보안 분야 조사

2021.04.08

정보보호학전공 1학년 노무승

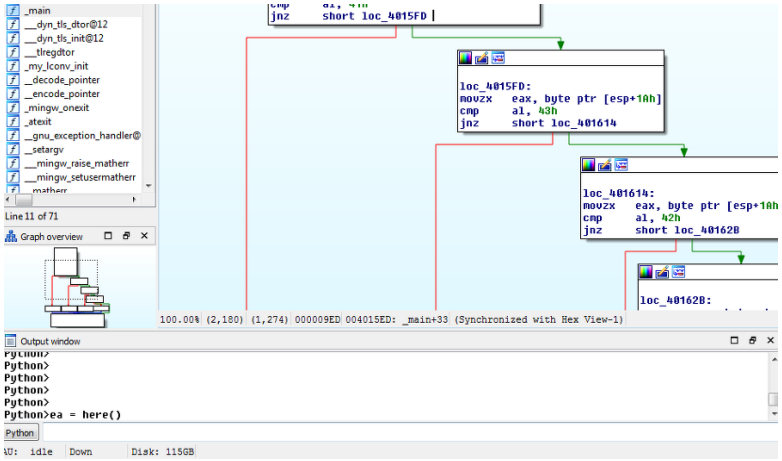
목차

1. 리버싱

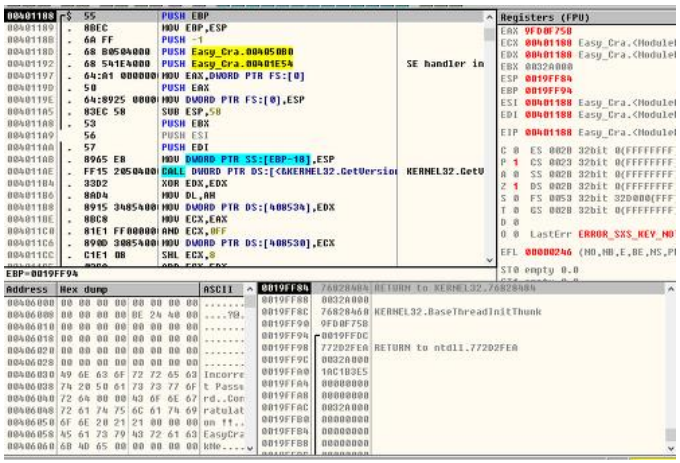
1-1. 리버싱이란?

정확한 명칭은 **리버스 엔지니어링**이고,

프로그램을 역분석하는 분야입니다.



IDA



올리디버거

1-2. 리버싱에는

정적 분석

파일을 실행시키지 않고,

파일의 바이너리 데이터만 가지고 분석하는 것.

동적 분석

파일을 실행시켜가며,

레지스터나 메모리를 보면서 분석하는 것.

1-3. 리버싱을 배우려면..

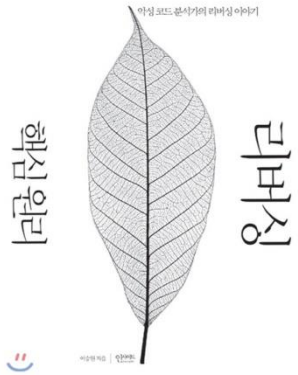
워게임 (보안 문제 실습 사이트)

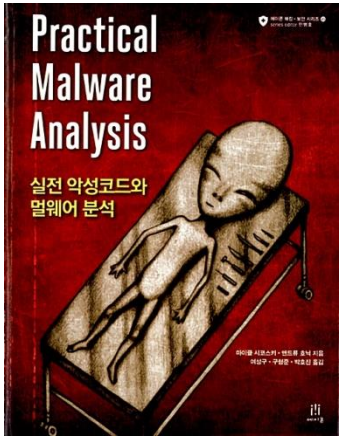
reversing.kr : 리버싱 문제 전문 워게임

codeengn.com : 리버싱 기초 부터 심화 문제 워게임

xcz.kr : 종합 워게임 (안드로이드 리버싱 등 실습 가능)

서적





1-3. 리버싱을 배워서..

