

네트워크 보안과 해킹

2009. 10

박종혁
(jhpark1@snut.ac.kr)
www.parkjonghyuk.net

네트워크 보안과 해킹

□ 네트워크 기본 이론

□ 정보 수집

□ 네트워크 해킹

□ 네트워크 보안

네트워크 기본 이론

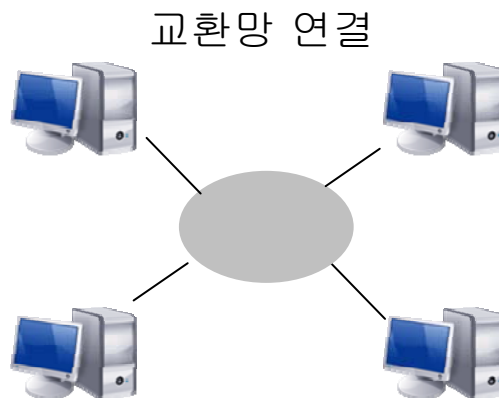
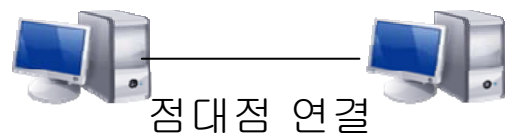
네트워크

□ 컴퓨터 네트워크(Computer Network)

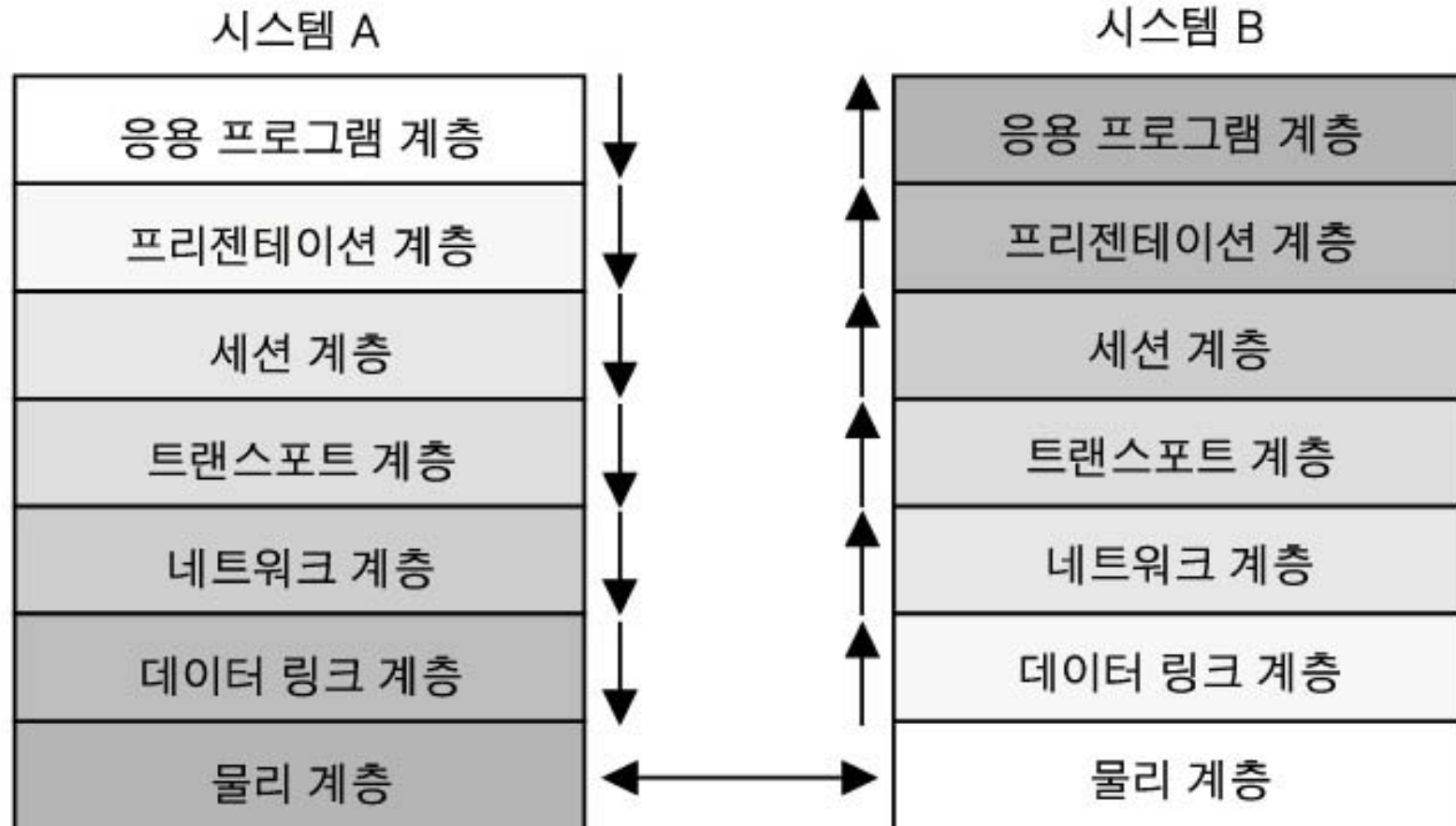
○ 데이터 전송과 처리를 유기적으로 결합하여 어떤 목적이나 기능을 수행

- 전송 : 컴퓨터에 의해 처리된 정보를 전송하는 것
- 데이터처리 : 컴퓨터에서 정보를 처리하는 것

□ 네트워크의 구성



OSI 7계층 구조(1)



OSI 7계층 구조 (2)

□ 물리적 계층

- 두 시스템간의 물리적 연결을 위한 전기적 메커니즘, 절차, 기능 등을 정의
- 전압 레벨, 전압 변환 시기, 물리적 데이터 최대 전송량, 최대 전송거리, 물리적 커넥터 등과 같은 특성을 정의
- 전송 매체로는 일반 랜 케이블(Twist Pair Cable), 동축 케이블, 광 케이블, 기타 무선 매체가 사용

□ 데이터 링크 계층

- 물리적 링크를 통하여 정보전송
- 흐름제어 : 수신측에 맞춰서 송신측의 속도, 전송량을 제어
- 오류제어 : 오류가 있을 시 재 전송을 요청, 신뢰성확보

OSI 7계층 구조 (3)

□ 네트워크 계층

- 네트워크를 통한 패킷의 전송을 담당
- 패킷이 목적지에 도착하기 위해 라우팅 알고리즘 사용하여 경로 설정
- 이 기종 네트워크들의 상호연결

□ 트랜스포트 계층

- 종단간 신뢰성 있는 데이터 전송을 담당
- 연결지향 or 비 연결지향
- 흐름제어, 오류제어 수행
- 혼잡제어 : 트래픽이 많이 있을 시 송신측의 송신량을 조절

OSI 7계층 구조 (4)

□ 세션계층

- 두 시스템간의 통신중 동기화와 데이터교환을 관리해줌
- 연결의 설정, 유지, 해제, 전송 데이터 속도조절

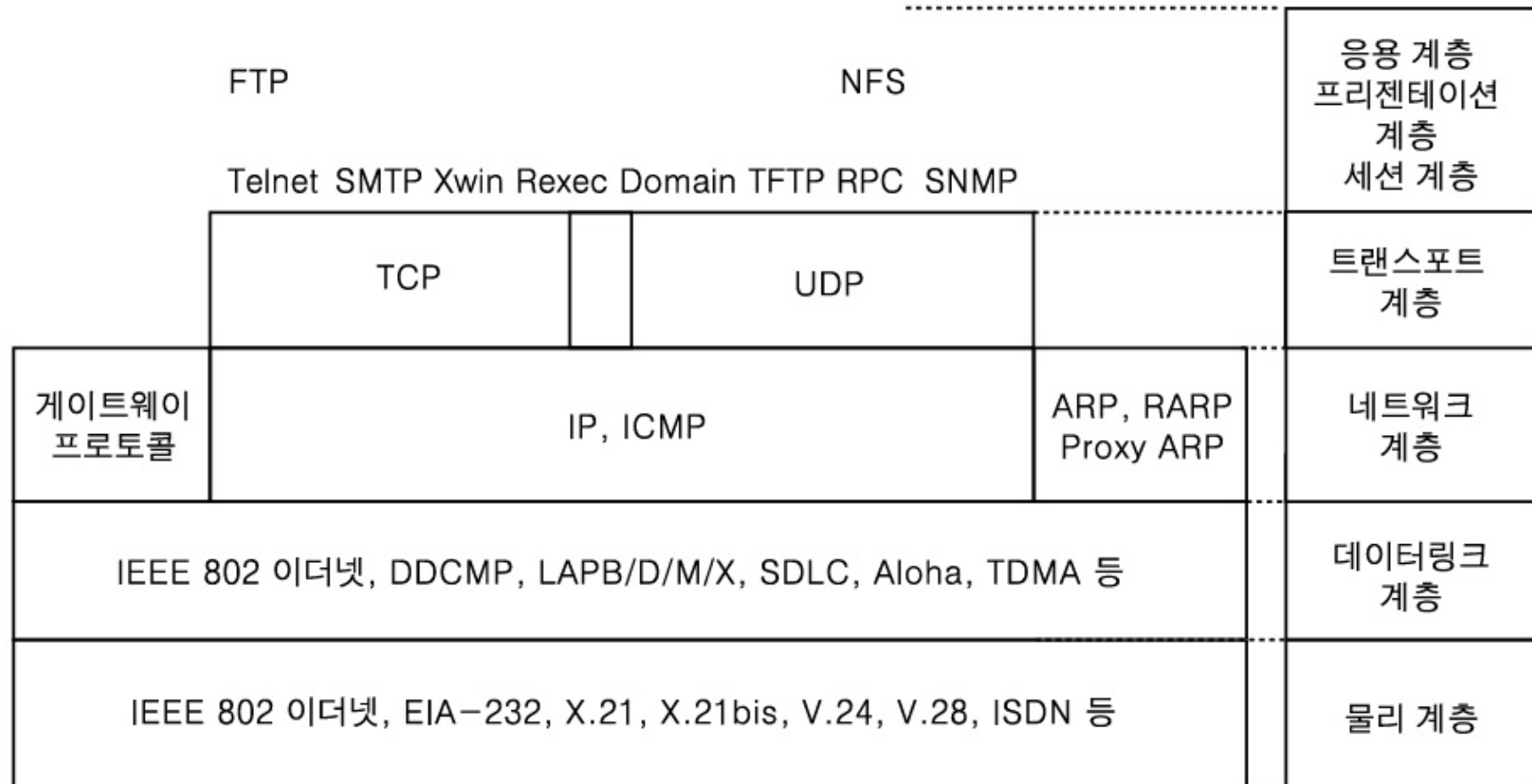
□ 프리젠테이션 계층

- 표현에 대한 방법 결정
- 코딩, 코덱, 암호화, 압축

□ 응용프로그램 계층

- Graphic User Interface
- Internet Explore, Outlook, Messenger
- HTTP, FTP, 터미널 서비스, 디렉토리 서비스

TCP/IP 구조 (1)



(a) TCP/IP 아키텍처

(b) OSI 아키텍처

인터넷 계층 (1)

□ IP(Internet protocol)

- 네트워크 계층의 가장 대표적인 프로토콜
- 하위 계층의 서비스를 이용하여 두 노드간의 데이터 전송 경로를 확립
- IP 주소 체계

비트 수	1	7	24
A 클래스	0	네트워크 주소	호스트 주소

비트 수	2	14	16
B 클래스	1	0	네트워크 주소 호스트 주소

비트 수	3	21	8	
C 클래스	1	1	0	네트워크 주소 호스트 주소

형 태	네트워크 번호 영역	가용 네트워크 주소 수
A Class	1.x.x.x ~ 126.x.x.x	126개
B Class	128.1.x.x ~ 191.254.x.x	16,382개
C Class	192.0.1.x ~ 223.255.254.x	2,097,150개

인터넷 계층 (2)

- ARP : IP에 해당하는 호스트의 하드웨어 주소를 찾는 기능
- RARP : ARP의 반대의 기능
- ICMP : 송신측의 상황과 목적지 노드의 상황을 진단

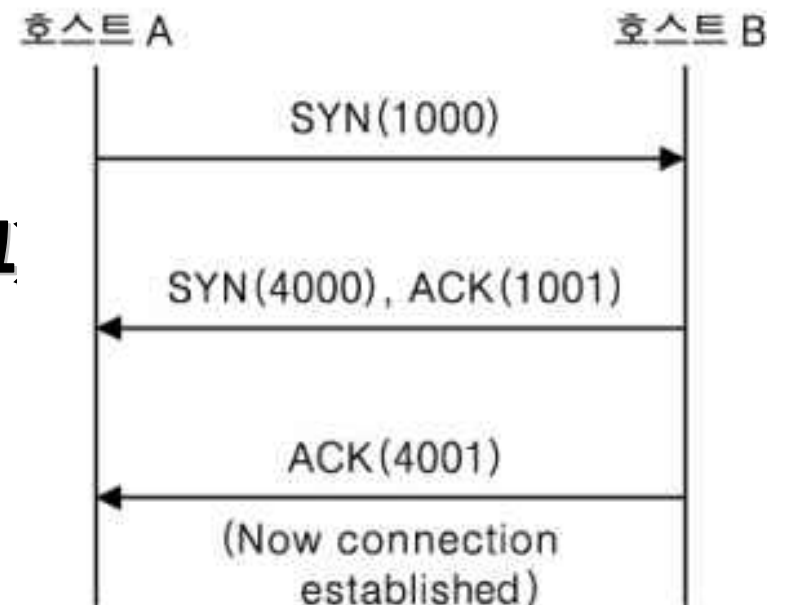
전송 계층 (1)

