SSL 스트립 공격

202112021 박채우

SSL

Secure Sockets Layer SSL은 암호규약을 뜻한다. 최근에는 TLS (Transport Layer Security)라는 이름으로 변경되었다.

SSL은 클라이언트/서버 응용 프로그램이 네트워크로 통신을 하는 과정에서 도청, 간섭, 위조를 방지하기 위해서 설계되었다. 암호화를 해서 최초, 마지막 과정에서 인증, 통신 기밀성을 유지시켜준다.

SSL

개인정보를 취급하는 모든 웹사이트는 SSL 인증서를 구축해야 하는 정보통신망법이 개정되었다.

제28조(개인정보의 보호조치)

① 정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다. 〈개정 2016.3.22.〉

1. 개인정보를 안전하게 처리하기 위한 내부관리계획의 수립·시행
2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영
3. 접속기록의 위조·변조 방지를 위한 조치
4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치
5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치
6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치

제67조(과태료) ②다음 각 호의 어느 하나에 해당하는 자는 1천만원 이하의 과태료에 처한다.

SSL

HTTPS 는 SSL/TLS 독립적인 보안계층 위에 HTTP 프로토콜을 얹어 보안된 HTTP통신을 하는 프로토콜을 의미한다. 즉 SSL은 HTTP 뿐만 아니라 FTP, SMTP 같은 다른 프로토콜에도 적용할 수 있다.

SSL 인증서

SSL 인증서는 클라이언트와 서버간 통신을 제 3자가 보증해주는 전자화된 문서이다. 클라이언트가 서버에 접속한 후 서버는 클라이언트에게 인증서를 전달하고 클라이언트에서 인증서가 신뢰할 수 있는 인증서인지 검증 한 후에 프로토콜을 이어 나간다.

SSL 인증서는 크게 2가지 역할을 한다.

1. 서버가 신뢰할 수 있는 서버임을 보장한다.
2. SSL 프로토콜 과정 중에 사용할 공개키를 클라이언트에게 제공한다.

SSL

SSL 통신은 핸드쉐이크, 전송, 세션종료 3가지 단계를 거치면서 클라이언트와 서버간 통신을 한다.

1. 핸드쉐이크

1. 클라이언트가 서버에 접속하는 Client Hello : 클라이언트에서 생성한 랜덤 데이터와 클라이언트가 지원하는 암호화 방식들을 서버에 전달
2. 서버가 응답하는 Server Hello : 서버에서 생성한 랜덤 데이터와 클라이언트가 전달한 암호화 방식 중 서버에서도 사용가능한 암호화 방식을 선택해 클라이언트에 전달
3. 클라이언트가 서버의 인증서가 CA에서 발급된 것인지 확인하고 클라이언트의 랜덤 데이터와 클라이언트의 랜덤 데이터를 조합해서 pre master secret키를 생성 후 서버로 전송
4. 서버는 pre master secret키를 복호화 후 서버와 클라이언트 모두 pre master secret 에서 master secret 를 획득

2. 세션

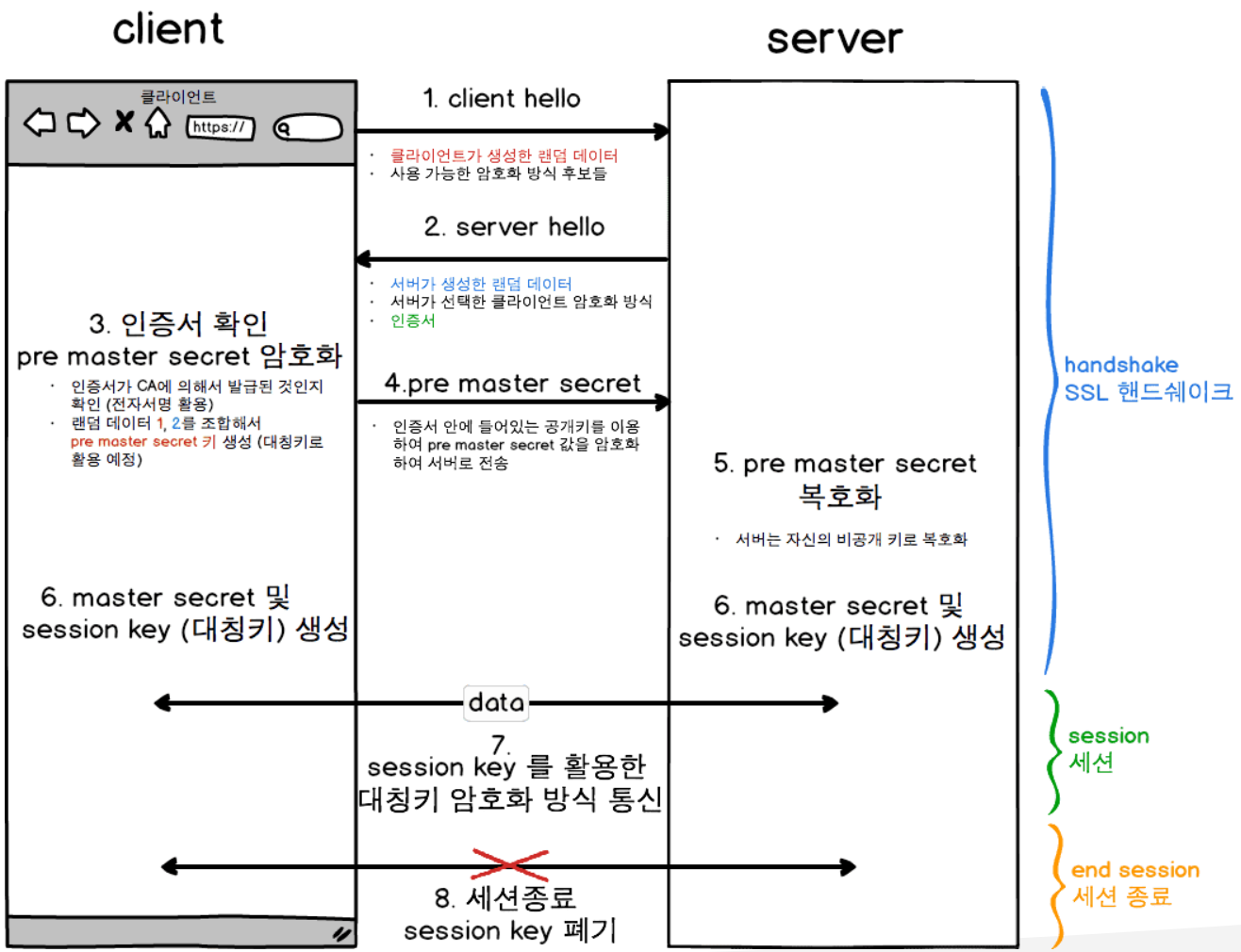
master secret은 session key를 생성한다. 즉 서버와 클라이언트 모두 같은 session key를 공유하고 있기 때문에 대칭키로 데이터를 암호화해서 전달한다.

