¾ DoS
Attacking, detecting
And blocking

What to exercise

How to attack DoS

How to block DoS

How to detect DoS

How to monitor DoS

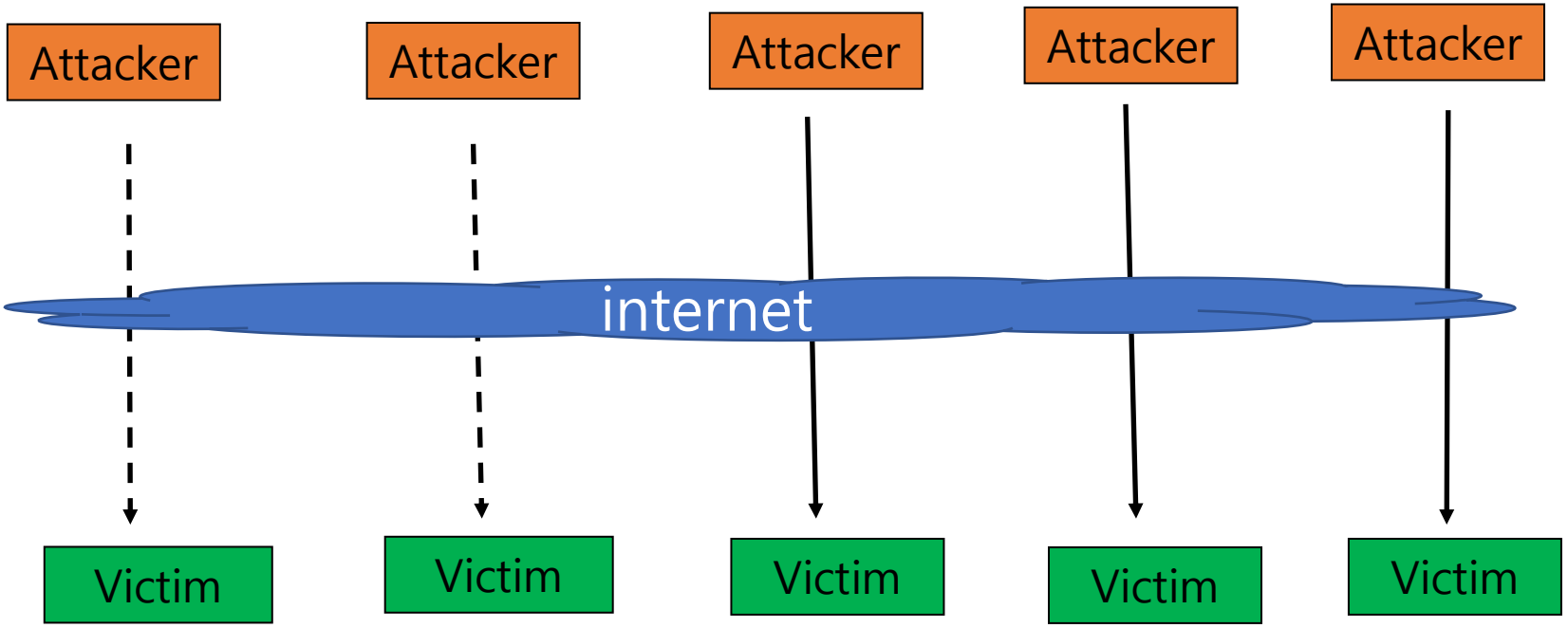
What kind od SW used?

- Windows CMD
- Linux command
- Python language(scapy)
- Machine learning
- Tools

3/4 layer DoS attacking types

Tradi/tional DoS

Ping of Death **SYN Flooding** **Teardrop** **Land attack** **Smurf**



First model of exercise
Ping of Death

- **Attacker** : making ping IMP packets larger than normal using ping and sending
- **Packets :** are routed through the network
- **Target :** network has to deal with all fragmented packets, so the load is much higher than a normal ping.