악성코드 분석가

모의해킹 전문가

게임 보안 솔루션 개발

버그 헌터

…

2. 웹 해킹

2-1. 웹 해킹이란?

웹 사이트와 DBMS의 다양한 취약점을 이용하여

웹 사이트나 DB, 또는 웹 사이트 사용자를 대상으로 공격하는 분야임.

버프슈트

sqlmap

2-2. 웹 해킹에는..

대표적으로

OWASP TOP 10 이 존재

OWASP Top 10 Vulnerabilities in 2021 are:

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfigurations
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging and Monitoring

https://www.immuniweb.com/resources/owasp-top-ten/

2-3. 웹 해킹을 배우려면..

워게임 (보안 문제 실습 사이트)

webhacking.kr : 웹해킹 문제 전문 워게임

실습 가상 환경

beebox (bWAPP)

DVWA

OWASP TOP 10이나 특정 기준으로 잡고, 직접 웹 사이트를 구축해서 공격과 방어를 실습해보는 것이 제일 효과적이라고 알려져 있음.

2-4. 웹 해킹을 배워서..

모의해킹 전문가

웹 개발자

버그 헌터

…

3. 포렌식

3-2. 포렌식에는..

시스템 포렌식

디스크 포렌식

메모리 포렌식

모바일 포렌식

네트워크 포렌식

....

3-1. 포렌식이란?

디지털 포렌식은 디지털 기기를 매개체로 하여 발생한 특정 행위의 사실관계를 법정에서 규명하고 증명하기 위한 절차와 방법임.

보안 업계에선 줄여서 포렌식이라 부르지만 원래는 **법의학**을 의미함.

3-3. 포렌식을 배우려면..

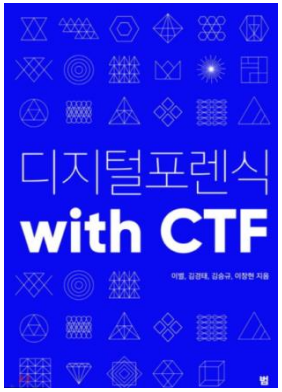
워게임 (보안 문제 실습 사이트)

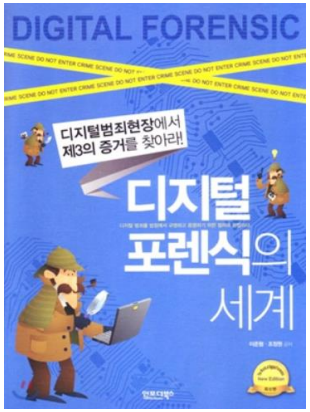
ctf-d.com : 포렌식 문제 전문 워게임

도움되는 사이트

https://github.com/proneer/Slides : 플레인비트 대표, 김진국 멘토님

서적





3-4. 포렌식을 배워서..

침해 사고 대응 (IR) 분석가

국가 (수사)기관 (경찰, 검찰, 국방, KISA, 금감원)

사설 복구 업체 (명xx기술)

디지털 포렌식 업체 연구원

4. 포너블

4-1. 포너블이란?

어떤 유저가 게임에서 승리했는데, own! 이라고 입력할 것을 pwn! 라고 입력한 것에서 유래되었다.

다른 말로는 **시스템 해킹**으로, 리버싱, 메모리 보호 기법 우회, 오버플로우 등을 이용해 상위 접근 권한을 얻는 것이 목표이다.

4-2. 포너블을 배우려면 ..

실습 가상 환경

해커스쿨 FTZ

해커스쿨 LOB

워게임 (보안 문제 실습 사이트)

pwnable.kr : 포너블 전용 워게임 (한국)

pwnable.tw : 포너블 전용 워게임 (타이완)

4-3. 포너블을 배워서..

모의 해킹 전문가

버그 헌터

~~CTF 고수~~

…

5. 암호학

5-1. 암호학이란?

민감한 정보를 보호하기 위한 기술이다.

