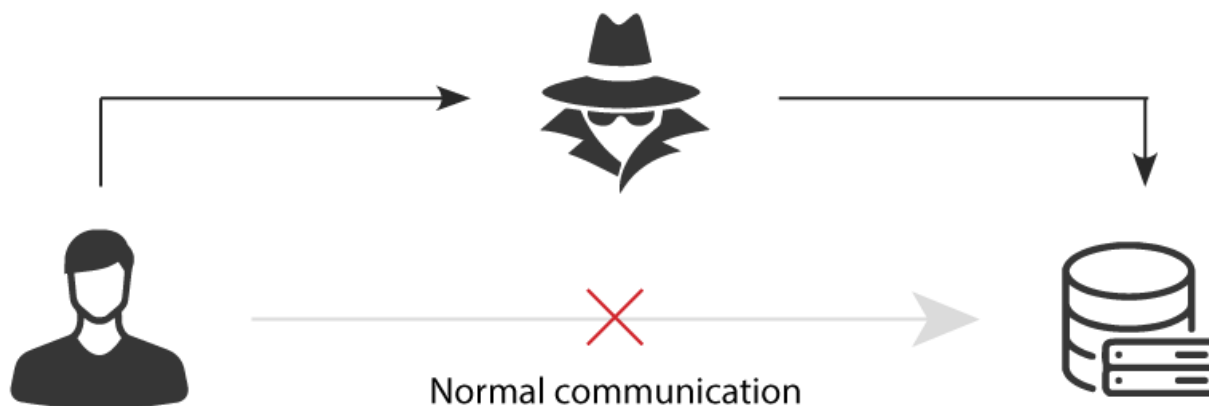


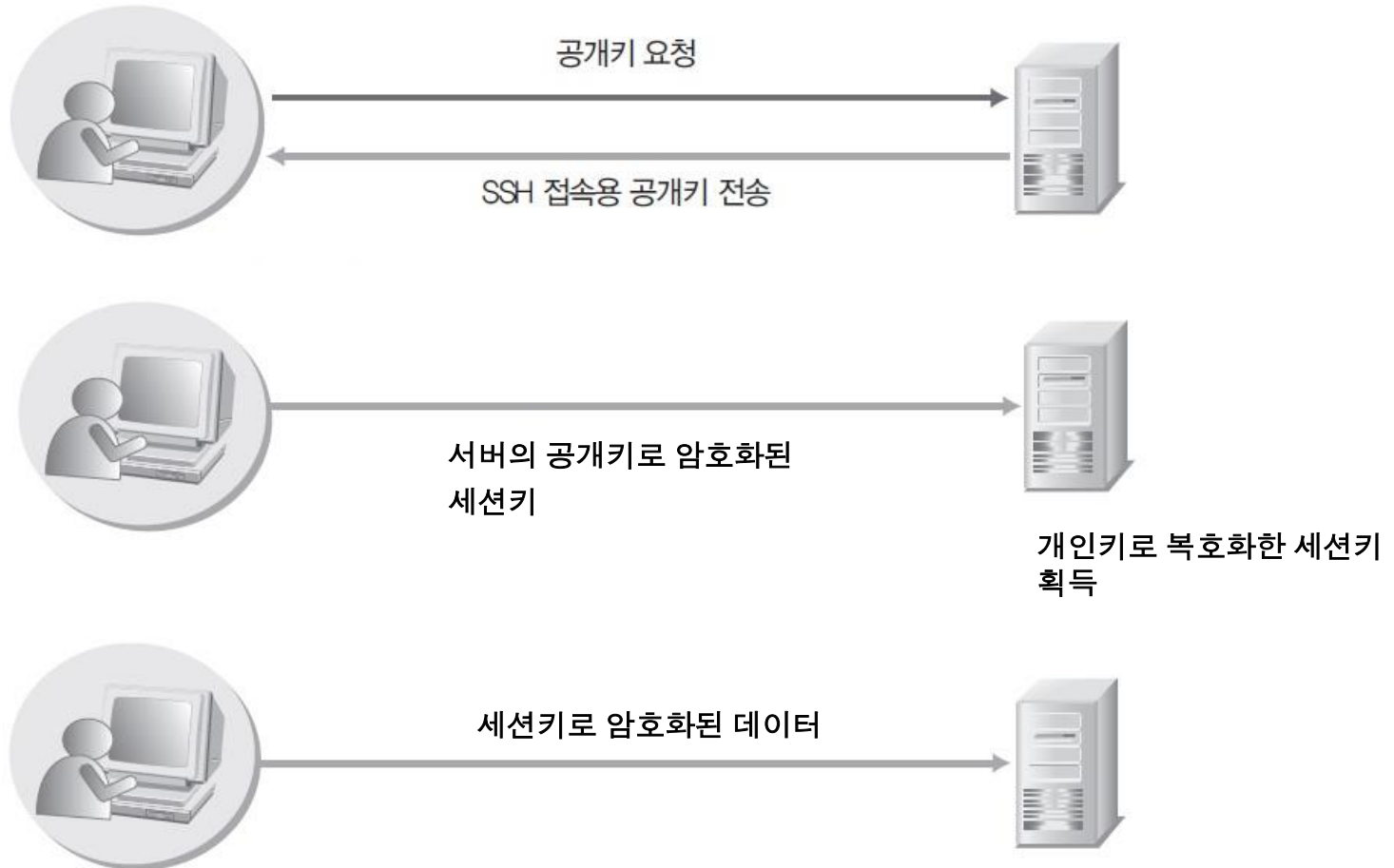
# SSL MITM

# MITM(MAN IN