Wireless Intrusion Detection & Prevention

WI-DP 침입탐지 및 방지시스템 구현

2018.11. 7

정보보호학과

지도교수: 유승재 교수님

6조: 패킷사냥꾼

김경수 박민석 유원상
신현석 전경준 윤서완

목 차

조원 편성

이 름	역 할
신현석(조장)	Mis-configured AP 탐지
김경수	방지시스템 구현
박민석	Ad-Hoc Connect 탐지
유원상	Client Mis-association 탐지
전경준	Fake AP, AP Mac Spoofing 탐지
윤서완	Log Viewer 구현 Web Interface (Front & Back End)

주제 선정

와이파이 공짜라고 무작정 이용하면 큰코 다쳐요!

좋아요

미심쩍으

[보안뉴스

이파이를

라 호텔

이 '공짜'

전국 1만3000여개 공공와이파이, 40%는 해킹에 무방비 노출

한지선

[IT비즈뉴

정보 탈

한 와이

는 해킹

보안 솔

용자인

를 우회

다.

Home > 전체기사

BYOD와 IoT 시대, 무선 네트워크 보안이 관건

좋아요 18개 | 입력 : 2016-07-05 11:03

가 가

WIPS로 비인가 무선 단말 접속 차단 및 보안 취약점 관리

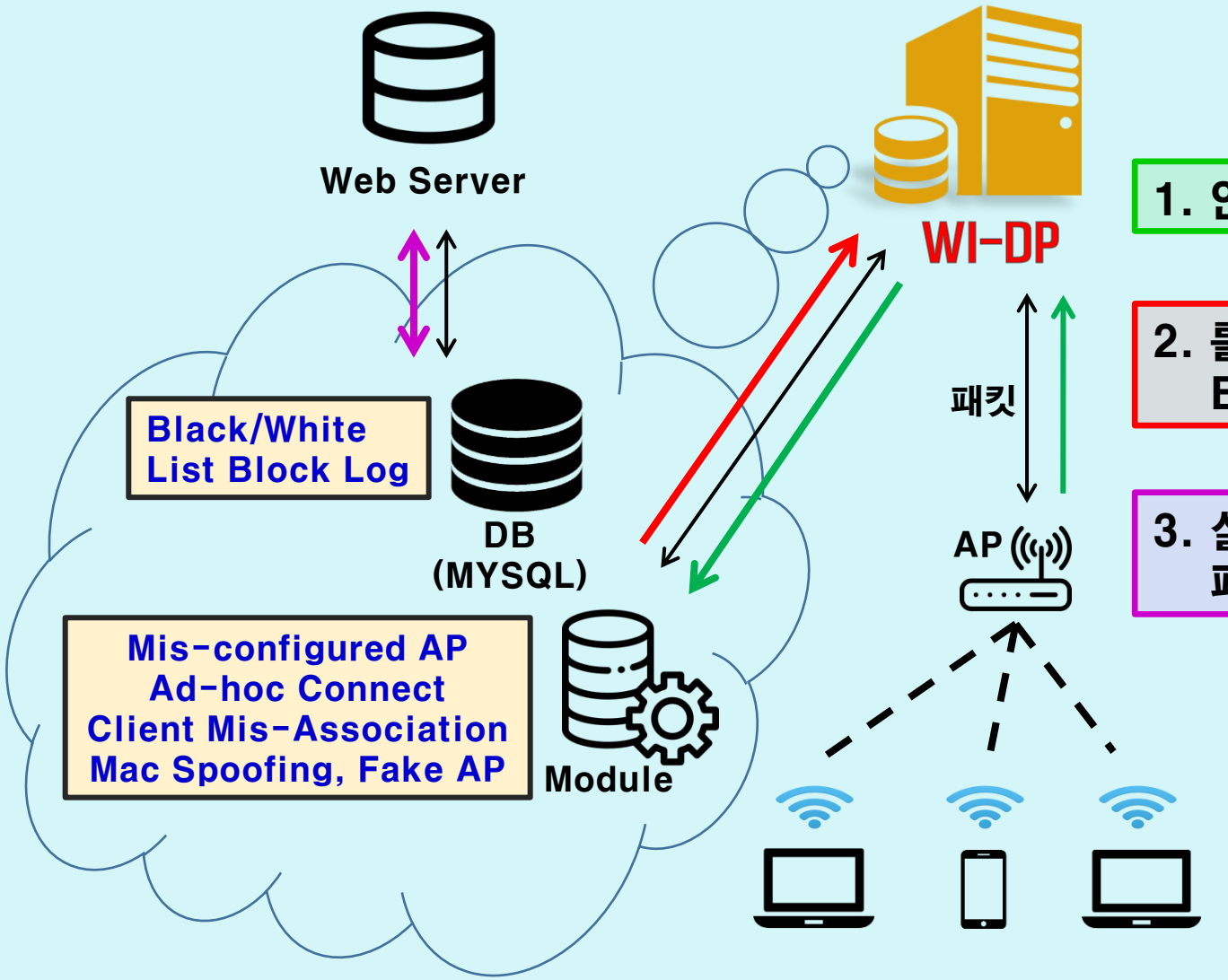
무선 보안, 금융 및 공공 분야 확대...지난해 매출 전년 대비 2배 성장