(ex. RSA, AES, SHA, MD5)

5-2. 암호학을 배우려면..

수학 수학 수학 수학 수학 수학 수학 코딩 수학 수학 수학 수학 수학 수학 수학

수학 수학 수학 수학 수학 수학 수학 코딩 수학 수학 수학 수학 수학 수학 수학

수학 수학 수학 코딩 수학 수학 수학 수학

수학 수학 수학 코딩 수학 수학 수학 수학

수학 수학 수학 코딩 수학 수학 수학 수학

수학 수학 수학 코딩 수학 수학 수학 수학

수학 수학 수학 코딩 수학 수학 수학 수학

수학 수학 수학 코딩 수학 수학 수학 수학

수학 수학 수학 코딩 수학 수학 수학 수학

수학 수학 수학 수학 수학 수학 수학 코딩 수학 수학 수학 수학 수학 수학 수학

수학 수학 수학 수학 수학 수학 수학 코딩 수학 수학 수학 수학 수학 수학 수학

5-3. 암호학을 배워서..

암호 개발자 (국정원..)

암호 취약점 분석 (국정원..)

암호 라이브러리 개발자

~~조금 더 deep한 지식들을 습득 가능..~~

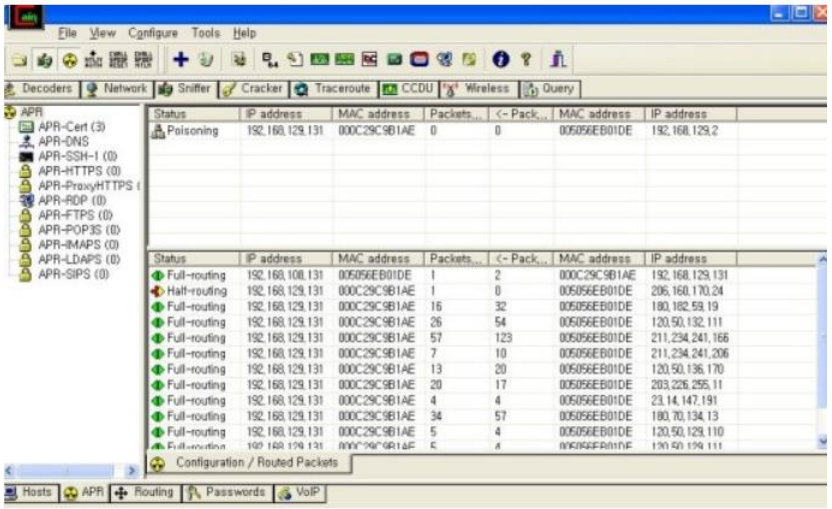
~~AI 분야로 쉽게 이직 가능..~~

…

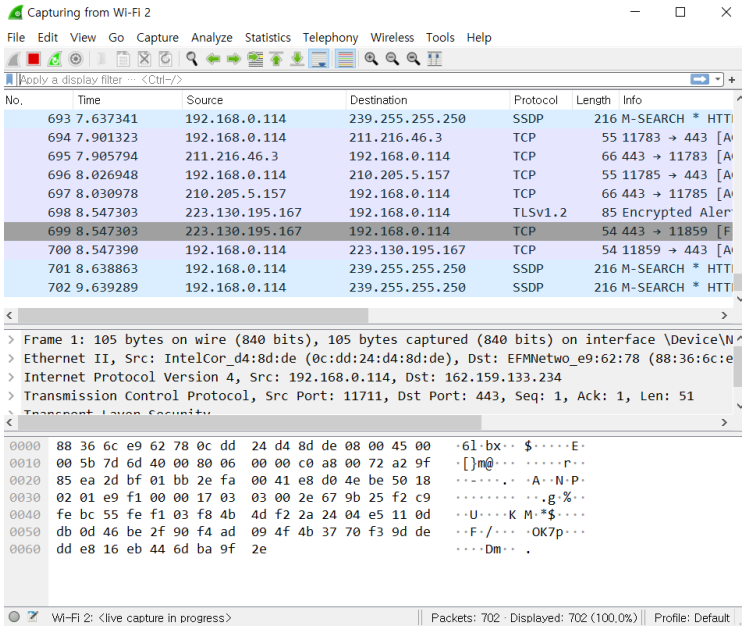
6. 네트워크

6-1. 네트워크 보안이란?

