info->Dev,Dev,sizeof(Dev));
25
26  while(true) {
27
28      printf("Choice : ");
29      scanf("%d",&Num);
30
31      sleep(1);
32
33      if (Num == 1) {
34          th_info->th_ex=1;
35          res = pthread_create(&p_thread[0], NULL, scan, (void *)th_info);
36          if (res < 0) {
37              perror("thread create error : ");
38              exit (0);
39          }
40      }
41      if (Num == 2) {
42          printf("\nStop Scanning....\n\n");
43          th_info->th_ex=0;
44          pthread_join(p_thread[0], (void **)&status);
45      }
```

현재 스레드의 식별자 정보를 담고 있음

scan 함수

```
36  while(my_th_info->th_ex) {
37      struct pcap_pkthdr* header;
38      const u_char* packet;
```

```
129     pcap_close(handle);
130     pthread_exit((void *)0);
131 }
```

완성!

사용자가 입력한 번호

```
sample: wlan0
Input : wlan0
Interface : wlan0

****  What Choice?  ****
*  1.Scanning          *
*  2.Stop Scanning     *
************************

Choice : 1
Choice :
no    BSSID                Ch    SSID
-----------------------------------------------
1     00:27:1c:e2:fc:7e    2
2     70:5d:cc:6e:bc:ae    2     kiss
3     00:27:1c:e2:fc:7f    2     U+NetFC81
4     88:3c:1c:b3:6d:56    3     KT_GiGA_2G_Wave2_6D52
2
5     88:36:6c:c0:c9:d6    2     oym

Stop Scanning....

Choice :
```

감사합니다

2020.12.01 김현진