[보안뉴스 김태형] BYOD(Bring Your Own Device) 시대. 기업의 직원들이 갖고 있는 모든 단말들은 제한 없이 와이파이로 네트워크에 연결이 가능하다. 하지만 이러한 무선 랜이 보안에 취약하다는 것은 주지의 사실. 무선랜을 사용하지 않아도 기업에서 무선침입방지(WIPS) 솔루션 도입은 꼭 필요하다.

무선 네트워크 시장 확대 및 사용률 증가와 무선 네트워크에 대한 낮은 보안 인식

⇨ 무선 공격을 실시간으로 감지하는 WIPS 시스템을 개발, 안전한 네트워크 구축

시스템 구상도



1. 인입 패킷 룰과 비교

2. 룰을 통과하지 못하면 Black List에 추가

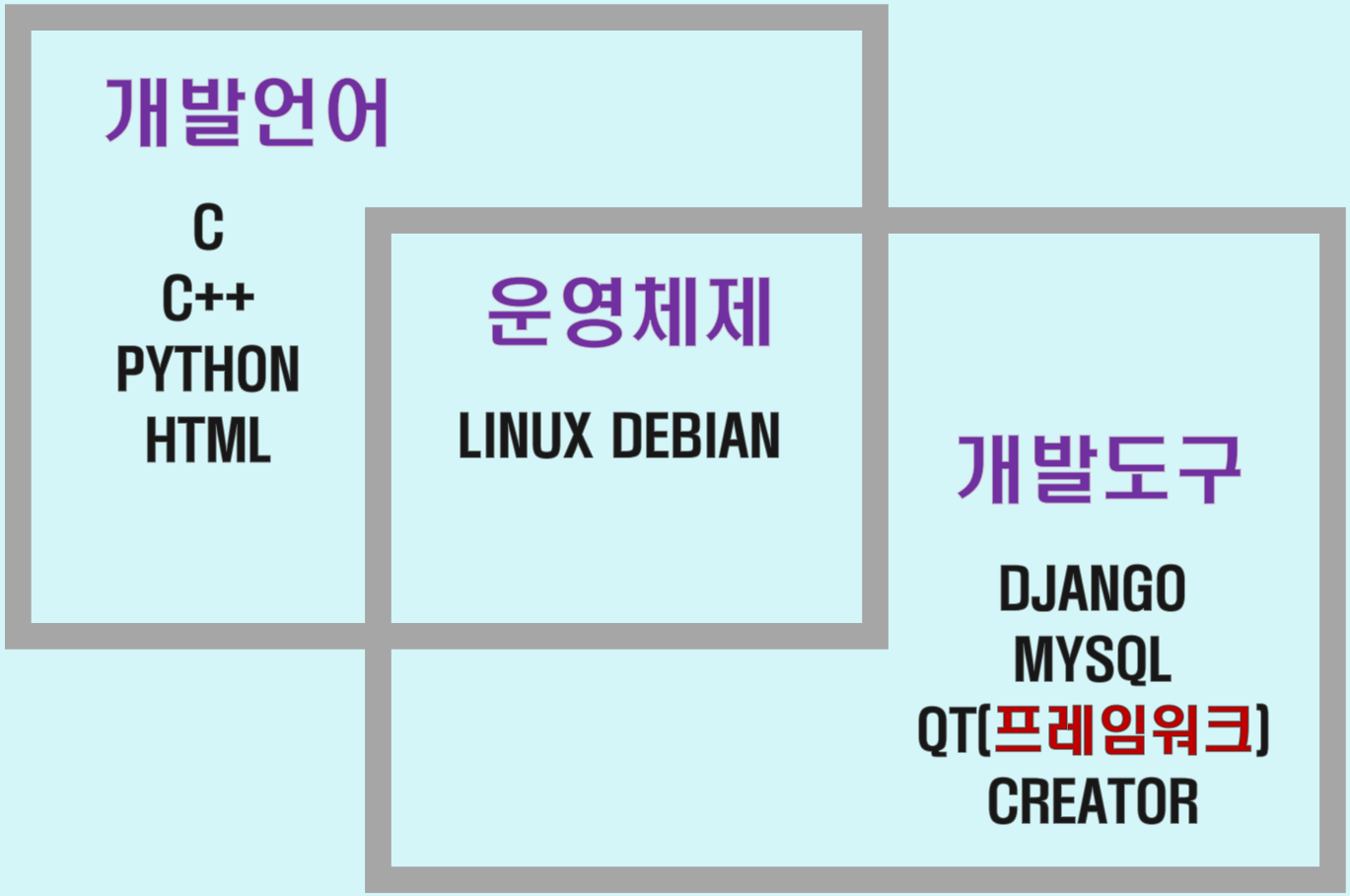
3. 실시간 차단 목록을 웹 페이지에서 출력/관리

추진 경과

기간 (2018년) / 작업	세부작업(월)	3	4	5	6	7	8	9	10
기획	자료수집								
Module 개발	Mis-configured AP								
	Ad-hoc Connect								
	Client Mis-association								
	Fake AP, AP Mac Spoofing								
Web 구축	HTML								
	django								
	DataBase								
종합	시험 및 보완								

개발 환경 및 시스템 개발(1/5)

개발 환경



개발 환경 및 시스템 개발(2/5)

요소 기술 개발(1/4)

❍ Ad-Hoc 연결

Ad hoc Connection

Ad-Hoc 네트워크 : P2P(Peer-To-Peer)라

Ad-hoc 탐지용 프로그램

```
void usrfunc::adhocFunc(listload& listMan2)
{
        WHTFlag = false; //true in whitelisted packet
        BLKFlag = false; //true in blacklisted packetd
//wht list!
        printf("CHECK IBSS\n\n");
        for(it = listMan2.WhiteList.begin();it !=listMan2.WhiteList.end();it++){
                bwDatas = (listload::bwList)it->second;
                 macCmpFlag = memcmp(&(bwDatas.apMac),&(MN->BSS),6);
