5주차 2차시 스푸핑공격

【학습목표】

1. 스푸핑 공격의 개념을 설명할 수 있다.
2. pttus 하이재킹 공격과 대응책에 대해 설명할 수 있다.

학습내용1 : 스푸핑 공격의 개념 및 응용

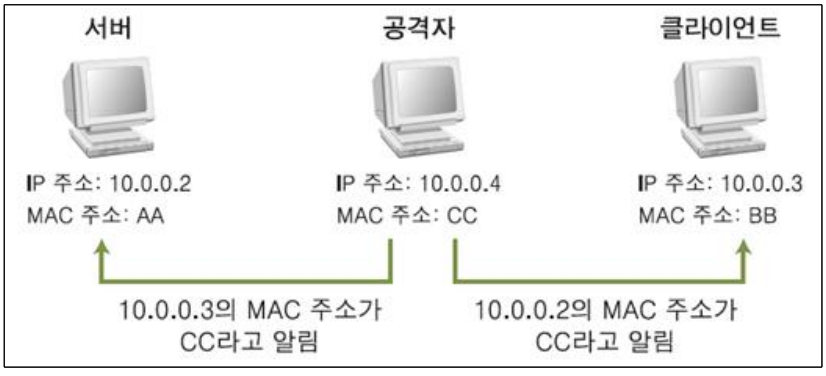
1. ARP 스푸핑 공격

- ARP(Address Resolution Protocol) 스푸핑 : MAC 주소를 속이는 것이며, 즉 MAC 주소를 속여 랜에서의 통신 흐름을 왜곡시킴

1) [표] ARP 스푸핑 공격 예에 사용되는 네트워크

호스트 이름	IP 주소	MAC 주소
서버	10.0.0.2	AA
클라이언트	10.0.0.3	BB
공격자	10.0.0.4	CC

2) 공격자가 서버와 클라이언트의 통신을 스니핑하기 위해 ARP 스푸핑 공격을 시도해보자
* [그림] ARP 스푸핑



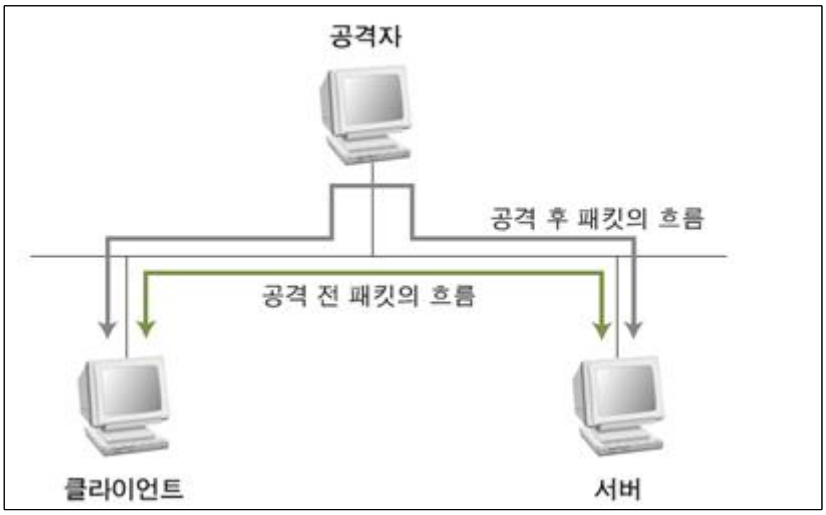
① 공격자는 서버의 클라이언트에게 10.0.0.2에 해당하는 가짜 MAC 주소 CC를 알리고, 서버에게는 10.0.0.3에 해당하는 가짜 MAC 주소 CC를 알림

② 공격자가 서버와 클라이언트 컴퓨터에 서로 통신하는 상대방을 공격자 자기 자신으로 알렸기 때문에 서버와 클라이언트는 공격자에게 각각 패킷을 보냄