□ TCP (Transmission Control Protocol)

○ TCP는 데이터의 흐름을 관리하고, 데이터가 정확한지 확인하는 역할

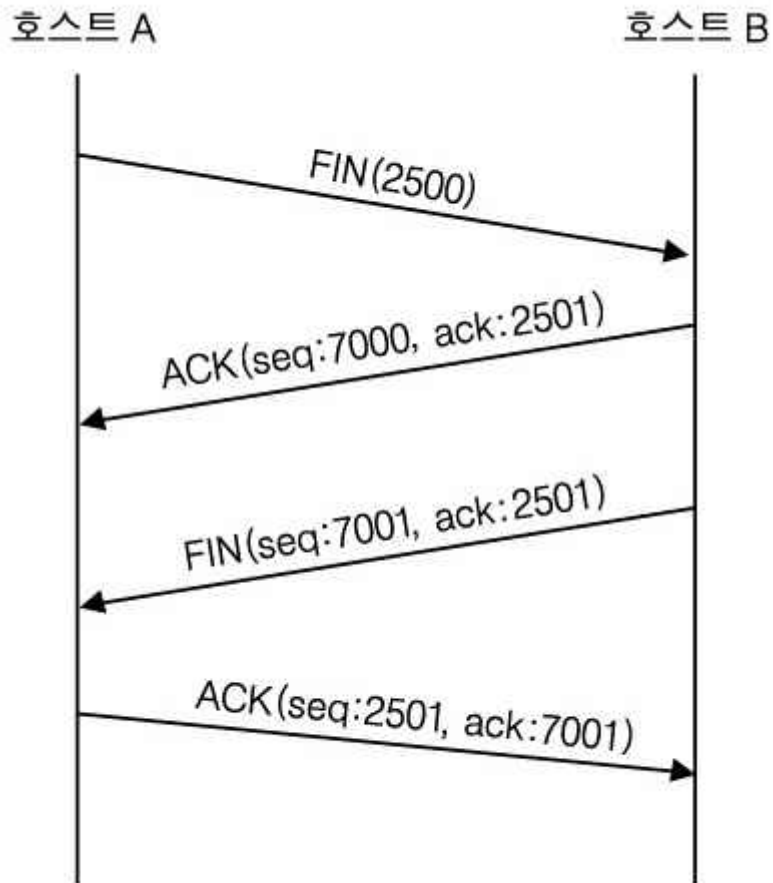
- 높은 신뢰성
- 가상회선 연결 방식
- 연결의 설정과 해제
- 데이터 체크섬
- 시간 초과와 재전송
- 데이터 흐름 제어

□ TCP 연결 설정(3-Way 핸드셰이크)



전송 계층 (2)

□ TCP 연결 종료(4-Way 핸드셰이크)



전송 계층 (3)

□ UDP(User Datagram Protocol)

○ 비연결 프로토콜로서 상대방이 보낸 응답을 확인하지 않음

○ UDP의 특징

- 비연결 지향형
- 네트워크 부하 감소
- 비신뢰성
- 전송된 데이터의 일부가 소실됨

정보 수집

풋프린팅

□ 풋프린팅

- 공격 대상의 정보를 모으는 방법(기술적인 해킹 공격, 신문, 게시판 등)
- 풋프린팅에는 매우 다양한 기법이 있으며, 매우 넓은 범위가 포함

□ 사회공학(Social Engineering)

- 기술적인 해킹에 의한 방법이 아닌,
- 개인적인 인간 관계, 업무적 관계 등을 이용한 방법, 넘어 훔쳐보기 등
- 비기술적인 경로를 이용해서 정보를 모으는 방법

포트

□ Well Known

포트 번호	서비스	서비스 내용
21 (TCP)	FTP	File Transfer Protocol FTP 연결 시 인증과 컨트롤을 위한 포트
23 (TCP)	Telnet	Telnet 서비스로서 원격지의 서버의 실행 창을 얻어낸다.
25 (TCP)	SMTP	Simple Message Transfer Protocol 메일을 보낼 때 사용하는 서비스
53 (UDP)	DNS	Domain Name Service 이름을 해석하는 데 사용하는 서비스
69 (UDP)	TFTP	Trivial File Transfer Protocol 인증이 존재하지 않는 단순한 파일 전송에 사용되는 서비스
80 (TCP)	HTTP	Hyper Text Transfer Protocol 웹 서비스

포트

□ Well Known

포트 번호	서비스	서비스 내용
110	POP3	Post Office Protocol 메일 서버로 전송된 메일을 읽을 때 사용하는 서비스
111	RPC	Sun의 Remote Procedure Call 원격에서 서버의 프로세스를 실행할 수 있게 한 서비스
138	NetBIOS	Network Basic Input Output Service 윈도우에서 파일을 공유하기 위한 서비스
143	IMAP	Internet Message Access Protocol. POP3와 기본적으로 같으나, 메일을 읽고 난 후에도 메일은 서버에 남는 것이 다름.
161	SNMP	Simple Network Management Protocol 네트워크 관리와 모니터링을 위한 서비스

스캔

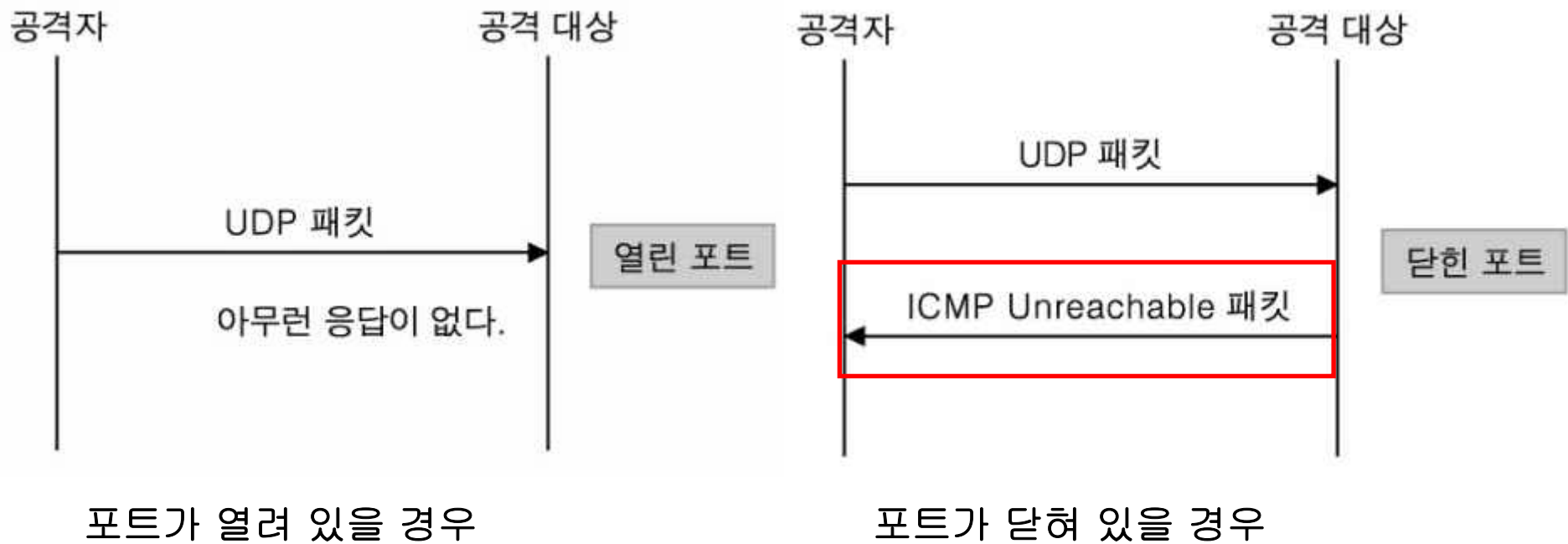
□ 스캔

- 스캔은 서비스를 제공하는 서버의 작동 여부와 제공하고 있는 서비스를 확인
- TCP 기반의 프로토콜의 질의(Request) 응답(Response) 메커니즘
- 열려있는 포트, 제공하는 서비스, 동작중인 데몬의 버전, 운영체제의 버전, 취약점 등 다양한 정보 획득 가능
- 일반적으로 nmap 사용

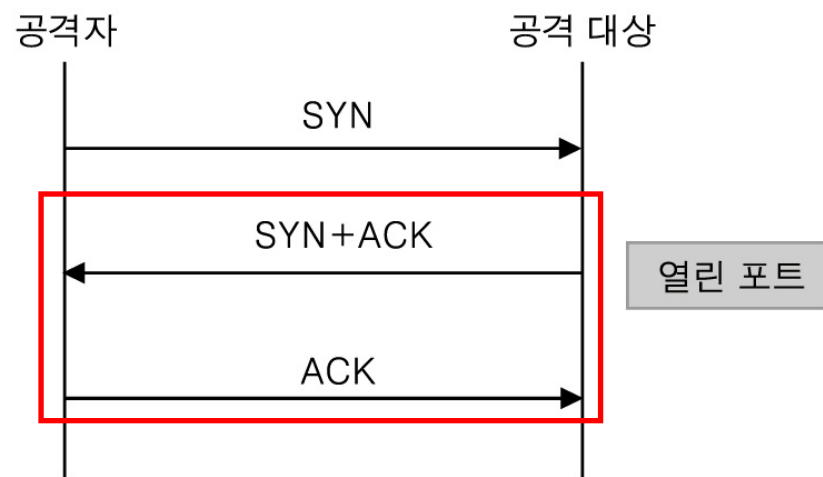
□ Ping & ICMP Scan

- Ping은 네트워크와 시스템이 정상적으로 작동하는지 확인하는 유틸
- ICMP(Internet Control Messaging Protocol)를 사용