                printf("MAP의 IBSS 값 %d 과 비교중\n",bwDatas.adHocStat);
                If(macCmpFlag == 0){
                        cmpFlag = memcmp(&(bwDatas.adHocStat),&(IBSS_Status),1);
                if(cmpFlag == 0){
                        printf("이미 저장된 IBSS!(WHITE)\n");
                        WHTFlag = true;
                        break;
```

~ 이하 생략 ~

개발 환경 및 시스템 개발(3/5)

요소 기술 개발(2/4)

❍ 비인가 AP 접속(Client Mis-Association)

Client Mis-association

인가된 클라이언트가 외부의 비인가 AP에 접속

비인가 AP 접속 탐지용 프로그램

```
void usrfunc::macCmp(listload& listMan2)
{
        WHTFlag = false; //true in whitelisted packet
        BLKFlag = false; //true in blacklisted packet
        RadiotapHeader *RH = (RadiotapHeader*)(pktPoint);
        int length = RH->length;
        ManagementFrame *MF = (ManagementFrame*)(pktPoint+length);
        int cmpFlag = 0;
        listload::bw_list::iterator it;
         printf("AP MAC CHECK\n\n");
//wht list!
        for(it = listMan2.WhiteList.begin();it !=listMan2.WhiteList.end();it++){
                bwDatas = (listload::bwList)it->second;
                printf("pkt compare with %02x %02x %02x %02x %02x %02x\n",bwDatas.a
                pMac[0],b wDatas.apMac[1],bwDatas.apMac[2],bwDatas.apMac[3],bwDat
                as.apMac[4],bwDatas.apMac[5]);
```