③ 공격자는 각자에게 받은 패킷을 읽은 후 서버가 클라이언트에 보내고자 하던 패킷을 클라이언트에게 정상적으로 보내주고, 클라이언트가 서버에게 보내고자 하던 패킷을 서버에게 보내줌

3) ARP 스푸핑 공격 후 패킷 결과

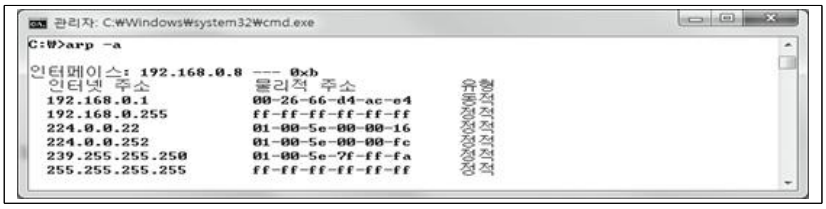
* [그림] ARP 스푸핑 공격에 따른 네트워크 패킷의 흐름



<윈도우에서는 arp -a 명령을 이용해 현재 인지하고 있는 IP와 해당 IP를 가지고 있는 시스템의 MAC 주소 목록을 다음과 같이 확인할 수 있음>

- 이것을 'ARP 테이블'이라고 함

* [그림] arp-a 명령의 실행 결과



4) ARP 스푸핑 공격을 당하기 전에 arp -a 명령을 실행한 결과

```
Internet Address Physical Address Type
10.0.0.2 AA Dynamic
```

5) ARP 스푸핑을 당한 후 arp -a 명령을 실행한 결과

```
Internet Address Physical Address Type
10.0.0.2 CC Dynamic
```

6) ARP 스푸핑에 대한 대응책

<ARP 테이블이 변경되지 않도록 arp -s [IP 주소] [MAC 주소] 명령으로 MAC 주소 값을 고정시키는 것>

```
arp -s 10.0.0.2 AA
```

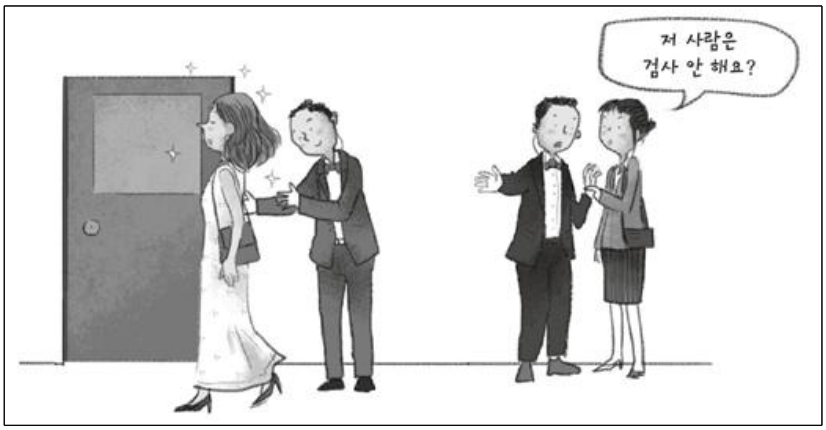
- -s(static)는 고정시킨다는 의미하며, 이 명령으로 Type 부분이 Dynamic에서 Static으로 바뀌게 됨
- 하지만 이 대응책은 시스템이 재부팅 될 때마다 수행해주어야 하는 번거로움이 있음

- 어떤 보안 툴은 클라이언트의 ARP 테이블의 내용이 바뀌면 경고 메시지를 보내기도 하지만 사실 ARP 스푸핑은 TCP/IP 프로토콜 자체의 문제로 근본적인 대책은 없음

2. IP 스푸핑 공격

* IP 스푸핑 : 쉽게 말해 IP 주소를 속이는 것
* 트러스트 : 파티에 초대한 사람 중 친분이 있는 사람은 초대장을 확인하지 않고 그냥 들여보내주는 것과 같은 개념