3. 세션 종료

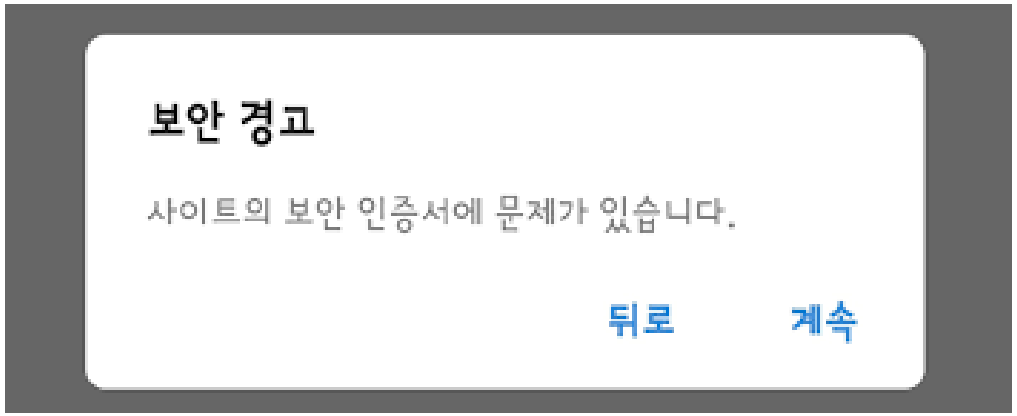
모든 데이터의 전송이 끝나면 SSL 통신이 끝났음을 서로에게 전달하며 이 과정에서 통신에서 사용한 session key를 폐기하게 된다.

