MITM
(Man In The Middle Attack)

https://youtu.be/2E9pg3J59hI

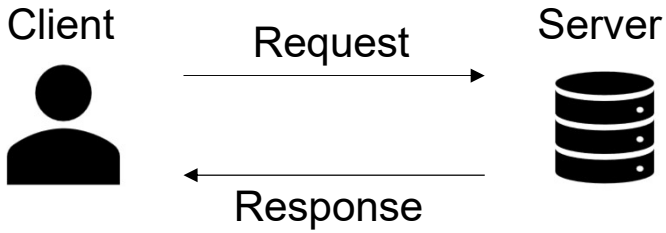
HTTP vs HTTPS(SSL/TLS)

MITM

MITM 실습

HTTP vs HTTPS

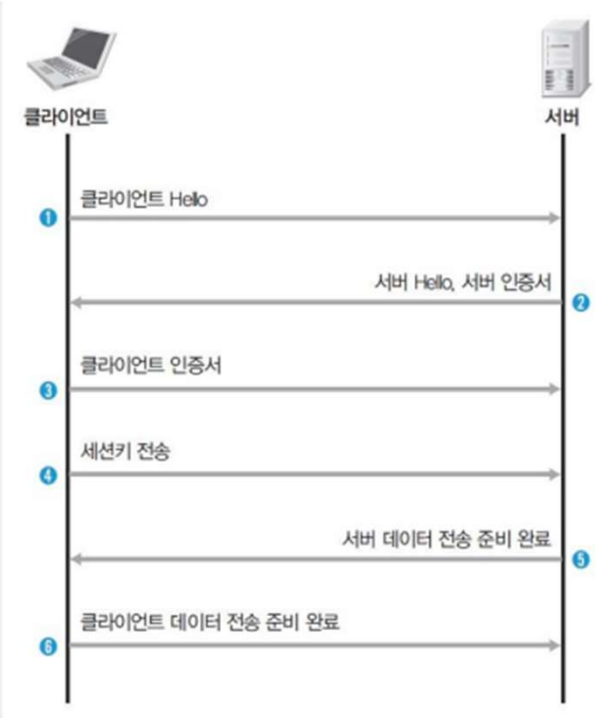
HTTP: 서버간 통신을 위한 통신 프로토콜, 클라이언트-서버 프로토콜이라고도 함.

