

네트워크 보안

2023. 07. 21 하계 워크샵 3주차 - [2]

한림대학교 정보과학대학 씨애랑

(HALLYM SECURITY TEAM SHIELD)



목차

- 스캐닝 (Scanning)
- 스니핑
- 스푸핑 (Spoofing)
- DoS 및 DDoS 공격



스캐닝 (SCANNING)

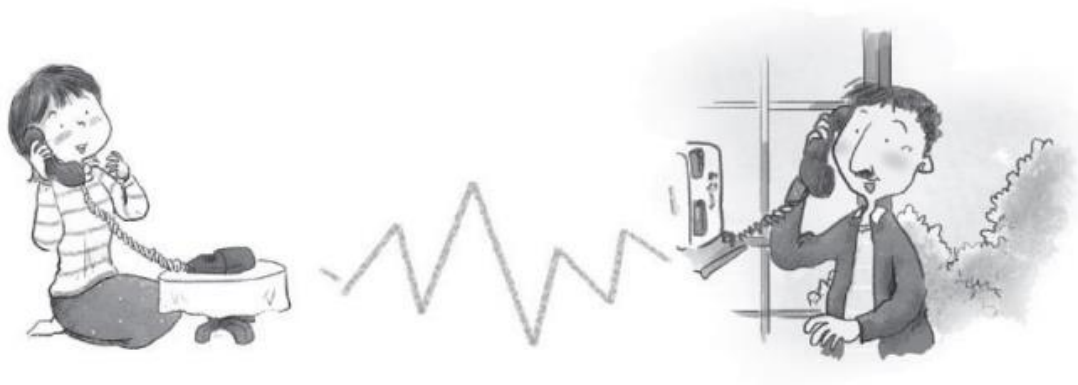
스캐닝 (Scanning)

■ 스캔 (Scan)

- 서비스를 제공하는 서버의 작동 여부와 서버가 제공하는 서비스를 확인하기 위한 작업
 - 전화를 걸었을 때 한쪽에서 '여보세요' 라고 말하면 다른 쪽도 '여보세요' 라고 말하며 서로를 확인하는 것과 같음.

■ Ping

- 네트워크와 시스템이 정상적으로 작동하는지 확인하기 위한 간단한 유틸리티
 - ICMP (Internet Control Message Protocol)를 사용하며, 기본적으로 TCP/IP 네트워크에서 사용



스캐닝 (Scanning)

■ ICMP 스캔

□ ICMP를 이용해 공격 대상 시스템의 활성화 여부를 알아보는 방법

- ① Echo Request (Type 8)와 Echo Reply (Type 0) 이용
- ② Timestamp Request (Type 13)와 Timestamp Reply (Type 14) 이용
- ③ Information Request (Type 15)와 Information Reply (Type 16) 이용
- ④ ICMP Address Mask Request (Type 17)와 ICMP Address Mask Reply (Type 18) 이용

→ 가장 일반적인 방법은 Echo Request (Type 8)와 Echo Reply (Type 0)



스캐닝 (Scanning)

■ ICMP 스캔

□ 윈도우에서의 실행 방법

- ① ICMP 패킷의 길이를 나타냄 (윈도우는 32바이트, 유닉스나 리눅스는 56바이트)
- ② 공격 대상에서 보내온 ICMP Echo Reply 패킷의 크기
- ③ Echo Request 패킷을 보낸 후 Reply 패킷을 받기까지의 시간
- ④ **TTL (Time To Live) 값**
- ⑤ Request 패킷의 개수, Reply 패킷의 개수, 손실된 패킷의 개수
- ⑥ Request 패킷을 보낸 후 Reply 패킷이 오기까지의 시간 정보

```
Administrator: C:\Windows\system32\cmd.exe
C:\W>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    5 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        6 Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\W>
```

윈도우 시스템에서 외부 특정 시스템으로 ping 을 실행한 결과



스캐닝 (Scanning)

■ ICMP 스캔

- Ping 실행 시 타겟 OS별 TTL 값

운영체제	ICMP Request 패킷 TTL	ICMP Reply 패킷 TTL
리눅스 커널 2.6	64	64
리눅스 커널 2.2-2.4	255	64
리눅스 커널 2.0	64	64
우분투	128	128
FreeBSD	255	255
솔라리스	255	255
HP-UX	255	255
윈도우 95	32	32
윈도우 98	128	32
윈도우 NT	128	32
윈도우 서버 2003, 2008, 2012	128	128
윈도우 10	64	64

운영체제별 TTL 값



스캐닝 (Scanning)

■ ICMP 스캔

- ICMP Echo Request 패킷이 막혔을 경우
 - ① Timestamp Request 패킷 이용
 - ② Information Request 패킷을 이용
 - ③ ICMP Address Mask Request와 Reply 패킷을 이용→ ICMP를 이용한 ping은 시스템 하나를 조사하기에 적절

운영체제	Information	Timestamp	Address Mask
리눅스 커널 2.2-2.6	×	○	×
FreeBSD	×	○	×
솔라리스	×	○	○
HP-UX	○	○	×
AIX v4	○	○	×
윈도우 98	×	○	○
윈도우 NT sp4	×	×	×
윈도우 2000 이상	×	○	×

운영체제별 Non Echo ICMP 패킷의 작동 여부

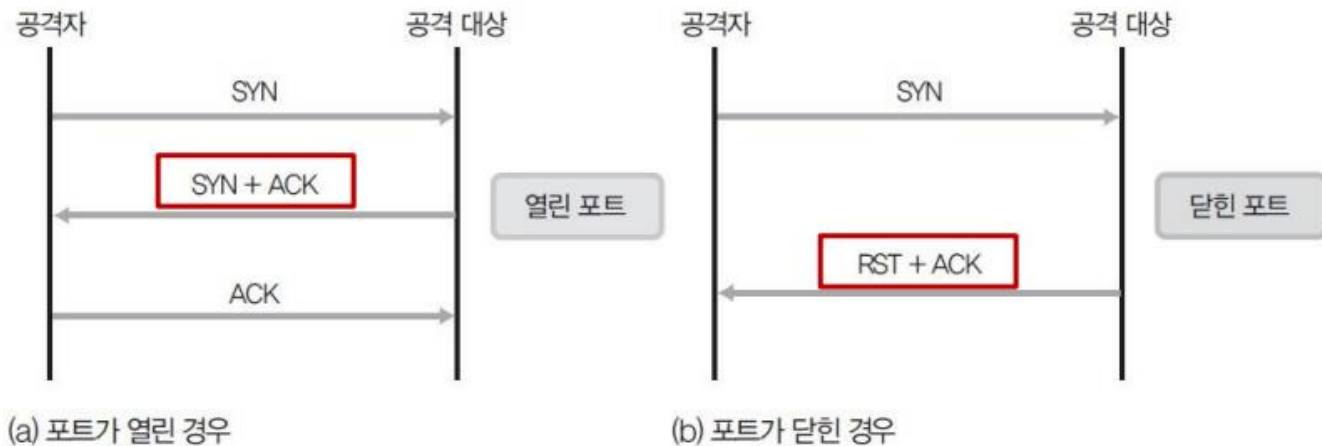


스캐닝 (Scanning)

■ TCP 및 UDP를 이용한 스캔

□ TCP Open 스캔

- TCP를 이용한 가장 기본적인 스캔



TCP Open 스캔



스캐닝 (Scanning)

■ TCP 및 UDP를 이용한 스캔

□ 스텔스 (Stealth) 스캔

- 로그를 남기지 않는 것만이 아니라, 공격 대상을 속이고 자 신의 위치를 숨기는 스캔 모드를 통칭
- 대표적인 경우로 TCP Half Open 스캔이 있음.