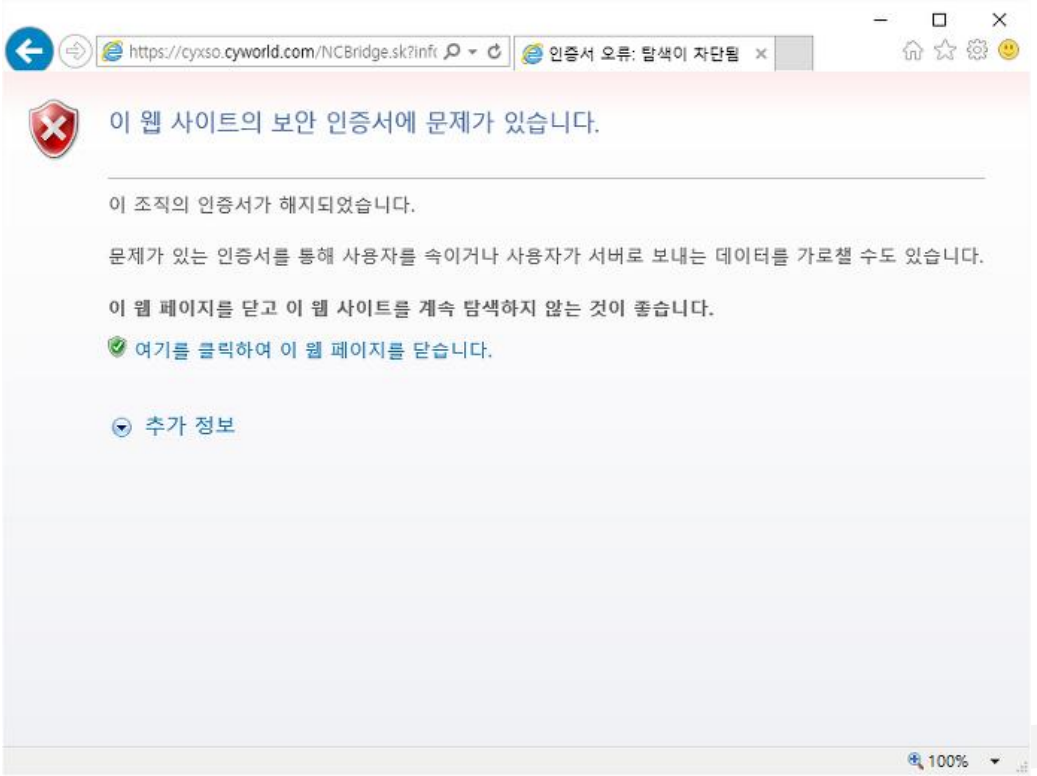
SSL

SSL 통신과정


client
server
클라이언트
https://
1. client hello
· 클라이언트가 생성한 랜덤 데이터
· 사용 가능한 암호화 방식 후보들
2. server hello
· 서버가 생성한 랜덤 데이터
· 서버가 선택한 클라이언트 암호화 방식
· 인증서
3. 인증서 확인
pre master secret 암호화
· 인증서가 CA에 의해서 발급된 것인지 확인 (전자서명 활용)
· 랜덤 데이터 1, 2를 조합해서 pre master secret 키 생성 (대칭키로 활용 예정)
4.pre master secret
· 인증서 안에 들어있는 공개키를 이용하여 pre master secret 값을 암호화하여 서버로 전송
5. pre master secret 복호화
· 서버는 자신의 비공개 키로 복호화
6. master secret 및 session key (대칭키) 생성
6. master secret 및 session key (대칭키) 생성
data
7.
session key 를 활용한 대칭키 암호화 방식 통신
8. 세션종료
session key 폐기
handshake
SSL 핸드쉐이크
session
세션
end session
세션 종료

SSL 스트립


보안 경고
사이트의 보안 인증서에 문제가 있습니다.
뒤로
계속


https://cyxso.cyworld.com/NCBridge.sk?inf
인증서 오류: 탐색이 차단됨
이 웹 사이트의 보안 인증서에 문제가 있습니다.
이 조직의 인증서가 해지되었습니다.
문제가 있는 인증서를 통해 사용자를 속이거나 사용자가 서버로 보내는 데이터를 가로챌 수도 있습니다.
이 웹 페이지를 닫고 이 웹 사이트를 계속 탐색하지 않는 것이 좋습니다.
여기를 클릭하여 이 웹 페이지를 닫습니다.
추가 정보
100%

SSL 스트립

말그대로 스트립 -> 벗기다로 해석할 수 있다. 즉 HTTPS 또는 FTPS 등 SSL 로 보호된 프로토콜들을 SSL를 벗겨 HTTP, FTP 등으로 다운그레이드 시켜 보안에 취약하게 만드는 공격을 SSL 스트립 공격이라 한다.

2009년 Moxie Marlinspike가 발표한 공격방식이다. 중간에 끼어들어 공격을 하므로 MITM 공격 방식의 일종에 해당한다.

SSL 스트립

SSL 스트립 취약점이 발생한 원인

대부분의 사람들은 https://~~를 직접 입력하여 웹사이트에 접속하는 것이 아닌 단순히 naver.com 등 주소를 입력하여 들어간다.

https:// 를 직접 입력하여 웹사이트에 접속하면 SSL 스트립 공격이 실행되지 않는다.

SSL 스트립

클라이언트와 서버가 이미 SSL 통신을 수행하고 있는 동안에서는 공격자가 클라이언트와 서버간 통신하는 데이터의 정보를 탈취할 수는 없다.

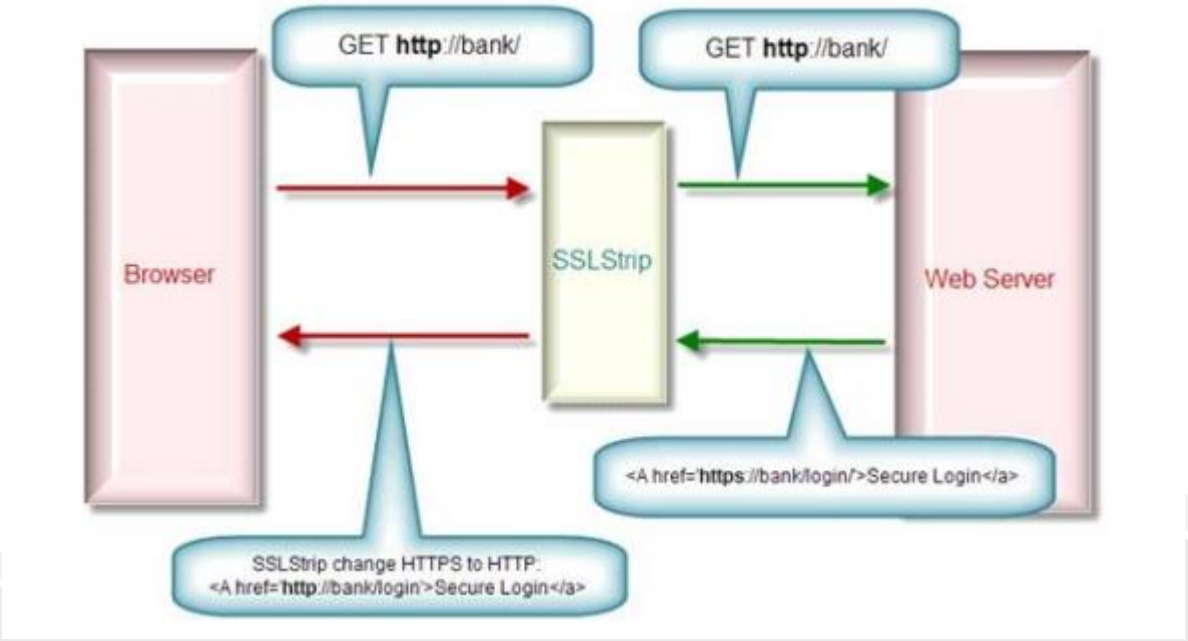
클라이언트가 처음 서버에게 연결 요청을 하는 그 과정속에서 SSL 스트립 공격을 통해 HTTP로 다운시켜버린다.