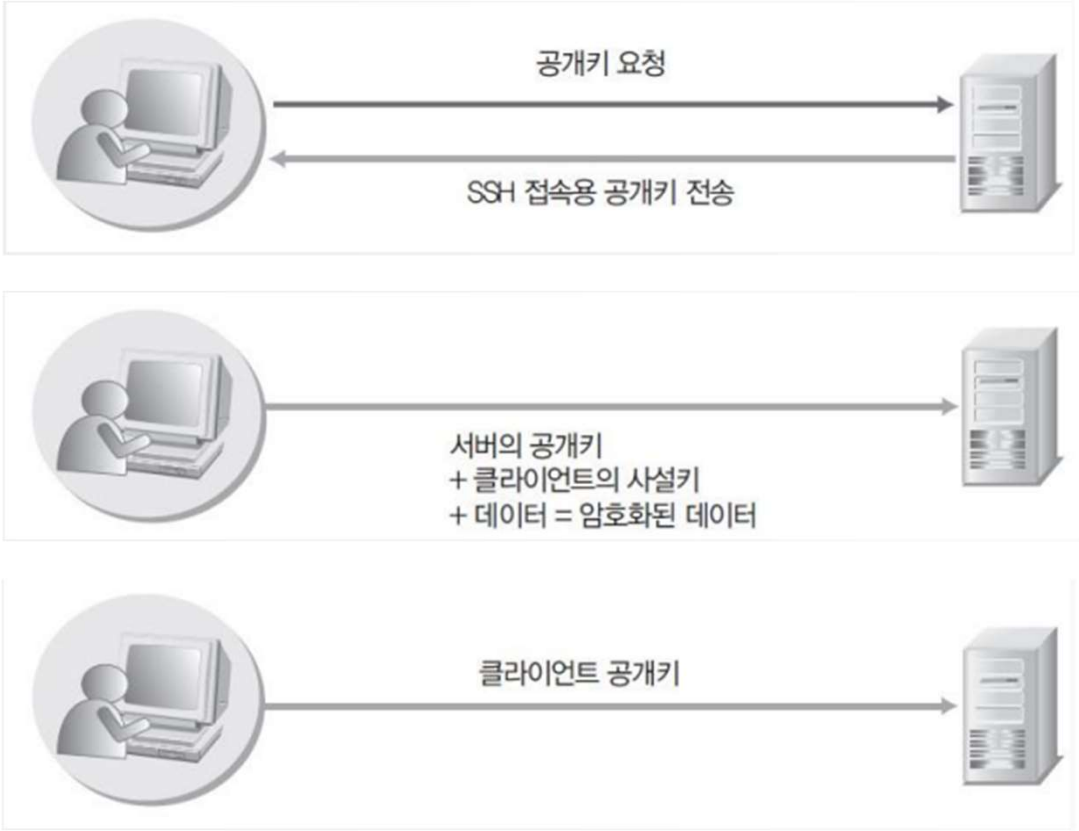


HTTPS: 인증 기관에서 인증서를 획득해 데이터를 암호화 해서 전송.

HTTPS(SSL)

암호화 기법(Hand-Shack)

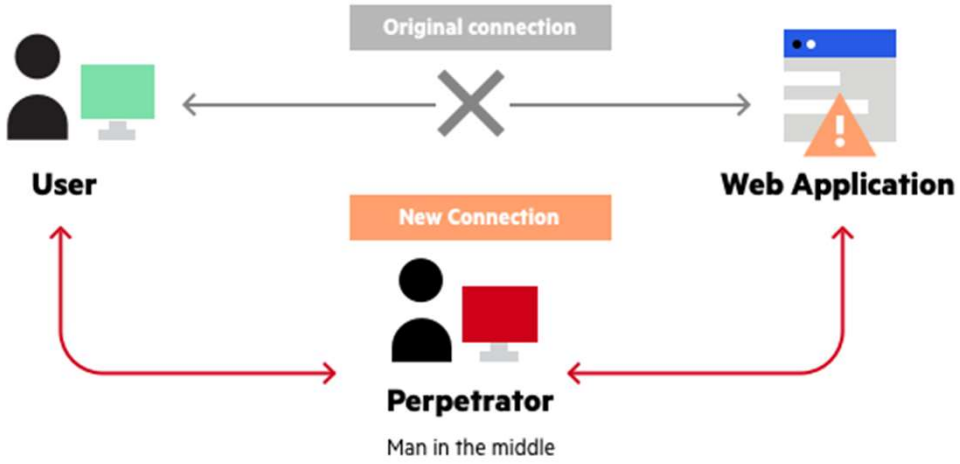




MITM

MITM(Man In The Middle Attack)

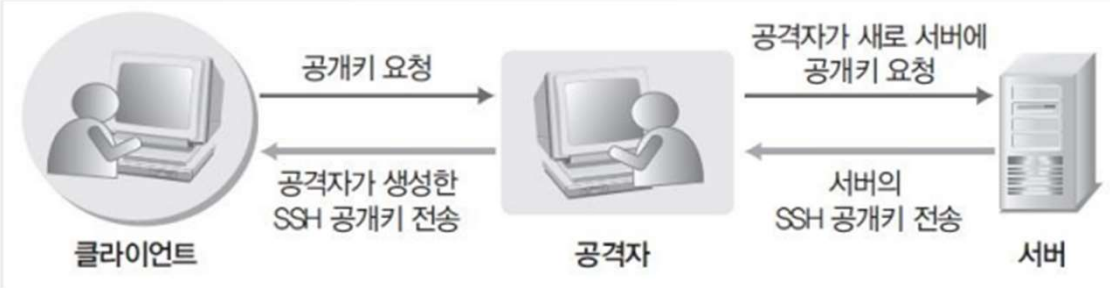
- 글자 그대로 누군가의 사이에 끼어드는 것
- 클라이언트와 서버의 통신에 암호화된 채널을 이용하면서 ARP 리다이렉트와 ICMP 리다이렉트, ARP 스푸핑이 무용지물이 되자 이를 극복하기 위해 탄생
- MITM은 패킷 내용을 바꾸기 시도



MITM

암호화 통신에 대한 MITM 공격

1단계: 클라이언트 서버에 ARP 스푸핑 같은 공격으로 네트워크 장악, 자신이 서버인 것처럼 행동
서버에는 자신이 클라이언트인 것처럼 행동



2단계: 정상적인 클라이언트가 서버에 암호화된 데이터를 보내면 공격자는 자신의 키로 복호화 후
서버의 키로 다시 암호화해서 서버로 전송

MITM 실습

MITM 실습: HTTPS가 적용되지 않은 사이트를 찾아 Header 내용을 변경해보기.

실습 환경: kali linux

사용 도구: ettercap

Q & A