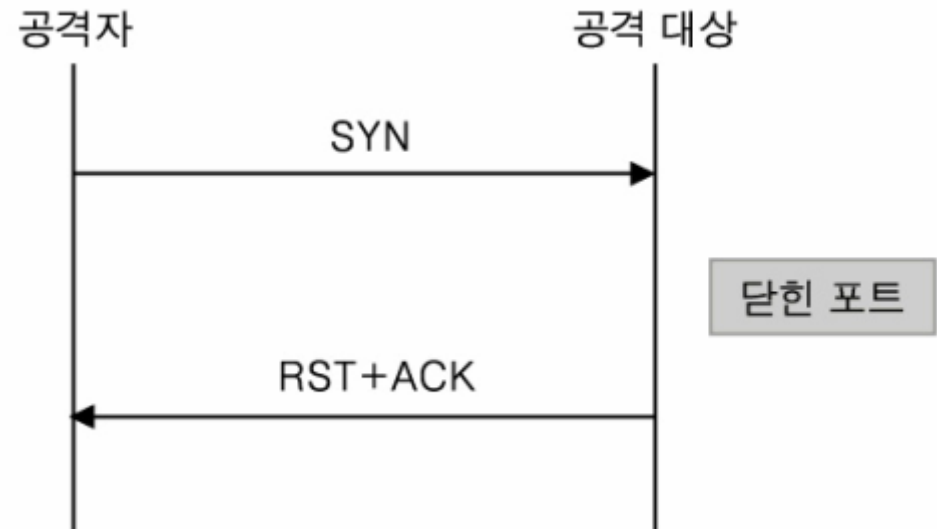
UDP Open 스캔



TCP Open 스캔

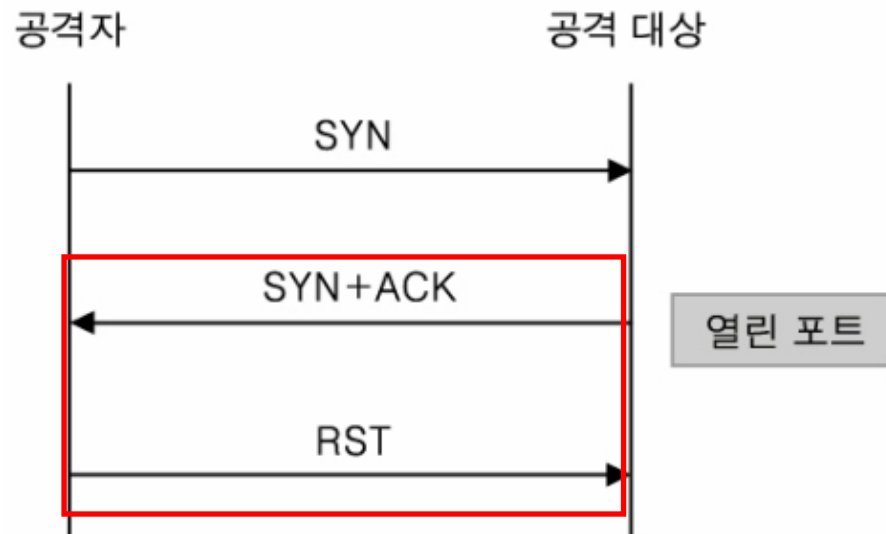


포트가 열려 있을 경우

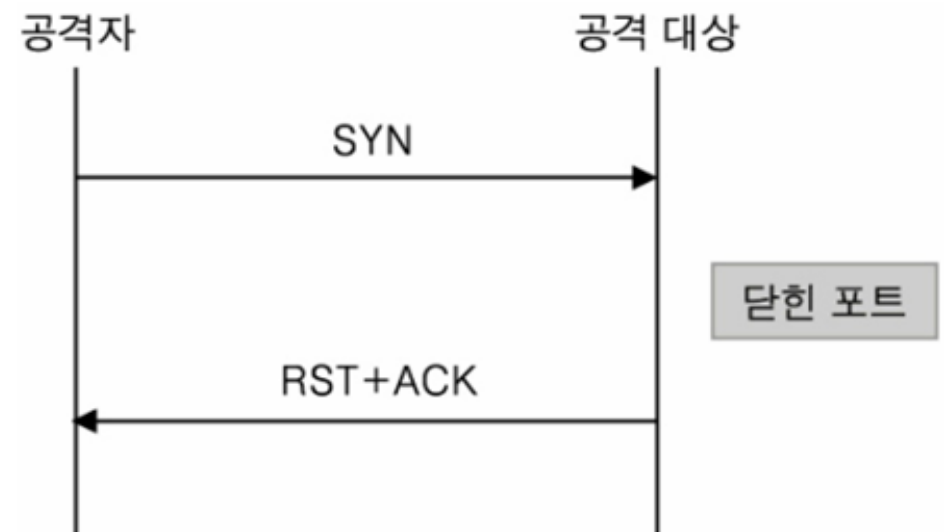


포트가 닫혀 있을 경우

Stealth 스캔 : TCP Half Open 스캔

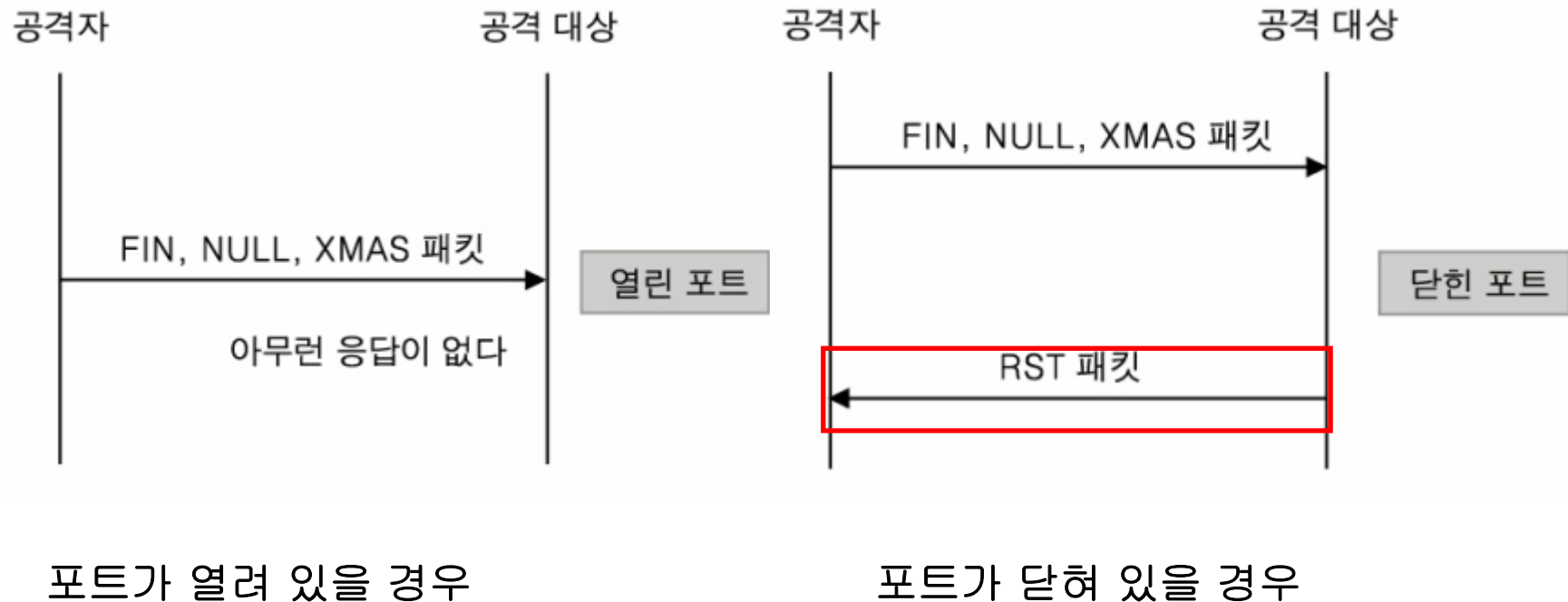


포트가 열려 있을 경우



포트가 닫혀 있을 경우

Stealth 스캔 : FIN, Xmas, Null 스캔



포트가 열려 있을 경우

포트가 닫혀 있을 경우

※ XMAS = ACK, FIN, RST, SYN, URG의 패킷 묶음

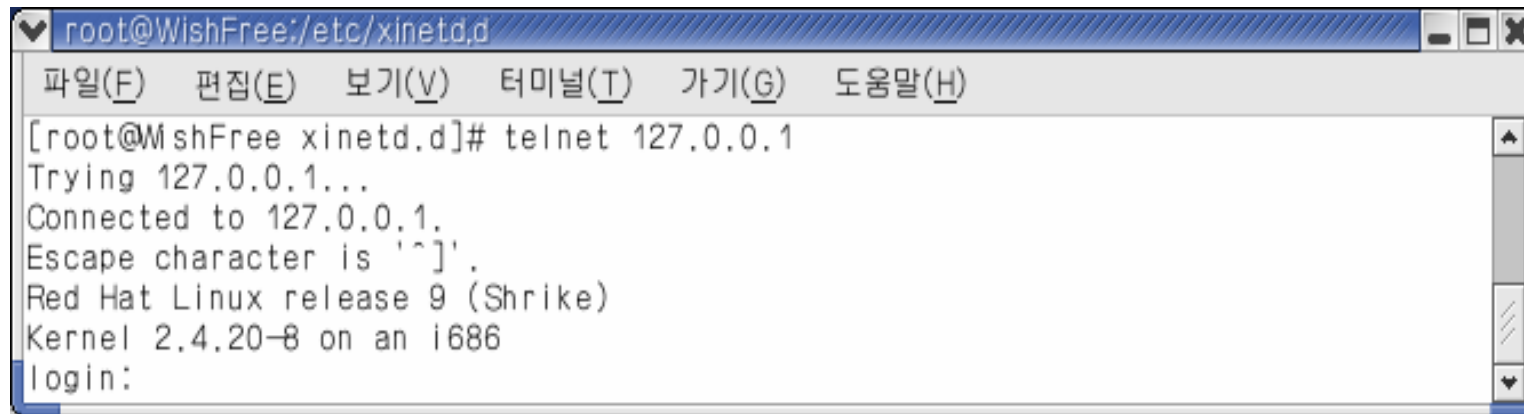
Stealth 스캔 : 시간차 공격

- 공격의 차단을 피하거나, 탐지를 회피하기 위해 특정한 시간 간격으로 스캔 패킷을 보내는 기법
- Paranoid : 5분이나 10분 간격
- Sneaky : WAN에서는 15초 단위로, LAN에서는 5초 단위
- Polite : 0.4초 단위
- Normal : 정상
- Aggressive : 호스트 타임 아웃 : 5분, 패킷 당 1.25초까지 응답대기.
- Insane : 호스트 타임 아웃 : 75초, 패킷 당 0.3초까지 응답대기

운영체제의 탐지(1)

□ 배너 그래빙(Banner Grabbing)

- Telnet과 같이 원격지의 시스템에 로그인을 시도하면 나타나는 안내문



```
root@WishFree:/etc/xinetd.d
파일(F) 편집(E) 보기(V) 터미널(T) 가기(G) 도움말(H)
[root@MshFree xinetd.d]# telnet 127.0.0.1
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Red Hat Linux release 9 (Shrike)
Kernel 2.4.20-8 on an i686
login:
```

- 운영체제의 버전과 커널 버전을 확인
- 배너 그래빙은 21, 23, 25, 110.143 포트에서도 가능

운영체제의 탐지(2)

□ 방화벽과 IDS의 탐지

○ Traceroute을 이용한 방법

```
root@WishFree:~  
파일(F) 편집(E) 보기(V) 터미널(T) 가기(G) 도움말(H)  
[root@WishFree root]# traceroute 211.174.51.104  
traceroute to 211.174.51.104 (211.174.51.104), 30 hops max, 38 byte packets  
 1 210.92.110.33 (210.92.110.33)  1.094 ms  2.566 ms  2.850 ms  
 2 192.168.54.161 (192.168.54.161)  1.542 ms  0.096 ms  0.060 ms  
 3 192.168.54.29 (192.168.54.29)  0.074 ms  0.098 ms  0.057 ms  
 4 192.168.51.53 (192.168.51.53)  0.076 ms  0.093 ms  0.059 ms  
 5 203.248.225.69 (203.248.225.69)  0.077 ms  0.061 ms  0.060 ms  
 6 210.120.248.173 (210.120.248.173)  8.775 ms  0.132 ms  0.061 ms  
 7 210.120.192.198 (210.120.192.198)  0.079 ms  0.065 ms  8.739 ms  
 8 210.92.194.214 (210.92.194.214)  0.142 ms  0.136 ms  3.532 ms  
 9 211.233.55.70 (211.233.55.70)  0.103 ms  0.129 ms  0.060 ms  
10 211.233.55.198 (211.233.55.198)  0.079 ms  0.124 ms  4.735 ms  
11 * * *  
12 * * *  
13 * * *  
14 * * *  
15 * * *
```

- ICMP Time Exceed Message가 돌아오지 않고, * 로 표시된 부분에 방화벽이 존재

운영체제의 탐지(3)

□ Port 스캔을 이용한 방법

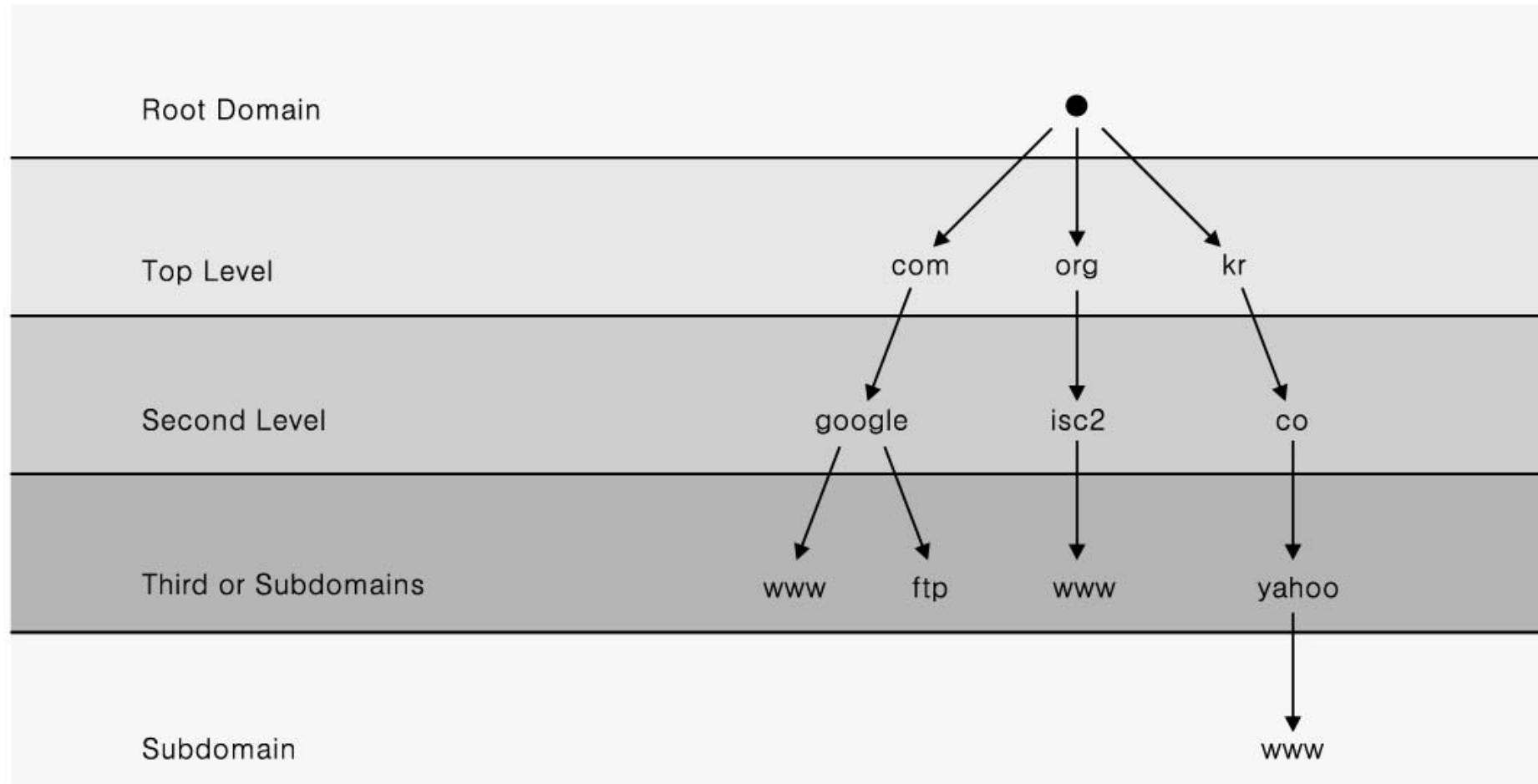
방 화 벽	
Check Point : Firewall - I	256,257,258
M.S. ISA	1078, 1080, 1745
어울림 Secure Works	3346,2890
Cisco PIX	530, 540
Astaro	1235, 1236
IDS(침입 탐지 시스템)	
Check Point : VPN Swite	300, 301
인젠 Neowatcher	1887
Snort	2350