1) [그림] 파티 주최자와의 트러스트를 이용해 인증 없이 파티에 참석하는 모습



- 유닉스 계열에서는 트러스트 인증법을 주로 사용
- 윈도우에서는 트러스트 대신 액티브 디렉토리 (Active Directory)를 주로 사용
- 트러스트 설정을 해주려면 유닉스에서는 /etc/host.equiv 파일에 다음과 같이 클라이언트의 IP와 접속 가능한 아이디를 등록해 주어야 함

```
① 200.200.200.200 root
② 201.201.201.201 +
```

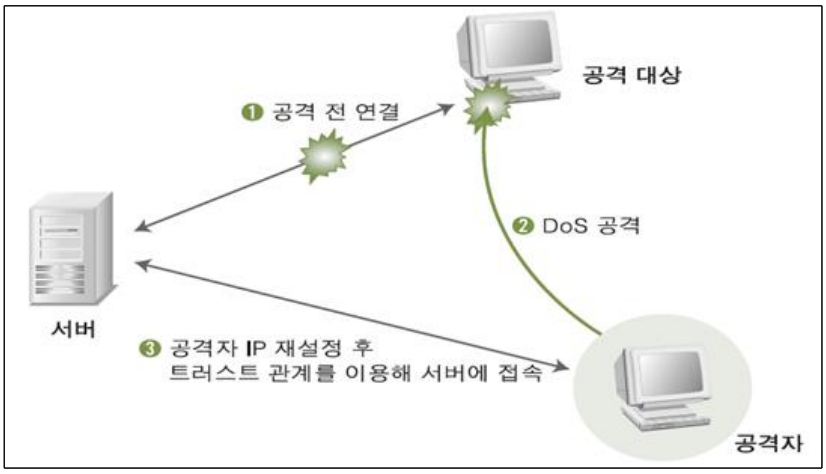
① 200.200.200.200에서 root 계정이 로그인을 시도하면 패스워드 없이 로그인을 허락하라는 의미

② 201.201.201.201에서는 어떤 계정이든 로그인을 허락하라는 것으로 +는 모든 계정을 의미
- 만일 ++라고 적힌 행이 있으면 IP와 아이디에 관계없이 모두 로그인을 허용하라는 의미

* 트러스트를 이용한 접속 네트워크에 패스워드를 뿌리지 않기 때문에 스니핑 공격에 안전한 것처럼 보임

- 하지만 인증이 IP를 통해서만 일어나기 때문에 공격자가 해당 IP를 사용해서 접속하면 스니핑을 통해서 패스워드를 알아낼 필요성 자체가 없어지는 문제점이 있음
- 실제로 공격은 트러스트로 접속하고 있는 클라이언트에 DoS 공격을 수행해 클라이언트가 사용하는 IP가 네트워크에 출현하지 못하도록 한 뒤, 공격자 자신이 해당 IP로 설정을 변경한 후 서버에 접속하는 형태로 이루어짐
- 공격자는 패스워드 없이 서버에 로그인할 수 있음