How to attack Ping, of Death

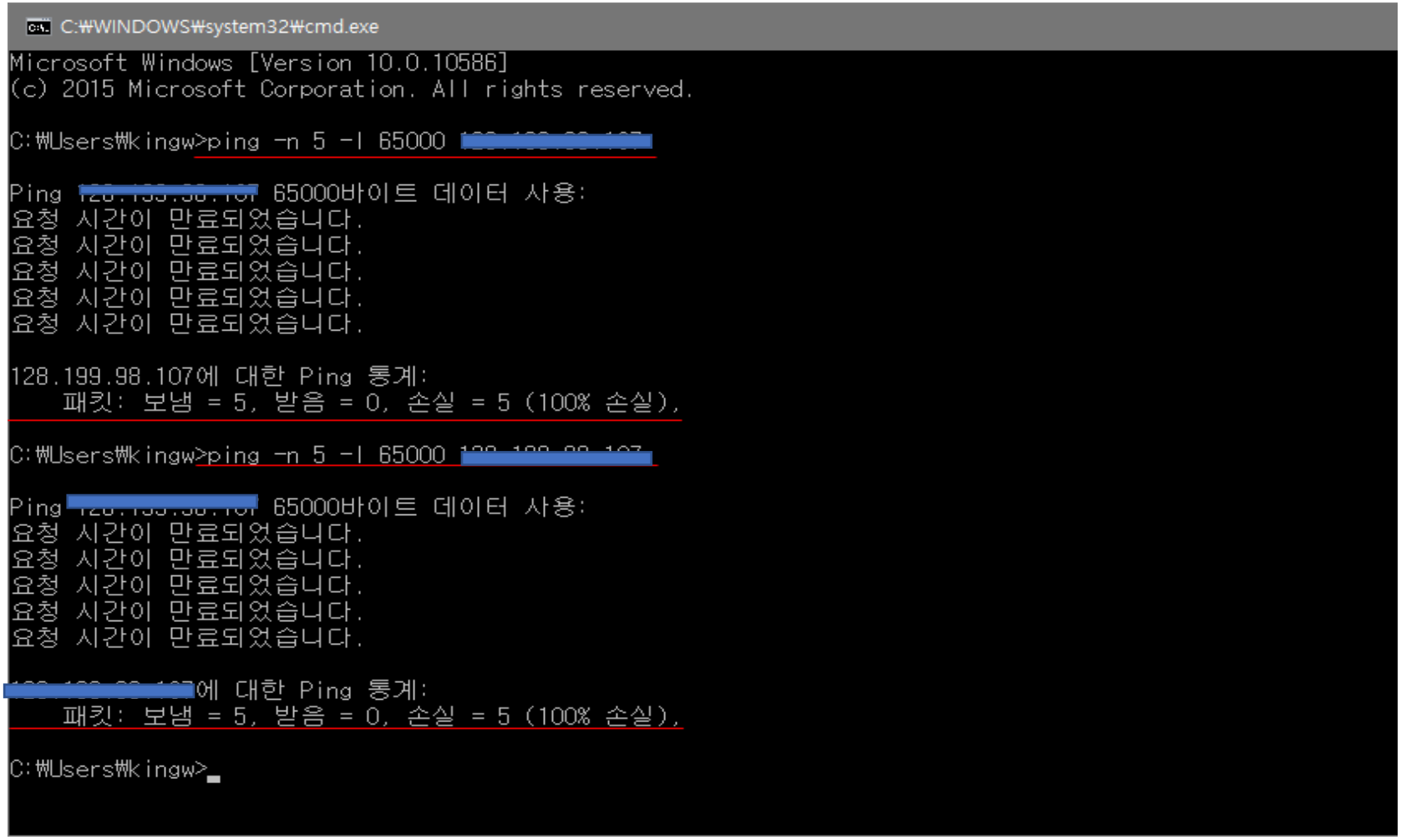
Packet splitting

- **Set** the maximum length of the ICMP packet
to 65,500 bytes
- **Send/ping** the maximum length of the ICMP packet to target

- **Big size packets split into** small size packet
If the maximum transmittable length of the network that a packet passes through is 100 bytes, Split into 655

How to attack, Ping of Death using window CMD prompt

Send 65000 byte packets 5 times to ubuntu server using ping command => Failed



How to attack, Ping of Death using window CMD prompt

- "ping 111.111.111.111 –t | 65500

- ping" sends the data packets to the victim

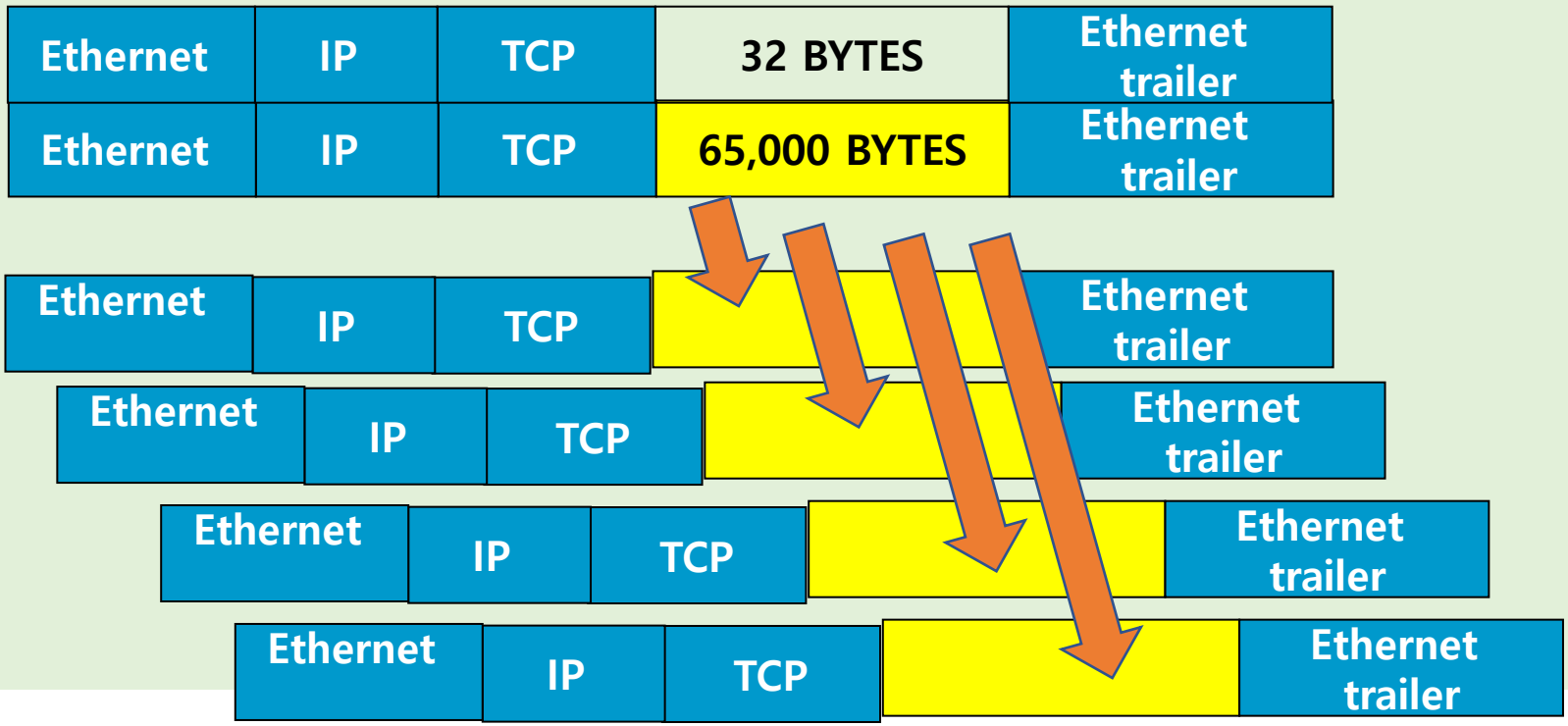
- "111.111.111.111" is the IP address of the victim