Whois 서버

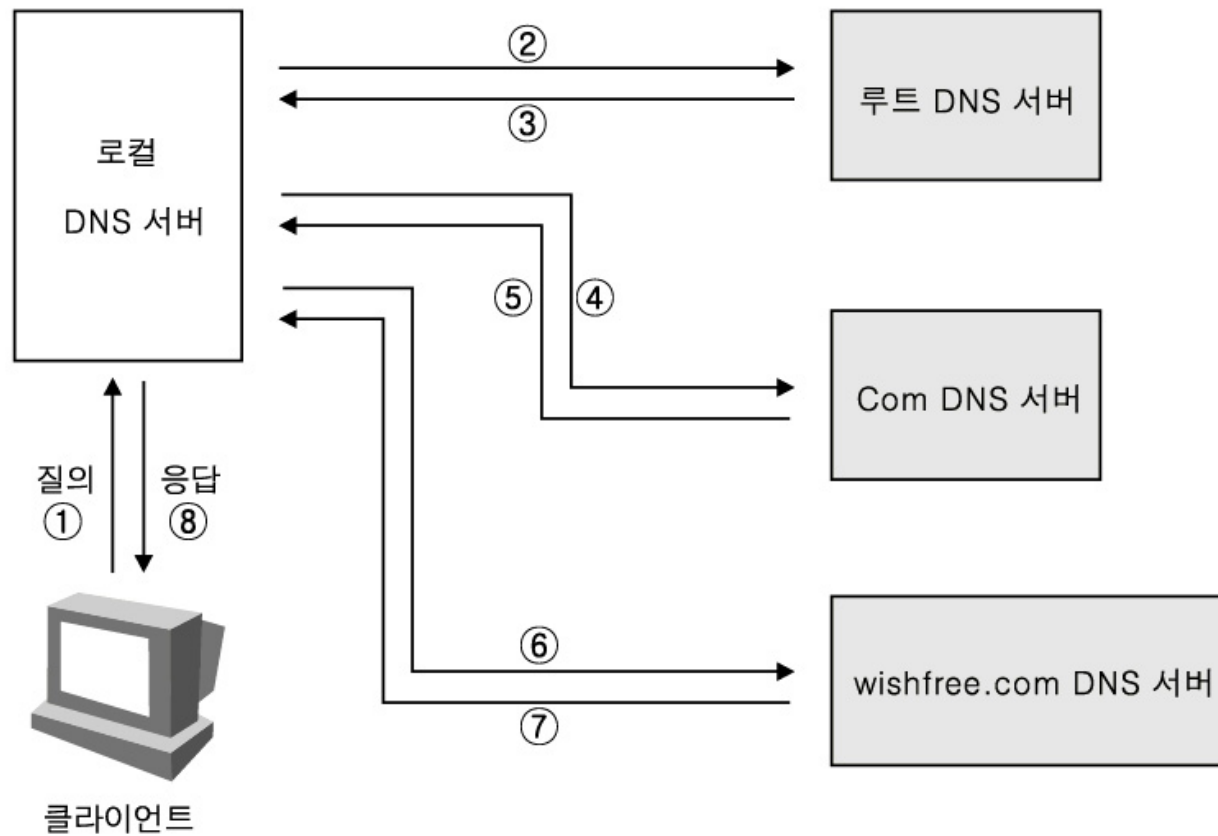
- 등록, 관리 기관
- 도메인 이름
- 목표 사이트 네트워크 주소와 IP 주소
- 관리자, 기술 관련 정보
- 등록자, 관리자, 기술 관리자
- 레코드 생성 시기와 업데이트 시기
- 주 DNS 서버와 보조 DNS 서버
- IP 주소의 할당 지역 위치
- 관리자 이메일 계정

담당 지역	Whois 서버	담당 지역	Whois 서버
유럽	www.ripe.net	호주	Whois.aunic.net
아시아	www.arin.net	프랑스	www.nic.fr

DNS의 계층 구조



DNS 서버 이름 해석 과정



IP 주소 추적

- 메일을 이용한 방법
- P2P 서비스를 이용한 방법
- 웹 게시판을 이용한 방법
- 채팅을 이용한 방법
- Traceroute를 이용한 방법

공유 자원 목록화

□ 목록화(Enumeration)

- 마치 목차를 써서 한 눈에 알아볼 수 있게 하는 것
- 실제 공격 바로 전단계
- 윈도우 시스템은 NetBIOS를 이용한 파일 공유
- 리눅스와 유닉스 시스템은 주로 NFS를 이용
- 윈도우와 유닉스가 동시에 사용되는 네트워크에서는 NetBIOS 를 이용한 Samba를 이용

네트워크 해킹

DoS 공격의 이해

□ DoS(Denial of Service) 공격

- 공격대상이 수용할 수 있는 능력 이상의 정보나 사용자 또는 네트워크의 용량을 초과 시켜 정상적으로 작동하지 못하게 하는 공격

□ DoS 공격 분류

- 1. 파괴 공격 : 디스크나 데이터, 시스템의 파괴
- 2. 시스템 자원의 고갈 : CPU, 메모리, 디스크의 사용에 과도한 부하를 가중시킴
- 3. 네트워크 자원의 고갈 : 쓰레기 데이터로 네트워크의 대역폭을 고갈 시킴

DoS 공격

□ Ping of Death

- Ping을 이용하여 ICMP 패킷을 정상적인 크기보다 아주 크게 만드는 것
- 공격대상 시스템은 정상적인 Ping의 경우보다 훨씬 많은 부하

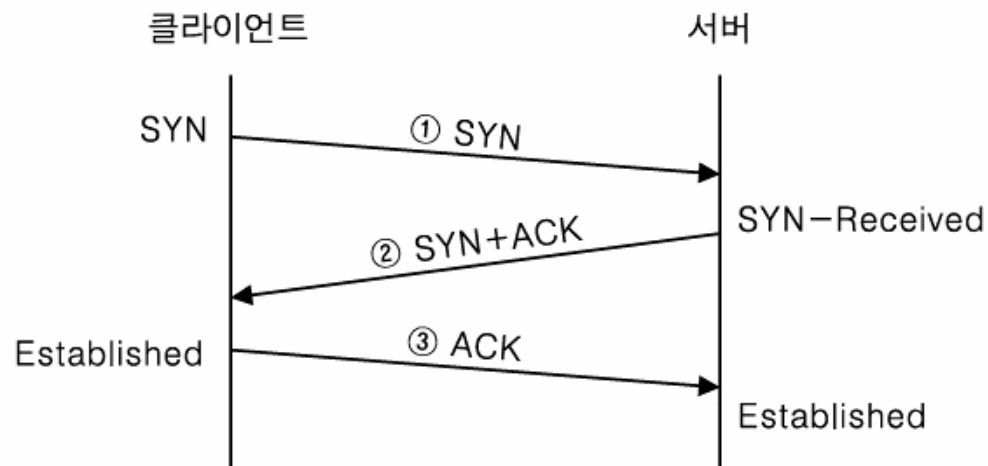
□ Syn Flooding

- 서버별 한정되어 있는 동시 사용자 수를 존재하지 않는 클라이언트가 접속한 것처럼 속임 → 다른 사용자가 서버에서 제공하는 서비스를 받지 못하게 하는 것

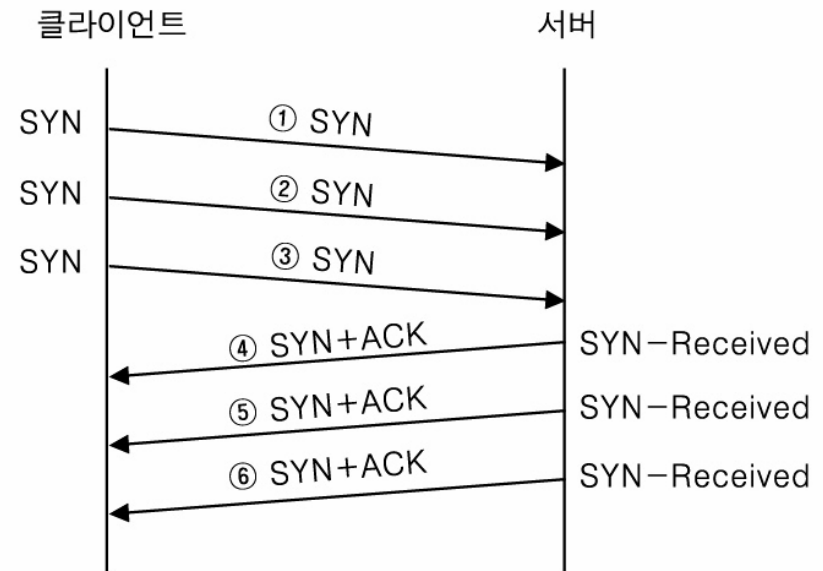
□ Boink, Bonk, Teardrop, LAND, Mail Bomb 등

Syn Flooding 공격 시 3Way 핸드셰이킹

정상적인 3Way 핸드셰이킹



Syn Flooding 공격 시 3Way 핸드셰이킹



Syn Flooding 보안 대책

- 보안 패치로서 대기 시간을 줄이는 것

- 예방할 수 있는 방법
 - 일차적으로 시스템에 패치
 - 다음으로는 IDS의 설치

- 아주 짧은 시간 안에 똑같은 형태의 패킷을 전송
- 매우 정형화된 형태로 네트워크에서 쉽게 인지가 가능
- 해당 ISP 업체에 연락하여 그에 해당하는 IP 대역을 접속 금지

Mail Bomb

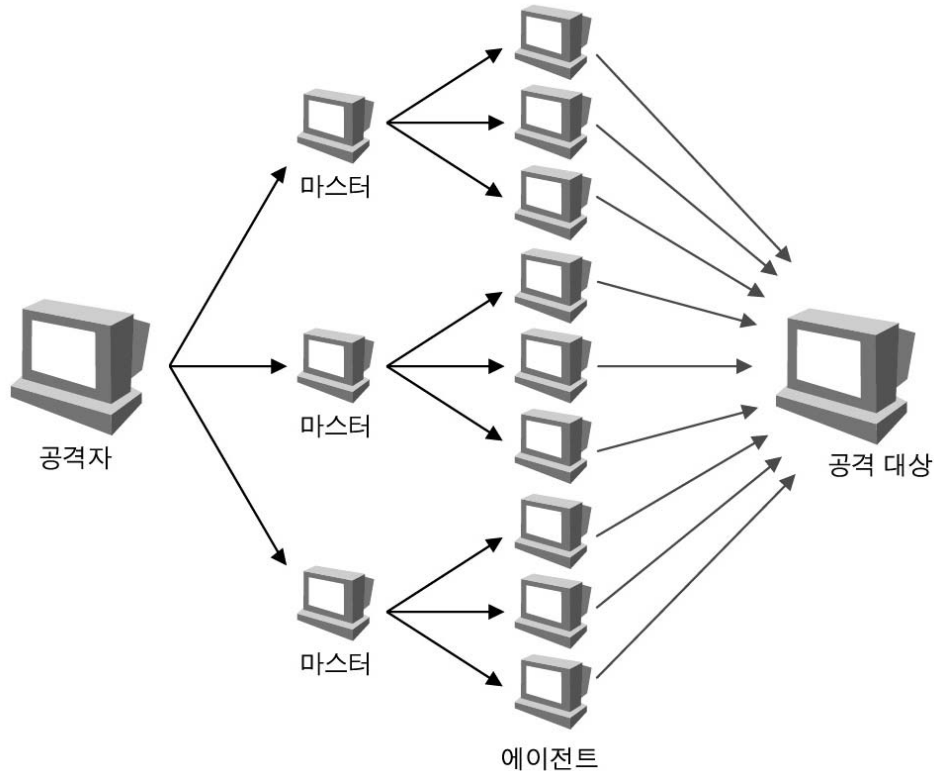
- Mail Bomb는 흔히 폭탄 메일이라고 함.
- 메일서버의 사용자 할당 디스크 공간이 가득 차면 받아야 하는 메일을 받을 수 없음.
 - ∴ 스팸 메일은 DoS 공격이 될 수도 있음
- 윈도우용 Mail Bomber Upyours



DDoS 공격

- DoS 공격이 짧은 시간에 여러 곳에서 일어나게 하는 공격
- 피해 양상이 상당히 심각하며, 확실한 대책이 없음
- 공격자의 위치와 구체적인 발원지를 파악하는 것이 불가능
- 자동화된 툴을 이용
- 공격의 범위가 방대
- 최종 공격대상 이외에도 공격을 증폭시켜주는 중간자가 필요

DDoS 공격의 구성 요소



- 공격자(Attacker) : 공격을 주도하는 해커의 컴퓨터
- 마스터(Master) : 공격자에게서 직접 명령을 받는 시스템으로 여러 대의 에이전트(Agent)를 관리하는 시스템
- 에이전트(Agent) : 공격대상(Target)에 직접적인 공격을 가하는 시스템

DDoS 공격의 일반적인 순서

- 1. 많은 사용자가 사용하며, 밴드와이드(Bandwidth)가 크다. 관리자가 모든 시스템을 세세하게 관리할 수 없는 곳에 계정을 획득하여 스니핑이나 버퍼 오버플로우 등의 공격으로 설치 권한이나 루트 권한을 획득한다.
- 2. 잠재적인 공격대상을 파악하기 위해 네트워크 블록 별로 스캐닝을 실시하여, 원격지에서 버퍼 오버플로우를 일으킬 수 있는 취약한 서비스를 제공하는 서버를 파악한다.
- 3. 취약한 시스템의 리스트를 확인한 뒤, 실제 공격을 위한 Exploit을 작성한다.
- 4. 권한을 획득한 시스템에 침투하여 Exploit을 컴파일하여 설치한다.
- 5. 설치한 Exploit로 공격을 시작한다.