~ 이하 생략 ~

개발 환경 및 시스템 개발(4/5)

요소 기술 개발(3/4)

❍ 보안정책 위반(Mis-Configured) AP

Mis-configured AP

암호화 미적용, WEP와 같은 약한 수준의 보안

보안정책 위반 탐지용 프로그램

```
int usrfunc::misconfigureAP(listload& listMan2)
{
                        ~ 중략 ~
 //**********************Flag set*********************
            if(sM.oUI[0] == 0x00 && sM.oUI[1] == 0x50 && sM.oUI[2] == 0xf2 &&
            sM.gCSS[0] == 0x00 && sM.gCSS[1] == 0x0f && sM.gCSS[2] == 0xac)//OUI 00-50-f2 &&
            OUI 00-0f-ac -> WPA2
            {
                        //a = 20; //WPA-2 flsg:20
                        sF.enc = WPA2;
                        sF.groupCipher = Cipher(sM.gCSS[3]);
                        sF.pairwiseCipher = Cipher(sM.pCSS[3]);
                        sF.auth = Auth(sM.aSS[3]);
            }
            else if(sM.oUI[0] == 0x00 && sM.oUI[1] == 0x50 && sM.oUI[2] == 0xf2)//OUI 00-50-f2
            -> WPA-1
                                    ~ 이하 생략 ~
```

개발 환경 및 시스템 개발(5/5)

요소 기술 개발(4/4)

❍ 불법복제 AP(Fake AP)

Fake AP

침입자는 기존의 무선 AP들과 이름이 같은

Fake AP 탐지용 프로그램

```
void usrfunc::fakeAp(listload& listMan2)
{
        WHTFlag = false; //true in whitelisted packet
        BLKFlag = false; //true in blacklisted packet
        uint8_t* pktPoint2 = this->pktPoint;
        printf("=============================================\n");
        printf("FAKE AP CHECK\n\n");
        struct packframes::WifiName *wifiName;
//BSSID*************************************************************//
        printf("BSSID: ");
        for(int i=0; i<6; i++)
        {
                printf("%02x ", mgmtFrame->addr3[i]);
        }
        printf("\n");
//SSID*************************************************************//
        pktPoint2 += (RTHeader->rth_length + sizeof(struct packframes::ManagementFrame)
```

~ 이하 생략 ~

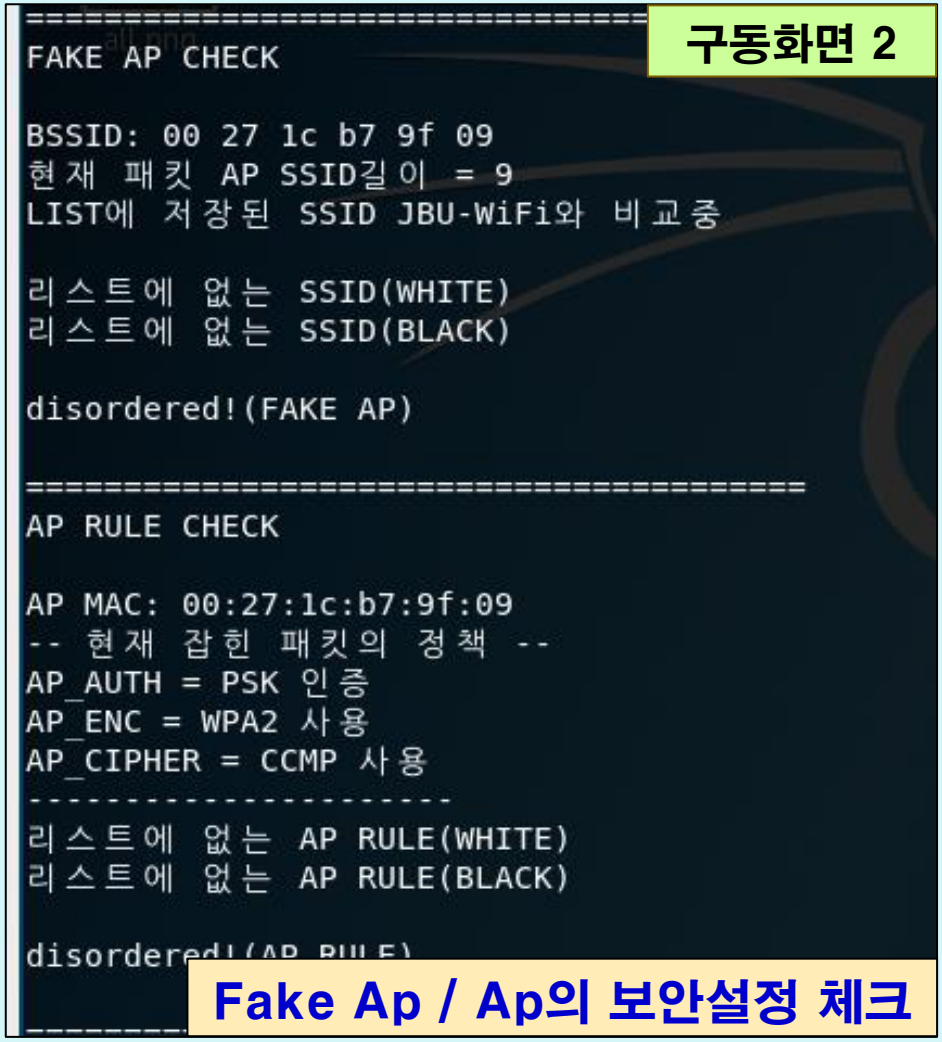
개발 시스템 운영(1/7)