TCP Half Open 스캔

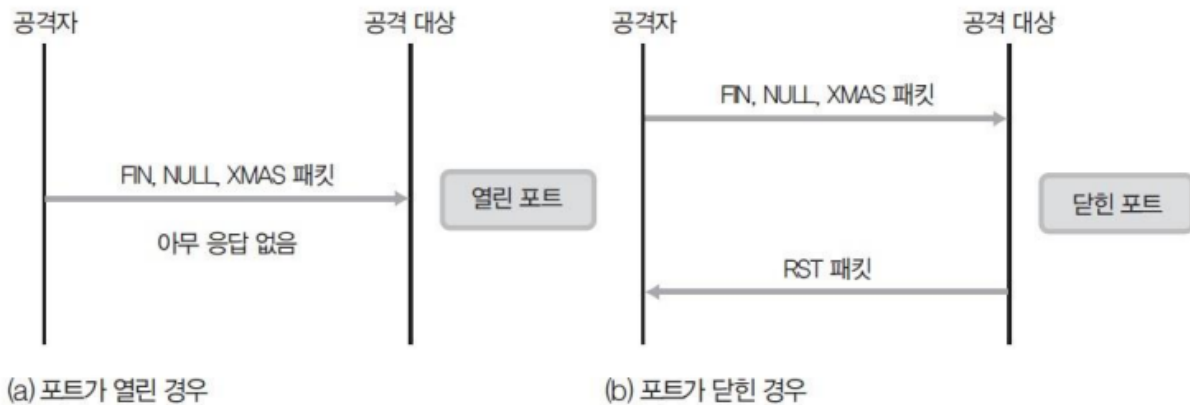


스캐닝 (Scanning)

■ TCP 및 UDP를 이용한 스캔

□ 스텔스 (Stealth) 스캔

- FIN (Finish) 스캔 : 포트가 열린 경우 응답이 없고, 닫힌 경우 RST 패킷이 돌아옴
- NULL 스캔 : 플래그(Flag) 값을 설정하지 않고 보낸 패킷
- XMAS 스캔 : ACK, FIN, RST, SYN, URG 플래그 모두를 설정 하여 보낸 패킷



FIN, NULL, XMAS 스캔



스캐닝 (Scanning)

■ TCP 및 UDP를 이용한 스캔

- ACK 패킷을 이용한 스캔
 - 모든 포트에 ACK 패킷을 보낸 후, 응답 RST 패킷 분석
 - 포트가 열린 경우, TTL 값이 64이하인 RST 패킷 또는 윈도우 가 0이 아닌 임의의 값을 가진 RST 패킷이 돌아옴.
 - 닫힌 경우엔 TTL 값이 일정하게 큰 값이며, 윈도우 크기가 0인 RST 패킷
- TCP 패킷을 이용한 스캔
 - 모든 시스템에 동일하게 적용되지 않으며, 많이 알려져서 거의 적용되지 않음
 - SYN 패킷을 이용한 스캔 방법은 세션을 성립하기 위한 정당한 패킷과 구별할 수 없기 때문에 아직도 유효함.

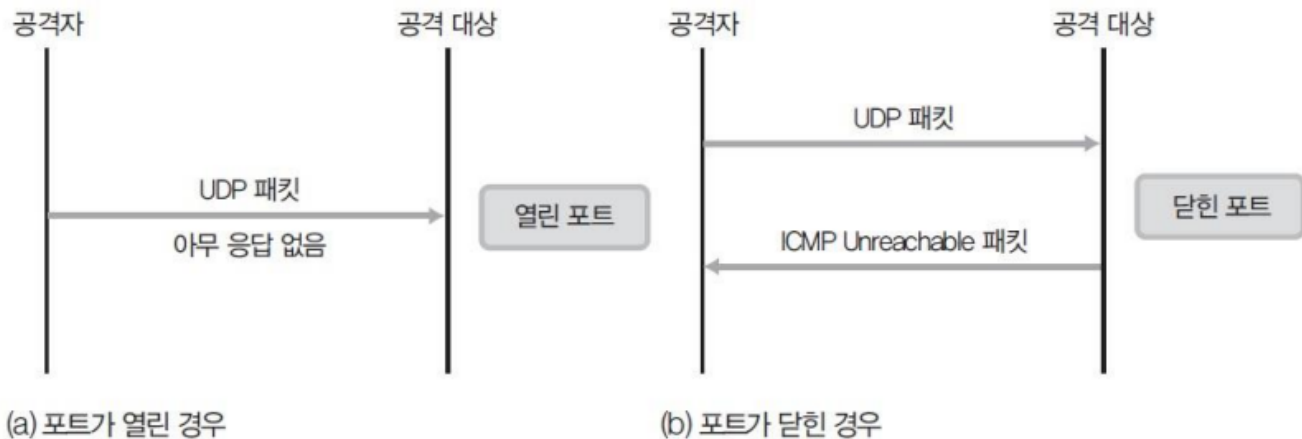


스캐닝 (Scanning)

■ TCP 및 UDP를 이용한 스캔

□ UDP 스캔

- 포트가 닫힌 경우 공격 대상이 ICMP Unreachable 패킷을 보 내지만, 열린 경우에는 보내지 않음



UDP 포트 스캔



스니핑

스니핑 공격

■ 스니핑 개념

- 도청 (Eavesdropping)과 엿듣기가 스니핑
- 전화선이나 UTP에 탭핑 (Tapping)해서 전기 신호를 분석하여 정보를 찾아냄
- 전기 신호를 이용해 분석하는 일



스니핑 공격

■ 프러미스큐어스 모드 (Promiscuous Mode)

- MAC 주소와 IP 주소에 관계없이 모든 패킷을 스니퍼에게 넘겨주는 것
- 리눅스나 유닉스 등의 운영체제에서는 랜 카드에 대한 모드 설정이 가능

■ TCP Dump

- 리눅스에서 가장 기본이 되는 스니핑 툴
- 처음에는 네트워크 관리를 위해 개발되었기 때문에 관리자 느낌이 강함
- TCP Dump로 획득한 증거 자료는 법적 효력이 있음



스니핑 공격

■ Fragrouter

- 스니핑을 보조해주는 툴로, 받은 패킷들을 기존 송신 자에게 정상적으로 전달하는 역할
- 스니핑을 하거나 세션을 가로챘을 때,
 - 공격자에게 온 패킷을 정상적으로 전달하기 위해서는 패킷 릴레이 기능이 반드시 필요함

```
root@kali:~# fragrouter
Version 1.6
Usage: fragrouter [-i interface] [-p] [-g hop] [-G hopcount] ATTACK

where ATTACK is one of the following:

-B1: base-1: normal IP forwarding
-F1: frag-1: ordered 8-byte IP fragments
-F2: frag-2: ordered 24-byte IP fragments
-F3: frag-3: ordered 8-byte IP fragments, one out of order
-F4: frag-4: ordered 8-byte IP fragments, one duplicate
-F5: frag-5: out of order 8-byte fragments, one duplicate
-F6: frag-6: ordered 8-byte fragments, marked last frag first
-F7: frag-7: ordered 16-byte fragments, fwd-overwriting
-T1: tcp-1: 3-whs, bad TCP checksum FIN/RST, ordered 1-byte segments
-T3: tcp-3: 3-whs, ordered 1-byte segments, one duplicate
-T4: tcp-4: 3-whs, ordered 1-byte segments, one overwriting
-T5: tcp-5: 3-whs, ordered 2-byte segments, fwd-overwriting
-T7: tcp-7: 3-whs, ordered 1-byte segments, interleaved null segments
-T8: tcp-8: 3-whs, ordered 1-byte segments, one out of order
-T9: tcp-9: 3-whs, out of order 1-byte segments
-C2: tcbl-2: 3-whs, ordered 1-byte segments, interleaved SYN's
-C3: tcbl-3: ordered 1-byte null segments, 3-whs, ordered 1-byte segments
-R1: tcbl-1: 3-whs, RST, 3-whs, ordered 1-byte segments
-I2: ins-2: 3-whs, ordered 1-byte segments, bad TCP checksums
-I3: ins-3: 3-whs, ordered 1-byte segments, no ACK set
-M1: misc-1: Windows NT 4 SP2 - http://www.dataprotect.com/ntfrag/
-M2: misc-2: Linux IP chains - http://www.dataprotect.com/ipchains/
```



스니핑 공격

■ Dsniff (디스니프)

- 스니핑을 위한 다양한 툴들이 패키지로 구성되어 만 들어진 것
 - 대표적인 스니핑 툴로 알려져 있음 암호화된 계정과 패스워드까지 읽어낼 수 있음.

ftp, telnet, http, pop, nntp, imap, snmp, ldap, rlogin, rip, ospf, pptp, ms-chap, nfs, yp/nis+, socks, x11, cvs, IRC, ATM, ICQ, PostageSQL, Citrix ICA, Symantec pcAnywhere, MS SQL, auth, info

Dsniff가 읽어낼 수 있는 패킷

툴	기능
filesnarf	NFS 트래픽에서 스니핑한 파일을 현재 디렉토리에 저장한다.
macof	스위치 환경에서 스위치를 허브와 같이 작동시키기 위하여 임의의 MAC 주소로 스위치의 MAC 테이블을 오버플로우(overflow)시킨다.
mailsnarf	SNMP와 POP 트래픽을 스니핑하여 이메일을 볼 수 있게 한다. 스니핑한 이메일은 mail 클라이언트로 볼 수 있다.
msgsnarf	AOL 메신저, ICQ 2000, IRC, Yahoo 메신저 등의 채팅 메시지를 선택하여 스니핑한다.
tcpskill	특정 인터페이스를 통해 탐지할 수 있는 TCP 세션을 모두 끊는다.
tcpsniff	ICMP source quench 메시지를 보내 특정 TCP 연결을 느리게 만든다. 속도가 빠른 네트워크에서 스니핑을 할 때 유용하다.
arpspoof	ARP 스푸핑 공격을 실행한다.
dnsspoof	DNS 스푸핑 공격을 실행한다.
urlsnarf	CLF(Common Log Format)에서 HTTP 트래픽을 스니핑하여 선택된 URL을 알려준다.