DoS, DDoS 공격에 대한 대응책

- 1. 방화벽 설치와 운영
- 2. IDS 설치와 운영
- 3. 안정적인 네트워크의 설계
- 4. 시스템 패치
- 5. 모니터링
- 6. 서비스별 대역폭 제한

스푸핑 공격

- 스푸핑(Spoofing)이란 '속이다'라는 의미.
- IP 주소, 호스트 이름, MAC 주소 등 여러 가지를 속일 수 있으며, 스푸핑은 이런 속임을 이용한 공격을 총칭.(ARP 스푸핑, IP 스푸핑, DNS 스푸핑 등)
- 인터넷이나 로컬에서 존재하는 모든 연결에 스푸핑이 가능하며, 정보를 얻어내는 것 외에도 시스템을 마비시키는 것도 가능.
- 흔히 일어나는, IP 충돌 문제 역시 고의가 아닌 IP 스푸핑이라고 생각할 수 있음.

세션 하이재킹 공격

□ 세션 하이재킹 공격

- 세션 하이재킹 공격이란 이미 인증을 받아 세션을 생성하여 유지하고 있는 연결을 여러 가지 방법으로 빼앗는 공격

□ TCP 세션 하이재킹 공격

- TCP 세션 하이재킹은 연결의 신뢰성을 확보하기 위한 시퀀스 넘버를 이용한 공격
- 클라이언트와 서버간의 통신을 관찰
- 트러스트를 이용한 세션은 물론 Telnet, FTP 등 TCP를 이용한 거의 모든 세션의 갈취가 가능
- 인증에 대한 문제점을 해결하기 위해 도입된 일회용 패스워드(One Time Password), 토큰 기반 인증(Token Based Authentication : Kerberos)을 이용한 세션의 갈취도 가능

세션 하이재킹 공격의 대응책

□ 데이터 전송의 암호화

□ 지속적인 인증(Continuous Authentication)

- 시스템에 로그인 후 다시 재인증 과정을 거치지 않는데, 어떤 특정한 행동을 하거나, 일정 시간이 되면 재 인증을 받은 유효한 사용자인지 확인

스니핑

- 정보를 데이터 속에서 찾는 것
- 스니핑 공격은 막는 것도 어려우며, 탐지 역시 쉽지 않음
- 스니핑 공격은 수동적(Passive) 공격
- 랜에서의 스니핑은 프러미스큐어스(Promiscuous) 모드에서 작동
- 프러미스큐어스 모드 : 자신의 주소 값을 무시하고 모든 패킷을 받아들이는 상태

스니핑 공격 도구

□ TCP Dump

- 가장 일반적으로 쓰이는 스니핑 도구
- 네트워크 관리를 위해 개발된 툴, Snort라는 IDS의 기반 프로그램
- TCP Dump는 법적 효력이 있음
- 법적 효력을 발휘하려면 법원에서 인정하는 규약에 따라야 함

□ DSniff

- DSniff는 스니핑을 위한 자동화 도구
- 스니핑을 위한 다양한 패키지 툴 제공
- 암호화된 계정과 패스워드까지 읽어내는 능력

□ Sniffer Pro (Window)

- 윈도우에서는 프리미스큐어스 모드가 지원되지 않음
- WinPCAP과 같은 라이브러리를 이용해서 스니핑이 가능
- 윈도우 스니퍼는 뛰어난 GUI(Graphic User Interface)를 이용한 네트워크 상태를 점검하거나 패킷의 통계를 내기 위한 목적으로 많이 사용

Telnet Login 시 TCPCDump 결과

□ 패스워드 : qwer1234의 경우

```
root@wishfree:~  
파일(F) 편집(E) 보기(V) 터미널(T) 가기(G) 도움말(H)  
23:00:30.010924 172.16.0.2.32876 > 172.16.0.3.23: P [tcp sum ok] 155:156(1) ack 147 win 5840 <nop,nop,timestamp 61101 41  
7475> (DF) [tos 0x10] (ttl 64, id 44146, len 53)  
0x0000 4510 0035 ac72 4000 4006 361b ac10 0002 E..5.r@.@.6.....  
0x0010 ac10 0003 806c 0017 3ff3 4969 5028 9864 .....l..?.lIP(.d  
0x0020 8018 16d0 56da 0000 0101 080a 0000 eead .....V.....  
0x0030 0006 5ec3 71 ..^q  
23:00:30.046217 172.16.0.3.23 > 172.16.0.2.32876: . [tcp sum ok] 147:147(0) ack 156 win 5792 <nop,nop,timestamp 417564 6  
1101> (DF) [tos 0x10] (ttl 64, id 49890, len 52)  
0x0000 4510 0034 c2e2 4000 4006 1fac ac10 0003 E..4..@.@.....  
0x0010 ac10 0002 0017 806c 5028 9864 3ff3 496a .....lP(.d?.lJ  
0x0020 8010 16a0 c7b9 0000 0101 080a 0006 5f1c .....  
0x0030 0000 eead ....  
23:00:30.194428 172.16.0.2.32876 > 172.16.0.3.23: P [tcp sum ok] 156:157(1) ack 147 win 5840 <nop,nop,timestamp 61119 41  
7564> (DF) [tos 0x10] (ttl 64, id 44147, len 53)  
0x0000 4510 0035 ac73 4000 4006 361a ac10 0002 E..5.s@.@.6.....  
0x0010 ac10 0003 806c 0017 3ff3 496a 5028 9864 .....l..?.lJP(.d  
0x0020 8018 16d0 506e 0000 0101 080a 0000 eebf .....Ph.....  
0x0030 0006 5f1c 77 ..w  
23:00:30.194729 172.16.0.3.23 > 172.16.0.2.32876: . [tcp sum ok] 147:147(0) ack 157 win 5792 <nop,nop,timestamp 417578 6  
1119> (DF) [tos 0x10] (ttl 64, id 49891, len 52)  
0x0000 4510 0034 c2e3 4000 4006 1fab ac10 0003 E..4..@.@.....  
0x0010 ac10 0002 0017 806c 5028 9864 3ff3 496b .....lP(.d?.lk  
0x0020 8010 16a0 c798 0000 0101 080a 0006 5f2a ....._*  
0x0030 0000 eebf ....  
23:00:30.383976 172.16.0.2.32876 > 172.16.0.3.23: P [tcp sum ok] 157:158(1) ack 147 win 5840 <nop,nop,timestamp 61138 41  
7578> (DF) [tos 0x10] (ttl 64, id 44148, len 53)  
0x0000 4510 0035 ac74 4000 4006 3619 ac10 0002 E..5.t@.@.6.....  
0x0010 ac10 0003 806c 0017 3ff3 496b 5028 9864 .....l..?.lkP(.d  
0x0020 8018 16d0 624c 0000 0101 080a 0000 eed2 .....bL.....  
0x0030 0006 5f2a 65 ..te  
23:00:30.384270 172.16.0.3.23 > 172.16.0.2.32876: . [tcp sum ok] 147:147(0) ack 158 win 5792 <nop,nop,timestamp 417597 6  
1138> (DF) [tos 0x10] (ttl 64, id 49892, len 52)  
0x0000 4510 0034 c2e4 4000 4006 1faa ac10 0003 E..4..@.@.....  
0x0010 ac10 0002 0017 806c 5028 9864 3ff3 496c .....lP(.d?.ll  
0x0020 8010 16a0 c771 0000 0101 080a 0006 5f3d .....q....._=
```

5. 스니핑 공격의 대응책

□ 스니퍼 탐지

- 네트워크에 이상 현상을 만들지 않음(사용자가 인지하기 어려움)
- 스니퍼는 프러미스큐어스 모드에서 작동 하는 것을 이용
- Ping을 이용 : 의심이 가는 호스트에 ping(존재하지 않는 MAC 주소로 위장) → ICMP Echo reply를 받으면 해당 호스트가 스니핑
- ARP를 이용 : 위조된 ARP request를 전송 → ARP response가 오면 프러미스 큐어스 모드로 설정
- DNS 방법 : 테스트 대상 네트워크로 Ping Sweep을 보내고 들어오는 Inverse-DNS lookup을 감시하여 스니퍼를 탐지
- 유인(Decoy)방법 : 가짜 계정과 패스워드를 네트워크에 뿌린다 → 가짜 계정과 패스워드를 이용하여 접속을 시도하는 시스템을 탐지
- ARP watch 툴 이용

NetBIOS

□ 윈도우의 파일 공유, 프린터 등의 일반 사무기기의 이용, WINS 등을 이용하는 데 사용

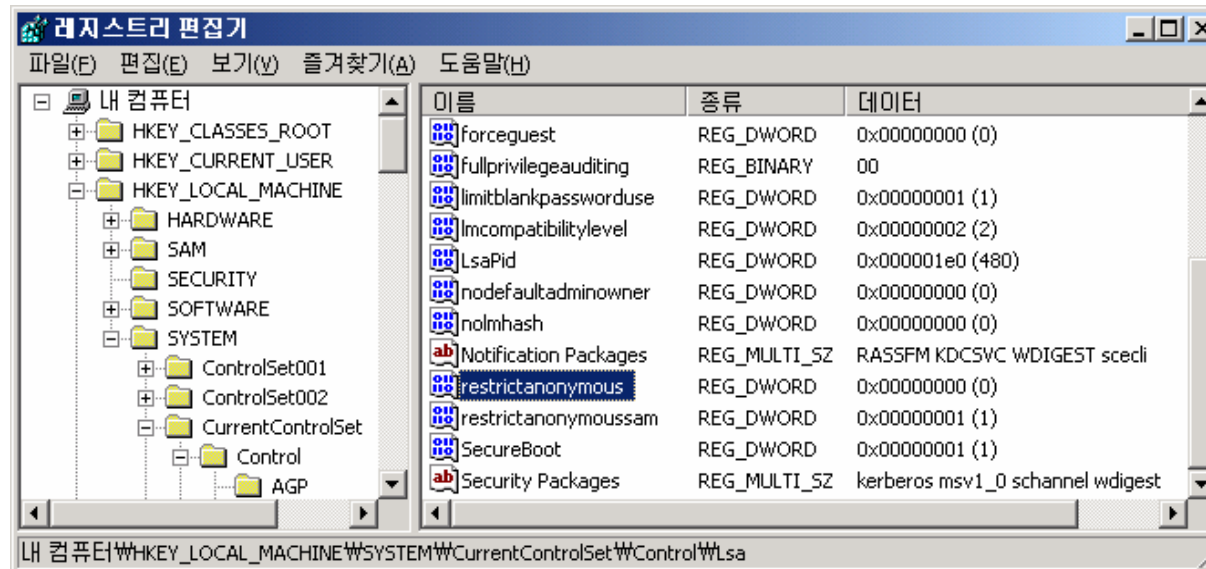
□ 보안취약점

○ 널 세션(Null Session)을 이용한 목록화

※ 널 세션 : 계정과 패스워드 없이 세션을 생성

널 세션의 차단

- 135-139번과 445번 포트를 닫기
- 개인용 방화벽, 'Microsoft 네트워크용 파일 및 프린터 공유' 체크 해제
- 레지스트리 편집기에서
Hkey_Local_Machine\System\CurrentControlSet\Control\Lsa의 restricanonymous 값을 1로 설정.



NetBIOS 공격에 대한 보안 대책

- 패스워드를 추측하기 어려운 것으로 설정
- 중요한 패스워드는 자주 교체
- 쓰지 않는 계정은 삭제
- 패스워드 입력에 실패할 경우 계정 잠금이 되도록 설정
- 로그인 이벤트에 대한 감사를 실시

네트워크 보안

방화벽

□ 방화벽의 기능과 목적

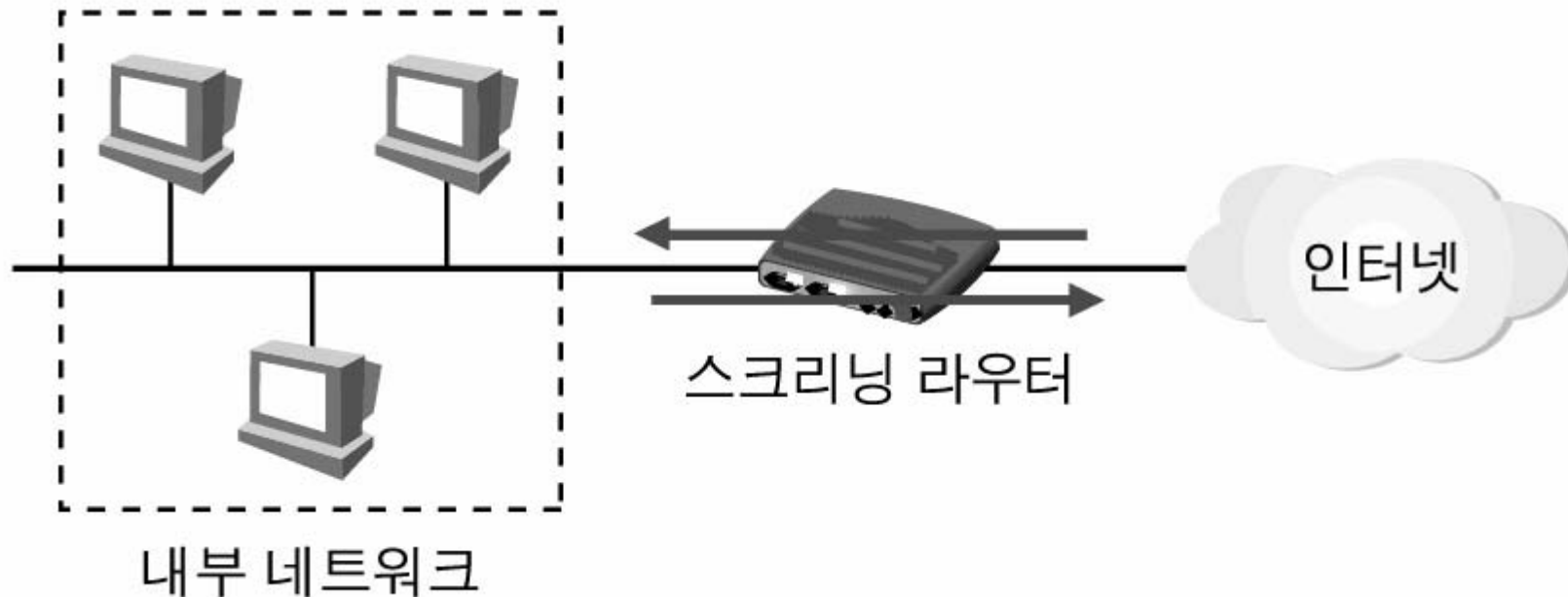
- 네트워크에서의 보안을 높이는 데 가장 일차적인 것
- 신뢰하지 않는 외부 네트워크와 신뢰하는 내부 네트워크 사이를 지나는 패킷을 정해 놓은 규칙에 따라 차단하거나 보내주는 기능

