SSL Strip MITM Attack [Sniffing]

공공 WI-FI 를 조심햇!...

01 SSL 이 뭘까?

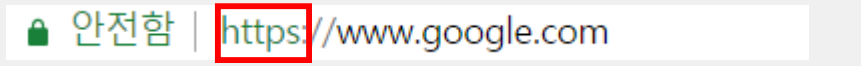
02 SSL Strip - Sniffing 원리는?

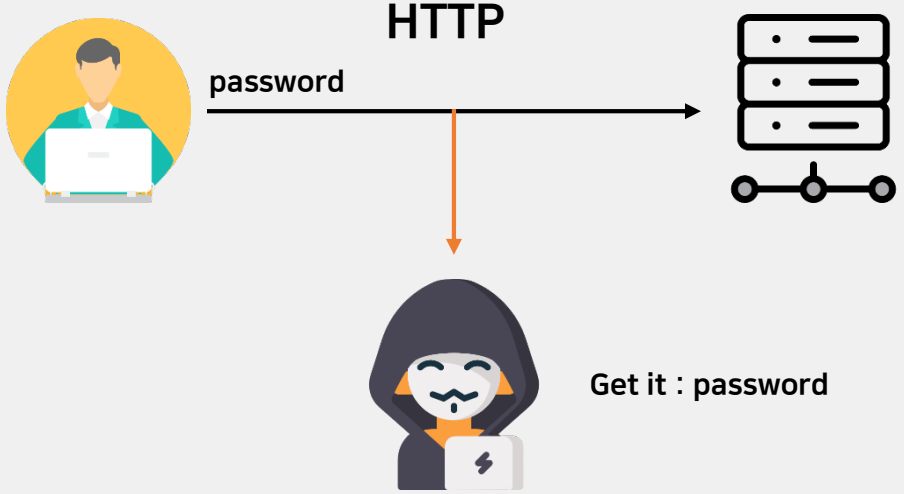
03 실습해 보자!..

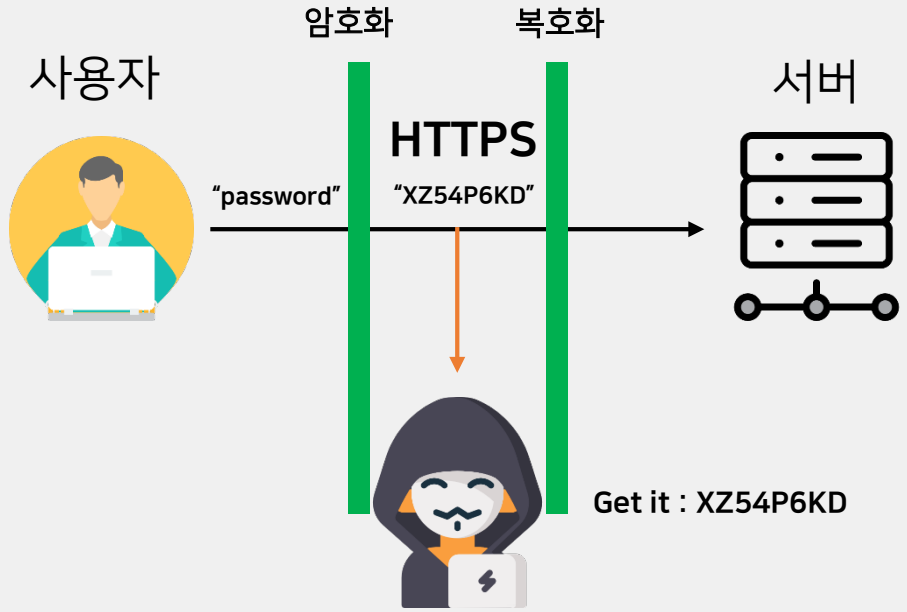
04 대응 방안은 있어?

SSL 이 뭘까 ?