Dsniff 에 포함된 툴



스니핑 공격

■ 스위칭 환경과 스니핑

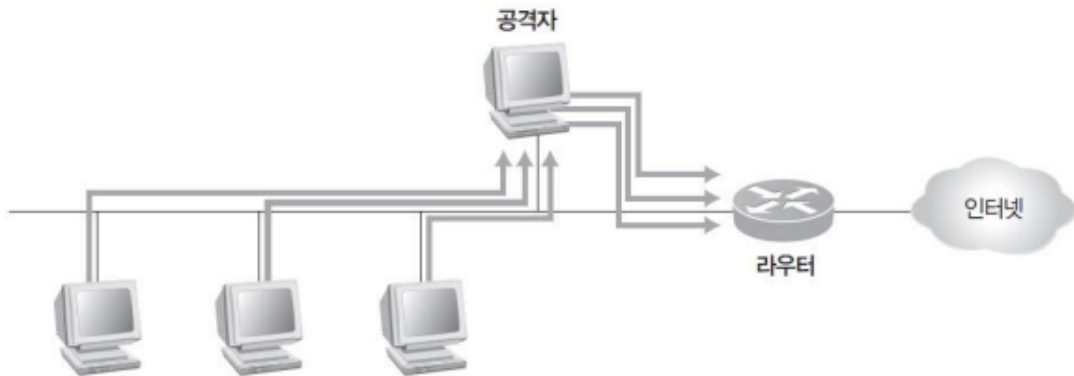
- 스위치는 각 장비의 MAC 주소를 확인하여 포트 할당
- 자신에게 향하지 않은 패킷 외에는 받아볼 수 없어 스니핑을 막게 됨
 - 즉, 스위치가 스니핑을 막기 위해 만들어진 장비는 아니지만 결과적으로는 저지할 수 있는 유용한 장비가 됨.
 - (공격자 입 장에서는 치명적인 장비)



스니핑 공격

■ ARP 리다이렉트와 ARP 스푸핑

- 공격자가 자신을 라우터라고 속이는 것
 - 기본적으로 2계층 공격으로, LAN에서 공격
- 공격자는 원래 라우터의 MAC 주소를 알아야 하며, 받은 모든 패킷들은 다시 라우터로 릴레이 해줘야 함
 - ARP 스푸핑은 호스트 대 호스트 공격, ARP 리다이렉트는 랜의 모든 호스트 대 라우터라는 점 외에는 큰 차이가 없음.



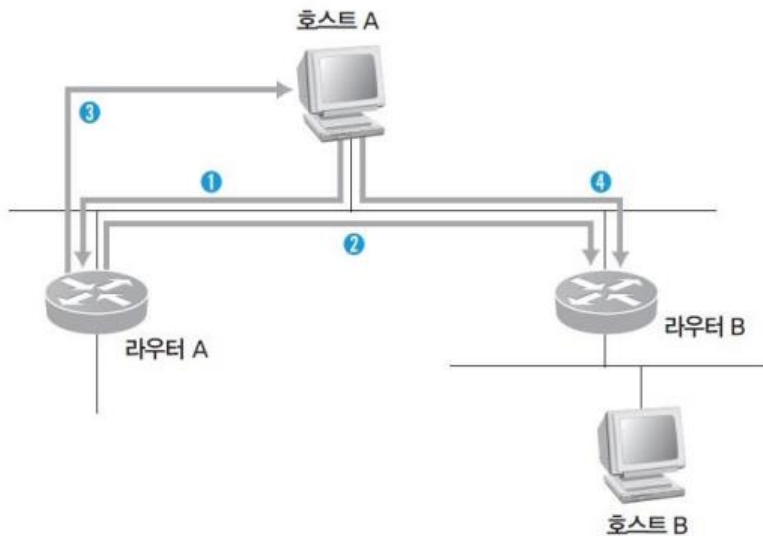
ARP 리다이렉트 개념도



스니핑 공격

■ ICMP 리다이렉트

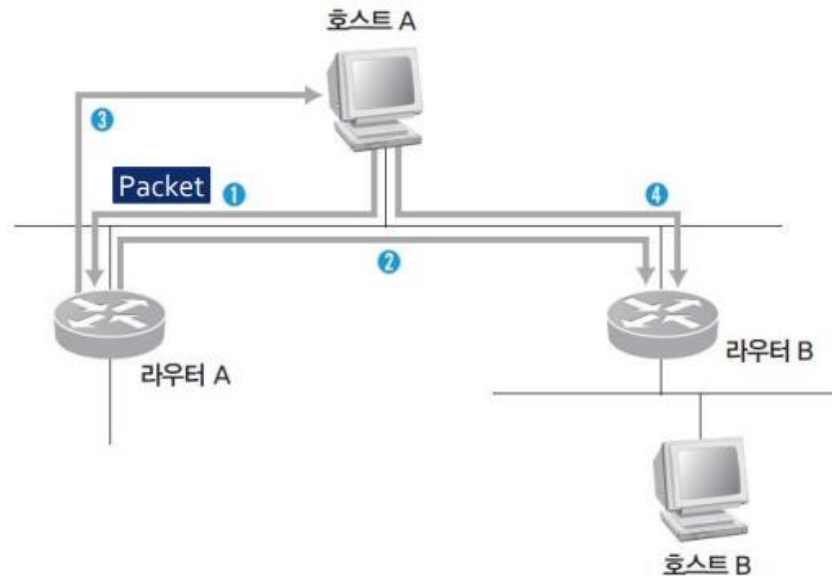
- 공격 대상에게 패킷을 보낸 후 라우터 A에 다시 릴레이시켜 스니핑함.
- 3계층에서 패킷을 주고받기 때문에 랜이 아니더라도 공격이 가능



스니핑 공격

■ ICMP 리다이렉트 동작

1. 호스트 A에 라우터 A가 기본 라우터로 설정되어 있으며,
 - 이로 인해 호스트 A가 호스트 B로 데이터를 보낼 때 패킷을 라우터 A로 보냄

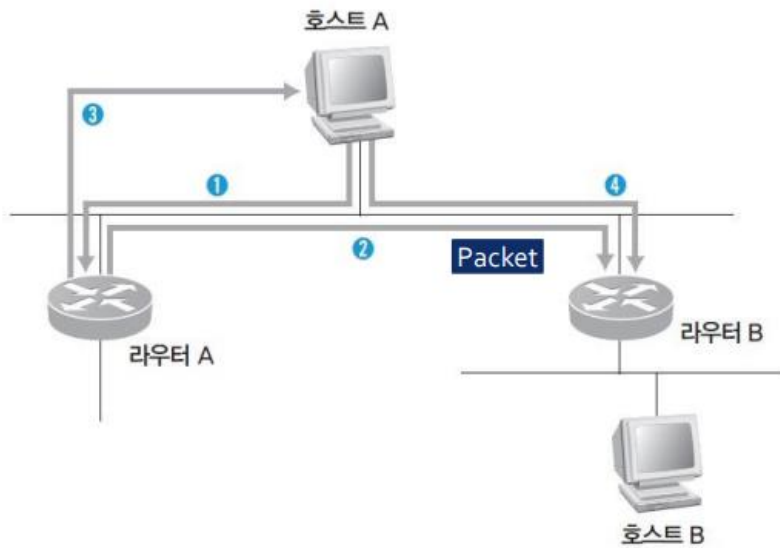


스니핑 공격

■ ICMP 리다이렉트 동작

2. 라우터 A는 호스트 B로 보내는 패킷을 수신

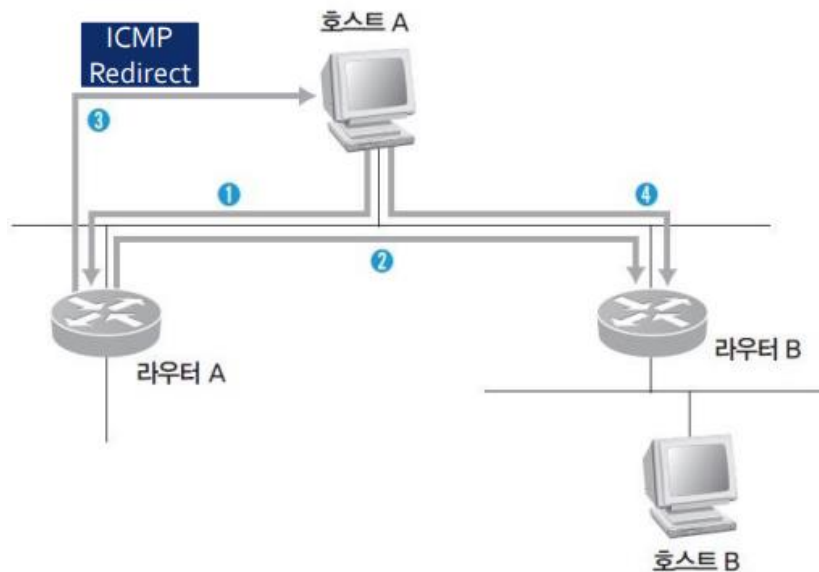
- 라우터 A는 라우팅 테이블을 검색하여 자신을 이용하는 것 보다 라우터 B를 이용하는 것이 더 효율적이라고 판단
- 해당 패킷을 라우터 B로 전송