□ 방화벽의 주된 기능

- 접근제어(Access Control)
- 로깅(Logging)과 감사추적(Auditing)
- 인증(Authentication)
- 데이터의 암호화

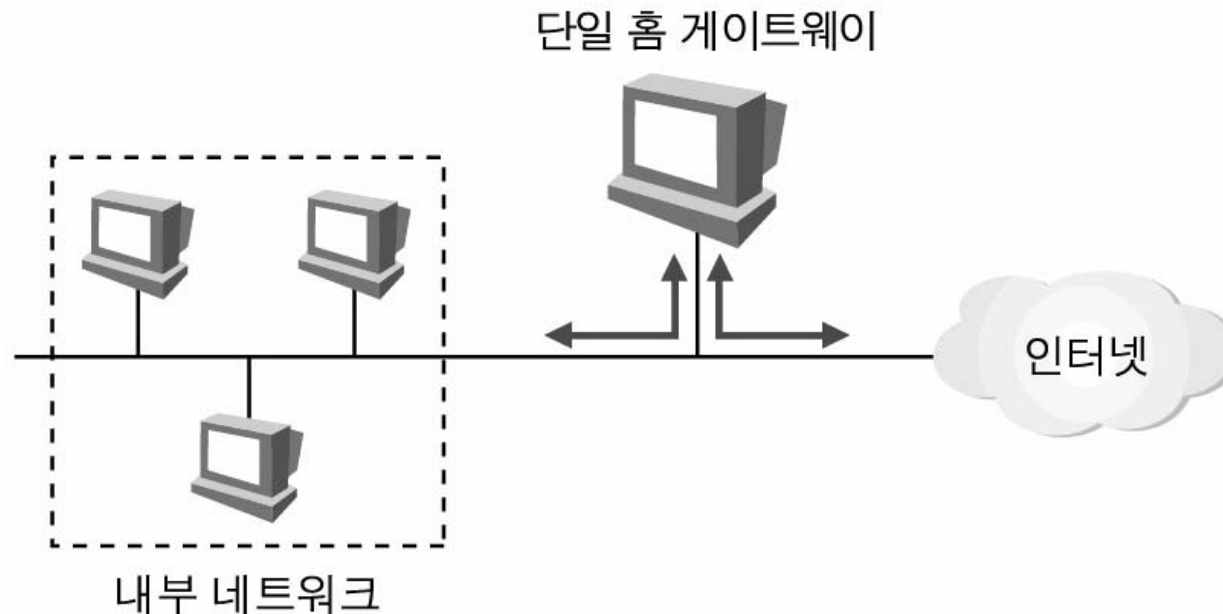
스크리닝(Screening) 라우터

- 3계층인 네트워크 계층과 4계층 트랜스포트(Transport) 계층에서 실행되며, IP 주소와 포트에 대한 접근 제어가 가능
- 외부 네트워크와 내부 네트워크의 경계선
- 라우터에 패킷 필터링 규칙을 적용하는 것으로 방화벽의 역할을 수행

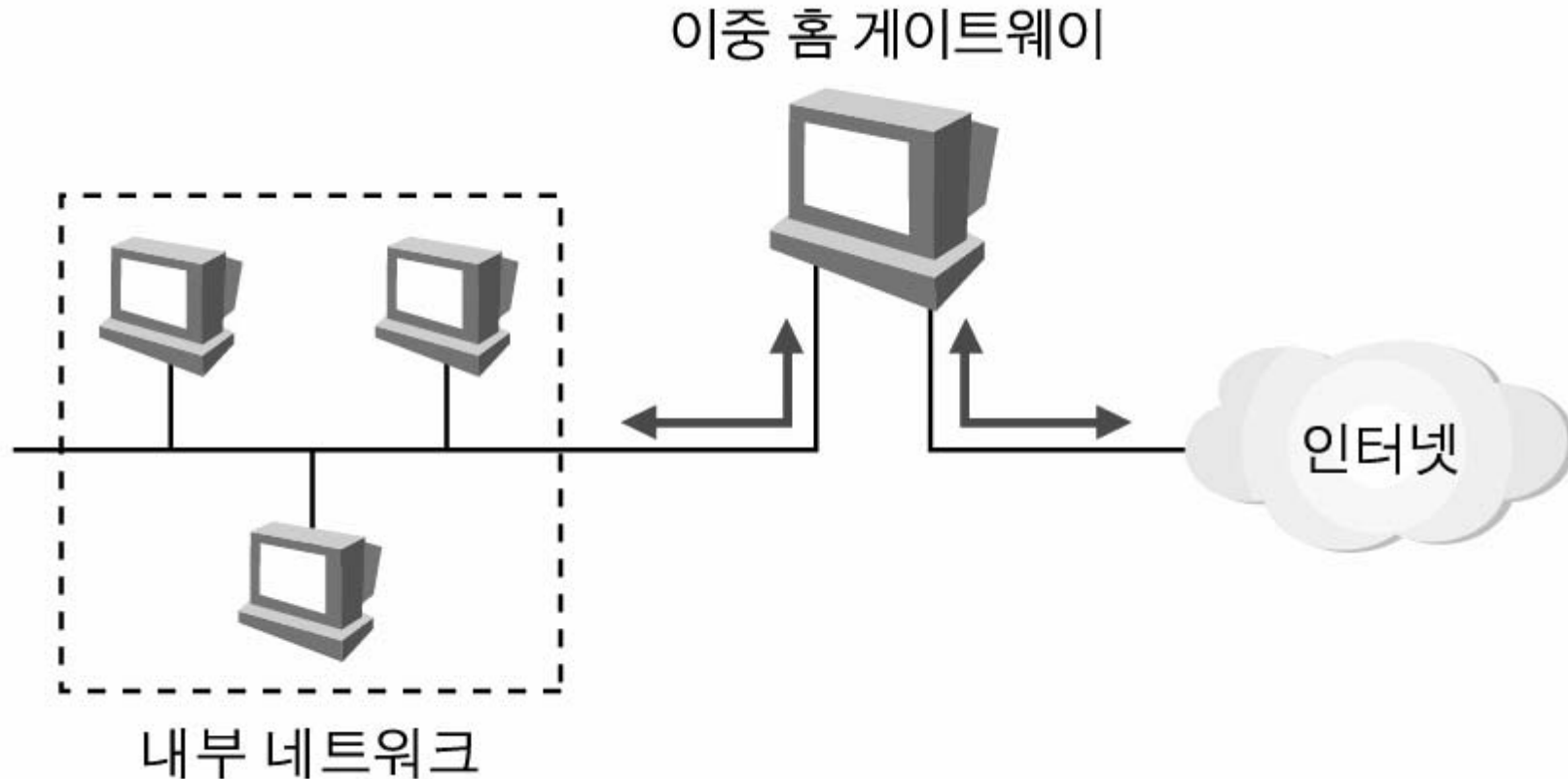


단일 홈 게이트웨이: Single Homed Gateway

- 강력한 보안 정책 실행 가능 (방화벽 구성)
- 방화벽이 손상되면 내부 네트워크에 대한 무조건적인 접속을 허용
- 방화벽으로의 원격 로그인 정보가 노출되어 방화벽에 대한 제어권을 공격자가 얻게 되면 내부 네트워크를 더 이상 보호할 수가 없음
- 2계층 공격 등을 통한 방화벽의 우회가 가능



이중 홈 게이트웨이: Dual Homed Gateway



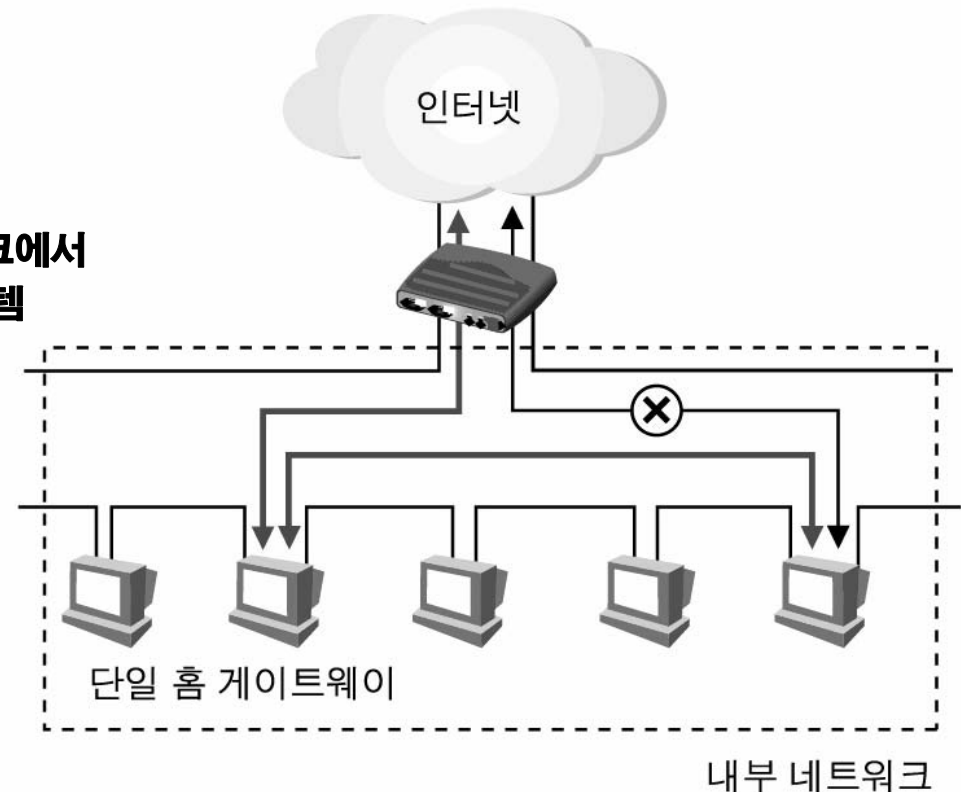
- 효율적인 트래픽의 관리
- 방화벽을 우회하는 것은 불가능

스크린된 호스트 게이트웨이- 단일 홈

- 스크리닝 라우터와 Single Homed Gateway의 조합
- 가장 많이 이용되는 구조이며 융통성이 좋음
- 스크리닝 라우터가 해커에 의해 해킹되면 베스천 호스트를 거치지 않고 내부 네트워크에 대한 직접적인 접근이 가능
- 구축 비용이 많이 듦

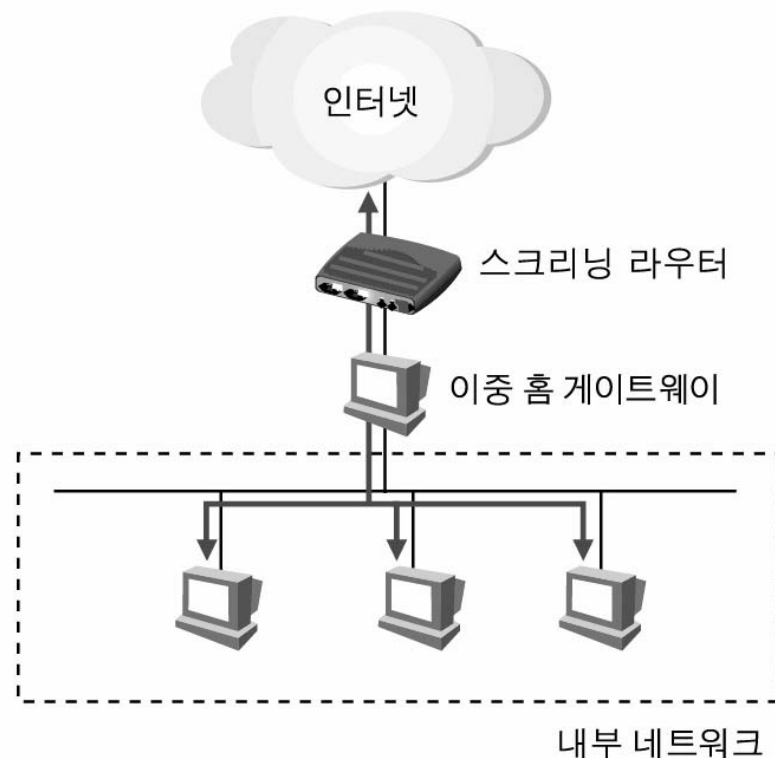
* 베스천 호스트:

외부공격에 대한 방어정책이 구현되어있는 네트워크에서 외부 접속에 대한 일차적인 연결을 받아들이는 시스템



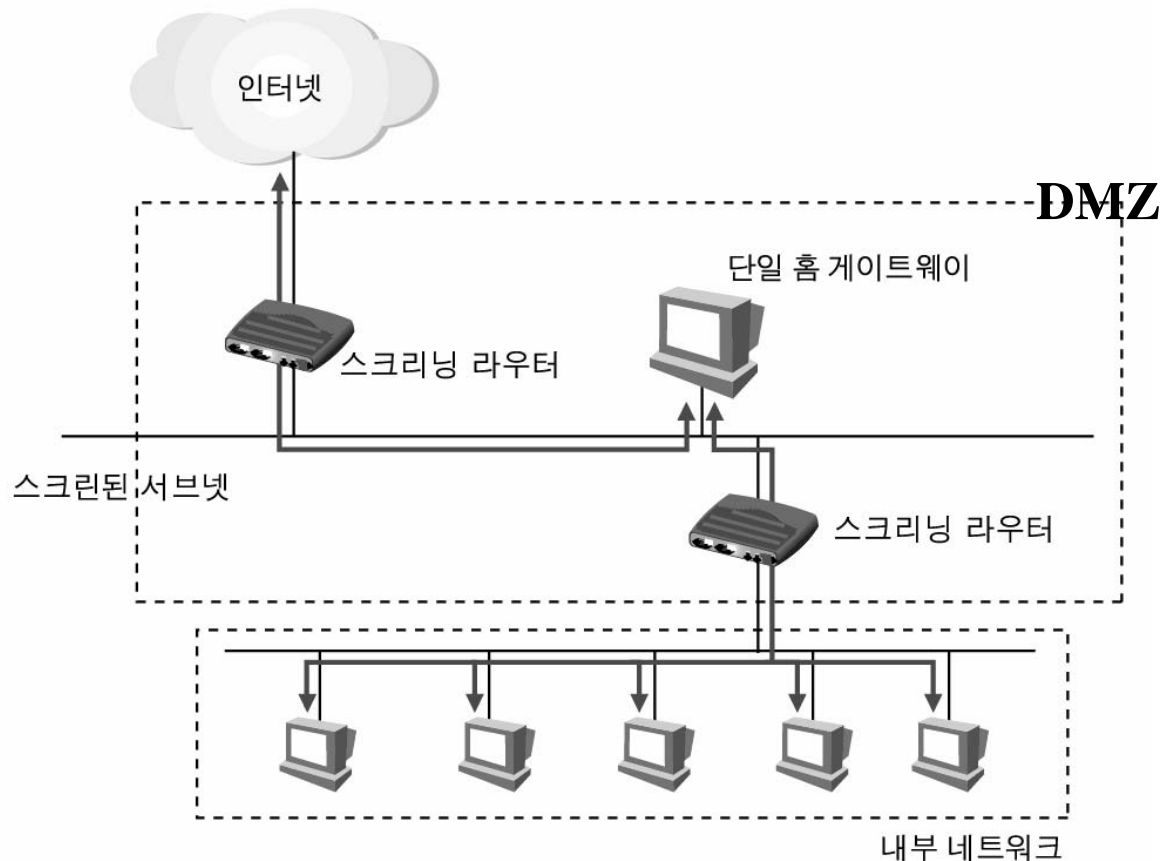
스크린된 호스트 게이트웨이- 이중 홈

- 2단계로 방어를 실행하므로 무척 안전
- 스크리닝 라우터에서 3계층과 4계층에 대한 접근 제어
- 베스천 호스트에서 7계층에 대한 접근 제어 실행



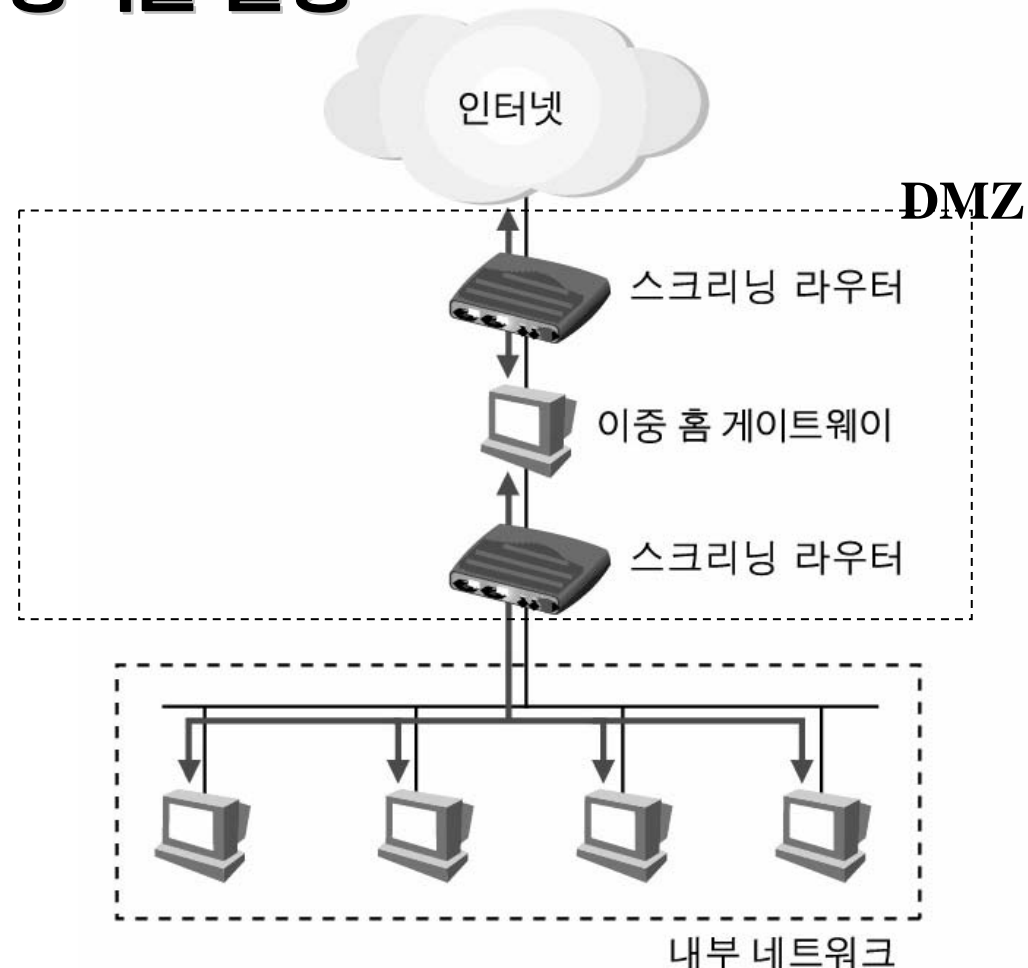
스크린된 서브넷 게이트웨이-단일 홈

- 외부 네트워크와 내부 네트워크 사이에 완충 지대(DMZ)를 두는 것
- 다른 방화벽의 모든 장점을 가지며 용통성이 매우 뛰어나며 매우 안전
- 설치하기 어렵고, 관리 또한 어려우며 서비스 속도가 느리며 가격도 비쌘



스크린된 서브넷 게이트웨이-이중 홈

- Single Homed Gateway를 쓴 경우보다는 빠르며 좀더 강력한 보안 정책을 실행



패킷 필터링

- **'명백히 허용하지 않은 서비스에 대한 거부'를 적용**
 - 1. 허용할 서비스를 확인한다.
 - 2. 제공하고자 하는 서비스가 보안의 문제점은 없는지와 허용에 대한 타당성을 검토한다.
 - 3. 서비스가 이루어지고 있는 형태를 확인하고, 어떤 규칙(Rule)을 적용할지 구체적인 결정을 한다.
 - 4. 방화벽에 실제 적용을 하고, 적용된 규칙을 검사한다.

NAT(Network Address Translation)

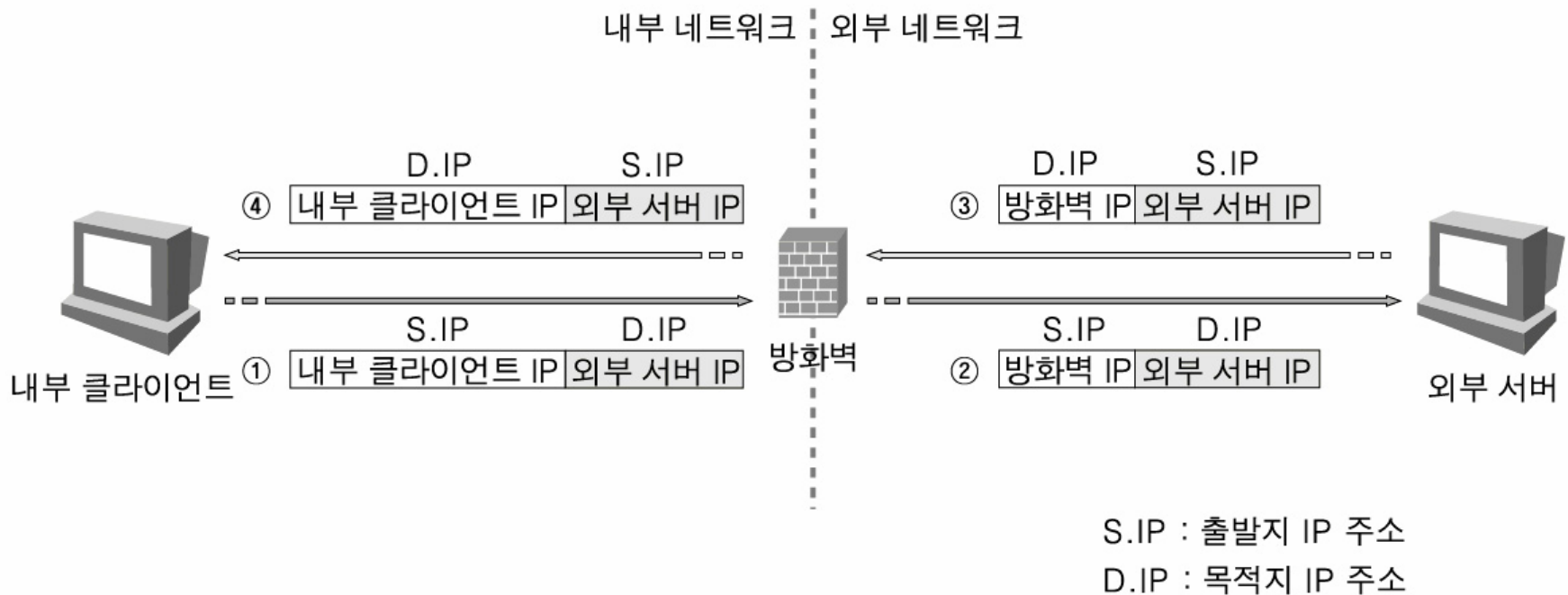
- 현재 가용 가능한 공인 주소의 부족문제를 해결하기 위해 개발된 기술 중 하나

- 내부 네트워크에서 시스템 사설 주소를 소유하고 있으나 외부로 접근할 때 라우팅이 가능한 외부 공인 주소를 NAT 규칙에 따라 할당 받아 접속

- NAT는 구현 방법에 따라 네 가지로 분류
 - Normal NAT
 - Reverse NAT
 - Redirect NAT
 - Exclude NAT

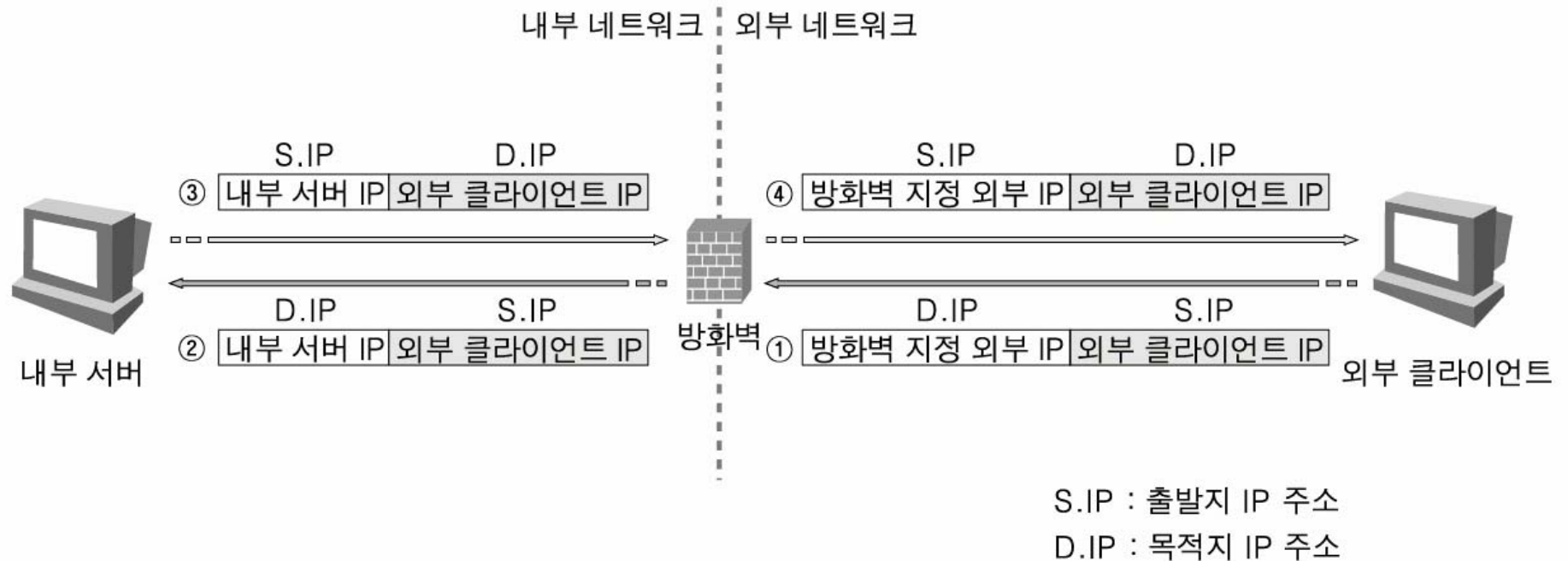
Normal NAT

□ 내부 사설 IP 주소를 가지고 있는 클라이언트가 외부로 접속을 하고자 할 때



Reverse NAT

□ 내부 네트워크에서 작동하는 서버에 외부 클라이언트 접속 시 동작



Redirect NAT & Exclude NAT

□ Redirect NAT

- Redirect NAT는 목적지 주소를 재지정할 때 사용
- 210.100.100.1로 사용되던 서버의 주소가 210.100.100.2로 바뀌게 되었을 경우, 210.100.100.1로 접속을 시도해온 패킷의 목적지 주소를 210.100.100.2로 바꾸어줌