SSL 스트립

공격 원리

key값을 서버와 클라이언트끼리 맞추기 위해 인증서를 전달하는 과정이 공격자에게 노출

이때 공격자는 자신이 만든 임의의 인증서로 교체한 후에 암호화된 데이터들을 복호화 할 수 있음



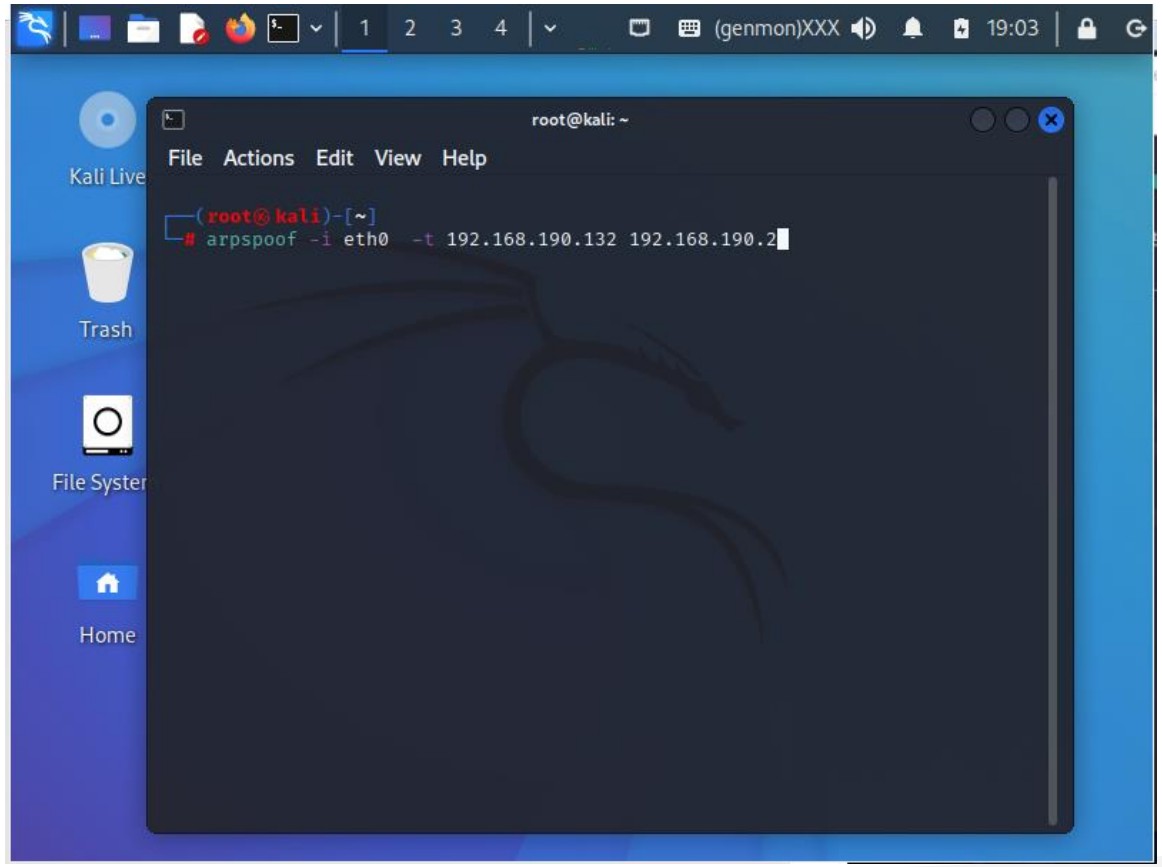
SSL 스트립

실습 시나리오

1. 클라이언트가 웹사이트에 최초 접근
2. 웹 서버는 클라이언트와 암호화된 통신을 하기 위해 HTTPS 연결을 유도
3. 공격자가 HTTPS를 가로채 클라이언트에게 HTTP로 전달
4. 클라이언트는 HTTP로 로그인을 시도하여 웹 서버로 전달
5. 공격자는 클라이언트가 웹에게 보낸 HTTP를 가로채서 HTTPS 로 다시 전달

