

# 자기주도 프로젝트

## 네트워크 보안 with Wireshark



## 계절학기

# 네트워크 보안 with Wireshark

## 이 승 윤 Project consultant

---

- 삼성 청년 SW 아카데미 프로젝트 컨설턴트
- 현대오트모빌 그룹사사업부
- 기업은행 IBK시스템 은행사업부
- Code For Korea
- 공인중개사



# Contents

- I 웹 보안
- II 패킷 스니핑 w/ Wireshark
- III 과제 설명
- IV 마치며



# 웹 보안



- ✓ 웹 보안의 필요성
  - ✓ 네트워크는 열려있는 곳
  - ✓ 적절히 방어하지 못하면 막심한 손해를 입게 됨
- ✓ 흔한 공격 방식
  - ✓ SQL Injection/Code Injection
  - ✓ XSS
  - ✓ CSRF
  - ✓ 세션 탈취
  - ✓ ...



# 가장 기본적인 웹 보안

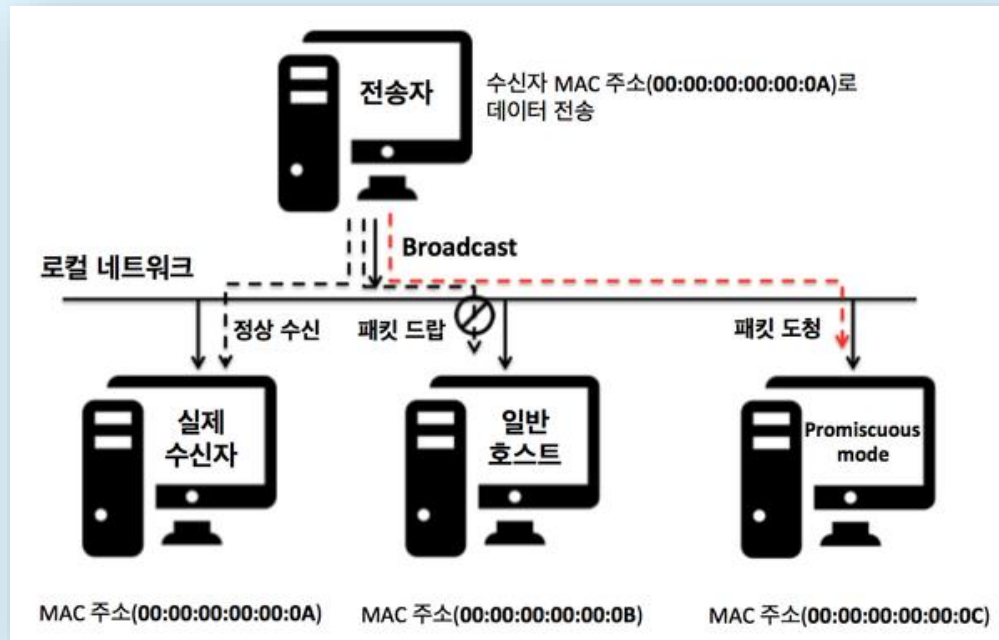
- ✓ ~~HTTP~~ → HTTPS
- ✓ 외부 접속 가능한 포트는 최소화(방화벽)
- ✓ 강력한 비밀번호 설정
- ✓ 접속/사용기록 로깅(logging)
- ✓ 입력 유효성 검사(FE 및 BE)
- ✓ 중요 정보 암호화 보관/전송
- ✓ 브라우저 보안 정책 준수

✓ 최대한 닫는다

✓ 암호화(통신, 저장)

# 패킷 스니핑 w/ Wireshark

- ✓ Wireshark : 네트워크 패킷 분석 도구
- ✓ 패킷 스니핑
  - ✓ Hub를 공유하는 같은 네트워크에 속한 패킷을 볼 수 있음.



# 패킷 스니핑 w/ Wireshark

The image shows a Wireshark packet capture window titled '\*Adapter for loopback traffic capture'. The left sidebar displays the 'Schemas' tree with 'sys' and 'test' databases. The main packet list shows several MySQL packets. Packet 305 is selected, showing a 'Request Query' from 127.0.0.1 to 127.0.0.1. The packet details pane shows the 'MySQL Protocol' section expanded, displaying 'Request Command Query' with 'Command: Query (3)' and 'Statement: select \* from test.table name\nLIMIT 0, 1000\n'. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
297	84.379264	127.0.0.1	127.0.0.1	MySQL	16677	Response TABULAR Response OK
301	86.457324	127.0.0.1	127.0.0.1	MySQL	49	Request Ping
305	86.460030	127.0.0.1	127.0.0.1	MySQL	93	Request Query
309	86.469185	127.0.0.1	127.0.0.1	MySQL	84	Request Query
313	87.395524	127.0.0.1	127.0.0.1	MySQL	67	Request Query
315	87.397812	127.0.0.1	127.0.0.1	MySQL	16677	Response TABULAR Response OK
331	90.406805	127.0.0.1	127.0.0.1	MySQL	67	Request Query
333	90.411899	127.0.0.1	127.0.0.1	MySQL	16677	Response TABULAR Response OK
349	93.423439	127.0.0.1	127.0.0.1	MySQL	67	Request Query

> Frame 305: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on 0  
> Null/Loopback  
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  
> Transmission Control Protocol, Src Port: 52344, Dst Port: 3306, Seq: 123456789  
MySQL Protocol  
  Packet Length: 45  
  Packet Number: 0  
  Request Command Query  
    Command: Query (3)  
    Statement: select \* from test.table name\nLIMIT 0, 1000\n

0000 02 00 00 00 45 00 00 59 b6 54 40 00 80 06 00 00  
0010 7f 00 00 01 7f 00 00 01 cc 78 0c ea cc 98 4e 00  
0020 40 ba 11 1a 50 18 04 56 90 c7 00 00 2d 00 00 00  
0030 03 73 65 6c 65 63 74 20 2a 20 66 72 6f 6d 20 20  
0040 65 73 74 2e 74 61 62 6c 65 5f 6e 61 6d 65 0a 20  
0050 49 4d 49 54 20 30 2c 20 31 30 30 30 0a 20 20 20

# 과제



- ✓ 패킷 스니핑 실습
- ✓ 암호화를 제공하지 않는 프로토콜 및 보완 방법 조사
  - ✓ DNS
  - ✓ FTP
  - ✓ Telnet
  - ✓ HTTP
  - ✓ MySQL
  - ✓ ...



마치며..



- ✓ 보안의 필요성/방법, 패킷 스니핑
- ✓ <https://www.kisa.or.kr/2060207?page=2>

33	<u>소프트웨어 개발 보안 가이드</u>	2021-11-29