□ Exclude NAT

- Normal NAT를 적용받지 않고 방화벽을 지나도록 설정
- 방화벽과 라우터 사이에 서버가 있는 경우와 같이 특정한 목적지에 대해서만 Normal NAT가 적용되지 않도록 설정 가능

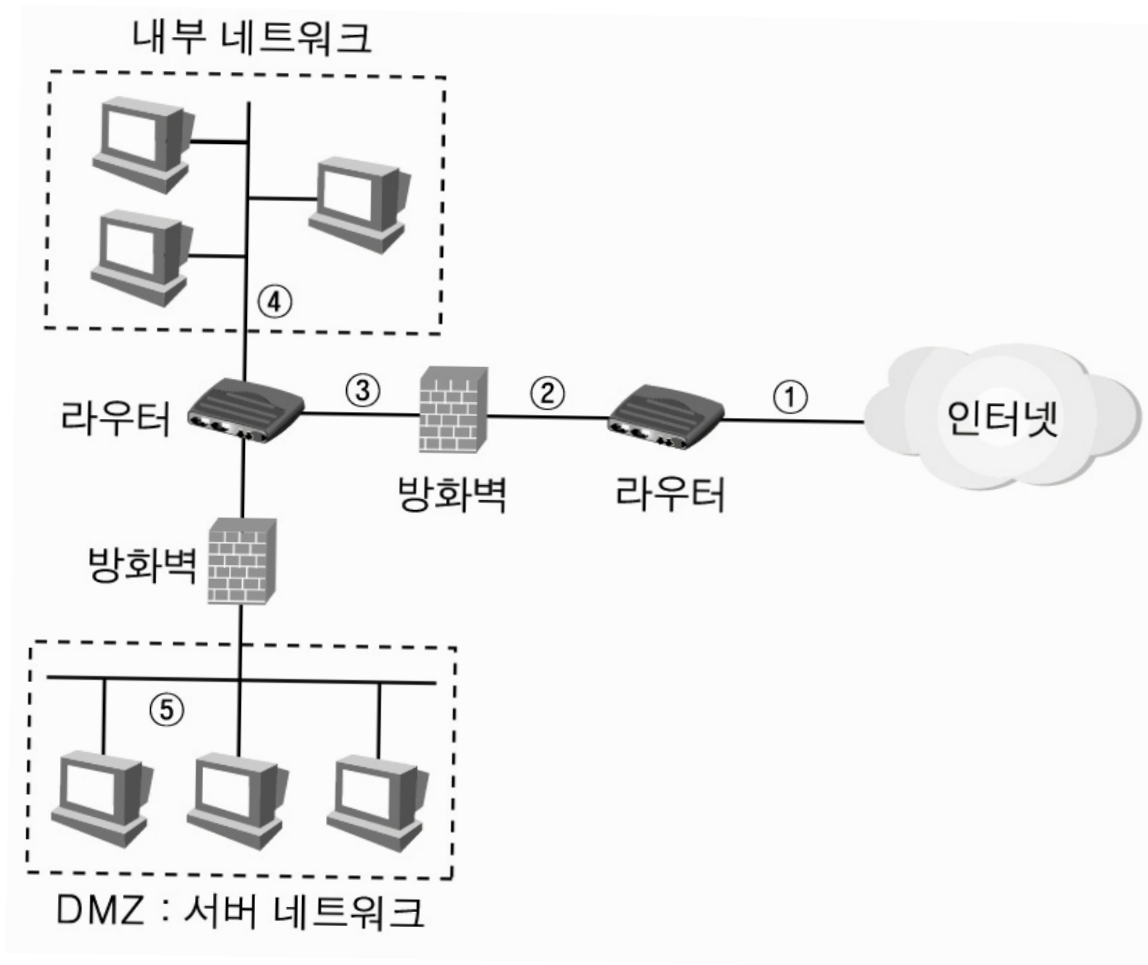
침입 탐지 시스템

- 네트워크에서 경찰과 같은 내부 감시자에 비유(침입에 대한 대응)

- IDS는 크게 네 가지 요소와 기능으로 구분된다.
 - 자료의 수집(Raw Data Collection)
 - 자료의 필터링과 축약(Data Reduction and Filtering)
 - 침입 탐지(Analysis and Intrusion Detection)
 - 책임 추적성과 대응(Reporting and Response)

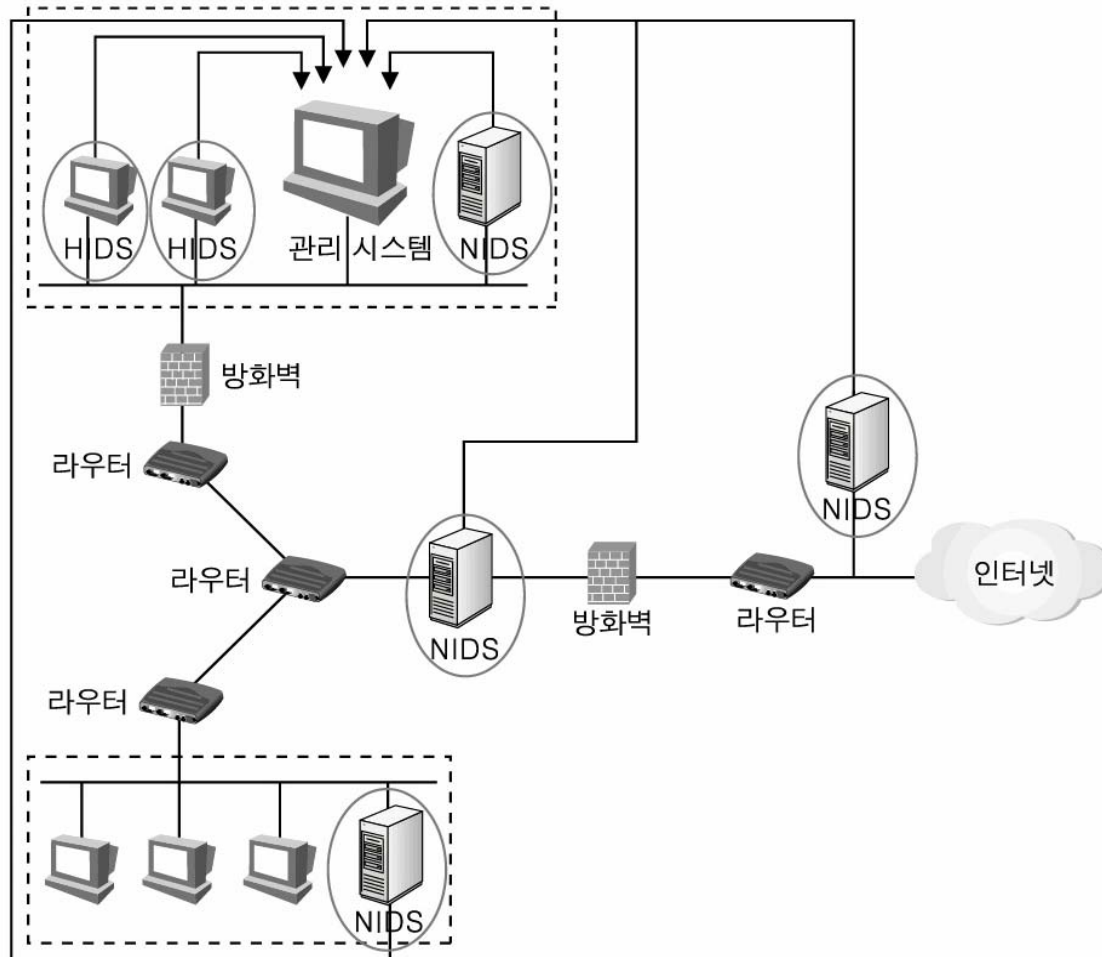
침입 탐지 시스템의 구조(1)

□ 침입 탐지 시스템의 설치 위치



침입 탐지 시스템의 구조(2)

□ 중앙 집중화된 IDS 관리



허니팟: Honey Pot (1)

- Honey Pot은 해커의 정보를 얻기 위한 하나의 개별 시스템
- 유인(Enticement) → 합법, 함정 (Entrapment) → 불법
- Honey Net은 Honey Pot을 포함한 하나의 네트워크
- 허니팟의 목적
 - 경각심(Awareness)
 - 정보(Information)
 - 연구(Research)

새로운 공격에 대해 대처할 수 있도록
하자는 데 초점

허니팟: Honey Pot (2)

□ 지원되어야 할 중요한 기능

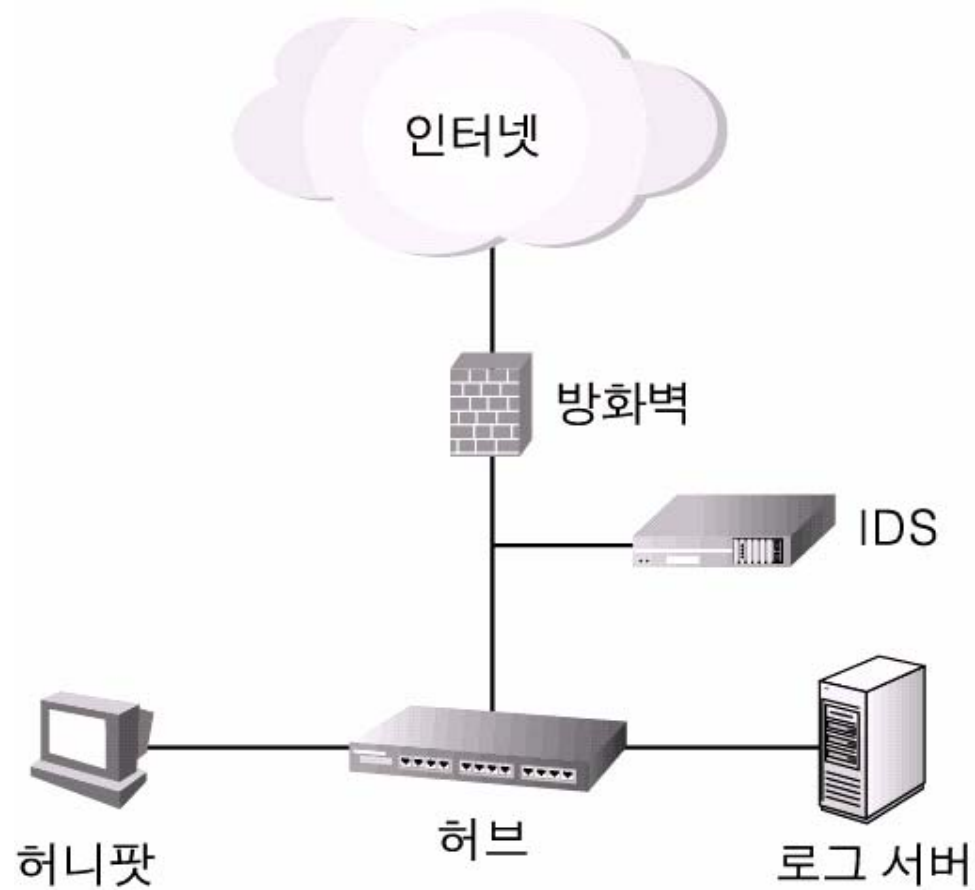
- 정보의 수집
- 시스템 제어

□ 허니팟의 요건

- 쉽게 해커에게 노출되어야 함
- 쉽게 해킹이 가능한 것처럼 취약해 보여야 함
- 시스템의 모든 구성 요소를 가지고 있어야 함
- 시스템을 통과하는 모든 패킷을 감시해야 함
- 시스템에 접속하는 모든 사람에 대해 관리자에게 알려야 함

허니팟: Honey Pot (3)

□ 허니넷의 구조



참고문헌

- 양대일, "정보보안 개론과 실습 시스템 해킹과 보안", 한빛 미디어, 2006.7
- 양대일, "정보보안 개론과 실습 네트워크 해킹과 보안", 한빛 미디어, 2005.8
- 최용락 외 3명, "컴퓨터 통신보안", 그린, 2006.1
- 홍승필, "유비쿼터스 컴퓨팅 보안", 한티미디어, 2006,9
- 박창섭, "암호이론과 보안", 대영사, 2006,2

질의응답

감사합니다