SSL 스트립

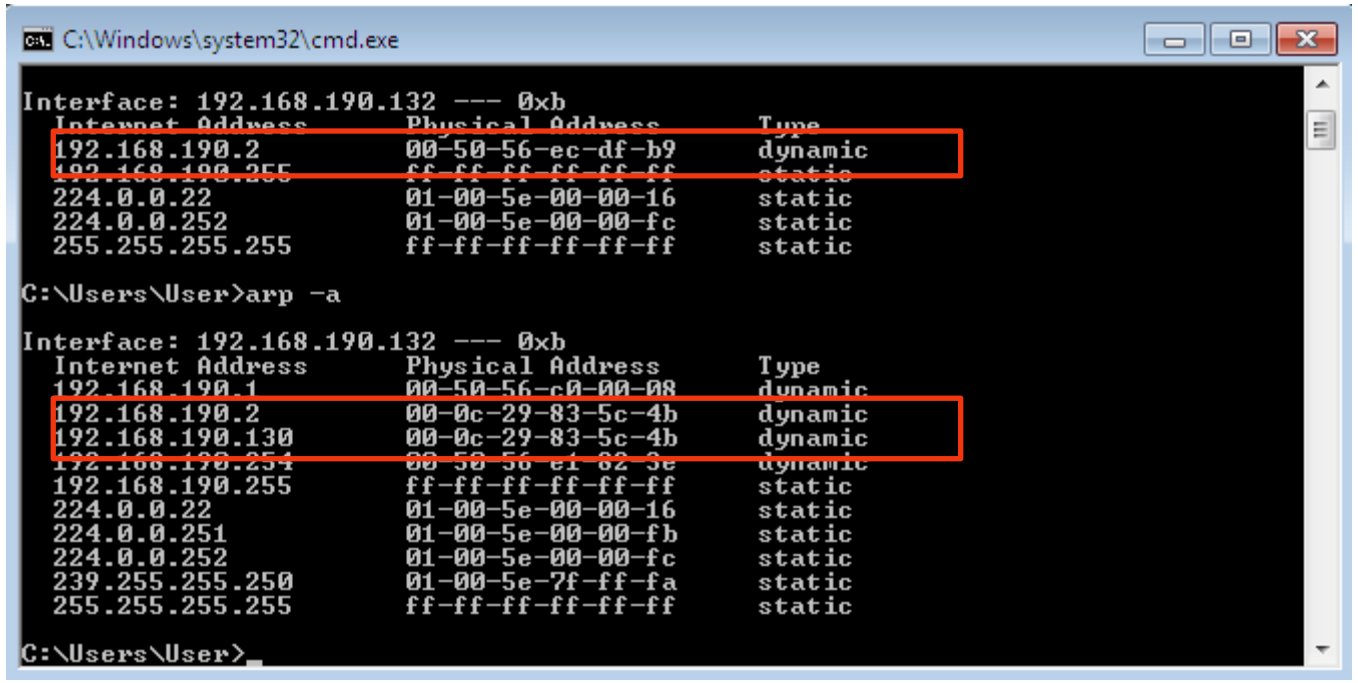
실습

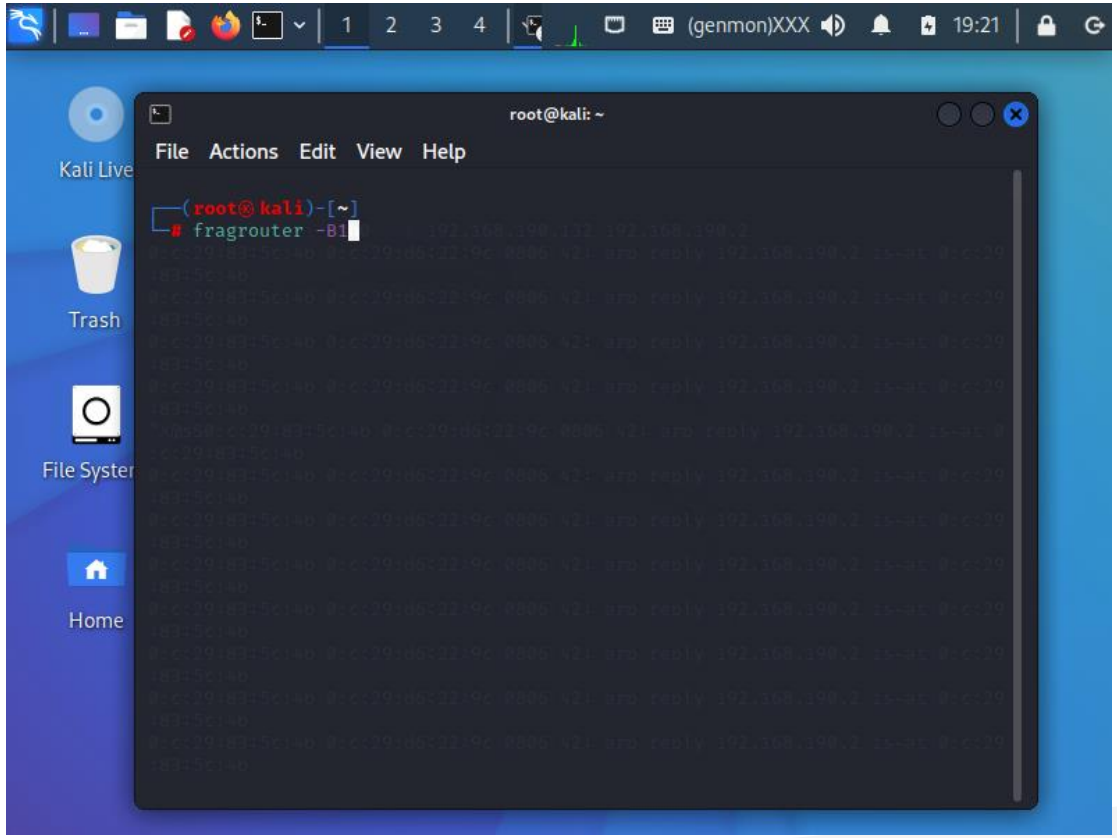


	IP주소	MAC주소
Attacker(칼리 리눅스)	192.168.190.130	00:0c:29:83:5c:4b
Victim(윈도우7)	192.168.190.132	00:50:56:ec:df:b9