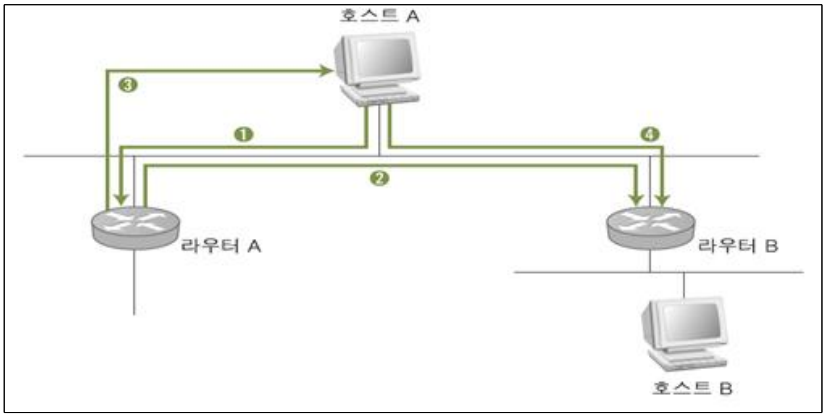
2) [그림] IP 스푸핑을 이용한 서버 접근



3. ICMP 리다이렉트 공격

* ICMP 리다이렉트 : 3계층에서 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는 공격

1) ICMP 리다이렉트 개념도
* [그림] ICMP 리다이렉트 개념도



① 호스트 A에 라우터 A가 기본으로 설정되어 있기 때문에, 호스트 A가 원격의 호스트 B로데이터를 보낼 때 패킷을 라우터 A로 보냄

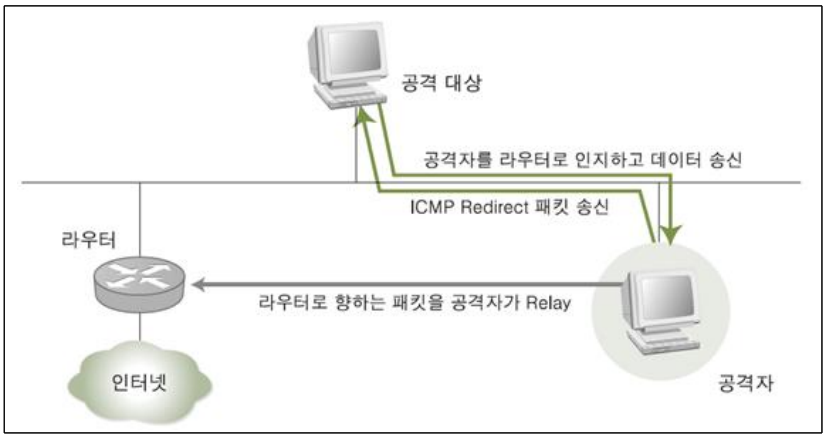
② 라우터 A는 호스트 B로 보내는 패킷을 수신함
- 그리고 라우팅 테이블을 검색하여 호스트 A에게 자신을 이용하는 것보다 라우터 B를 이용하는 것이 더 효율적이라고 판단하여 해당 패킷을 라우터 B로 보냄

③ 라우터 A는 호스트 B로 향하는 패킷을 호스트 A가 자신에게 다시 전달하지 않도록, 호스트 A에 ICMP 리다이렉트 패킷을 보내서 호스트 A가 호스트 B로 보내는 패킷이 라우터 B로 바로 향하도록 함

④ 호스트 A는 라우팅 테이블에 호스트 B에 대한 값을 추가하고, 호스트 B로 보내는 패킷은 라우터 B로 전달함

<공격자가 라우터 B가 되어 ICMP 리다이렉트 패킷도 공격 대상에게 보낸 후 라우터 A에게 다시 릴레이시켜주면 모든 패킷을 스니핑 할 수 있음>

2) [그림] ICMP 리다이렉트 공격 개념도

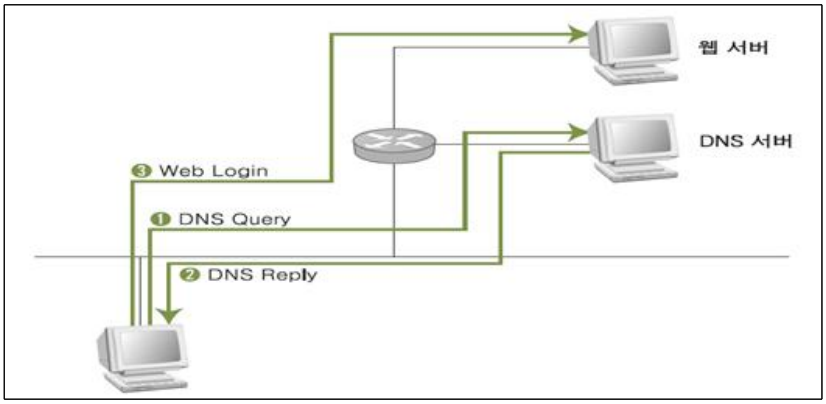


4. DNS 스푸핑 공격

* DNS 스푸핑 공격 : 실제 DNS 서버보다 빨리 공격 대상에게 DNS Response 패킷을 보내, 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격