THE MIDDLE) 공격

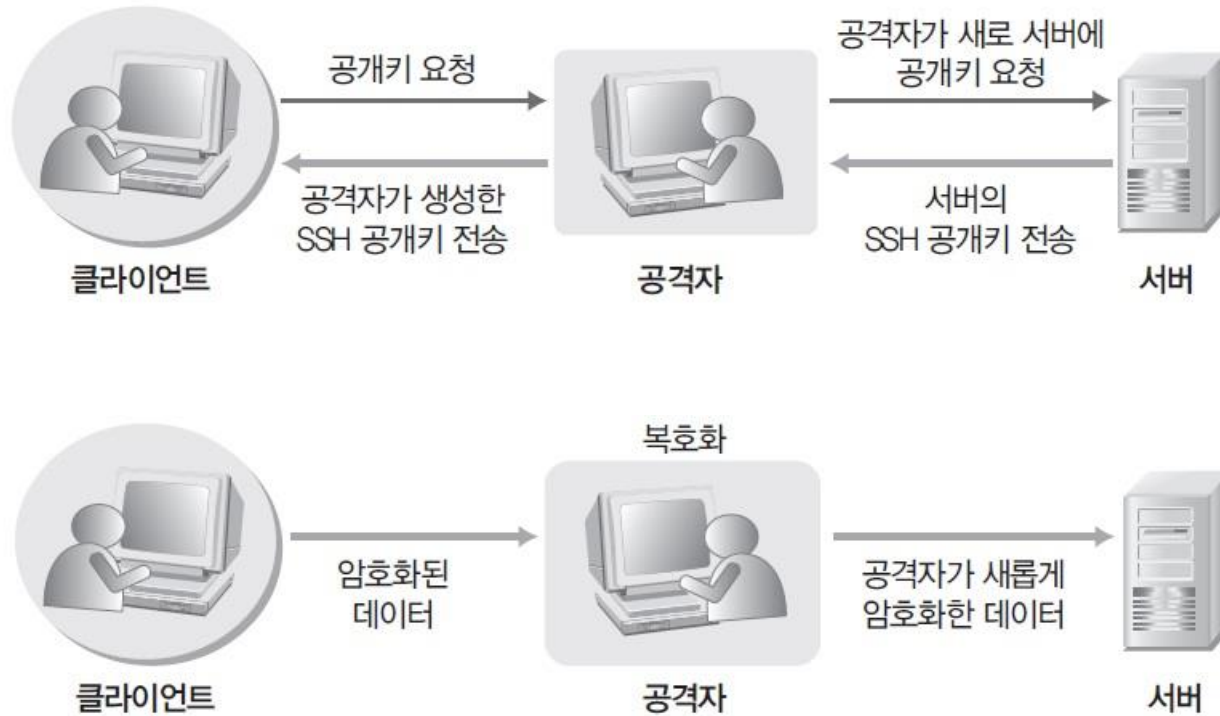
- ▶ 통신 중간에 끼어들어 통신 상대방인 것처럼 속여 메시지를 도청하거나 위변조하는 공격



