프로젝트(Adeauth)

- Deauth 패킷을 이용한 와이파이 차단 -

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY

정보보안융합S/W 정영호

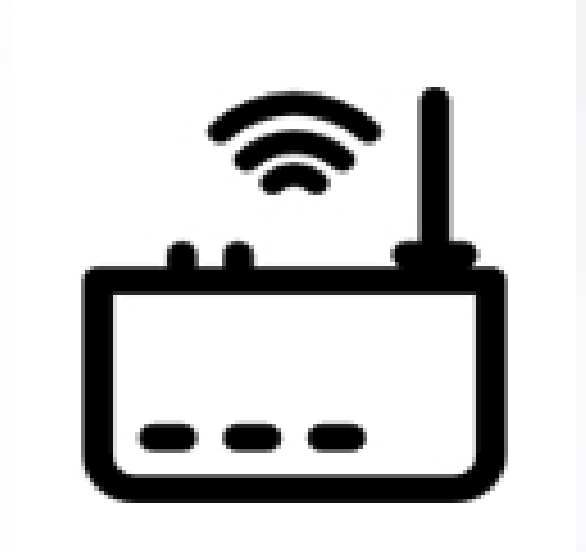
Contents

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY

무선 통신

CCIT
CULTURE CONTENTS &
INFORMATION TECHNOLOGY

무선통신



AP(Access Point)

Station

보통 공유기를 AP라하며 AP에 연결된 장치들(스마트폰, 노트북) 등을 Station이라 한다.

무선 네트워크 용어

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY

SSID

BSSID

SSID(Service Set Identifier) WLAN의 NETWORK 이름
BSSID(Basic Service Set Identifier) AP의 MAC주소

AP의 통신

AP는 각자 사용하는 Channel 주파수 대역이 존재함

AP 탐지 원리

AP의 경우 주기적으로 Beacon frame 패킷을Broadcast시켜 자신의 존재 유무를 station들에게 인식시킴.
이로인해 station들은 AP의 존재를 알게되고 와이파이라는 연결을 통해 커넥션이 이루어짐.

Deauth 패킷

AP가 자신의 활동, 즉 더 이상의 AP에 대한 기능을 그만하고 종료하겠다는 의미의 패킷

프로그램 동작원리

동작원리

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY

AP

Monitor 모드의 Attacker

1. AP의 Beacon프레임을 탐지하여 해당 AP의 채널과 SSID, MAC주소 등을 수집한다.
2. 수집한 데이터를 토대로 Deauth패킷을 만든다. (출발지 주소를 수집한 AP Mac으로 설정)
3. 생성된 Deauth패킷을 Broadcast하거나 특정 Dev의 Mac주소를 목적지로 전송한다.
4. Deauth 패킷을 받은 Dev는 AP가 Deauth 패킷을 전송한줄 알게되며 와이파이기능이 중지된다.

사용가능한 분야

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY

- 특정 방화벽 보안강화로 사용가능
- 장치와 AP 등을 관리하면서 허용되지 않은 장치에 대해 Deauth 공격을 하고 등록된 기기는 공격하지 않는 방법으로 보안을 강화시킬수 있음
- AP에 대한 암호를 알고 네트워크 대역에 접속을 하더라도 네트워크 사용이 불가하기때문에 보안성이 좋음