1) 정상적인 DNS 서비스

* [그림] 정상적인 DNS 서비스



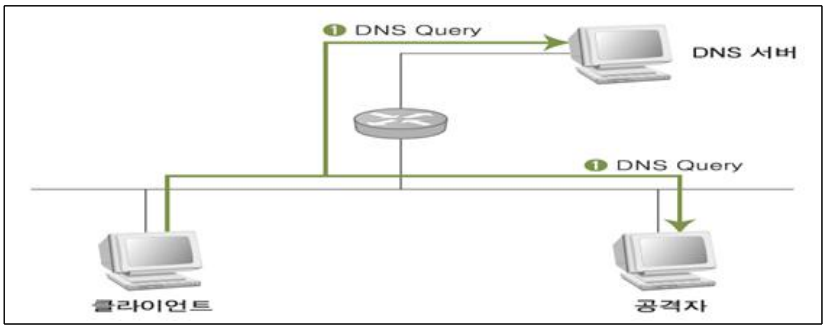
① 클라이언트가 DNS 서버에게 접속하고자 하는 IP 주소(www.wishfree.com과 같은 도메인 이름)를 물어봄
- 이때 보내는 패킷은 DNS Query

② DNS 서버가 해당 도메인 이름에 대한 IP 주소를 클라이언트에게 보내줌

③ 클라이언트가 받은 IP 주소를 바탕으로 웹 서버를 찾아감

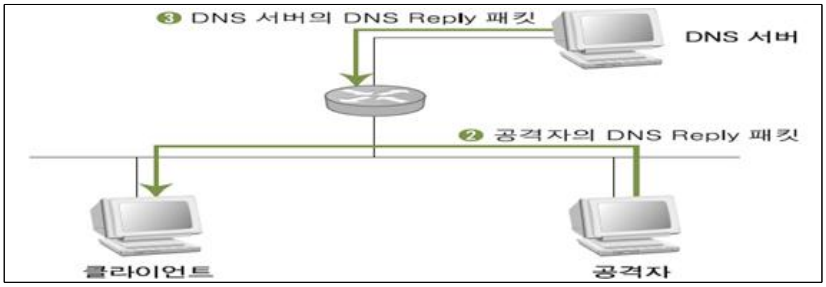
① 클라이언트가 DNS 서버로 DNS Query 패킷을 보내는 것을 확인
- 이때 보내는 패킷은 DNS Query
- 스위칭 환경일 경우에는 클라이언트 DNS Query 패킷을 보내면 이를 받아야 하므로 ARP 스푸핑과 같은 선행 작업이 필요함
- 만약 허브를 쓰고 있다면 모든 패킷이 자신에게도 전달되므로 클라이언트가 DNS Query 패킷을 보내는 것을 자연스럽게 확인할 수 있음

* [그림] DNS Query



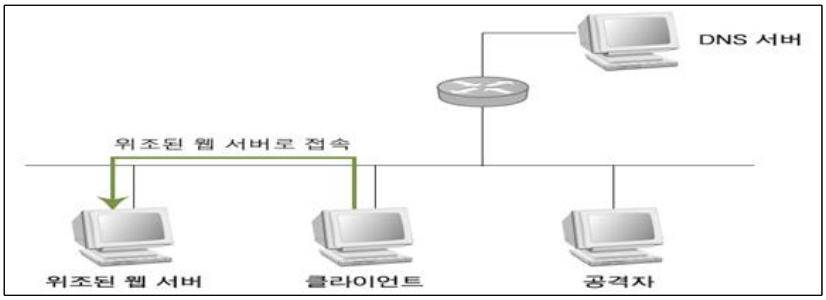
② 공격자는 로컬에 존재하므로 DNS 서버보다 지리적으로 가까움
- DNS 서버가 올바른 DNS Response 패킷을 보내주기 전에 클라이언트에게 위조된 DNS Response 패킷을 보낼 수 있음