스니핑 공격

■ ICMP 리다이렉트 동작

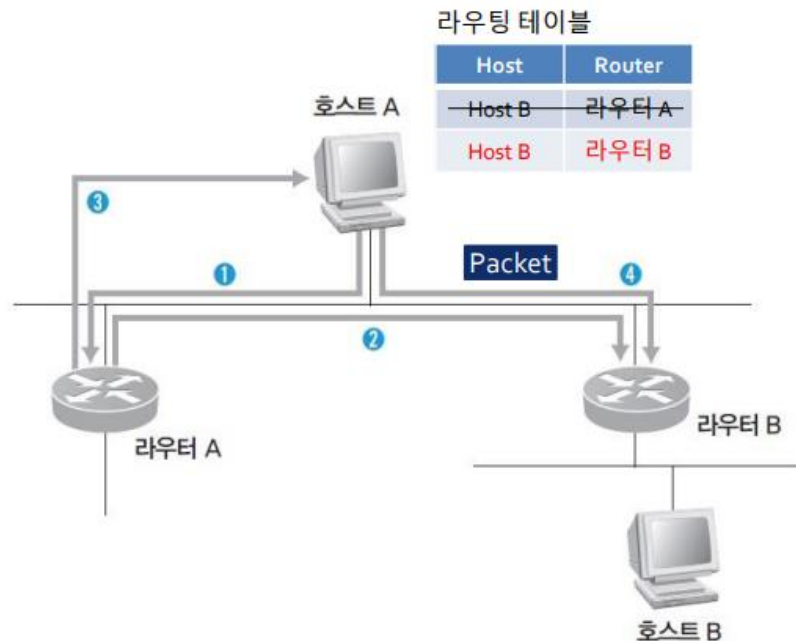
3. 라우터 A는 호스트 A에게 ICMP 리다이렉트 패킷을 전송
- 호스트 A가 호스트 B로 보내는 패킷이 라우터 B로 바로 향 하도록 함



스니핑 공격

■ ICMP 리다이렉트 동작

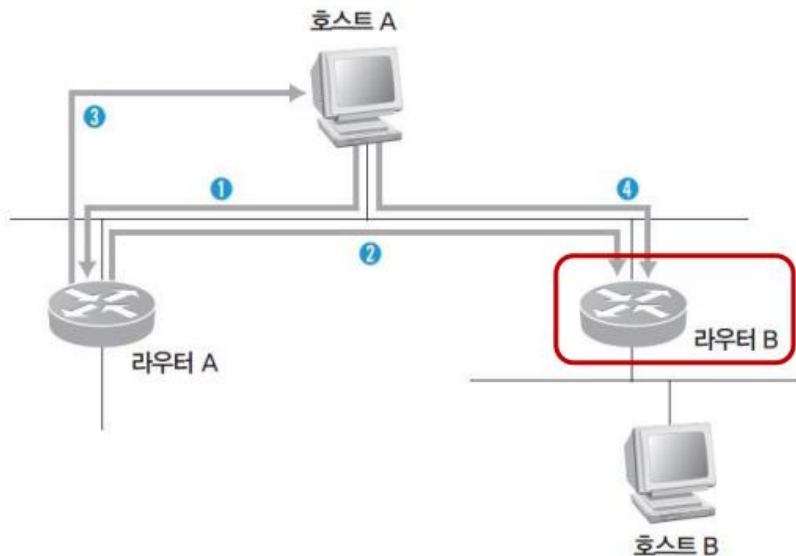
4. 호스트 A는 라우팅 테이블에 호스트 B를 추가하고, 향후 호스트 B로 보내는 패킷은 라우터 B로 전달



스니핑 공격

■ ICMP 리다이렉트 공격

- 공격자가 라우터 B가 되어, ICMP 리다이렉트 패킷도 공격 대상 (호스트 A)에
 - 보낸 후 라우터 A에 다시 릴레이 시켜주면 모든 패킷을 스니핑 할 수 있음.



스니핑 공격

■ 스위치 재밍(Switch Jamming)

- 스위치를 직접 공격
 - 스위치의 MAC 테이블을 위한 캐시 공간에 버퍼 오버 플로우 공격을 수행
 - MAC 테이블의 저장 공간을 모두 사용하여 (의미없는 값들로 저장) 스위치를 허브와 같은 기능만을 사용하도록 하는 공격
 - 최근에는 많은 스위치들이 MAC 테이블의 캐시와 연산 장치가 사용하는 캐시가 독립적으로 나뉘어 있어
 - 스위치 재밍 공격이 통하지 않음.



스푸핑 (SPOOFING)

스푸핑 (Spoofing)

■ 스푸핑 공격에 대한 이해

- 스푸핑 (Spoofing) - '속이다'를 의미함.
 - 인터넷이나 로컬에서 존재하는 모든 연결에 스푸핑 가능
 - 정보를 얻어내기 위한 중간 단계의 기술로 사용하는 것 외에 시스템을 마비시키는 데 사용할 수도 있음.
- 스푸핑 공격 대비책
 - 관리하는 시스템의 MAC 주소를 확인하여 테이블로 만들어 둬.
 - 브로드캐스트 ping을 네트워크에 뿌려 그에 답하는 모든 시스템에 대한 MAC 주소 값을 시스템 캐시에 기록함.
 - - arp -a로 현재 IP 주소 값과 MAC 주소의 대칭 값 비교하여 엉뚱한 MAC 주소로 맵핑되어 있는 항목을 확인



스푸핑 (Spoofing)

■ 스푸핑 공격 실습

- 공격자 시스템 : 리눅스 우분투 데스크탑
- 필요 프로그램 : fping
 - ping과 마찬가지로 ICMP (인터넷 제어 메시지 프로토콜) echo request 를 네트워크 호스트에 보내는 도구
 - 여러 호스트에 ping message를 전송할 때 일반적으로 사용
 - fping은 명령어 입력 시,
 - 호스트 수를 정의하거나 IP 주소 또는 호스트 목록이 있는 파일을 지정할 수 있다는 점에서 ping 과는 차이점이 있음.

옵션

- a : ping에 응답한 장비만 나타냄
- g : ping sweep할 IP주소의 범위
- q : 결과 값에서 Echo Request 를 숨김
- 4 : IPv4주소를 이용하여 전송
- 6 : Ipv6주소를 이용하여 전송

```
wishfree@ubuntu-14: ~  
wishfree@ubuntu-14:~$  
wishfree@ubuntu-14:~$ fping -a -g 192.168.0.1/24  
192.168.0.1  
192.168.0.2  
192.168.0.100  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.3  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.4  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.5  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.6  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.7  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.8  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.9  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.10  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.11  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.12  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.13  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.14  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.15  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.16  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.17  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.18  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.19  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.20
```

192.168.0.1/24 네트워크에 브로드캐스트로 icmp message 보내기



스푸핑 (Spoofing)

■ 스푸핑 공격 실습 (IP 및 MAC 주소 수집)

□ fping

- fping 설치가 되어 있지 않을 경우 - > apt-get install fping 을 통해 fping 설치

```
root@IVNSEC-VM: /home/user
File Edit View Search Terminal Help

inet 192.168.43.129 netmask 255.255.255.0 broadcast 192.168.43.255
inet6 fe80::4396:568:5f7f:2dff prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:74:a8:1f txqueuelen 1000 (Ethernet)
RX packets 826763 bytes 859359377 (859.3 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 374283 bytes 38035649 (38.0 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 107480 bytes 74973635 (74.9 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 107480 bytes 74973635 (74.9 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@IVNSEC-VM:/home/user# fping

Command 'fping' not found, but can be installed with:

apt install fping

root@IVNSEC-VM:/home/user# apt-get install fping
```