SSL 스트립

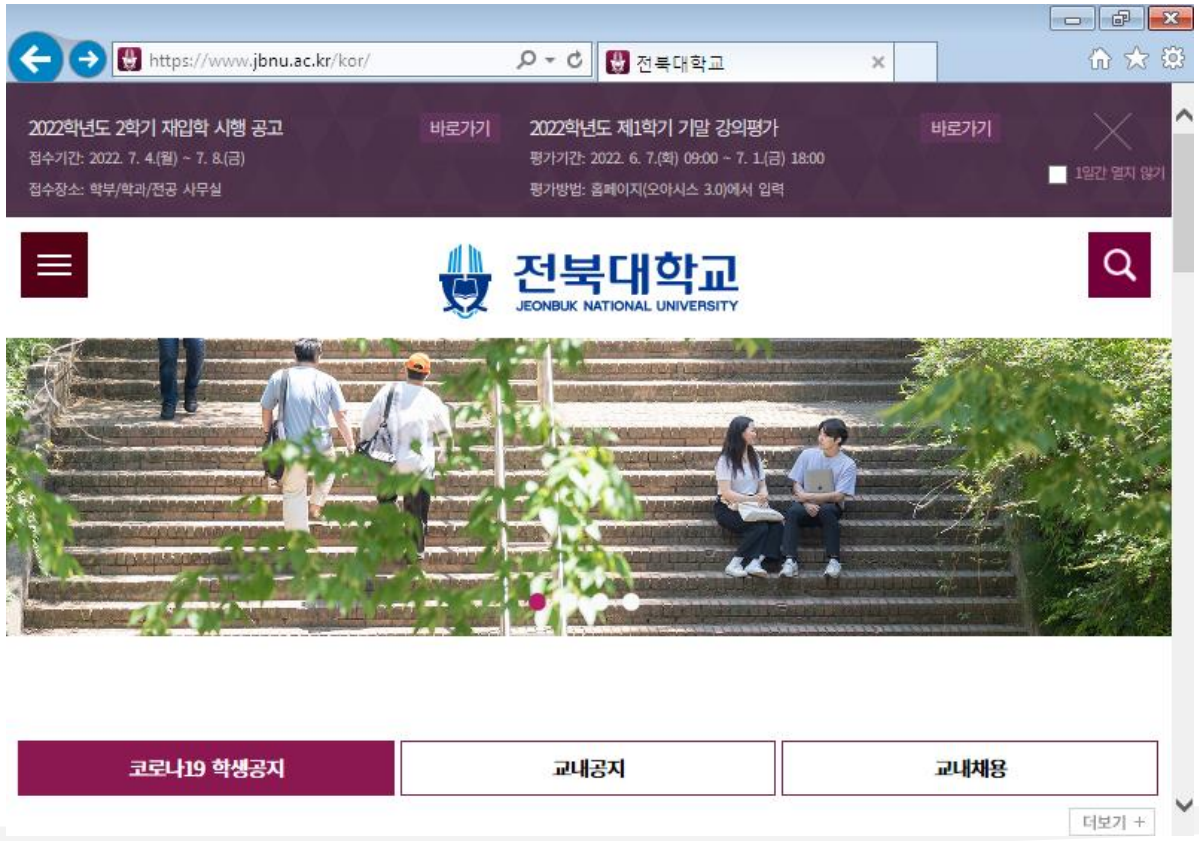
실습

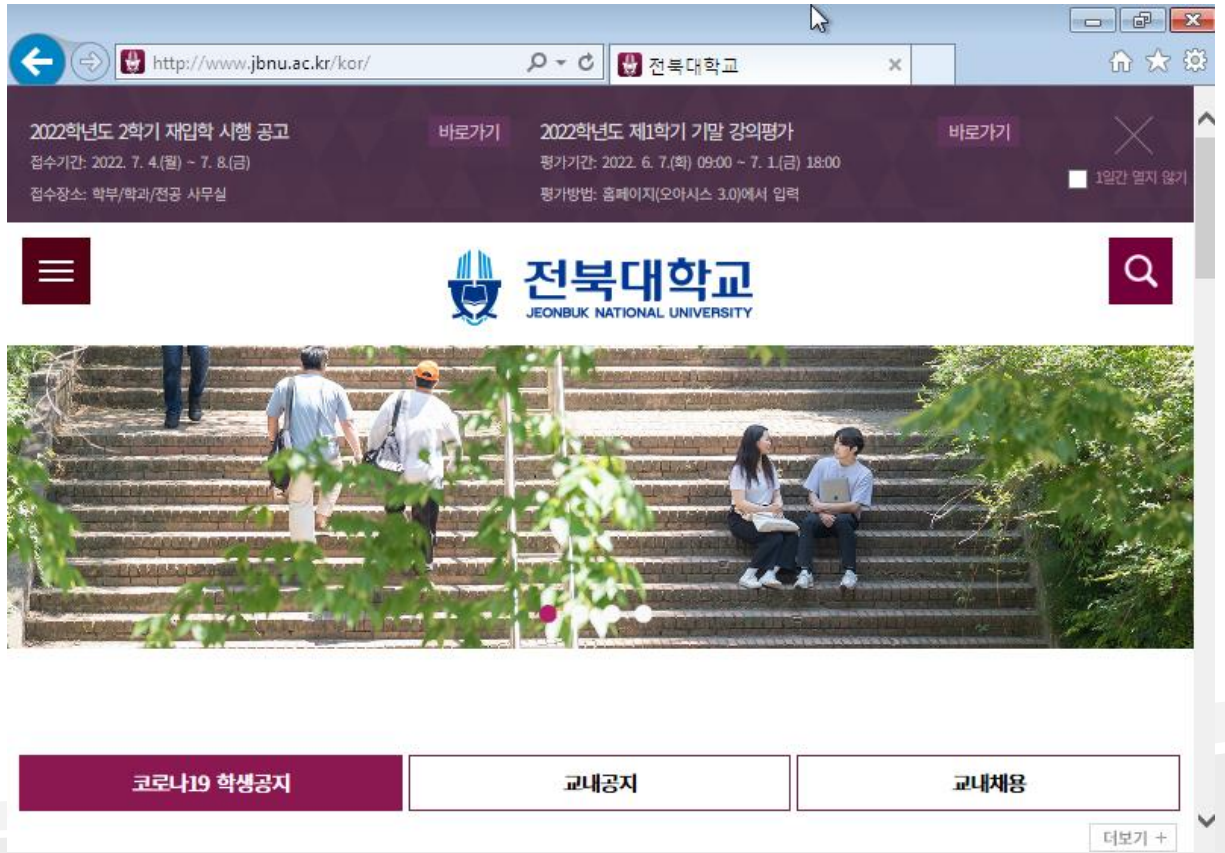

C:\Windows\system32\cmd.exe
Interface: 192.168.190.132 --- 0xb
Internet Address Physical Address Type
192.168.190.2 00-50-56-ec-df-b9 dynamic
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.252 01-00-5e-00-00-fc static
255.255.255.255 ff-ff-ff-ff-ff-ff static
C:\Users\User>arp -a
Interface: 192.168.190.132 --- 0xb
Internet Address Physical Address Type
192.168.190.1 00-50-56-c0-00-08 dynamic
192.168.190.2 00-0c-29-83-5c-4b dynamic
192.168.190.130 00-0c-29-83-5c-4b dynamic