- "–t" means the data packets should be sent until the program is stopped

- "–l" specifies the data load to be sent to the victim

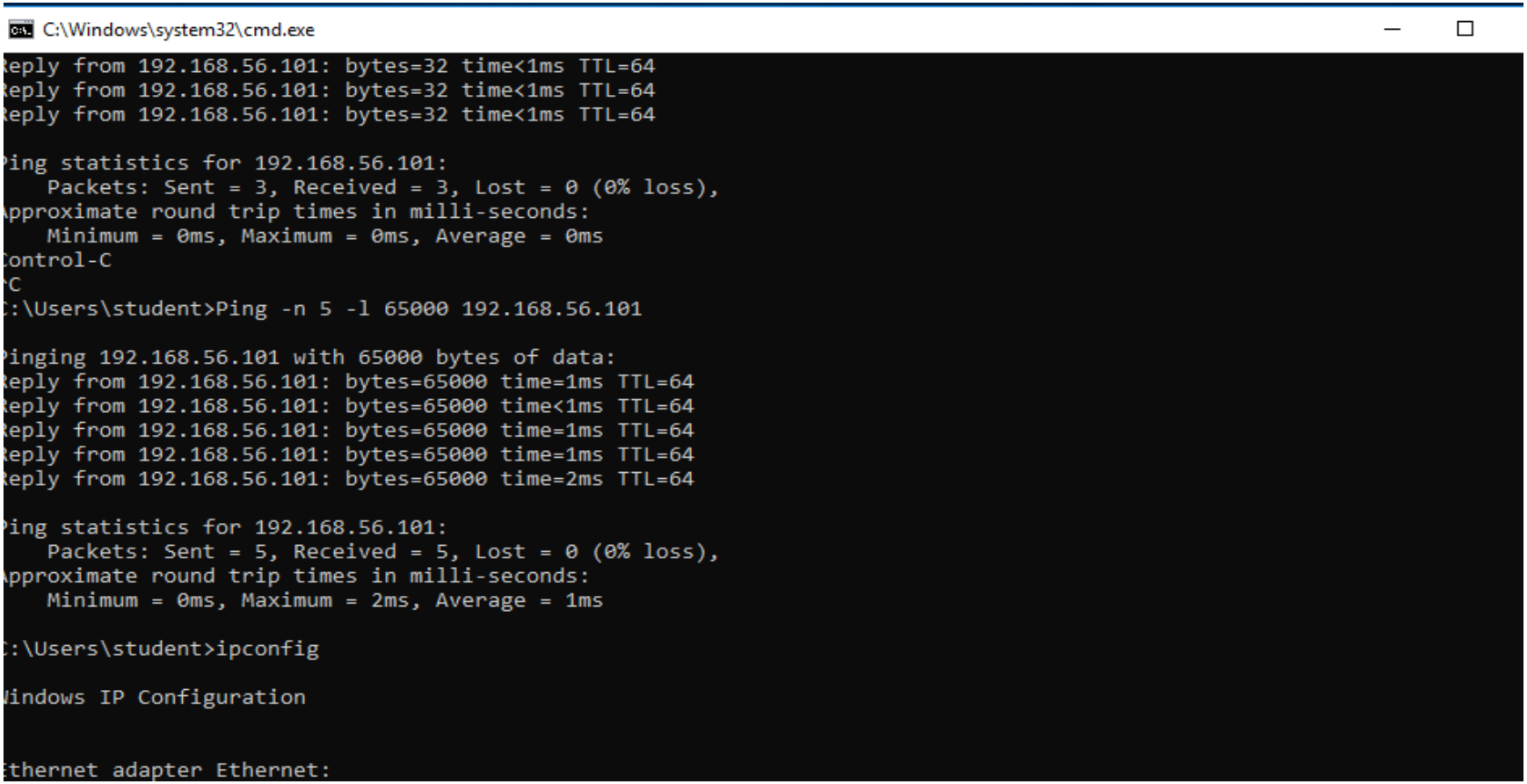
How to attack

Packets are being divided into several IMCP packets



How to attack, Ping of Death using window CMD prompt