시스템 구동

구동화면 1

Ap MAC / Ad-hoc 체크

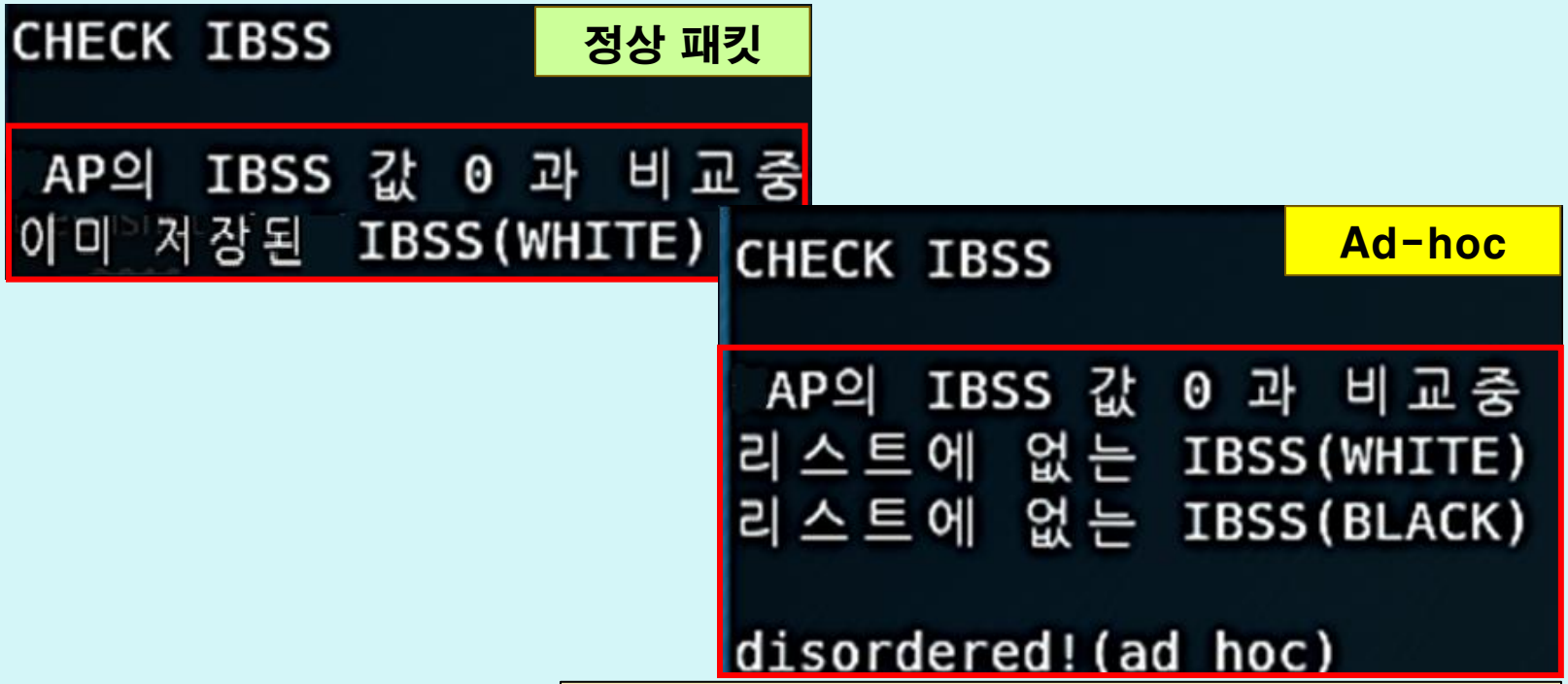
구동화면 2



Fake Ap / Ap의 보안설정 체크

개발 시스템 운영(2/7)

탐지 1 : Ad-hoc 네트워크 탐지



화이트&블랙 리스트 X -> 블랙리스트에 추가
IBSS 값을 비교하여 Ad-hoc 판별

개발 시스템 운영(3/7)

탐지 2 : 외부 AP 접속 탐지

정상 패킷

```
AP MAC CHECK

pkt compare with ac a3 1
현재 패킷의 bssid  ac a3
이미 저장된 AP MAC(WHITE
```

비인가 AP

```
AP MAC CHECK

pkt compare with ac a3 1e 89 c3 e0
현재 패킷의 bssid  00 27 1c b7 9f 09
리스트에 없는 AP MAC(WHITE)
리스트에 없는 AP MAC(BLACK)
disordered!(AP MAC)
```

화이트&블랙 리스트 X -> 블랙리스트에 추가

무선랜 프로토콜 MAC 주소를 비교하여 비인가 AP 판별

개발 시스템 운영(4/7)

탐지 3 : 보안정책 위반 탐지

정상 패킷

```
AP RULE CHECK

AP MAC: 00:27:1c:b7:9f:09
-- 현재 잡힌 패킷의 정책 --
AP_AUTH = PSK 인증