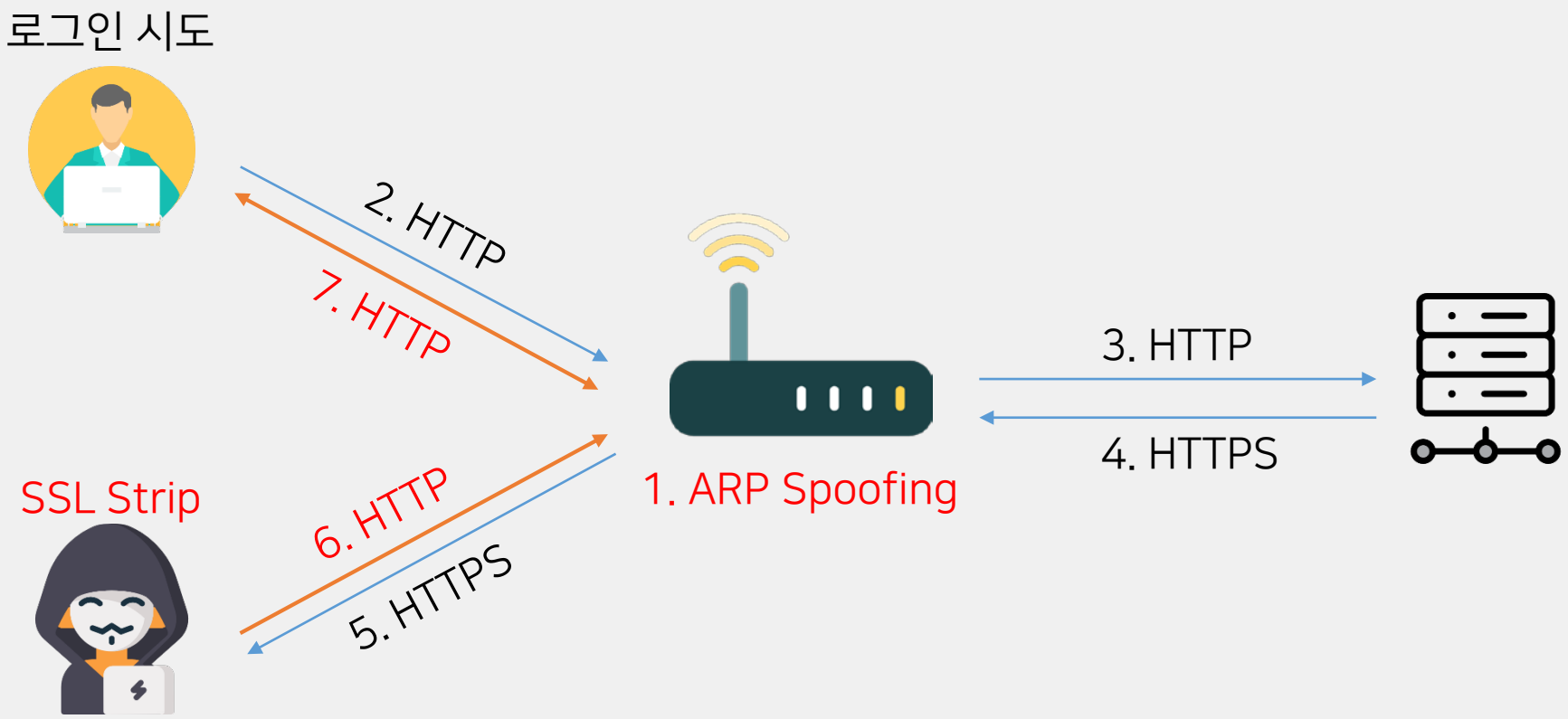
SSL ≒ HTTPS | HTTP → HTTPS







SSL Strip - Sniffing 원리는 ?



실습해보자!...

[공격자] KaliLinux_2018.2

[이용자] Windows 7

대응 방안은 ?

사용자

1. 중요정보를 전송하는 페이지 ex) login 페이지가 https:// 로 시작하는지 체크해야 합니다.
2. 신뢰할 수 없는 WI-FI 사용을 지양해야 합니다.
3. 신뢰할 수 없는 WI-FI를 사용중 이라면 ARP Mac-address 를 스태틱 걸어 줍니다.

WI-FI 관리자

1. WPA2 이상의 쉽게 유추할 수 없는 패스워드를 사용해야합니다.
2. 공개 목적이 아니라면, IP/MAC 인증 등의 추가 인증을 넣어야 합니다.

웹 서비스 제공자

1. SSL을 통해 정보를 보호하는 구간에서 HTTP 사용을 방지하고 HTTPS를 강제 사용하도록 해야 합니다.
2. 서버 및 네트워크의 트래픽이 비교적 적은 서비스는 가능하다면 웹 사이트 전체에 SSL을 적용하여 HTTPS 가 HTTP로 변경될 수 없도록 해야 합니다.

THANK YOU