스푸핑 (Spoofing)

■ 스푸핑 공격 실습 (IP 및 MAC 주소 수집)

□ fping

- fping 사용 전, '>arp -a' 를 통해 현재 호스트에 MAC 주소 및 IP 주소가 매핑된 테이블이 존재하는지 확인

```
root@IVNSEC-VM: /home/user
File Edit View Search Terminal Help
oot@IVNSEC-VM:/home/user# arp -a
gateway (192.168.43.2) at 00:50:56:ea:78:15 [ether] on ens33
(192.168.43.254) at 00:50:56:e3:9f:c2 [ether] on ens33
oot@IVNSEC-VM:/home/user#
```



스푸핑 (Spoofing)

■ 스푸핑 공격 실습 (IP 및 MAC 주소 수집)

□ fping

- fping 을 이용한 브로드캐스트 ping 보내기 > `fping -a -g 192.168.0.1/24`

```
root@IVNSEC-VM: /home/user
File Edit View Search Terminal Help
root@IVNSEC-VM:/home/user#
root@IVNSEC-VM:/home/user# fping -a -g 192.168.43.1/24
192.168.43.1
192.168.43.2
192.168.43.129
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.4
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.4
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.3
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.3
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.7
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.7
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.6
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.6
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.5
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.5
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.10
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.10
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.9
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.9
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.8
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.8
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.13
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.13
ICMP Host Unreachable from 192.168.43.129 for ICMP Echo sent to 192.168.43.12
```

192.168.43.1/24 네트워크에 ping 보내기

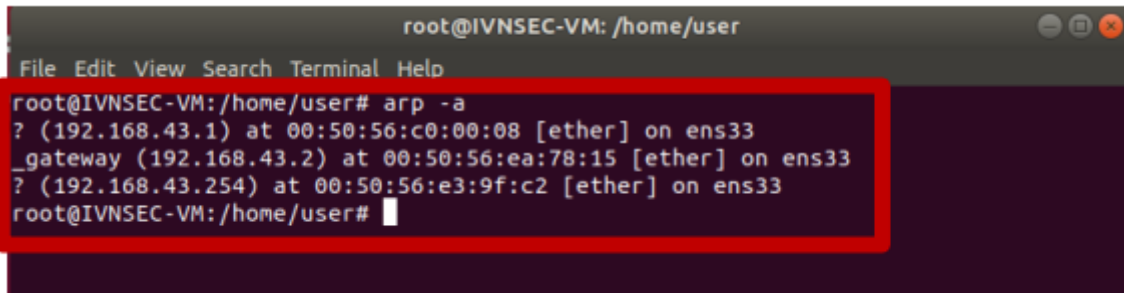


스푸핑 (Spoofing)

■ 스푸핑 공격 실습 (IP 및 MAC 주소 수집)

□ fping

- Arp -a를 이용하여 MAC address와 IP address 리스트 확인



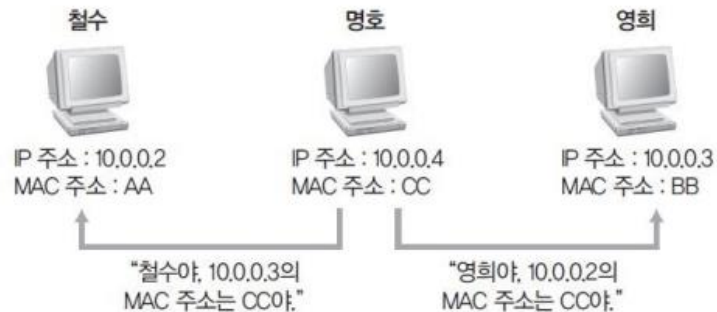
```
root@IVNSEC-VM: /home/user
File Edit View Search Terminal Help
root@IVNSEC-VM:/home/user# arp -a
? (192.168.43.1) at 00:50:56:c0:00:08 [ether] on ens33
_gateway (192.168.43.2) at 00:50:56:ea:78:15 [ether] on ens33
? (192.168.43.254) at 00:50:56:e3:9f:c2 [ether] on ens33
root@IVNSEC-VM:/home/user#
```



스푸핑 (Spoofing)

■ ARP 스푸핑에 대한 이해

- MAC 주소를 속이는 것
 - (2계층에서 작동해 공격 대상이 같은 랜에 있어야 함.)



ARP 스푸핑 예

호스트 이름	IP 주소	MAC 주소
철수	10.0.0.2	AA
영희	10.0.0.3	BB
명호	10.0.0.4	CC



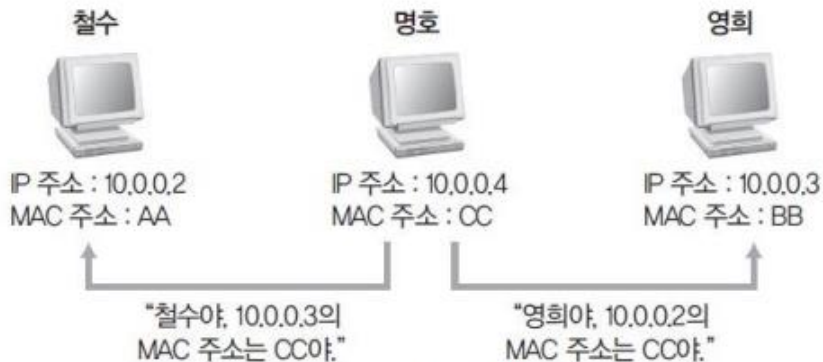
스푸핑 (Spoofing)

■ ARP 스푸핑에 대한 이해

□ MAC 주소를 속이는 것

- 필수) 2계층에서 작동해 공격 대상이 같은 랜에 있어야 함
- ARP 스푸핑 순서

- 1) 명호는 철수에게 영희 (IP 주소 10.0.0.3)의 MAC주소가 명호 자신의 MAC 주소인 CC라고 알림. 마찬가지로, 영희에게도 철수 (IP 주소 10.0.0.2)의 MAC 주소가 CC라고 알림
- 2) 명호는 철수와 영희로부터 패킷을 전달 받음
- 3) 명호는 각자 철수와 영희에게 받은 패킷들을 읽은 후에 철 수가 영희에게 보내려던 패킷을 영희에게 보내주고, 영희가 철수에게 보내려던 패킷을 철수에게 정상적으로 전송함



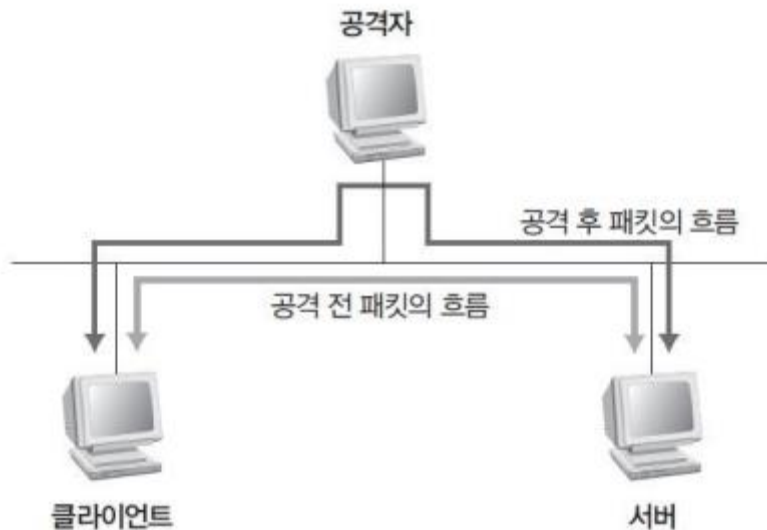
ARP 스푸핑 예



스푸핑 (Spoofing)

■ ARP 스푸핑에 대한 이해

- ARP 스푸핑 : 스니핑에서의 공격 흐름과 유사함



ARP 스푸핑 공격의 개념도



스푸핑 (Spoofing)

■ IP 스푸핑

- IP 스푸핑에 대한 이해
 - 트러스트(Trust)
 - 시스템에 접속할 때 자신의 IP 주소로 인증하면 로그인 없이 접속이 가능하게 만든 것
 - (스니핑은 막을 수 있지만, IP만 일치하면 인증 우회가 가능)
 - SSO (Single Sign On) : 트러스트에 대한 약점이 알려지면서 개발됨.
 - 대표적인 예는 커beros(Kerberos)를 쓰는 윈도우의 액티브 디렉토리, 썬 마이크로시스템즈의 NIS+ 등이 있음
 - 트러스트의 설정과 역할
 - ./etc/hosts.equiv : 시스템 전체에 영향을 미침
 - ~/.\$HOME/.rhost : 사용자 한 사람에 귀속하는 파일

형식	내용
host_name	host_name의 접근을 허용한다.
host_name user_name	user_name에 대한 host_name의 접근을 허용한다.
+	모든 시스템의 접근을 허용한다.
+ user_name	user_name에 대한 모든 시스템의 접근을 허용한다.
- host_name	host_name의 접근을 차단한다.
host_name - user_name	user_name에 대한 host_name의 접근을 차단한다.
+ @netgroup	netgroup에 대한 모든 시스템의 접근을 허용한다.