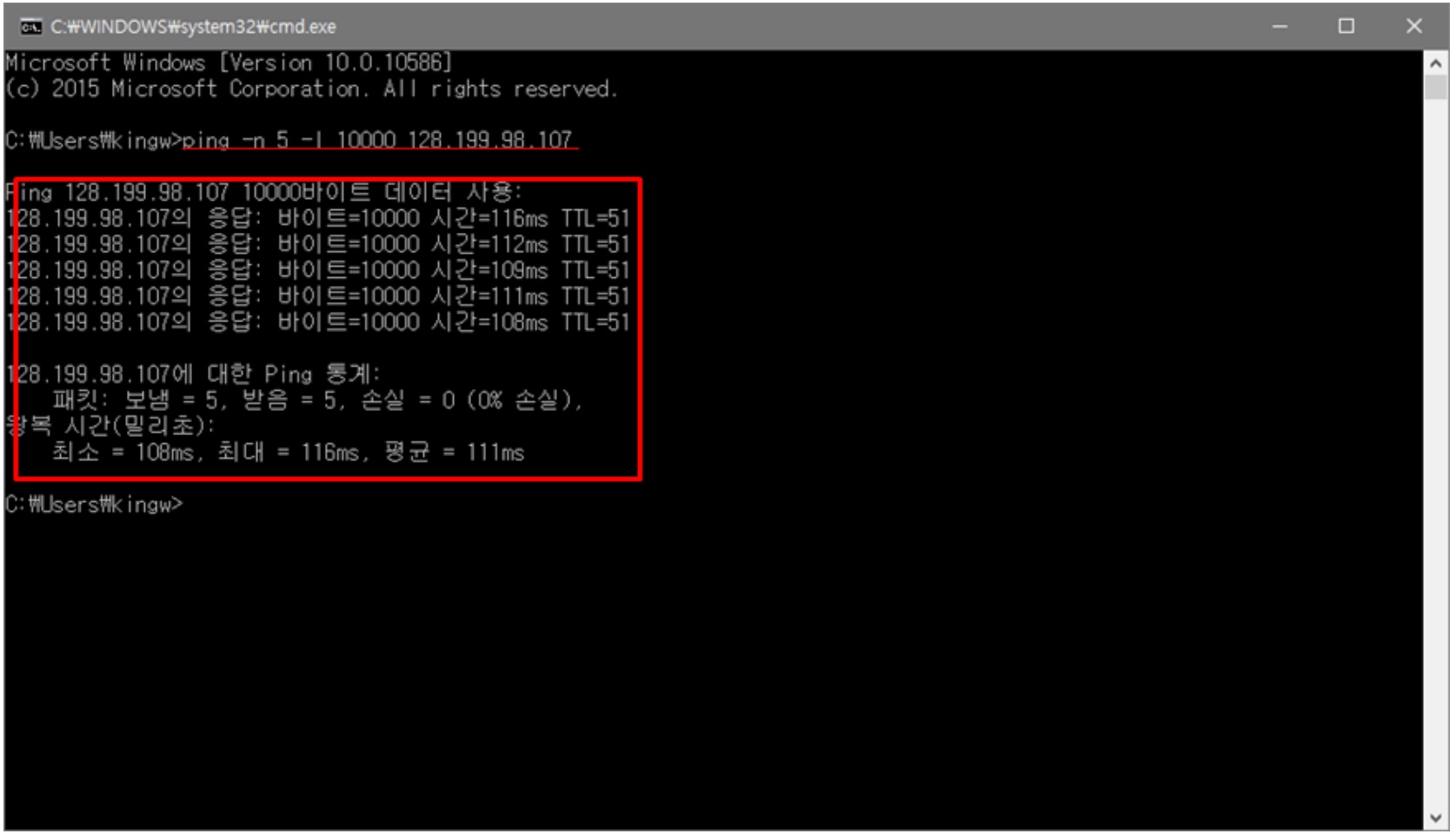
Send 65000 byte packets 5 times to ubuntu server using ping command => succeeded



How to attack, Ping of Death

using window CMD prompt

Send smaller 10000 byte ICMP packets 10000 byte packets 5 times to ubuntu => succeeded