네트워크 통신과 관련하여 보안하고 해킹하는 분야



카인과 아벨
(ARP 스푸핑 툴)



와이어샤크
(네트워크 패킷 확인)

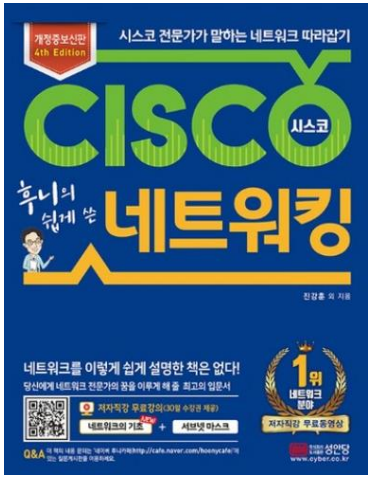
6-2. 네트워크 보안을 배우려면..

이론 + 실습 + 코딩

(서적) (칼리리눅스) (프로그램 제작)

(와이어샤크)

서적



6-3. 네트워크 보안을 배워서..

모의 해킹

보안 관제

전산 업무

…

7. 융합 보안

7-1. 융합 보안이란?

물리보안과 정보보안의 간의 융합

7-2. 융합보안을 배우려면..

융합 보안 대학원에 진학하는 것 이외에는

뭐라고 딱히 정의하기는 어렵지만, 경험 상으로 실습은..

.

RF (전파) 해킹 → HackRF One

RFID 카드 해킹 → Proxmark 3 Easy

MS 카드 해킹 → 스키머 (MSR605X, ...)

블루투스 해킹 → Ubertooth One, HackRF One

자물쇠 해정 → 락피킹

하드웨어 해킹 → UART, JTAG, Flash 추출, ...

802.11(와이파이) 해킹 → Monitor Mode 지원 랜카드

7-3. CTF와 연관이 없을까?

– 이번 대회의 문제 출제 경향과 느낌?

최상명 : 최신 트렌드에 맞게 모바일, 스마트폰 등과 관련된 주제의 문제가 비중 있게 다루어졌고, 시스템, 웹 등의 문제가 골고루 섞여서 어느 쪽으로도 치우치지 않은 다양한 문제가 출제되었습니다. 특히 블루투스 문제는 해킹대회에서 처음 접하는 문제라 신선했습니다. 해킹방어대회는 항상 새로운 주제의 문제들이 나와서 계속해서 참가하게 만듭니다. 대회를 통해서 항상 새로운 것들을 많이 배워갑니다.

하동주 : 다른 대회들과는 다르게 이 대회는 매번 새롭고 다양한 형태의 문제들이 출제되고 있어서 재미있는 것 같습니다. 다만 올해 본선에서는, 개인적으로 이 대회의 특색이라 생각했던 침해사고 대응, 악성코드 분석 문제들이 없어서 아쉬웠습니다.

김태형 : 최신 이슈와 관련된 문제들이 출제되어서 많은 생각을 하게 된 것 같습니다. 그리고 문제들이 함정이 많아서 초반에 방향을 잘못 잡을 경우에 시간을 많이 낭비하는 경우가 많았던 것 같습니다.

최현우 : 예선전부터 예사롭지 않은 문제들이 많았습니다. 덕분에 고생을 많이 했죠. 하지만 블루투스, ARM프로세서 등 다양한 유형의 문제들로 인해 즐거운 대회였습니다. 벌써부터 다음 대회가 기대되네요.

2010년 KISA 7회 해킹방어대회 우승자 인터뷰 中

(https://www.boannews.com/media/view.asp?idx=21538&kind=1)

8. 보안 개발

8-1. 보안 개발이란?