# SSH 접속 과정 REVIEW

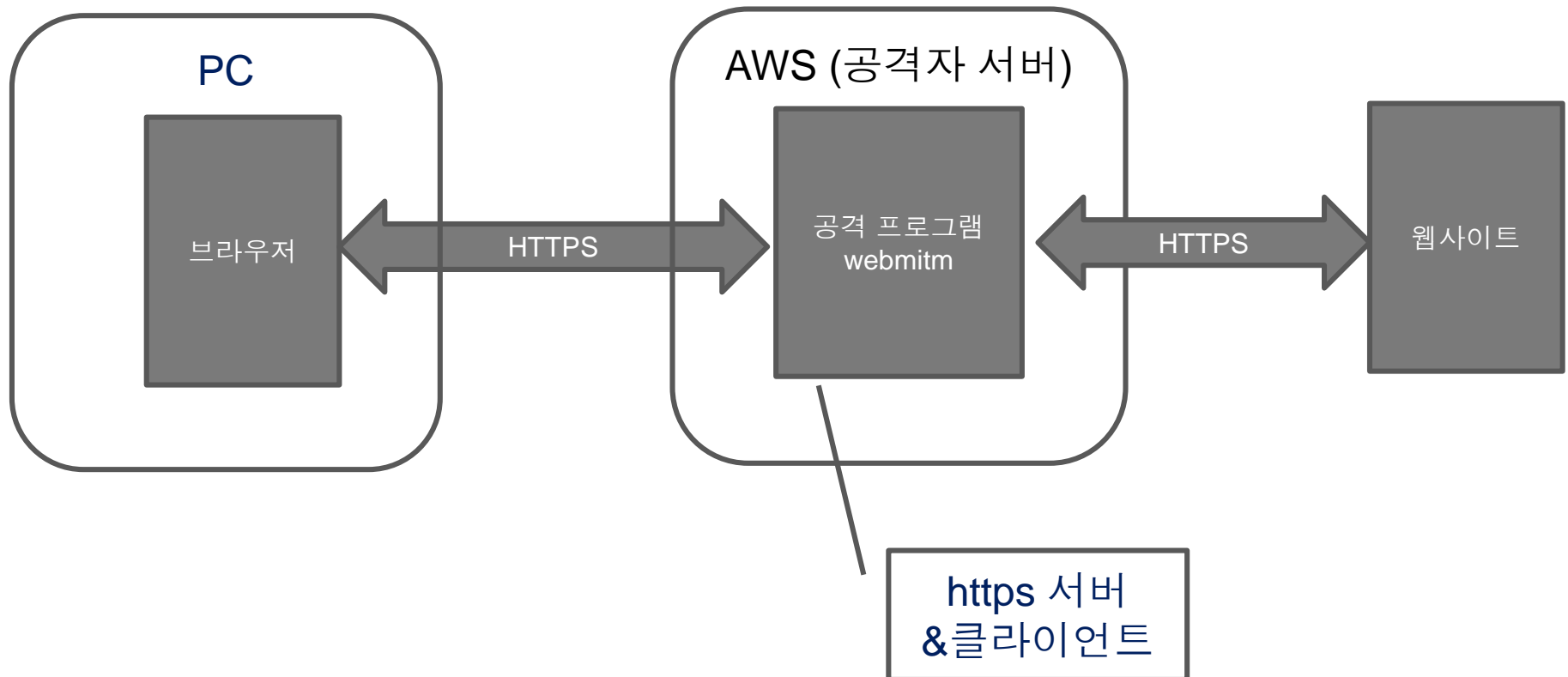


# SSH MITM



# SSL MITM

## ▶ 가상 머신 사용하지 않음



# MITM 로 