How to attack, Ping of Death using Linux command hping3

hping3 intallation

(sudo) apt- get install hping3

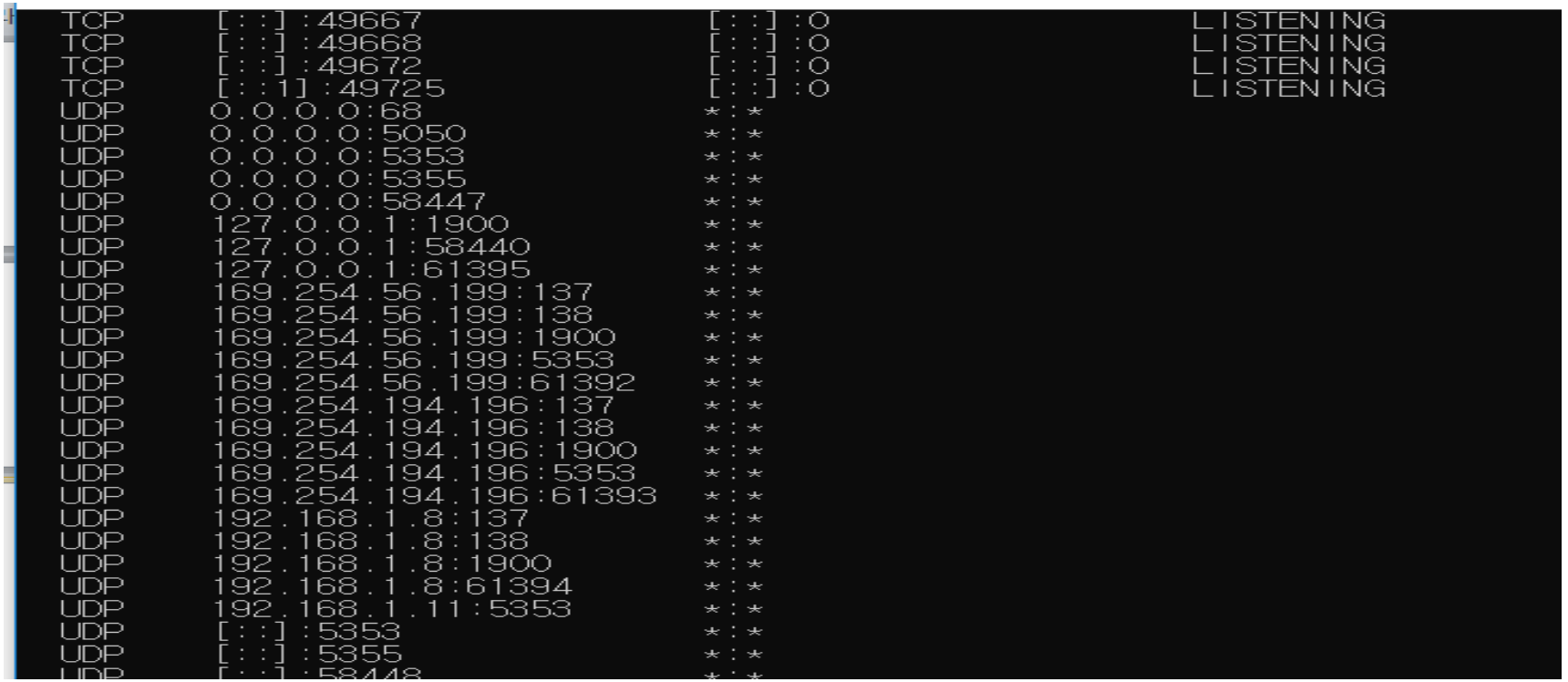
Ping of Death attacking

hping3 --icmp --rand-source 111.111.0.1 -d 65000

How to detect DoS attack

How to detect DoS attacking on Window

CMD netstat



```
  TCP     [::]:49667             [::]:0                 LISTENING
  TCP     [::]:49668             [::]:0                 LISTENING
  TCP     [::]:49672             [::]:0                 LISTENING
  TCP     [::1]:49725            [::]:0                 LISTENING
  UDP     0.0.0.0:68             *:*
  UDP     0.0.0.0:5050           *:*
  UDP     0.0.0.0:5353           *:*
  UDP     0.0.0.0:5355           *:*
  UDP     0.0.0.0:58447          *:*
  UDP     127.0.0.1:1900         *:*
  UDP     127.0.0.1:58440        *:*
  UDP     127.0.0.1:61395        *:*
  UDP     169.254.56.199:137     *:*
  UDP     169.254.56.199:138     *:*
  UDP     169.254.56.199:1900    *:*
  UDP     169.254.56.199:5353    *:*
  UDP     169.254.56.199:61392   *:*
  UDP     169.254.194.196:137    *:*
  UDP     169.254.194.196:138    *:*
  UDP     169.254.194.196:1900   *:*
  UDP     169.254.194.196:5353   *:*
  UDP     169.254.194.196:61393  *:*
  UDP     192.168.1.8:137        *:*
  UDP     192.168.1.8:138        *:*
  UDP     192.168.1.8:1900       *:*
  UDP     192.168.1.8:61394      *:*
  UDP     192.168.1.11:5353      *:*
  UDP     [::]:5353              *:*
  UDP     [::]:5355              *:*
  UDP     [::]:58448             *:*
```

How to detect DoS attacking on Window

CMD netstat -a

```
C:₩Users₩B-020>netstat -a

활성 연결

  프로토콜  로컬 주소          외부 주소              상태
  TCP    0.0.0.0:135      DESKTOP-B3JBNIS:0      LISTENING
  TCP    0.0.0.0:443      DESKTOP-B3JBNIS:0      LISTENING
  TCP    0.0.0.0:445      DESKTOP-B3JBNIS:0      LISTENING
  TCP    0.0.0.0:902      DESKTOP-B3JBNIS:0      LISTENING
  TCP    0.0.0.0:912      DESKTOP-B3JBNIS:0      LISTENING
  TCP    0.0.0.0:1158     DESKTOP-B3JBNIS:0      LISTENING
  TCP    0.0.0.0:1521     DESKTOP-B3JBNIS:0      LISTENING
  TCP    0.0.0.0:3938     DESKTOP-B3JBNIS:0      LISTENING
  TCP    0.0.0.0:5040     DESKTOP-B3JBNIS:0      LISTENING
  TCP    0.0.0.0:5520     DESKTOP-B3JBNIS:0      LISTENING
  TCP    0.0.0.0:7680     DESKTOP-B3JBNIS:0      LISTENING
  TCP    0.0.0.0:49664    DESKTOP-B3JBNIS:0      LISTENING
```