AP_ENC = WPA2 사용
AP_CIPHER = CCMP 사용
----------------------
이미 저장된 AP RULE(WHITE)
```

보안정책 위반

```
AP RULE CHECK

AP MAC: 00:27:1c:b7:9f:09
-- 현재 잡힌 패킷의 정책 --
AP_AUTH = PSK 인증
AP_ENC = WPA2 사용
AP_CIPHER = CCMP 사용
----------------------
리스트에 없는 AP RULE(WHITE)
리스트에 없는 AP RULE(BLACK)

disordered!(AP RULE)
```

화이트&블랙 리스트 X -> 블랙리스트에 추가
보안정책을 비교하여 보안정책 위반 판별

개발 시스템 운영(5/7)

탐지 4 : Fake AP 탐지

정상 패킷

```
==========
FAKE AP CHECK

BSSID: 18 c5 01 10 d3
현재 패킷 AP SSID길이
LIST에 저장된 SSID JBU

이미 저장된 SSID(WHITE
```

Fake Ap

```
==========
FAKE AP CHECK

BSSID: 00 27 1c b7 9f 09
현재 패킷 AP SSID길이 = 9
LIST에 저장된 SSID JBU-WiFi와 비교중

리스트에 없는 SSID(WHITE)
리스트에 없는 SSID(BLACK)

disordered!(FAKE AP)
```