유도하는 방법

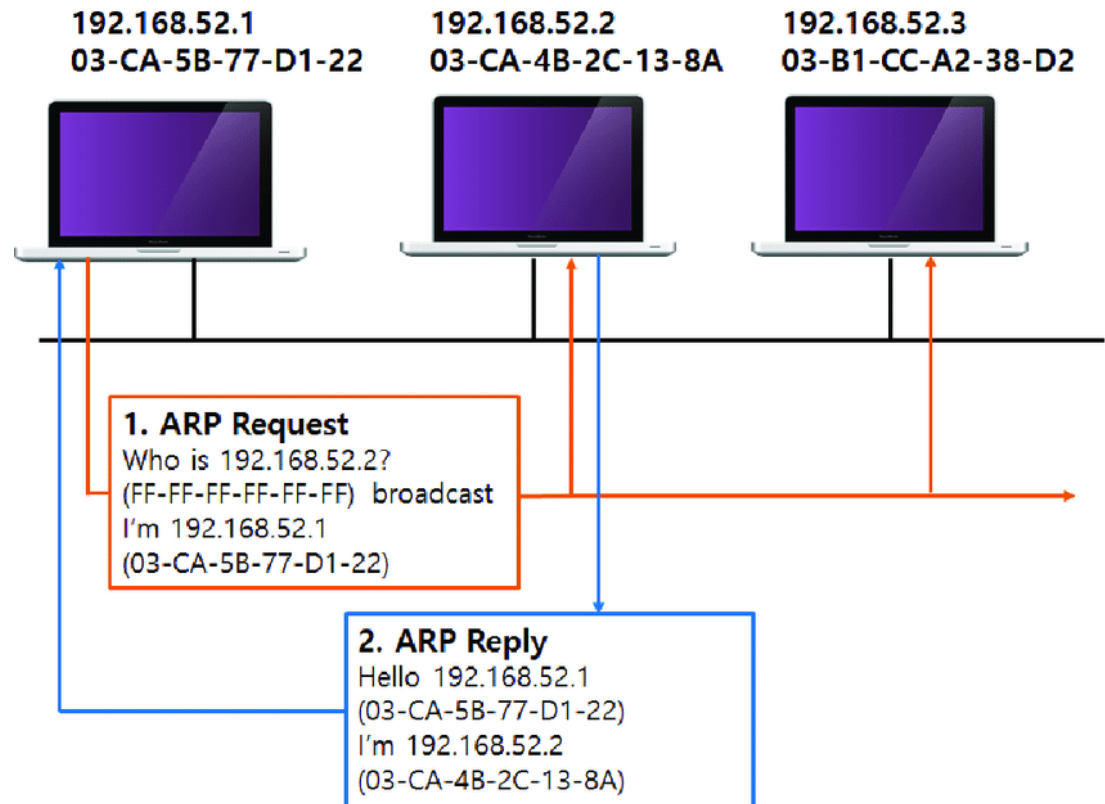
- ▶ ARP 스푸핑
- ▶ DNS 스푸핑
- ▶ hosts 파일 변경
  - DNS 보다 먼저 참조하는 hosts 파일을 변경