스푸핑 (Spoofing)

■ IP 스푸핑

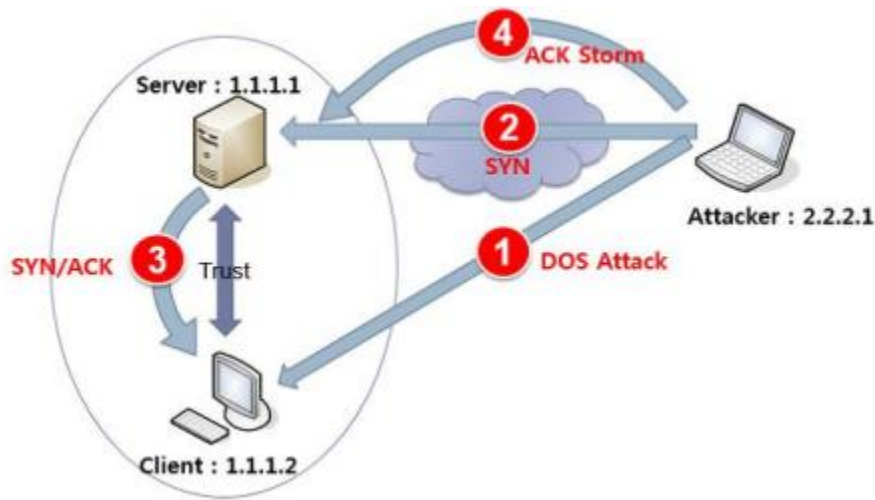
- IP 주소를 속이는 것
- 최근에는 계정의 패스워드가 같아야만 패스워드를 묻지 않도록 변경되었고,
 - SSH를 사용하도록 권고하기 때문에 IP 스푸핑 공격이 이루어지지 않음.



스푸핑 (Spoofing)

■ IP 스푸핑 - 원격지에서의 IP 스푸핑

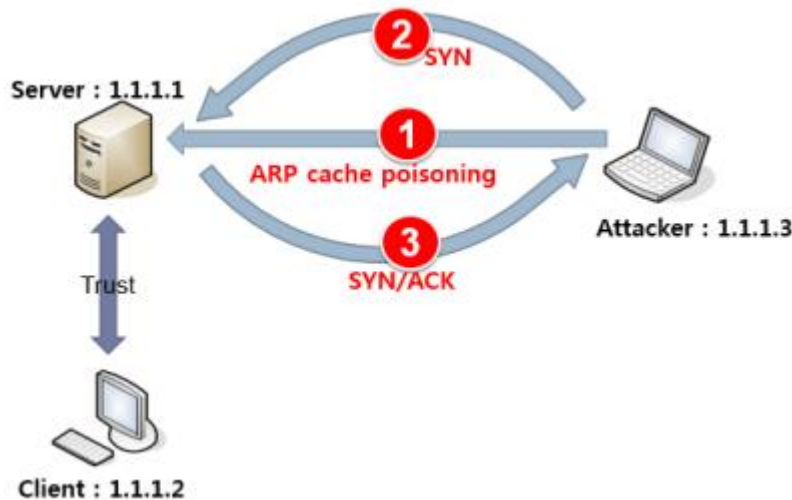
1. 공격자는 클라이언트에 TCP SYN flooding 공격
2. 공격자는 클라이언트의 IP로 서버에 연결 요청
3. 서버는 클라이언트에서 온 패킷으로 알고, 클라이언트에 SYN/ACK 패킷을 전송
4. 공격자는 클라이언트에서 ACK 패킷을 보낸 것처럼 속이면서 IP 스푸핑 공격으로 서버를 속임



스푸핑 (Spoofing)

■ IP 스푸핑 - 내부 네트워크에서의 IP 스푸핑

1. 서버에게 공격자를 클라이언트로 인식시키기 위해 공격자가 서버로 ARP Cache Poisoning 공격을 수행
2. 서버에게 SYN 패킷을 전송
3. 서버는 1.1.1.2라는 주소에게 응답을 하지만 ARP 공격으로 인해 MAC 주소를 잘못 저장하고 있음
 - 클라이언트가 아닌 공격자에게 SYN/ACK 패킷을 전달함



스푸핑 (Spoofing)

■ IP 스푸핑

- IP 스푸핑의 보안 대책
 - 가장 좋은 보안 대책은 트러스트를 사용하지 않는 것
 - 트러스트를 사용해야 한다면 트러스트된 시스템의 MAC 주소를 static으로 지정



DOS 및 DDOS 공격

DoS 및 DDoS 공격

■ DoS 공격에 대한 이해

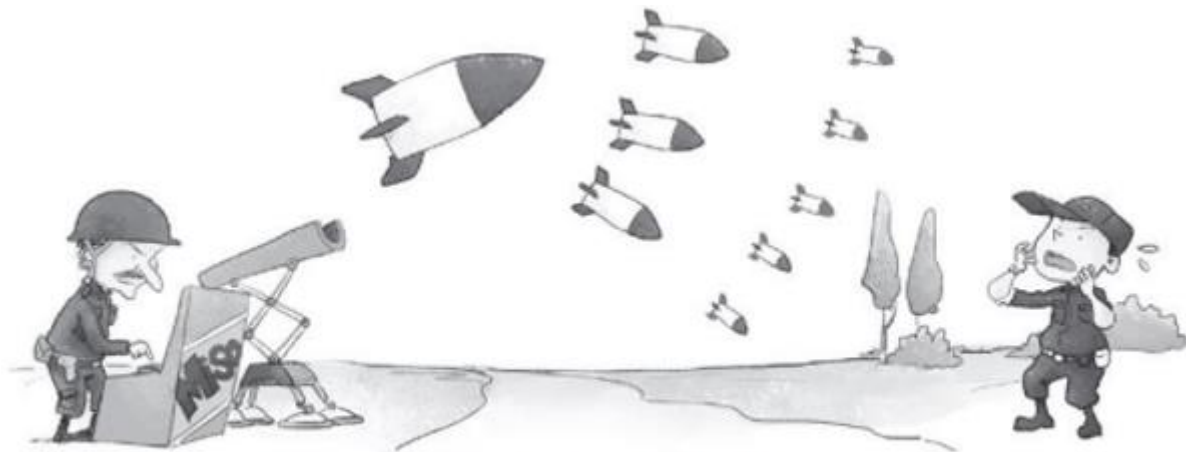
- DoS (Denial of Service, 서비스 거부)
 - 공격 대상이 수용할 수 있는 능력 이상의 정보를 제공하거나 사용자 또는 네트워크 용량을 초과시켜
 - 정상적으로 작동하지 못하게 하는 공격
 - DoS 공격의 특징
 - 파괴 공격 : 디스크, 데이터, 시스템 파괴
 - 시스템 자원 고갈 공격 : CPU, 메모리, 디스크의 과다한 사용 으로 인한 부하 가중
 - 네트워크 자원 고갈 공격 : 쓰레기 데이터로 네트워크 대역 폭의 고갈



DoS 및 DDoS 공격

■ Ping of Death 공격

1. ping을 이용하여 ICMP 패킷의 크기를 정상보다 아주 크게 만듦.
2. 크게 만들어진 패킷은 네트워크를 통해 라우팅되어 공격 네트워크에 도달하는 동안 아주 작은 조각으로 쪼개짐.
3. 공격 대상은 조각화된 패킷을 모두 처리해야 하므로 정상적인 ping보다 부하가 훨씬 많이 걸림.