모든 연결 및 수신 대기 포트

How to detect DoS attacking on Window

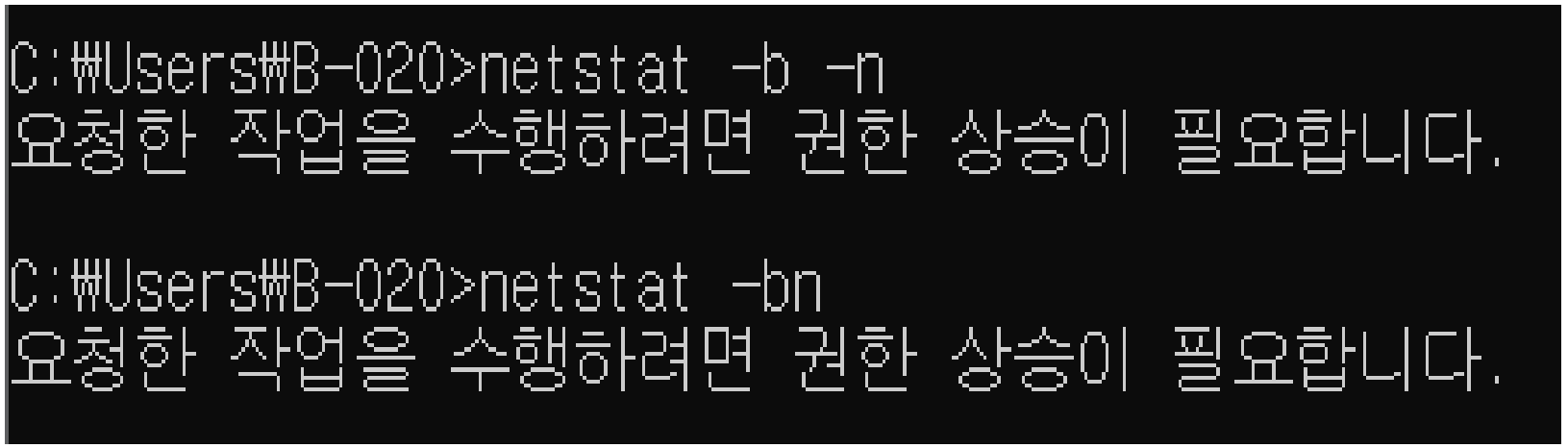
CMD netstat -an

Check with netstat if you are under attack

See information about the currently connected session

How to detect DoS attacking on Window

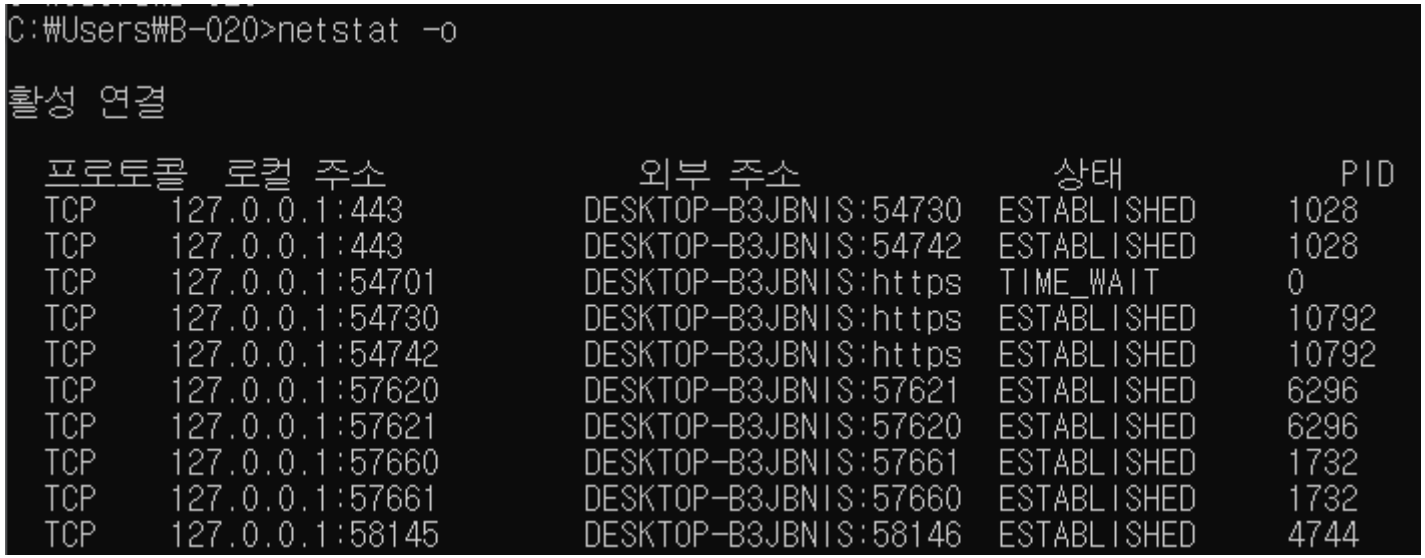
CMD netstat -b-n



- 각 연결/수신 대기 포트 생성과 관련된 실행 파일을 표시 (권한이 없을 경우 사용 불가)

How to detect DoS attacking on Window

CMD netstat -o



```
C:₩Users₩B-020>netstat -o

활성 연결

  프로토콜  로컬 주소          외부 주소          상태           PID
  TCP    127.0.0.1:443          DESKTOP-B3JBNIS:54730  ESTABLISHED     1028
  TCP    127.0.0.1:443          DESKTOP-B3JBNIS:54742  ESTABLISHED     1028
  TCP    127.0.0.1:54701        DESKTOP-B3JBNIS:https  TIME_WAIT       0
  TCP    127.0.0.1:54730        DESKTOP-B3JBNIS:https  ESTABLISHED     10792
  TCP    127.0.0.1:54742        DESKTOP-B3JBNIS:https  ESTABLISHED     10792
  TCP    127.0.0.1:57620        DESKTOP-B3JBNIS:57621  ESTABLISHED     6296
  TCP    127.0.0.1:57621        DESKTOP-B3JBNIS:57620  ESTABLISHED     6296
  TCP    127.0.0.1:57660        DESKTOP-B3JBNIS:57661  ESTABLISHED     1732
  TCP    127.0.0.1:57661        DESKTOP-B3JBNIS:57660  ESTABLISHED     1732
  TCP    127.0.0.1:58145        DESKTOP-B3JBNIS:58146  ESTABLISHED     4744
```

- 각 연결의 소유자 프로세스 ID

How to detect DoS attacking on Window

CMD netstat -rn

```
C:₩Users₩B-020>netstat -rn
===========================================================================
인터페이스 목록
  3...08 2e 5f 1d 24 77 ......Broadcom NetXtreme Gigabit Ethernet
 10...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 11...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  1...........................Software Loopback Interface 1
===========================================================================
```

라우팅 테이블 정보

How to detect DoS attacking on Window

CMD netstat -s

Netstat options

- netstat -a : 모든 연결 및 수신 대기 포트를 표시
- netstat -n : 주소 및 포트 번호를 숫자 형식으로 표시
- netstat -b : 각 연결/수신 대기 포트 생성과 관련된
- 실행 파일을 표시 (권한이 없을 경우 사용 불가)

netstat -bn : -b 옵션으로 실행 파일이 표시
-n 옵션으로 주소와 포트 번호 숫자로 표시
(권한이 없을 경우 사용 불가)