# ARP스푸핑

## ▶ ARP

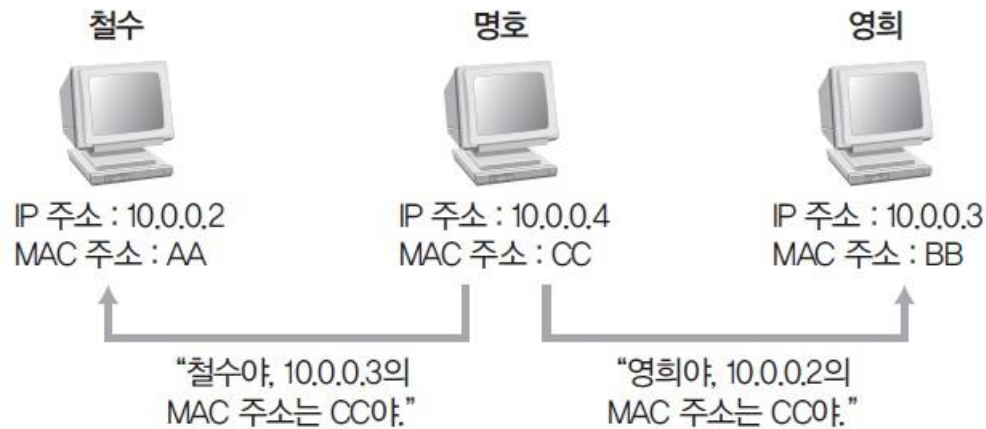
- IP ↔ MAC주소
- 조회

CMD > arp -a



# ARP 스푸핑

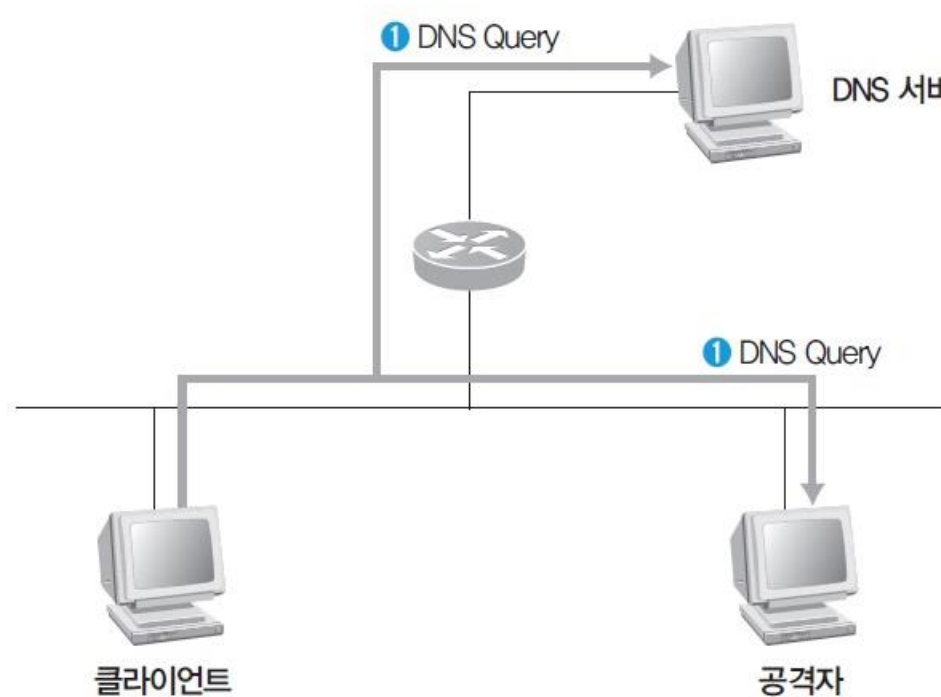
## ▶ ARP 스푸핑





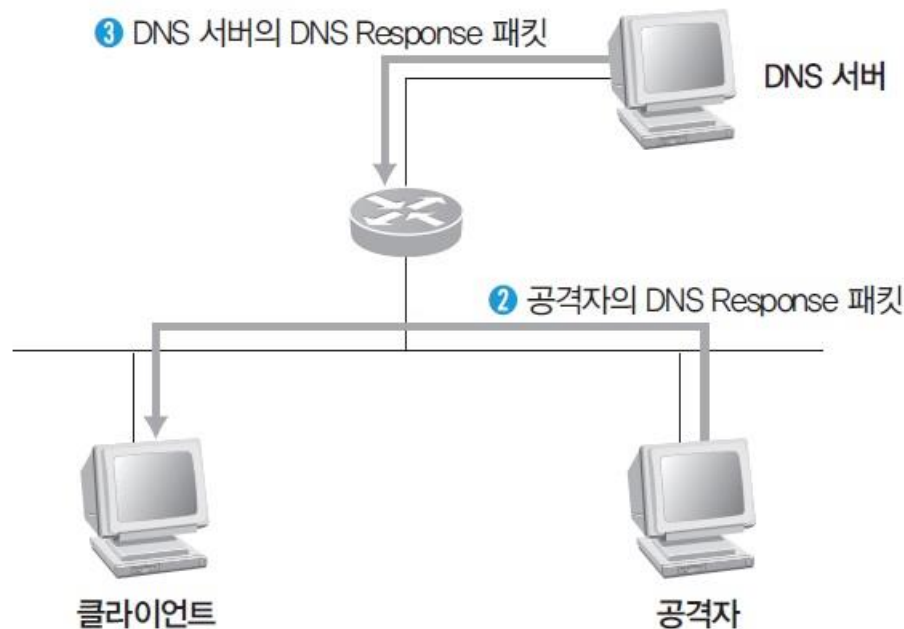
# DNS 스푸핑

- ① 클라이언트가 DNS 서버로 DNS Query 패킷을 보내는 것을 확인(ARP 스푸핑과 같은 선행 작업이 필요)