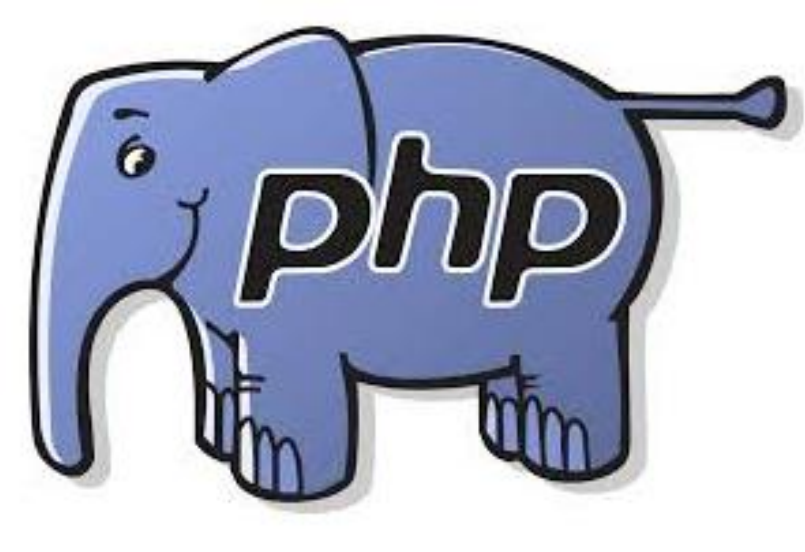
개발환경

개발환경

TP-LINK

개발환경

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY



Mysql Table 구성

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY

Table 명 = ap_data, dev_data

ap_data -> ap의 mac주소와 channel, SSID, memo로 구성

dev_data -> device의 mac주소와 사용자이름(user_name), memo로 구성

Table 구성

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY

```
create table ap_data
(
        ap_mac char(18) not null,
        channel int not null,
        SSID char(32),
        memo char(30),
        primary key(ap_mac)
);
```

```
create table station_data
(
        dev_mac char(18) not null,
        user_name char(30) not null,
        memo char(30),
        primary key(dev_mac)
);
```

Table 구성

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY

ap_data

Field	Type	Null	Key	Default	Extra
ap_mac	char(18)	NO	PRI	NULL	
channel	int(11)	NO		NULL	
SSID	char(32)	YES		NULL	
memo	char(30)	YES		NULL	

dev_data

Field	Type	Null	Key	Default	Extra
dev_mac	char(18)	NO	PRI	NULL	
user_name	char(30)	NO		NULL	
memo	char(30)	YES		NULL	

Table 구성

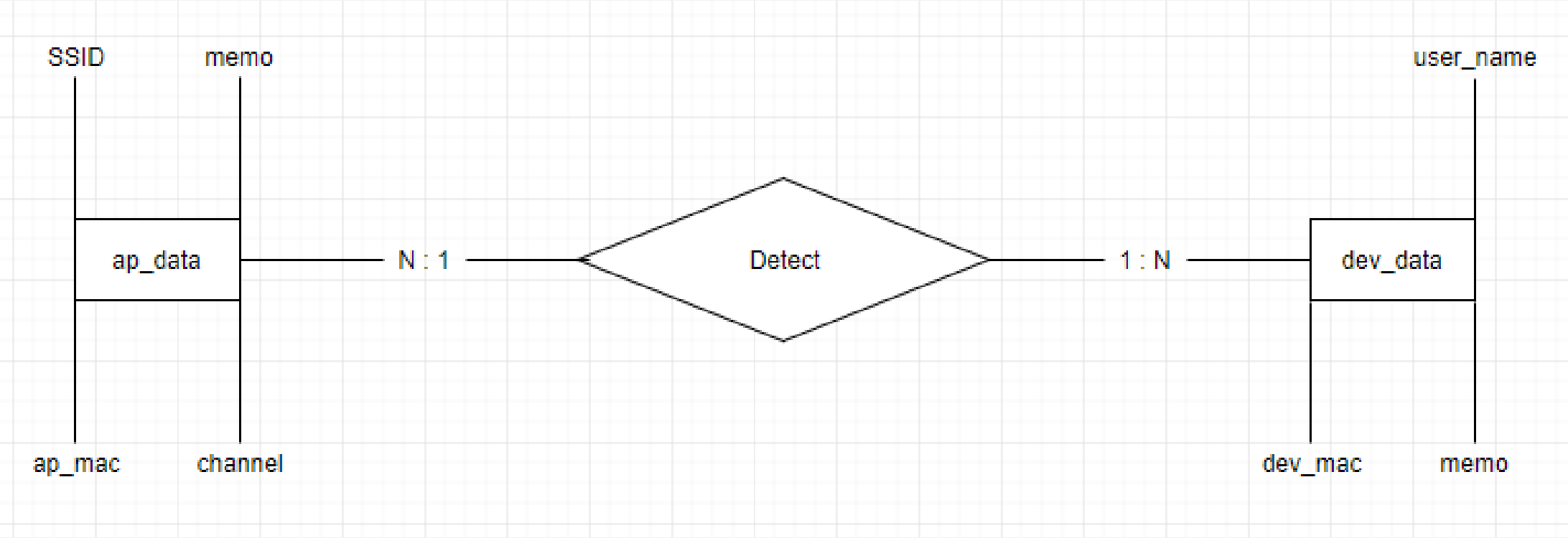
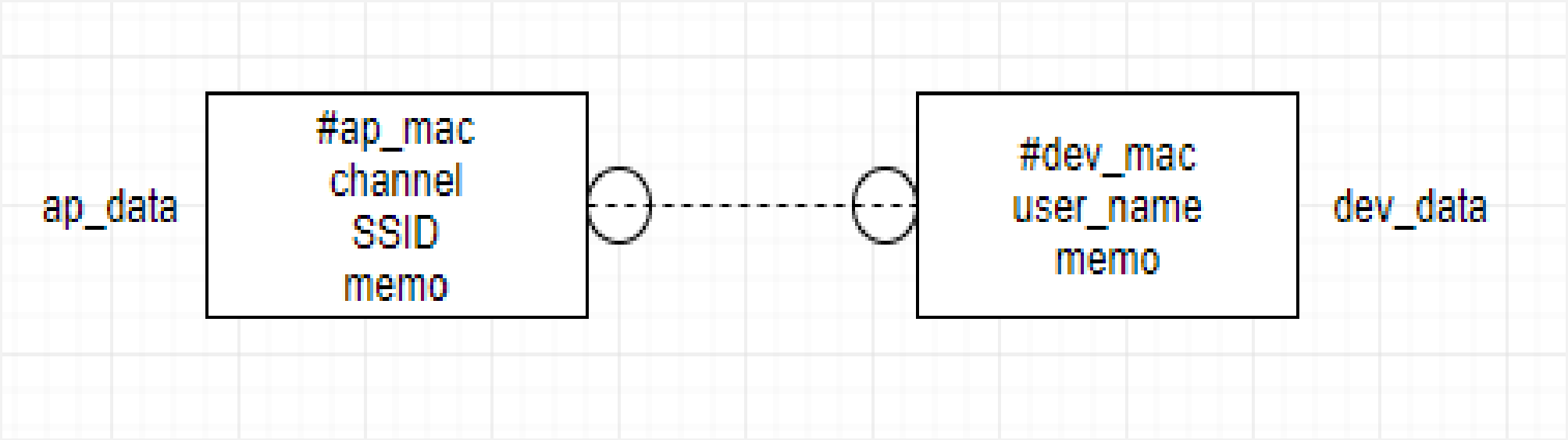
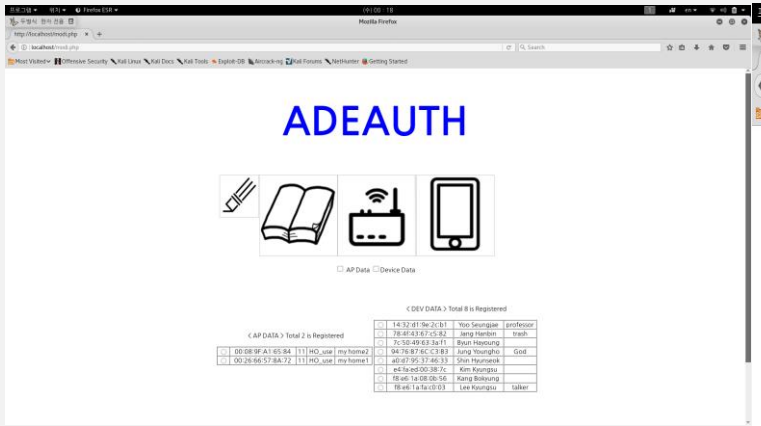