보안 '관련' 개발

1. 보안, 모의해킹 프로그램을 개발하는 것
2. 개발을 보안성 있게 하는 것 (ex. 시큐어코딩)

...

8-2. 보안 개발을 배우려면

1. 보안, 모의 해킹 프로그램을 개발할테야 ..

先 보안 기반 지식, 後 개발

(ex. 지뢰찾기 리버싱 -> 맵핵 개발)

(ex. ARP 프로토콜 분석 -> ARP 스푸핑 툴 개발)

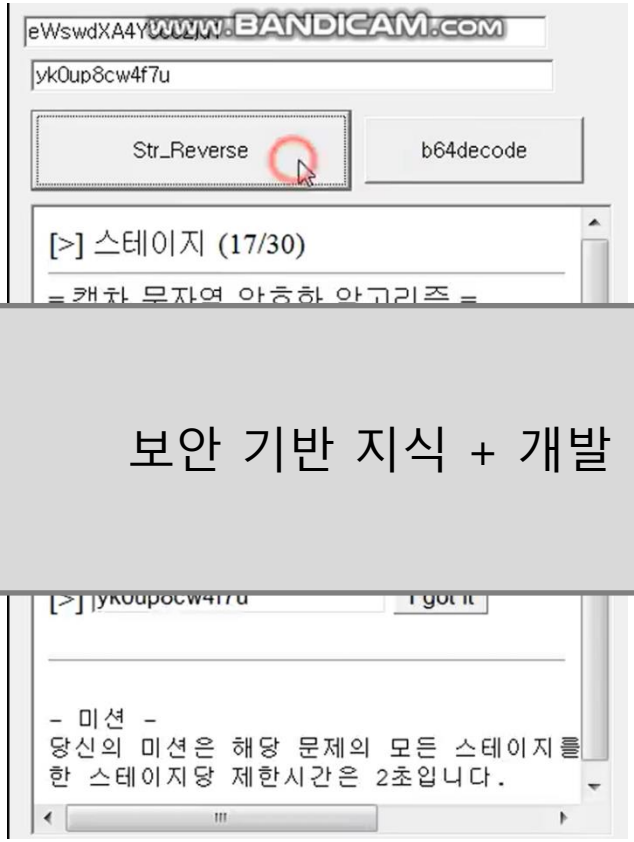
2. 안전한 프로그램을 개발할테야 ..

다양한 언어들을 익히고,

해당 언어의 취약한 함수, 흐름에 대한 보완 방법을 알고 있어야 함.

(ex. C언어의 경우 strcmp -> memcmp)

8-3. CTF와 연관이 없을까?