* [그림] 공격자와 DNS 서버의 DNS Response



③ 클라이언트는 공격자가 보낸 DNS Response 패킷을 올바른 패킷으로 인식하고, 웹에 접속
- 지리적으로 멀리 떨어져 있는 DNS 서버가 보낸 DNS Response 패킷은 버림

* [그림] 공격 성공 후 도착한 DNS 서버의 DNS Response



2) hosts 파일에는 URL과 IP 정보가 등록되어 있음

```
127.0.0.1 localhost
200.200.200.123 www.wishfree.com
201.202.203.204 www.sysweaver.com
```

학습내용2 : 세션 하이재킹 공격

1. 세션 하이재킹(Session Hijacking)의 정의

* 세션 : 사용자와 컴퓨터, 또는 두 대의 컴퓨터 간의 활성화된 상태
* 세션 하이재킹 : 두 시스템 간 연결이 활성화된 상태, 즉 로그인(Login)된 상태를 가로채는 것을 뜻함

1) [그림] 자리 가로채기

2. TCP 세션 하이재킹

<TCP가 가지는 고유한 취약점을 이용해 정상적인 접속을 빼앗는 방법>
- TCP는 클라이언트와 서버간 통신을 할 때 패킷의 연속성을 보장하기 위해 클라이언트와 서버는 각각 시퀀스 넘버를 사용함
- 이 시퀀스 넘버가 잘못되면 이를 바로 잡기 위한 작업을 하는데, TCP 세션 하이재킹은 서버와 클라이언트에 각각 잘못된 시퀀스 넘버를 위조해서 연결된 세션에 잠시 혼란을 준 뒤 자신이 끼어들어가는 방식

① 클라이언트와 서버 사이의 패킷을 통제
- ARP 스푸핑 등을 통해 클라이언트와 서버 사이의 통신 패킷이 모두 공격자를 지나가게 하도록 하면 됨

② 서버에 클라이언트 주소로 연결을 재설정하기 위한 RST(Reset) 패킷을 보냄
- 서버는 해당 패킷을 받고, 클라이언트의 시퀀스 넘버가 재설정된 것으로 판단하고, 다시 TCP 쓰리웨이 핸드셰이킹을 수행

③ 공격자는 클라이언트 대신 연결되어 있던 TCP 연결을 그대로 물려받음

3. 세션 하이재킹 공격에 대한 대응책

- SSH와 같이 세션에 대한 인증 수준이 높은 프로토콜을 이용해서 서버에 접속해야 함
- 클라이언트와 서버 사이에 MAC 주소를 고정시켜주는 줌
- 주소를 고정시키는 방법은, 앞서도 언급했지만 ARP 스푸핑을 막아주기 때문에 결과적으로 세션 하이재킹을 막을 수 있음

【학습정리】

1. ARP(Address Resolution Protocol) 스푸핑은 MAC 주소를 속이는 것. 즉, MAC 주소를 속여 랜에서의 통신 흐름을 왜곡시키는 공격방법이다.

2. IP 스푸핑 공격은 IP 주소를 속이는 방법으로 공격한다.

3. ICMP 리다이렉트는 3계층에서 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는 공격이다.

4. DNS 스푸핑 공격은 DNS 서버보다 빨리 공격 대상에게 DNS Response 패킷을 보내, 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격이다.

5. 세션 하이재킹은 두 시스템 간 연결이 활성화된 상태, 즉 로그인(Login)된 상태를 가로채는 공격이다.