192.168.190.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
C:\Users\User>


(genmon)XXX
19:21
Kali Live
Trash
File Syster
Home
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
fragrouter -B1

SSL 스트립

실습

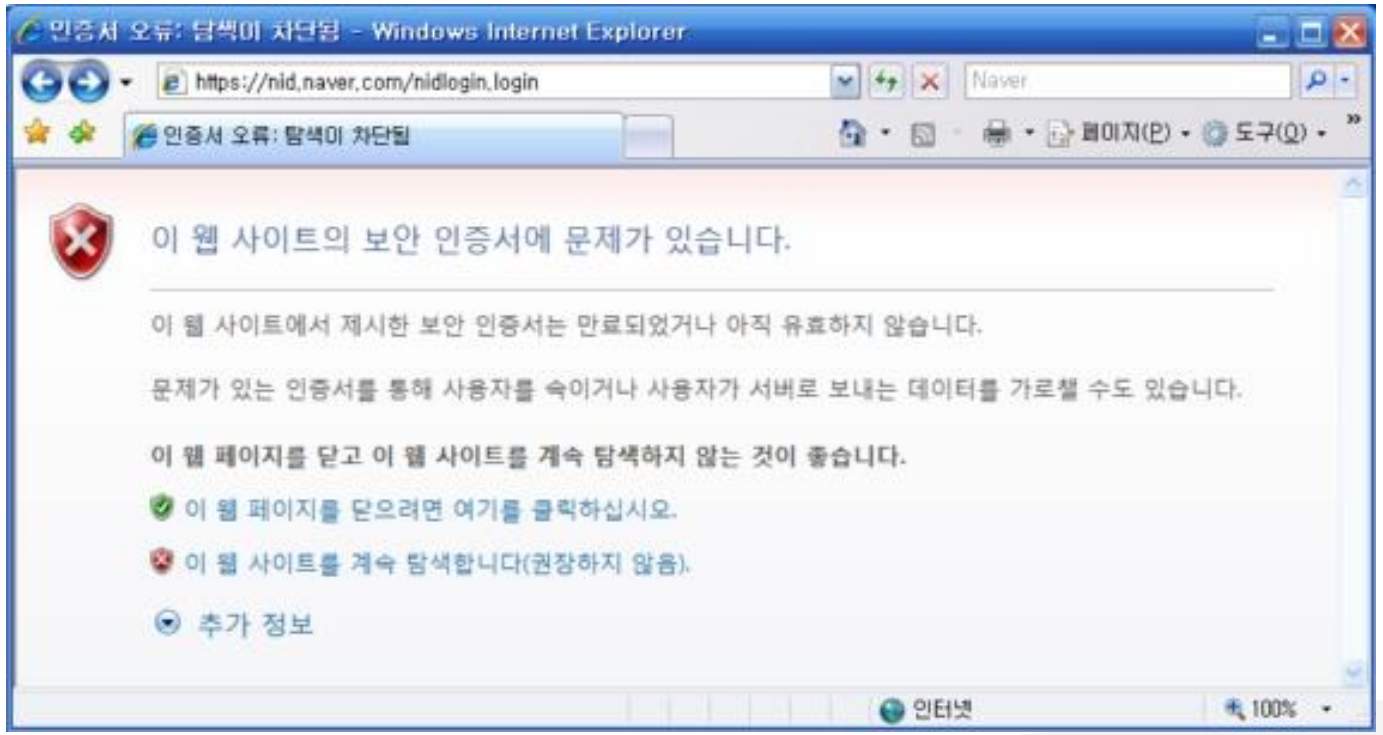

https://www.jbnu.ac.kr/kor/
전북대학교
2022학년도 2학기 재입학 시행 공고
바로가기
접수기간: 2022. 7. 4.(월) ~ 7. 8.(금)
접수장소: 학부/학과/전공 사무실
2022학년도 제1학기 기말 강의평가
바로가기
평가기간: 2022. 6. 7.(화) 09:00 ~ 7. 1.(금) 18:00
평가방법: 홈페이지(오아시스 3.0)에서 입력
1일간 열지 않기
전북대학교
JEONBUK NATIONAL UNIVERSITY
코로나19 학생공지
교내공지
교내채용
더보기 +