Ping of Death 공격의 개념

DoS 및 DDoS 공격

■ Ping of Death 공격

□ 패킷 분할



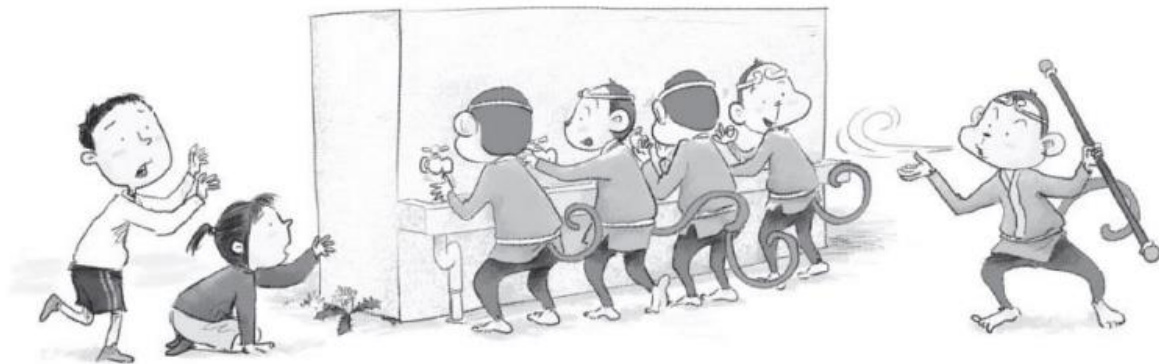
- ICMP 패킷의 최대 길이를 65,500바이트로 임의로 설정
- 최대 크기인 65,500바이트로 네트워크에 ping을 보내면 패킷은 전송에 적절한 크기로 분할
- 패킷이 지나가는 네트워크의 최대 전송 가능 길이가 100바이트라면 패킷 하나가 655개로 분할



DoS 및 DDoS 공격

■ SYN Flooding

- 서버별로 한정되어 있는 접속 가능 공간에 존재하지 않는 클라이언트가 접속한 것처럼 속여 다른 사용자가 서비스를 제공받지 못하게 하는 것



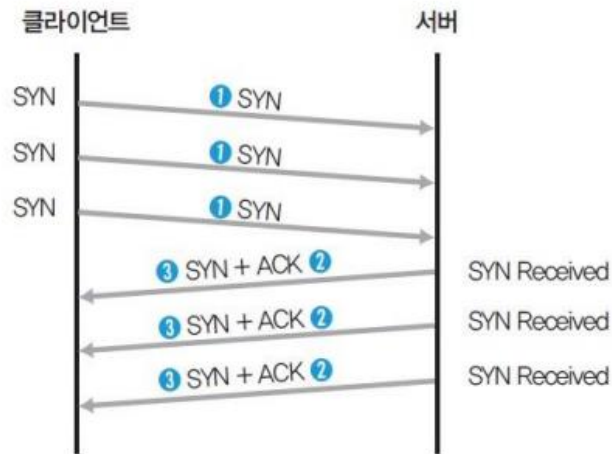
SYN Flooding 공격의 개념

DoS 및 DDoS 공격

■ SYN Flooding

- 서버별로 한정되어 있는 접속 가능 공간에 존재하지 않는
 - 클라이언트가 접속한 것처럼 속여 다른 사용자 가 서비스를 제공받지 못하게 하는 것

1. 공격자는 많은 숫자의 SYN 패킷을 서버에 보냄
2. 서버는 받은 SYN 패킷에 대한
3. SYN/ACK 패킷을 각 클라이언트로 보냄
4. 서버는 자신이 보낸 SYN/ACK 패킷에 대한 ACK 패킷을 받지 못함
5. 서버는 세션의 연결을 기다리게 되고 공격은 성공함



SYN Flooding 공격 시 쓰리웨이 핸드셰이킹



DoS 및 DDoS 공격

■ SYN Flooding 수행

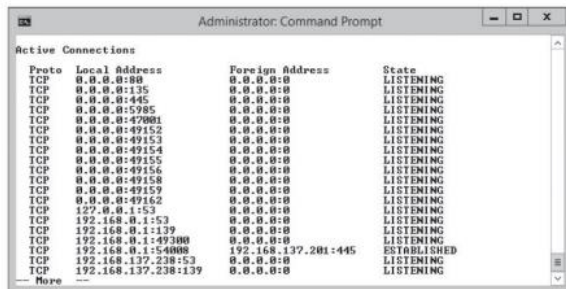
- hping3을 이용하면 아주 짧은 시간에 많은 패킷을 보내 SYN Flooding 공격을 간단히 수행할 수 있음
- > hping3 --rand-source 192.168.0.100 -p 80 -S

```
root@ubuntu-14: /  
root@ubuntu-14: /#  
root@ubuntu-14: /# hping3 --rand-source 192.168.0.1 -p 80 -S  
HPING 192.168.0.1 (eth0 192.168.0.1): S set, 40 headers + 0 data bytes
```

SYN Flooding 공격 수행

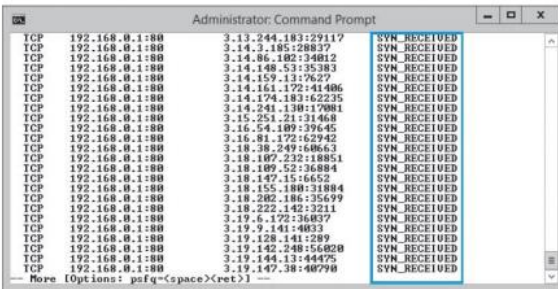
- -p 80 : 80번 포트에 대해 패킷 전송
- -S : TCP 패킷 중 SYN만 전송

- 공격 확인 : 현재 연결된 세션에 관한 정보를 볼 수 있는 netstat로 공격 받고 있는지 확인



Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:80	0.0.0.0:	LISTENING
TCP	0.0.0.0:135	0.0.0.0:	LISTENING
TCP	0.0.0.0:445	0.0.0.0:	LISTENING
TCP	0.0.0.0:5985	0.0.0.0:	LISTENING
TCP	0.0.0.0:470001	0.0.0.0:	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:	LISTENING
TCP	0.0.0.0:49153	0.0.0.0:	LISTENING
TCP	0.0.0.0:49154	0.0.0.0:	LISTENING
TCP	0.0.0.0:49155	0.0.0.0:	LISTENING
TCP	0.0.0.0:49156	0.0.0.0:	LISTENING
TCP	0.0.0.0:49158	0.0.0.0:	LISTENING
TCP	0.0.0.0:49159	0.0.0.0:	LISTENING
TCP	0.0.0.0:49162	0.0.0.0:	LISTENING
TCP	127.0.0.1:53	0.0.0.0:	LISTENING
TCP	192.168.0.1:53	0.0.0.0:	LISTENING
TCP	192.168.0.1:1379	0.0.0.0:	LISTENING
TCP	192.168.0.1:493000	0.0.0.0:	LISTENING
TCP	192.168.0.1:540008	192.168.137.201:445	ESTABLISHED
TCP	192.168.137.238:53	0.0.0.0:	LISTENING
TCP	192.168.137.238:137	0.0.0.0:	LISTENING

SYN Flooding 공격 전의 netstat 상태



Proto	Local Address	Foreign Address	State
TCP	192.168.0.1:80	3.13.244.183:29117	SYN_RECEIVED
TCP	192.168.0.1:80	3.14.3.195:28837	SYN_RECEIVED
TCP	192.168.0.1:80	3.14.86.182:34812	SYN_RECEIVED
TCP	192.168.0.1:80	3.14.148.53:35383	SYN_RECEIVED
TCP	192.168.0.1:80	3.14.159.13:7627	SYN_RECEIVED
TCP	192.168.0.1:80	3.14.161.172:41406	SYN_RECEIVED
TCP	192.168.0.1:80	3.14.174.183:52235	SYN_RECEIVED
TCP	192.168.0.1:80	3.14.241.138:17081	SYN_RECEIVED
TCP	192.168.0.1:80	3.15.251.21:31468	SYN_RECEIVED
TCP	192.168.0.1:80	3.16.54.109:39645	SYN_RECEIVED
TCP	192.168.0.1:80	3.16.81.172:62942	SYN_RECEIVED
TCP	192.168.0.1:80	3.18.38.249:68663	SYN_RECEIVED
TCP	192.168.0.1:80	3.18.187.232:18851	SYN_RECEIVED
TCP	192.168.0.1:80	3.18.109.52:36884	SYN_RECEIVED
TCP	192.168.0.1:80	3.18.147.15:6652	SYN_RECEIVED
TCP	192.168.0.1:80	3.18.155.188:31884	SYN_RECEIVED
TCP	192.168.0.1:80	3.18.282.186:35699	SYN_RECEIVED
TCP	192.168.0.1:80	3.18.222.142:3211	SYN_RECEIVED
TCP	192.168.0.1:80	3.19.6.172:36837	SYN_RECEIVED
TCP	192.168.0.1:80	3.19.9.141:4033	SYN_RECEIVED
TCP	192.168.0.1:80	3.19.158.141:289	SYN_RECEIVED
TCP	192.168.0.1:80	3.19.142.248:56820	SYN_RECEIVED
TCP	192.168.0.1:80	3.19.144.13:44475	SYN_RECEIVED
TCP	192.168.0.1:80	3.19.147.38:40790	SYN_RECEIVED