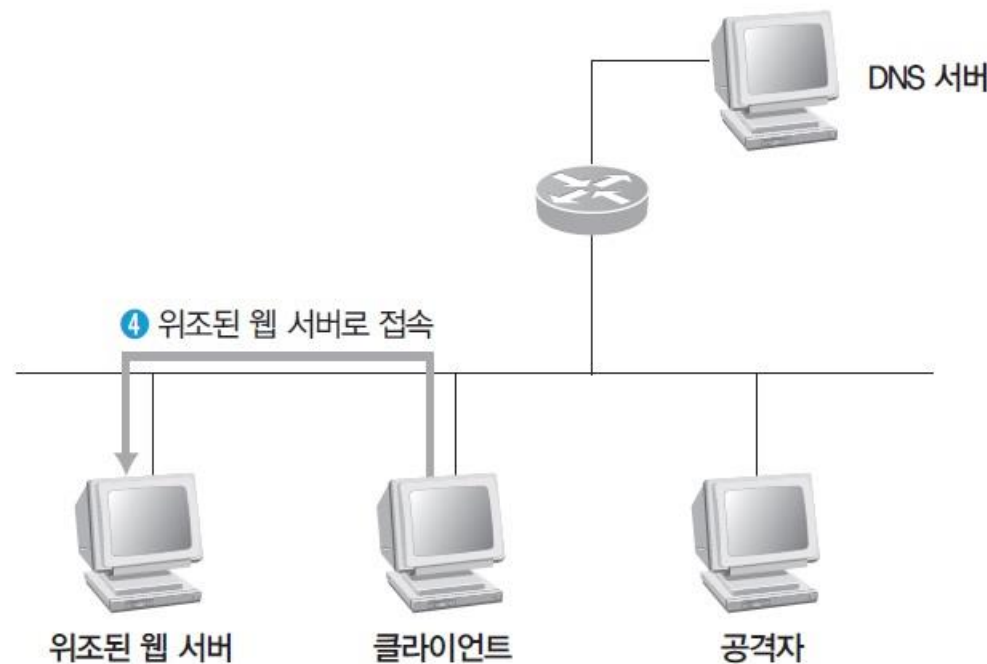
# DNS 스푸핑

- ② DNS 서버가 올바른 DNS Response 패킷을 보내주기 전에 위조된 DNS Response 패킷을 클라이언트에게 보냄



# DNS 스푸핑

- ③ 클라이언트는 공격자가 보낸 DNS Response 패킷을 올바른 패킷으로 인식하고 가짜 웹서버에 접속



# SSL접속해 보기

▶ [hosting.whois.co.kr](https://hosting.whois.co.kr)

The screenshot shows the homepage of [hosting.whois.co.kr](https://hosting.whois.co.kr). The browser address bar displays the URL. The main banner features a green background with white text: "11월에 웹호스팅을 신청하시면 스타벅스 커피를 100% 드립니다." (If you apply for web hosting in November, we will give you 100% Starbucks coffee). Below the banner is a yellow button labeled "웹호스팅 상품보기" (View web hosting products). The text "대한민국 No.1 호스팅 후이즈" (No.1 Hosting in Korea, HUIZ) is also visible. The footer includes a navigation menu with links for "도메인" (Domain), "메일" (Mail), "호스팅" (Hosting), "SSL인증서" (SSL Certificate), "홈페이지" (Homepage), "쇼핑몰" (Shopping Mall), "마케팅" (Marketing), "그룹웨어" (Groupware), "IDC" (IDC), and "공유오피스" (Co-working Office). A "로그인" (Login) button and a "회원가입" (Sign Up) button are present. The page also shows a "카톡 업무 지시" (Kakao Business Instruction) and a "네이버 협업툴" (Naver Collaboration Tool) link. The date and time "2021년 10월 21일(목) 0시" are displayed at the bottom right.