http://www.jbnu.ac.kr/kor/
전북대학교
2022학년도 2학기 재입학 시행 공고
바로가기
접수기간: 2022. 7. 4.(월) ~ 7. 8.(금)
접수장소: 학부/학과/전공 사무실
2022학년도 제1학기 기말 강의평가
바로가기
평가기간: 2022. 6. 7.(화) 09:00 ~ 7. 1.(금) 18:00
평가방법: 홈페이지(오아시스 3.0)에서 입력
1일간 열지 않기
전북대학교
JEONBUK NATIONAL UNIVERSITY
코로나19 학생공지
교내공지
교내채용
더보기 +

SSL 스트립

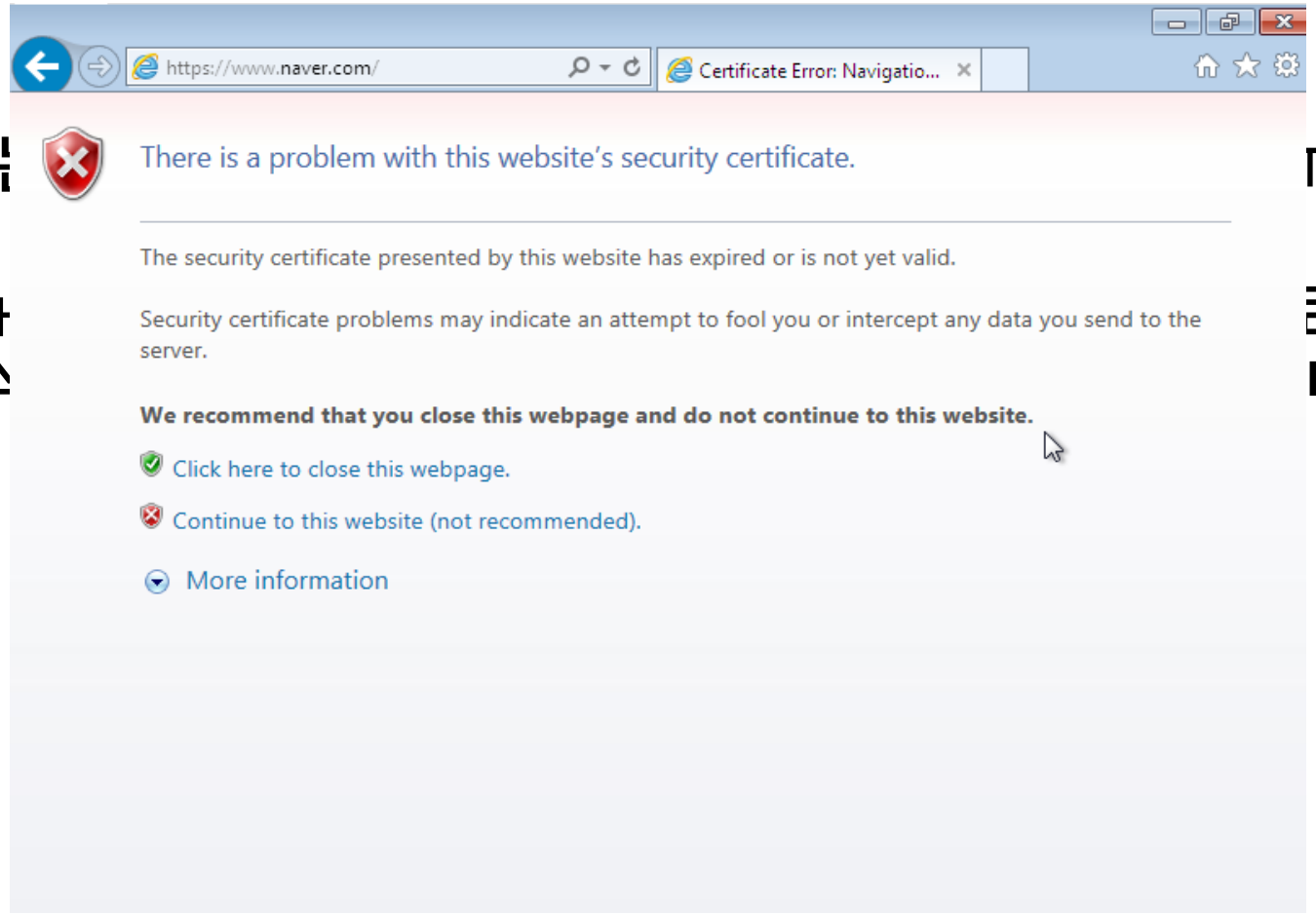
피해 시스템에서의 증상

주의 요함



예방대책

1. 서버



TS 기능을 사용한다.

HSTS는 H

쿠키만 사용해서 서로
통신할 수

다. 즉 보안을 강화시키는
목적으로

예방대책

2. 직접 Https://~ 입력해서 웹에 접근하면 SSL 스트립 공격이 통하지 않는다.

3. 안전하지 않은 공용 와이파이 / 네트워크 등을 사용하지 않는다.