SYN Flooding 공격 후의 netstat 상태



DoS 및 DDoS 공격

■ SYN Flooding 보안 대책

- 시스템 패치 업데이트
- 침입 탐지 시스템 및 침입 차단 시스템 설치
- 짧은 시간 안에 똑같은 형태의 패킷을 보내는 형태의 공격을 인지했을 경우,
 - 그에 해당하는 IP 주소 대역의 접속을 금지하거나 방화벽 또는 라우터에서 해당 접속을 금지시킴.
- 7계층 DoS 공격
 - 최근의 DoS 공격은 웹 어플리케이션 등을 대상으로 공격 방향을 전환

	3, 4계층 DoS 공격	7계층 DoS 공격
주요 공격	<ul style="list-style-type: none">• 대역폭 고갈 공격• 세션 고갈 공격	<ul style="list-style-type: none">• 서버의 자원 고갈 공격
주요 프로토콜	<ul style="list-style-type: none">• TCP, UDP, ICMP	<ul style="list-style-type: none">• HTTP, SMTP, FTP, VoIP 등
특징	<ul style="list-style-type: none">• 단순한 Flooding 형태의 트래픽을 대량으로 발생시켜 공격• Spoofed IP로 비정상적인 트래픽을 이용한 공격의 비율이 높음• 보안 장비를 통해 방어 가능	<ul style="list-style-type: none">• 정상 트래픽을 이용한 공격• 소량의 트래픽을 이용한 공격• 특정 어플리케이션의 취약점을 이용한 공격

3, 4 계층 DoS 공격과 7 계층 DoS 공격의 차이



DoS 및 DDoS 공격

■ 7계층 공격의 주요 특징

- 정상적인 TCP/UDP 연결 기반의 공격으로,
 - 변조된 IP 가 아닌 정상 IP를 이용한 접속 요청 후 공격이 진행되어
 - 정상 사용자의 트래픽과 구분하기가 어려워 탐지가 어려움.
 - 소량의 트래픽을 이용한 공격으로 오랜 시간에 걸쳐 서서히 공격이 진행되어 탐지가 어려움.
 - 특정 서비스의 취약점을 이용하여 공격(현재까지는 웹 서비스의 취약점을 이용한 공격이 주를 이루고 있음)

■ 웹 어플리케이션에 대한 DoS 공격 유형

- HTTP GET Flooding 공격
 - 공격 대상 시스템에 TCP 쓰리웨이 핸드셰이킹 과정을 통해 정상적으로 접속한 뒤,
 - HTTP의 GET Method를 통해 특정 페이지를 무한대로 실행하는 방식
- HTTP CC 공격
 - DoS 공격 기법에 'Cache-Control: no-store, must-revalidate' 옵션을 사용하면,
 - 웹 서버는 캐시를 사용하지 않고 응답을 해야 하므로 웹 서비스의 부하가 증가



DoS 및 DDoS 공격

■ 웹 어플리케이션에 대한 DoS 공격 유형

- 동적 HTTP Request Flooding 공격
 - 요청 페이지를 변경하여 웹 페이지를 지속적으로 요청하는 기법

- Slow HTTP Header DoS (Slowloris) 공격
 - 서버로 전달할 HTTP 메시지의 Header 정보를 비정상적으로 조작하여 웹 서버가 헤더 정보를 완전히 수신할 때까지
 - 연결을 유지하도록 하여 시스템 자원을 소비시켜 다른 클라이언트의 정상적인 서비스를 방해하는 공격
 - 불안정한 메시지를 수신한 웹 서버는 클라이언트의 요청이 끝나지 않은 것으로 인식하여 웹 로그를 기록하지 않음.

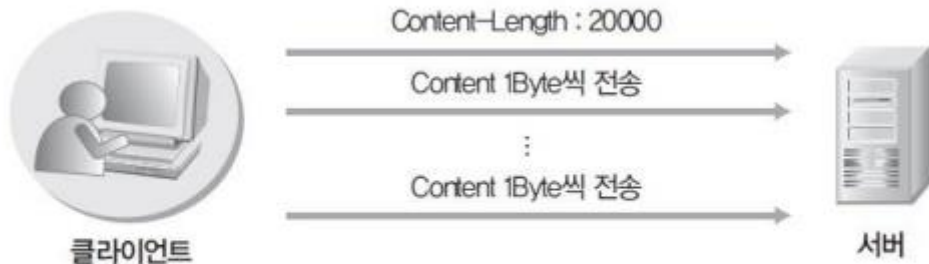


DoS 및 DDoS 공격

■ 웹 어플리케이션에 대한 DoS 공격 유형

□ Slow HTTP POST 공격

- 2010년 11월 미국 워싱턴에서 개최된 2010 OWASP AppSec Conference에서 소개
- 웹 서버와의 커넥션을 최대한 장시간 동안 유지하여 웹 서버가 정상적인 이용자의 접속을 받아들일 수 없게 하는 방식
- 필요로 하는 Content-Length를 설정하면 Slow HTTP POST 공격을 어느 정도 대응 가능



Slow HTTP POST 공격의 구조



DoS 및 DDoS 공격

■ DDoS (Distributed Denial of Service)

- DoS 공격이 발전된 것
- 피해 양상이 상당히 심각하지만 확실한 대책이 없음.
- 공격자의 위치와 구체적인 발원지를 파악하는 일이 무척 어려워 여전히 대응이 어려운 공격 중의 하나
- 특성상 대부분의 DDoS 공격은 자동화된 툴을 이용

■ DDoS 공격이 이루어지기 위한 기본 구성

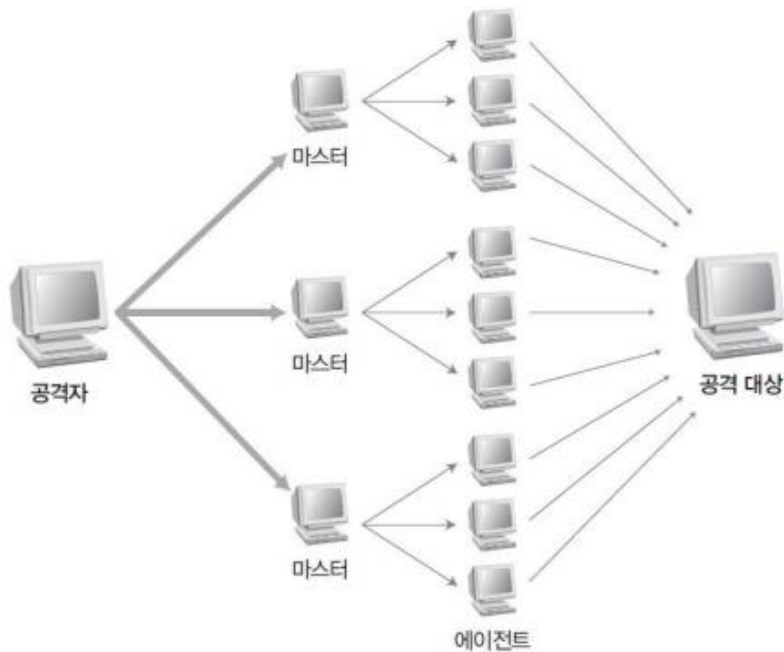
- 공격자 (Attacker) : 공격을 주도하는 해커의 컴퓨터
- 마스터 (Master) : 공격자에게 직접 명령을 받는 시스템, 여러 대의 에이전트 관리
- 핸들러 (Handler) 프로그램 : 마스터 시스템 역할을 수행하는 프로그램
- 에이전트 (Agent) : 공격 대상에 직접 공격을 가하는 시스템
- 데몬 (Daemon) 프로그램 : 에이전트 시스템 역할을 수행하는 프로그램



DoS 및 DDoS 공격

■ DDoS 공격 구성

- DoS 공격에서의 공격자와 타겟 서버가 1:1로 매칭되는 형태가 아닌, N:1로 구성되는 형태
- DDoS 공격에서는 중간자 역할을 하는 마스터와 에이전트가 피해자이기도 함



DoS 및 DDoS 공격

■ DDoS 공격 순서

- ① 많은 사용자들이 사용하며 대역폭이 넓고 관리자가 모든 시스템을 세세하게 관리할 수 없는 곳의 계정을 획득한 후, 스니핑이나 버퍼 오버플로우 등의 공격으로 설치 권한이나 루트 권한을 획득
- ② 잠재적인 공격 대상을 파악하기 위해 네트워크 스캐닝으로 원격지에서 버퍼 오버플로우를 일으킬 수 있는 취약한 서비스를 제공하는 서버 파악
- ③ 취약한 시스템 목록을 확인한 후 실제 공격을 위한 Exploit을 작성
- ④ 권한을 획득한 시스템에 침투하여 Exploit을 컴파일하여 설치
- ⑤ 설치한 Exploit으로 공격 시작



THANK

YOU