- netstat -o : 각 연결의 소유자 프로세스 ID를 표시
- netstat -rn : 라우팅 테이블 정보를 표시
- netstat -s -p : 프로토콜별 통계를 표시(ipv4, ipv6, tcp, udp등)
- netstat –s –p tcp : tcp에 대한 통계를 표시

권한 상승 방법 : cmd 아이콘에 우클릭 -> 관리자 권한으로 실

How to detect DoS attacking on Ubuntu

net-tools package on Ubuntu

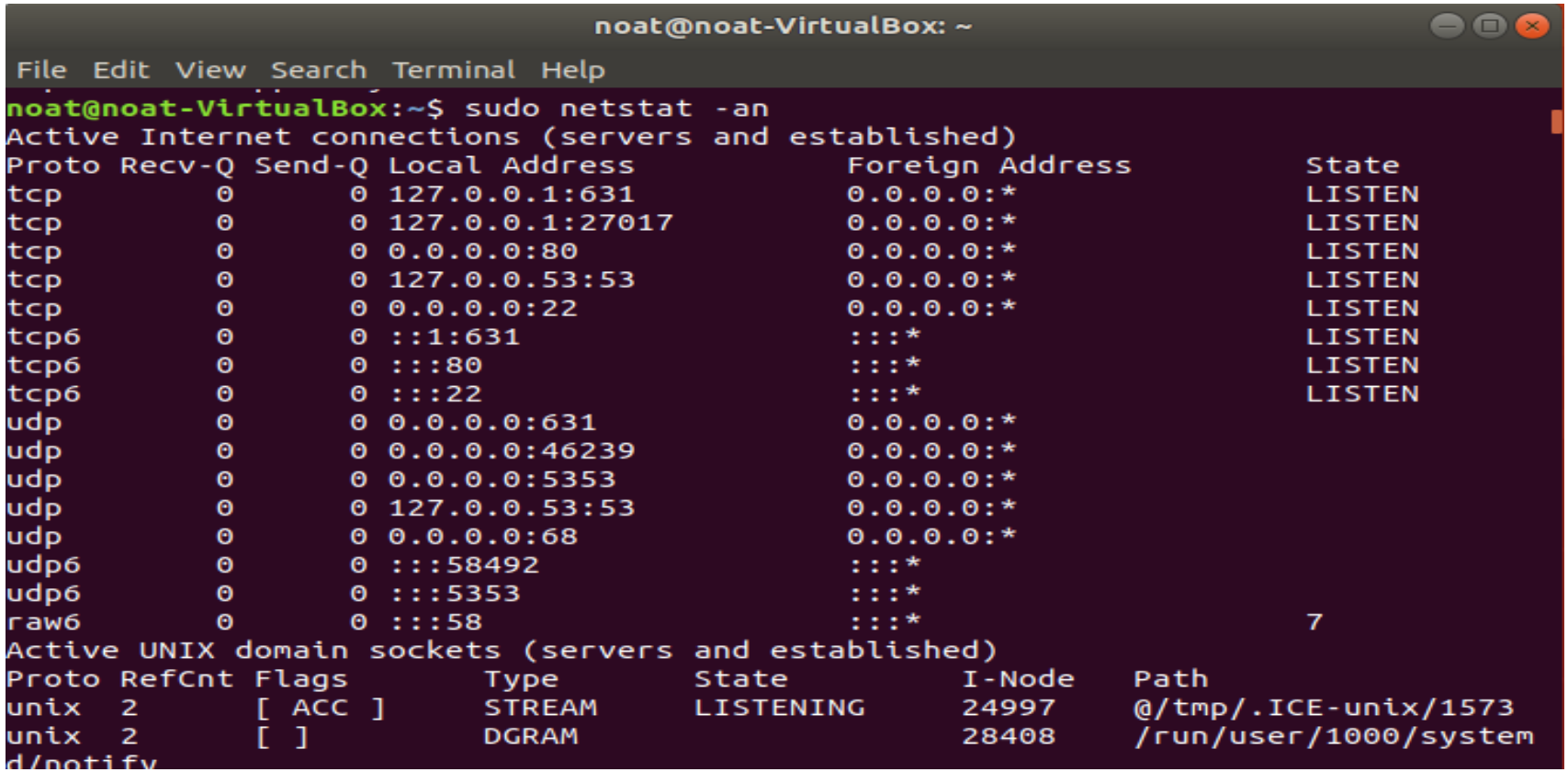
- In Ubuntu 20.04 LTS version, tools for using the Linux network subsystem are not installed by default.
- Commands (programs) such as ifconfig and netstat cannot be used.

- So you need to install net-tools.

```
sudo apt-get install net-tools -y
```

How to detect DoS attacking on Ubuntu

Syn-flooding detect on Linux



How to detect DoS attacking on Ubuntu

If you use **-t** option, it will filter the output to display TCP connections only:

```
netstat -t
```

How to detect DoS attacking on Ubuntu

The netstat command most of the time used with **-tulnp** options to display listening ports (sockets)

```
root@awsvps3:~# netstat -tulnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      32048/mysqld
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      28842/systemd-resol
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1161/sshd
tcp6       0      0 :::80                   :::*                    LISTEN      1606/apache2
tcp6       0      0 :::22                   :::*                    LISTEN      1161/sshd
tcp6       0      0 :::443                  :::*                    LISTEN      1606/apache2
udp        0      0 127.0.0.53:53           0.0.0.0:*                           28842/systemd-resol
udp        0      0 172.31.43.119:68        0.0.0.0:*                           28837/systemd-netwo
root@awsvps3:~#
```

How to detect DoS attacking

Check with netstat if you are under attack

- netstat –na on windows CMD
- netstat –na | grep on Linux **(non pretest in class)**

- Local Address, Foreign Address, State, etc.