보안 기반 지식 + 개발

17회 POC 해킹캠프 CTF

9. 관심 분야

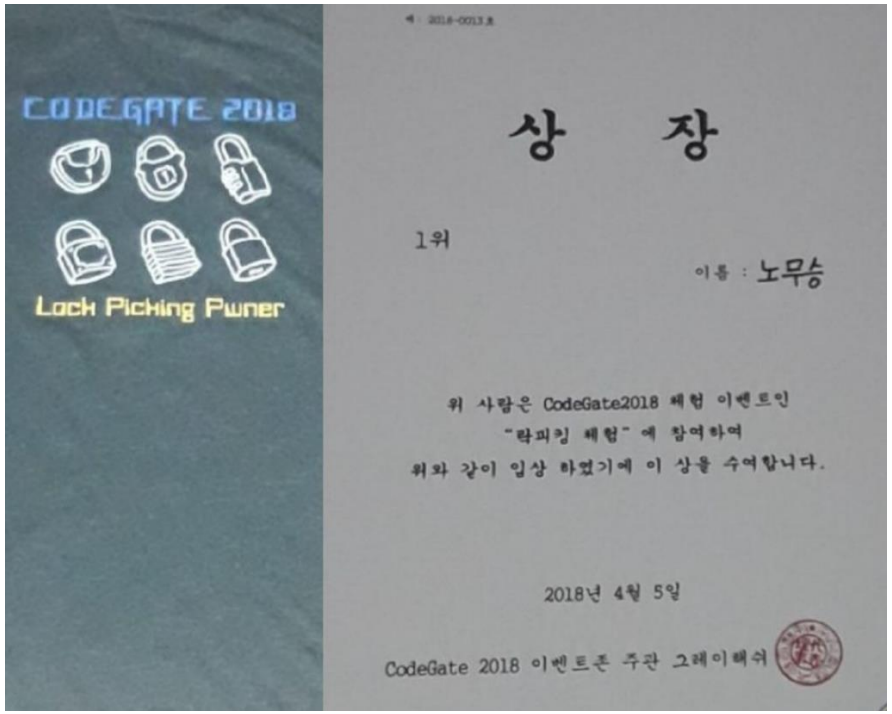
9-1. 관심 분야

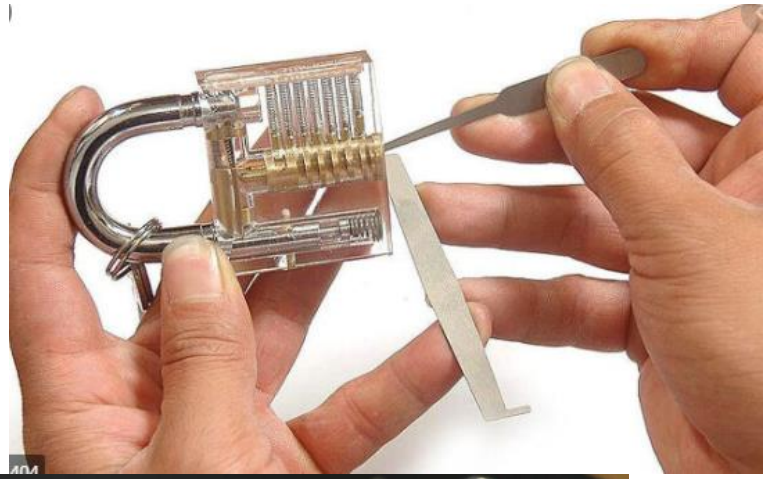
연구 분야 : 융합 보안

CTF 분야 : ??? (윈도우 리버싱, 포렌식)

9-2. 해 본 것들(?)

락피킹

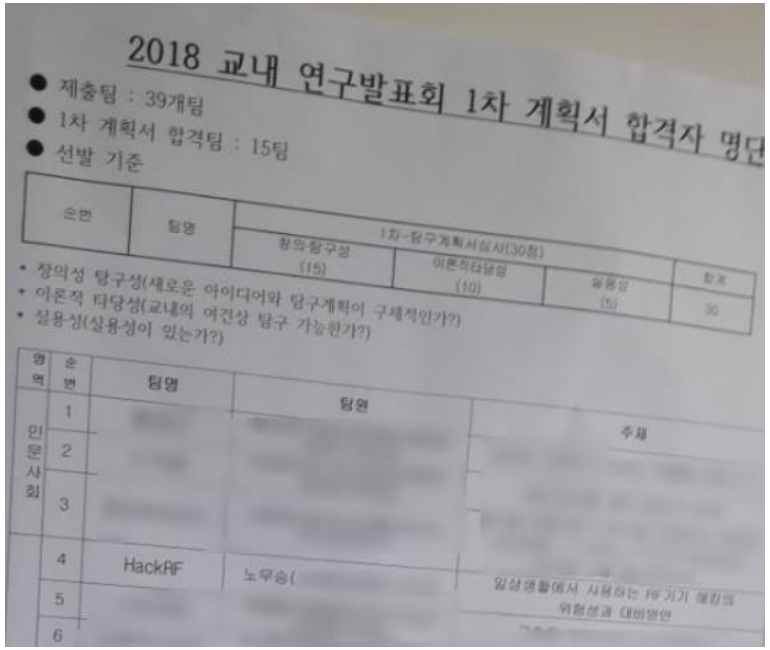

CODEGATE 2018
Lock Picking Pwner
상 장
1위
이름 : 노무승
위 사람은 CodeGate2018 해킹 이벤트인
"락피킹 해킹" 에 참여하여
위와 같이 입상 하였기에 이 상을 수여합니다.
2018년 4월 5일
CodeGate 2018 이벤트존 주관 그레이해쉬




자물쇠의 비밀
덮어볼까요?
화/목 밤 11시 10분 KBS2
무승이가 손에 쥔 것은? 바로 자물쇠

9-2. 해 본 것들(?)