# 윈도우즈 HOSTS파일 변경

## ▶ 변경 (관리자 권한) 후 접속해보기

- 백신의 경고 무시
- 브라우저 재실행 필요

내 PC > OS (C:) > windows > system32 > drivers > etc

이름	수정한 날짜
hosts	2021-11-09 오전 12:22

```
*hosts - Windows 메모장
파일(F) 편집(E) 서식(Q) 보기(V) 도움말(H)
# localhost name resolution is handled within DNS itself.
#      127.0.0.1      localhost
#      ::1           localhost
자기 aws ip 주소 hosting.whois.co.kr
자기 aws ip 주소 member.whois.co.kr
```

# MITM 프로그램 설치, 실행

## ▶ dsniff

```
ubuntu@ip-172-31-13-205:~/10$ sudo apt install dsniff
```

## ▶ 실행

```
ubuntu@ip-172-31-13-205:~/10$ sudo webmitm
```

- 처음 실행시 SSL서버용 인증서 생성 : webmitm.crt
    - 키와 인증서 모두 포함
  - 이후 실행 시 위 인증서 사용하여 웹서버처럼 동작
- 👉 오류 발생, 키 길이 부족

# CA 키쌍 생성, 인증서 SS

## ▶ 서버 인증서 만들기

- 저번 시간에 한 것이 있으면 이 페이지는 건너뛰

## ▶ openssl 간략화 도구 설치

```
$ sudo apt install easyrsa
```

## ▶ 폴더 및 script 설치

```
$ make-cadir ca
```

## ▶ pki 폴더 설치

```
$ cd ca [ 이후로 경로는 주욱 ~/ca $ ]
```

```
$ ./easyrsa init-pki
```

## ▶ CA 키쌍 생성 및 인증서

```
$ ./easyrsa build-ca nopass
```

# 서버인증서 생성

- ▶ 서버 키 쌍, 인증요청서 생성 : CN은 자기 이름으로

```
$ ./easysrsa gen-req server nopass
```

- ▶ 서버 인증서 발행

```
$ ./easysrsa sign-req server 자기이름
```

- ▶ 인증서와 키 파일 내용 (PEM 부분) 을 ~\$ webmitm.crt 의 PEM 부분  
에 overwrite 하기

```
pki/private/자기이름.key
```

```
pki/issued/자기이름.crt
```



# MITM 실행 및 포트 열기

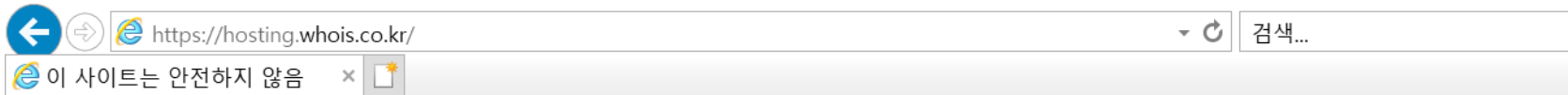
## ▶ webmitm 실행

```
ubuntu@ip-172-31-13-205:~/10$ sudo webmitm
webmitm: relaying transparently
```

## ▶ AWS https 포트 개방

인바운드 규칙 정보						
보안 그룹 규칙 ID	유형 정보	프로토콜 정보	포트 범위 정보	소스 정보	설명 - 선택 사항	정보
sgr-01c7fee59348ab9e6	SSH ▼	TCP	22	사용자 ... ▼ Q 0.0.0.0/0 ✕		삭제
sgr-0adef2fefa72f667	HTTPS ▼	TCP	443	사용자 ... ▼ Q 0.0.0.0/0 ✕		삭제
sgr-000932714bd9f4b2e	HTTP ▼	TCP	80	사용자 ... ▼ Q 0.0.0.0/0 ✕		삭제
sgr-0f6f1822b92fd8546	사용자 지정 TCP ▼	TCP	1194	사용자 ... ▼ Q 0.0.0.0/0 ✕		삭제

# 다시 접속하기



## 이 사이트는 안전하지 않습니다.

다른 사람이 사용자를 속이거나 사용자가 서버로 보내는 정보를 도용하려 함을 의미할 수 있습니다. 이 사이트를 즉시 닫아야 합니다.

✓ 이 탭 닫기

➔ 추가 정보

PC가 이 웹 사이트의 보안 인증서를 신뢰하지 않습니다.  
웹 사이트 보안 인증서의 호스트 이름이 방문하려는 웹 사이트와 다릅니다.

오류 코드: DLG\_FLAGS\_INVALID\_CA  
DLG\_FLAGS\_SEC\_CERT\_CN\_INVALID

✗ 웹페이지로 이동(권장하지 않음)

# SSL서버 인증서 오류 2가지

- ▶ 신뢰하지 못하는 CA가 발행
- ▶ CN domain name 과 같아야 함



인증서 오류

인증서

일반 자세히 인증 경로

인증서 정보

신뢰된 인증 기관에서 이 인증서를 검증할 수 없습니다.