SSID
memo
user_name
ap_data
N : 1
Detect
1 : N
dev_data
ap_mac
channel
dev_mac
memo

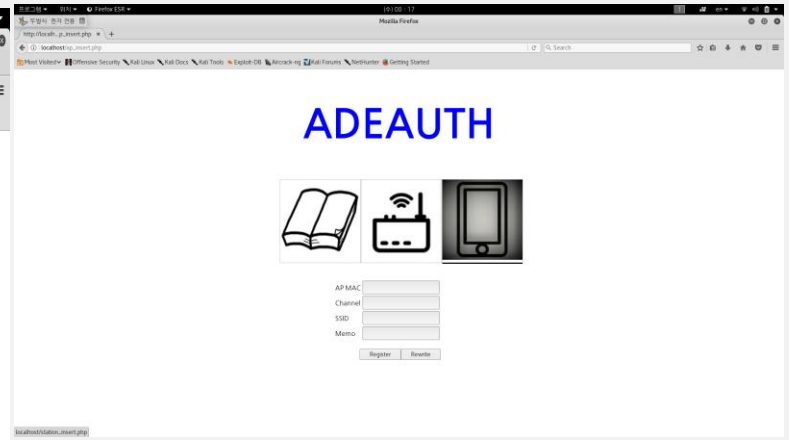
Table 구성


ap_data
#ap_mac
channel
SSID
memo
#dev_mac
user_name
memo
dev_data

Adeauth 웹페이지

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY





시 연

Q & A
감사합니다