=> State SYN_RECEIVED

=> Waiting for a confirmation message from the client, this process is instantaneous

=> SYN_RECV Determining Syn Flooding Attacks

- When many messages are displayed

How to Use netstat Command in Linux

10 basic examples of Linux Netstat command

https://www.binarytides.com/linux-netstat-command-examples/

To list all ports and connections regardless of their state or protocol, use:

https://phoenixnap.com/kb/netstat-command

https://linux.die.net/man/8/netstat

How to block DoS attack

Basic protection techniques using Linux

- **Iptables is the default firewall for Linux computers.**
- **Remember to harden your firewall: block all the incoming traffic except the traffic you REALLY need on your server.**
- **Allow management only from trusted sources.**
  The easiest case is an attack from one host without IP spoofing.

Basic Linux iptables protection tech. against DoS

```
# iptables -A INPUT -p tcp -m state --state NEW -m
recent --update --seconds 60 --hitcount 20 -j DROP

# iptables -A INPUT -p tcp -m state --state NEW -m
recent --set -j ACCEPT
```

These rules limit the rate of SYN requests from one IP to 20 per minute.

SYN Flood Attacks- "How to protect?"- article - (hakin9.org)

How to protect DoS attacking
Block syn-flooding on Linux

- If you are using UFW before using IPtables, disable it.
-
  UFW disable : ufw disable
- UFW(Uncomplicated Firewall)
-

  https://ndb796.tistory.com/262

How to protect DoS attacking Block syn-flooding on Linux

Install iptables through the Linux command line

$ sudo apt-get install iptables

https://vitux.com/how-to-block-allow-ping-using-iptables-in-ubuntu/

Verify the installation and check the version number

$ iptables -- version

How to protect DoS attacking Basic iptables protection techniques for Linux

'Normal' values are between 536 and 65535

```
# iptables -t mangle -I PREROUTING -p tcp -m tcp --dport 80 -m state --state NEW -m tcpmss ! --mss 536:65535 -j DROP
```

SYN Flood Attacks- "How to protect?"- article - (hakin9.org)

How to protect DoS attacking Block Invalid Packets

iptables -t mangle -A PREROUTING -m conntrack --ctstate INVALID -j DROP

This rule blocks all packets that are not a SYN packet and don’t belong to an established TCP connection.

https://javapipe.com/blog/iptables-ddos-protection/

Block New Packets That Are Not SYN

```
iptables -t mangle -A PREROUTING -p tcp ! --syn -m
conntrack --ctstate NEW -j DROP
```

This blocks all packets that are new (don't belong to an established connection) and don't use the SYN flag.

This rule is similar to the "Block Invalid Packets" one, but we found that it catches some packets that the other one doesn't.

Block Packets With Bogus TCP Flags

```
iptables -t mangle -A PREROUTING -p tcp --tcp-flags FIN,SYN FIN,SYN -j DROP

iptables -t mangle -A PREROUTING -p tcp --tcp-flags SYN,RST SYN,RST -j DROP

iptables -t mangle -A PREROUTING -p tcp --tcp-flags FIN,RST FIN,RST -j DROP

iptables -t mangle -A PREROUTING -p tcp --tcp-flags FIN,ACK FIN -j DROP

iptables -t mangle -A PREROUTING -p tcp --tcp-flags ACK,URG URG -j DROP

iptables -t mangle -A PREROUTING -p tcp --tcp-flags ACK,PSH PSH -j DROP

iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL NONE -j DROP
```

The above ruleset blocks packets that use bogus TCP flags, ie.

TCP flags that legitimate packets wouldn't use.

Block syn-flooding on Linux

- iptables -N syn-flood
- iptables -A syn-flood -p tcp --tcp-flags ALL SYN,FIN -m limit --limit 12/second --limit-burst 24 -j RETURN
- iptables -A syn-flood -j DROP

Block syn-flooding on Linux

- iptables firewall is based on some set of rules.
- We can add the following rule in order to block pings to and from the server.

- $ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j REJECT

https://vitux.com/how-to-block-allow-ping-using-iptables-in-ubuntu/

Block syn-flooding on Linux

```
iptables -A syn-flood -m limit --limit 10/second --
limit-burst 50 -j RETURN

# log attacks

iptables -A syn-flood -j LOG --log-prefix "SYN flood: "

# silently drop the rest

iptables -A syn-flood -j DROP
```

- → Save configuration:
  service iptables save
- → Restart iptables firewall:
  service iptables restart

Block **Smurf**

- Solaris: add to: /etc/rc2.d/S69inet

```
ndd -set /dev/ip
```

- Linux: apply firewall in level receive through ipfw

```
ipfwadm -I -a deny -P icmp -D

10.10.10.0 -S 0/0 0 8 ipfwadm -I -a deny -P icmp -D
10.10.10.255

-S 0/0 0 8
```

Site references

https://www.guru99.com/ultimate-guide-to-dos-attacks.html

Iptables Tutorial: Ultimate Guide to Linux Firewall (phoenixnap.com)

linux command to prevent dos attack by using netstat and iptables

SYN Flood Attacks- "How to protect?"- article - (hakin9.org)

https://vitux.com/how-to-block-allow-ping-using-iptables-in-ubuntu/

https://javapipe.com/blog/iptables-ddos-protection/