발급 대상: server

발급자: Easy-RSA CA

유효 기간(시작) 2021-11-09 부터 2024-10-24

# 과제1

- ▶ 직전 페이지 인증서 내용 cn 자기이름 나오게 캡처
- ▶ 1.jpg

# 피싱, 파밍

- ▶ 여기까지가 가짜 웹사이트로 유도되는 피싱, 파밍과 같음
- ▶ 차이점
  - 피싱, 파밍은 가짜 사이트를 만들어서 운용
  - MITM은 진짜 사이트를 중계
  - MITM 피싱은 relay 이기 때문에 모든 인증 수단을 중계할 수 있다.
    - 대응 방안은 지정 단말
    - -> IP spoofing , MAC spoofing 에 의해 무력화됨

# 패킷 내용 보기

## ▶ ssldump

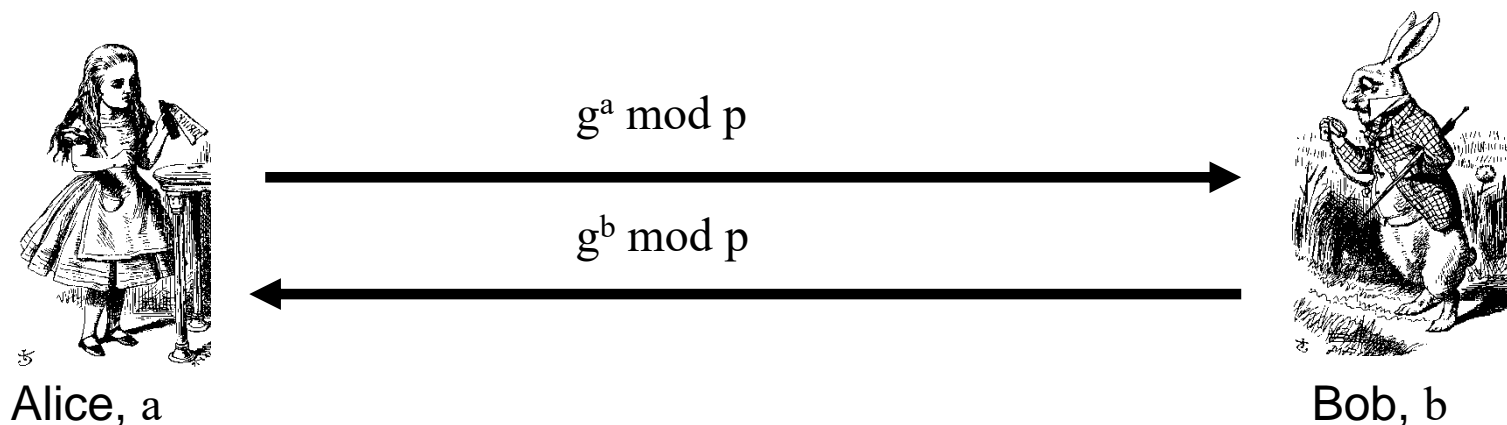
```
ubuntu@ip-172-31-13-205:~/10$ sudo apt install ssldump
```

## ▶ ssl packet dump

```
ubuntu@ip-172-31-13-205:~/10$ sudo ssldump -i eth0 -k webmitm.crt -d
```

# EPHEMERAL DIFFIE-HELLMAN

▶ 패킷 캡처한 것으로는 복호화 불가능



👉 webmitm에서 decrypt packet을 출력해야

# 과제2

## ▶ 서버 인증서 cn을 도메인 이름과 맞추고,

- 추가로

확장된 키 사용
인증서 키 사용
인증서 대상 대체 이름
인증서 서명 알고리즘
인증서 서명 값
필드 값
중요하지 않음 TLS WWW 서버 인증(OID.1.3.6.1.5.5.7.3.1)

인증서 대상 대체 이름
인증서 서명 알고리즘
인증서 서명 값
필드 값
중요하지 않음 DNS 이름: hosting.whois.co.kr

## ▶ CA인증서를 가져와서 trust list 에 넣은 후 사이트 접속 결과 확인하기

- 브라우저 창에 어떻게 표시되는지 확인

## ▶ 2.jpg