

실습 환경 : 공격자 Kali(192.168.20.50) 타겟 CentOS(192.168.20.200), Window2008(192.168.20.201)

<네트워크 해킹 방지 대책>

UTM을 이용하여 방화벽을 구성한다.

1. 침입 방지 설정 확인

침입 방지

☒ 글로벌
 ☒ 공격 패턴
 ☒ DoS/플러딩 방지
 ☒ 포트 검사 방지
 ☐ 예외
 ☐ 고급

이 테이블은 사용 가능한 IPS 규칙 그룹을 보여줍니다. 성능을 향상하려면 로컬 네트워크에서 실행 중인 서비스 또는 소프트웨어와 일치하지 않는 그룹을 선택 취소해야 합니다. 각 활성 그룹에 대해 다음과 같은 세 가지 옵션을 설정할 수 있습니다.

- **동작:** 기본적으로 그룹의 규칙마다 합리적인 기본 동작이 포함되어 있습니다. 그룹에 대해 경고 또는 드롭을 설정하여 이러한 기본값을 재정의할 수 있습니다.
- **규칙 기간:** 기본적으로 12개월 미만의 IPS 패턴을 사용하는 것이 좋습니다. 이는 전체 패치 수준, 레거시 시스템 또는 기타 보안 요구 사항 등의 개별 요소에 따라 달라질 수 있습니다.
- **부가 경고 추가:** 이 옵션을 활성화하면 그룹에 경고 목적으로만 사용되는 규칙도 포함됩니다. 이러한 규칙이 잠재적으로 거짓 경보를 유발할 수도 있기 때문에 기본적으로 포함되지는 않습니다.
- **알림:** 이 옵션을 활성화하면, 이 그룹에 탐지될 때마다 알림이 전송됩니다.

변경을 완료하면 페이지의 맨 아래에 있는 적용 버튼을 클릭하십시오.

상태 / 그룹 이름	동작	규칙 기간	옵션
<input checked="" type="checkbox"/> 운영 체제 대상 공격 (4회 공격, 55개 경고)	드롭 ▼	12개월 미: ▼	<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> Windows (3회 공격, 54개 경고)	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> 리눅스 ()	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> 기타 (1회 공격, 1개 경고)	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> 서버에 대한 공격 (10회 공격, 32개 경고)	드롭 ▼	12개월 미: ▼	<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> HTTP 서버 (4개 경고)	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> 일반 ()	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> 아파치 (1개 경고)	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> 마이크로소프트 IIS (3개 경고)	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> 프론트페이지 ()	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> PHP ()	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> CGI ()	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> 메일 서버 (2회 공격, 14개 경고)	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> Exchange ()	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> Sendmail ()	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> POP3 ()	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> IMAP (7개 경고)	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> SMTP (2회 공격, 7개 경고)	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> 데이터베이스 서버 ()	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> Microsoft SQL 서버 ()	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> MySQL ()	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지
<input checked="" type="checkbox"/> 보통 SQL 공격 ()	드롭 ▼		<input type="checkbox"/> 추가 경고 추가 <input checked="" type="checkbox"/> 공지

- 네트워크 보호 '침입방지' 메뉴에서 IPS(공격 방지) 톨을 확인한다.

2. TCP Syn Flooding 공격 방지

SOPHOS UTM 9

admin | ? | C | ⚙

검색 | 침입 방지

대시보드 | 관리 | 정의 및 사용자 | 인터페이스 및 라우팅 | 네트워크 서비스 | **네트워크 보호** | 방화벽 | NAT | 침입 방지 | 서버 포트 별런싱 | VoIP | 고급

글로벌 | 공격 패턴 | **DoS/플러딩 방지** | 포트 검사 방지 | 예외 | 고급

TCP SYN 플러드 방지

☒ TCP SYN 플러드 방지 사용

모드: 원본과 대상 주소

로그: 제한

원본 패킷 속도 (패킷/초): 50

대상 패킷 속도 (패킷/초): 50

TCP SYN 플러드 방지 설정이 성공적으로 저장되었습니다.