전파 해킹 (수신만)



2018 교내 연구발표회 1차 계획서 합격자 명단

- 제출팀 : 39개팀
- 1차 계획서 합격팀 : 15팀
- 선발 기준

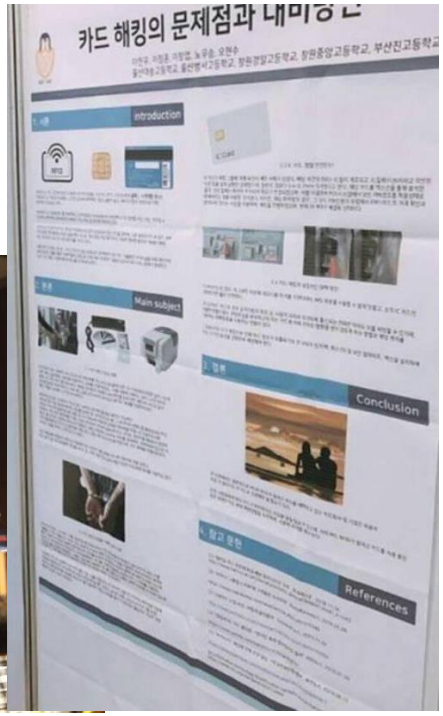
순번	팀명	1차-탐구계획서심사(30점)			
		창의탐구성 (15)	이론적타당성 (10)	실용성 (5)	합계

- 창의성 탐구성(새로운 아이디어와 탐구계획이 구체적인가?)
- 이론적 타당성(교내의 여건상 탐구 가능한가?)
- 실용성(실용성이 있는가?)

영역	순번	팀명	팀원	주제
인문사회	1			
	2			
	3			
	4	HackRF	노우승(	일상생활에서 사용하는 IT 기기 해킹의 위험성과 대비방안
	5			
	6			

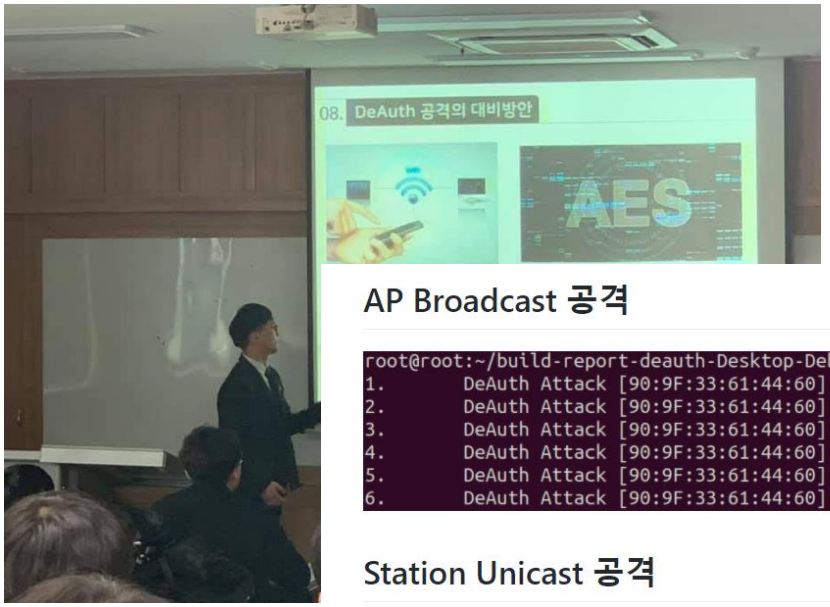
9-2. 해 본 것들(?)