화이트&블랙 리스트 X -> 블랙리스트에 추가
SSID, BSSID, MAC주소를 비교하여 FAKE AP 판별

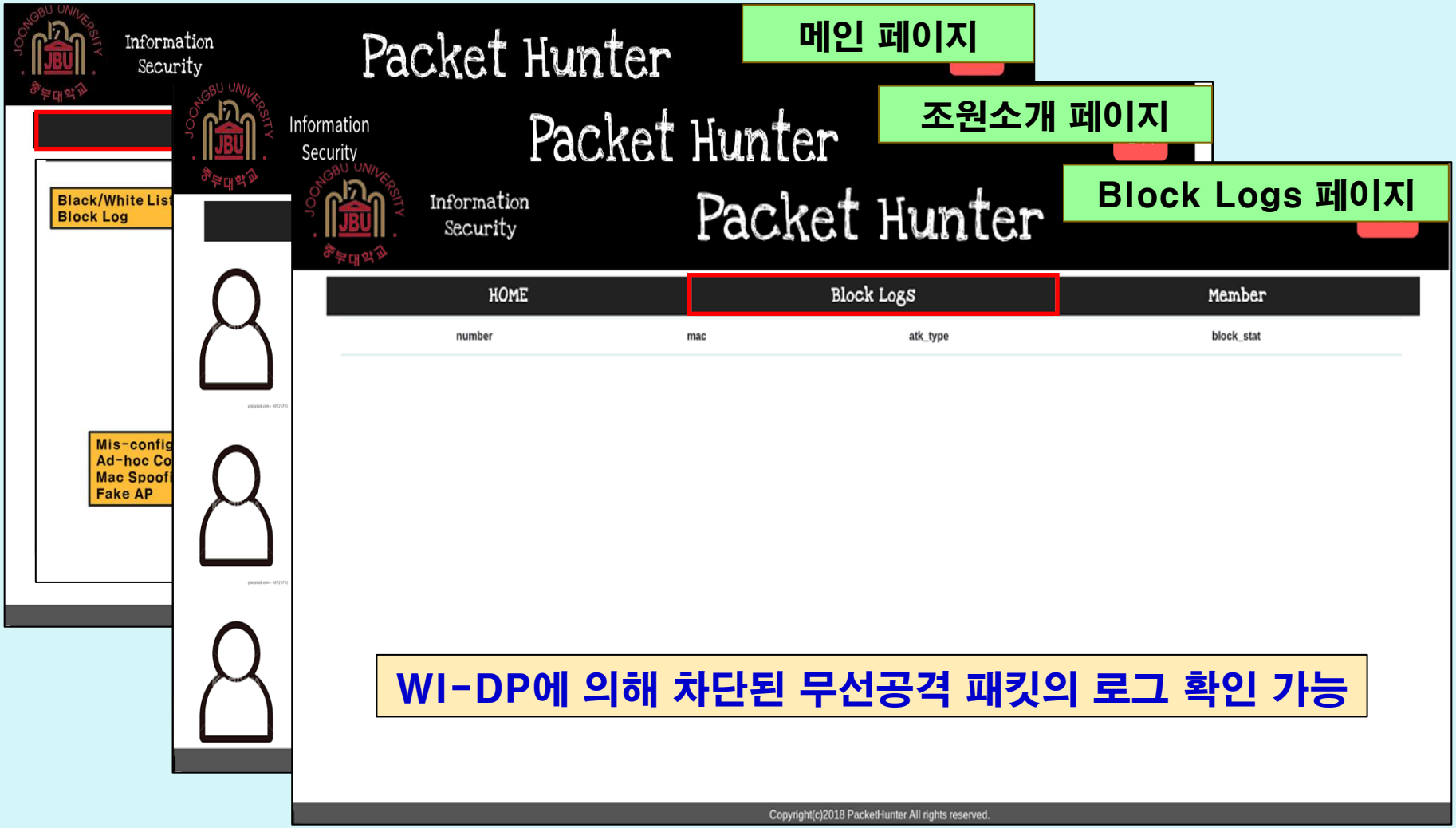
개발 시스템 운영(6/7)

관리자 페이지

관리자 페이지에서 Black / White 리스트 내용 등의 데이터베이스 값 조회 및 수정이 가능

개발 시스템 운영(7/7)

웹 페이지



결론 및 기대효과

❍ 침입탐지 및 방어시스템 개발 성과

- 무선 공격에 대한 위협 탐지 및 차단 기능을 제공하고, 화이트/블랙 리스트 관리의 편리성을 높이며 차단패킷 정보 확인이 가능

- 또한 무선 패킷분석 및 취약점 점검도구로 활용이 가능하며 모듈화로 프로그램 확장 및 재사용 용이

❍ 기대 효과 및 교훈

- 이 시스템 운영 시 보안이 대폭 강화된 무선 네트워크 환경 구축이 가능할 것으로 기대

- 무선 프로토콜 학습 및 소프트웨어 개발 경험을 통해 이 분야 실무 기술 역량을 배양하고 팀워크의 중요성을 체험하는 기회

감사합니다.

Q & A