적용

- 네트워크 보호 → 침입 방지 → Dos&플러딩 방지 → TCP STN 플러드 방지 사용

공격

```
[root@kali: ~]# hping3 -I eth0 --syn 192.168.20.200 -p 80 --flood --spoof 119.119.112.112
HPING 192.168.20.200 (eth0 192.168.20.200): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

[hping3 -I eth0 --syn 192.168.20.200 -p 80 --flood --spoof 119.119.112.112]

확인

eth0: Capturing - Wireshark

No.	Time	Source	Destination	Protocol	Info
2315	30.067340	192.168.20.200	119.119.112.112	TCP	http > 21774 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
2316	30.067350	192.168.20.200	119.119.112.112	TCP	http > 34958 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
2317	30.267247	192.168.20.200	119.119.112.112	TCP	http > 37558 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
2318	30.267281	192.168.20.200	119.119.112.112	TCP	http > 19177 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
2319	30.267293	192.168.20.200	119.119.112.112	TCP	http > 46958 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
2320	30.267304	192.168.20.200	119.119.112.112	TCP	http > 18309 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
2321	30.267314	192.168.20.200	119.119.112.112	TCP	http > 15672 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
2322	30.267323	192.168.20.200	119.119.112.112	TCP	http > 42816 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
2323	30.267333	192.168.20.200	119.119.112.112	TCP	http > 26224 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
2324	30.467105	192.168.20.200	119.119.112.112	TCP	http > 46150 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
2325	30.467139	192.168.20.200	119.119.112.112	TCP	http > 27124 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
2326	30.467162	192.168.20.200	119.119.112.112	TCP	http > 38484 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
2327	30.667910	192.168.20.200	119.119.112.112	TCP	http > 36686 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
2328	30.667959	192.168.20.200	119.119.112.112	TCP	http > 32278 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
2329	32.627379	192.168.20.100	192.168.20.1	TCP	krb524 > 50127 [PSH, ACK] Seq=3555 Ack=3209 Win=36096 Len=31

Frame 1809 (58 bytes on wire, 58 bytes captured)

Ethernet II, Src: Vmware_14:3b:a5 (00:0c:29:14:3b:a5), Dst: Vmware_e4:a5:d0 (00:0c:29:e4:a5:d0)

Internet Protocol, Src: 192.168.20.200 (192.168.20.200), Dst: 119.119.112.112 (119.119.112.112)

Transmission Control Protocol, Src Port: http (80), Dst Port: 38404 (38404), Seq: 0, Ack: 1, Len: 0

시스템 정보

정보(M) | 편집(E) | 보기(V) | 도움말(H)

프로세스 | 자원 | 파일시스템

CPU 사용 기록

CPU1: 0.0% CPU2: 0.0% CPU3: 0.0%

메모리 및 스왑 사용 기록

사용자 메모리: 380.0 MB 사용중, 전체 999.9 MB 38.0 %

사용중인 스왑: 0 바이트 사용중, 전체 1.0 GB 0.0 %

네트워크 사용 기록

받은: 204 바이트/s 전체: 259.4 KB

보낸: 0 바이트/s 전체: 284.4 KB

- UTM 방화벽 설정으로 부하가 발생하지 않는다.

3. UDP Flooding 공격 방지

UDP 플러드 방지

☒ UDP 플러드 방지 사용

모드: 원본과 대상 주소

로깅: 제한

원본 패킷 속도 (패킷/초): 50

대상 패킷 속도 (패킷/초): 50

UDP 플러드 방지는 차단된 UDP 패킷 플러드를 감지하고 차단합니다.

적용

UDP 플러드 방지 설정이 성공적으로 저장되었습니다.

- 네트워크 보호 → 침입 방지 → Dos&플러딩 방지 → UDP 플러드 방지 사용

공격

```
[root@kali: ~]# hping3 -I eth0 --udp 192.168.20.200 -p 53 --flood --spoof 119.119.112.112
HPING 192.168.20.200 (eth0 192.168.20.200): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

[hping3 -I eth0 --udp 192.168.20.200 -p 53 --flood --spoof 119.119.112.112]

확인

The figure consists of two screenshots. The left screenshot shows a Wireshark packet capture on the eth0 interface, filtered for UDP. It displays a series of 'Malformed Packet' entries for DNS requests from 119.119.112.112 to 192.168.20.200 on port 53. The right screenshot shows the Windows Task Manager 'System' tab, displaying system performance metrics: CPU usage is 0.0% for all three cores, memory usage is 38.2% (381.6 MB used of 999.9 MB total), and network usage is 0.0% (0 B/s sent/received).

- UTM 방화벽 설정으로 부하가 발생하지 않는다.

4. ICMP Flooding 공격 방지

ICMP 플러드 방지

☒ ICMP 플러드 방지 사용

모드: 원본과 대상 주소

로깅: 제한

원본 패킷 속도 (패킷/초): 10

대상 패킷 속도 (패킷/초): 20

ICMP 플러드 방지는 ICMP 패킷 플러드를 감지하고 차단합니다.

ICMP 플러드 방지 설정이 성공적으로 저장되었습니다.

적용

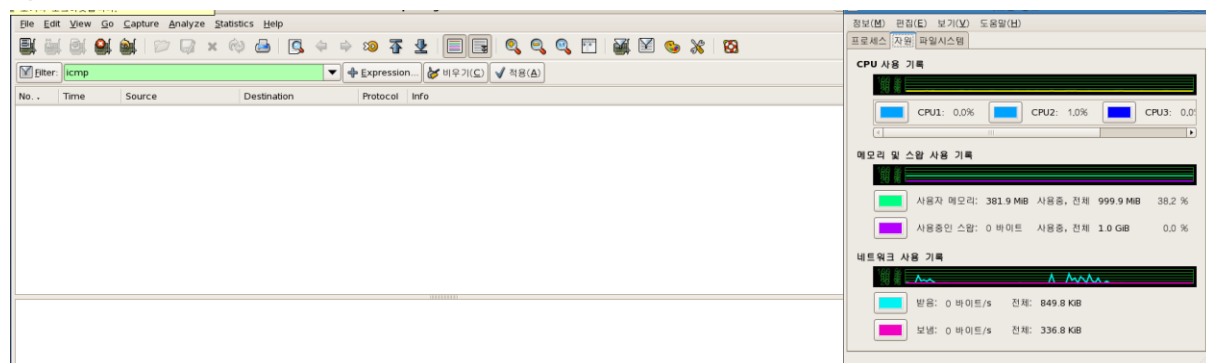
- 네트워크 보호 → 침입 방지 → Dos&플러딩 방지 → ICMP 플러드 방지 사용

공격

```
[root@kali: ~]# hping3 -I eth0 --icmp 192.168.20.200 --flood --spooof 119.112.119.112 -d 60000
HPING 192.168.20.200 (eth0 192.168.20.200): icmp mode set, 28 headers + 60000 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.20.200 hping statistic ---
23699 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@kali: ~]#
```

[hping3 -I eth0 --icmp 192.168.20.200 --flood --spooof 119.112.119.112 -d 60000]

확인



- 방화벽 기본 설정에서 ICMP를 차단하고 있기 때문에 Ping이 수신 되지 않는다.

이와 같이 UTM 방화벽을 설정하여 다양한 네트워크 공격을 방지할 수 있습니다.