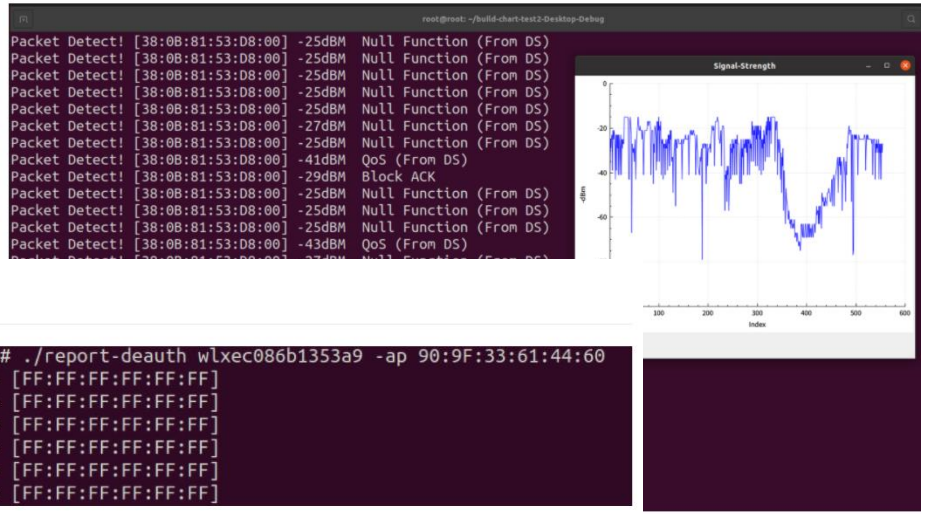
카드 해킹
(교통 카드 금액 변조..)
(도어락 카드 복제..)



9-2. 해 본 것들(?)

802.11 해킹





AP Broadcast 공격

```
root@root:~/build-report-deauth-Desktop-Debug# ./report-deauth wlxec086b1353a9 -ap 90:9F:33:61:44:60
1.       DeAuth Attack [90:9F:33:61:44:60] -> [FF:FF:FF:FF:FF:FF]
2.       DeAuth Attack [90:9F:33:61:44:60] -> [FF:FF:FF:FF:FF:FF]
3.       DeAuth Attack [90:9F:33:61:44:60] -> [FF:FF:FF:FF:FF:FF]
4.       DeAuth Attack [90:9F:33:61:44:60] -> [FF:FF:FF:FF:FF:FF]
5.       DeAuth Attack [90:9F:33:61:44:60] -> [FF:FF:FF:FF:FF:FF]
6.       DeAuth Attack [90:9F:33:61:44:60] -> [FF:FF:FF:FF:FF:FF]
```

Station Unicast 공격

```
root@root:~/build-report-deauth-Desktop-Debug# ./report-deauth wlxec086b1353a9 -ap 90:9F:33:61:44:60 -stn 50:77:05:96:30:0
a
1.       DeAuth Attack [50:77:05:96:30:0A] -> [90:9F:33:61:44:60]
2.       DeAuth Attack [50:77:05:96:30:0A] -> [90:9F:33:61:44:60]
3.       DeAuth Attack [50:77:05:96:30:0A] -> [90:9F:33:61:44:60]
4.       DeAuth Attack [50:77:05:96:30:0A] -> [90:9F:33:61:44:60]
5.       DeAuth Attack [50:77:05:96:30:0A] -> [90:9F:33:61:44:60]
6.       DeAuth Attack [50:77:05:96:30:0A] -> [90:9F:33:61:44:60]
7.       DeAuth Attack [50:77:05:96:30:0A] -> [90:9F:33:61:44:60]
8.       DeAuth Attack [50:77:05:96:30:0A] -> [90:9F:33:61:44:60]
^C
```

9-3. 해보고 싶은 것

블루투스 해킹 &

RF 해킹 추가 연구 &

802.11 해킹 추가 연구

감사합니다!