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 **드롭**을 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.

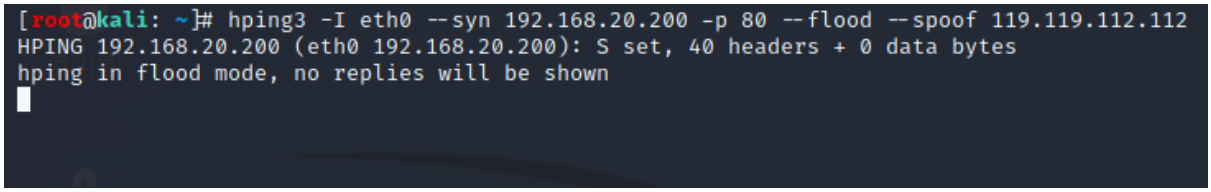
상태 / 그룹 이름	동작	규칙 기간	옵션
운영 체제 대상 공격 (4회 공격, 55개 경고)	드롭	12개월 미	추가 경고 추가 / 공지
Windows (3회 공격, 54개 경고)	드롭		추가 경고 추가 / 공지
리눅스 ()	드롭		추가 경고 추가 / 공지
기타 (1회 공격, 1개 경고)	드롭		추가 경고 추가 / 공지
서버에 대한 공격 (10회 공격, 32개 경고)	드롭	12개월 미	추가 경고 추가 / 공지
HTTP 서버 (4개 경고)	드롭		추가 경고 추가 / 공지
일반 ()	드롭		추가 경고 추가 / 공지
아파치 (1개 경고)	드롭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

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

2. TCP Syn Flooding 공격 방지

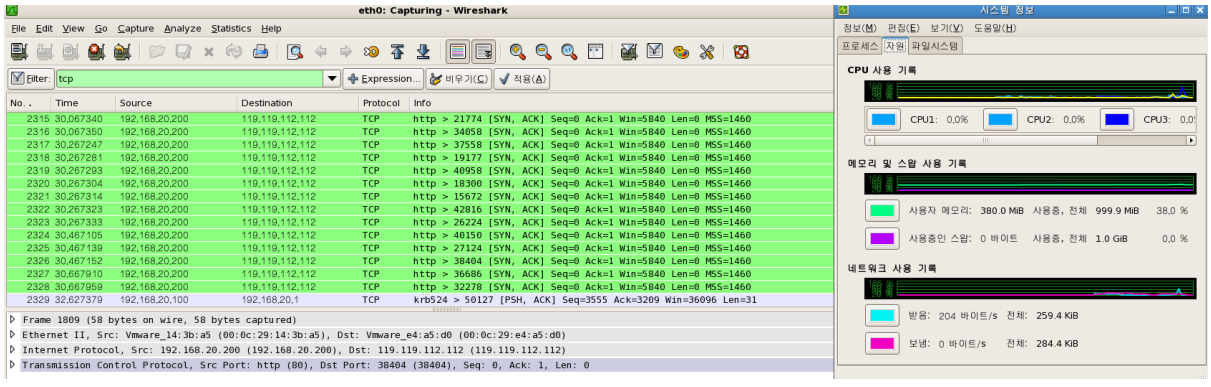
- 네트워크 보호 → 침입 방지 → Dos&플러딩 방지 → TCP STN 플러드 방지 사용

공격



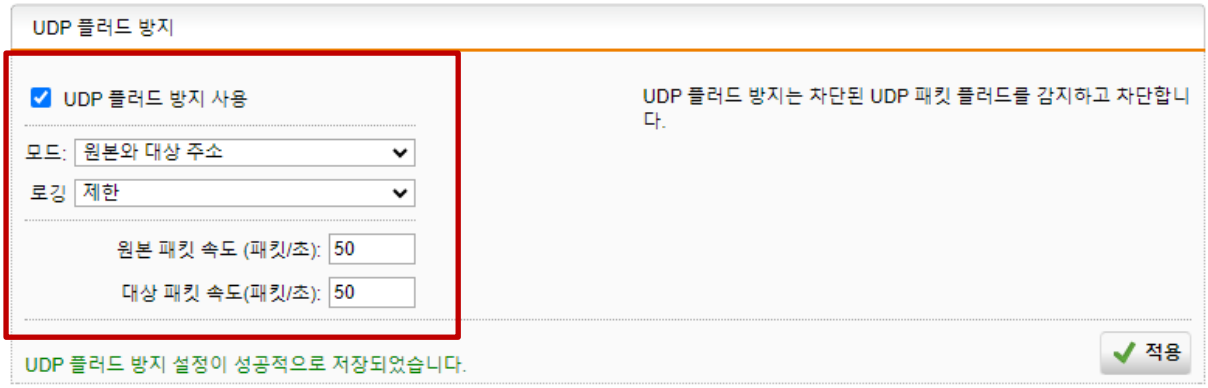
[hping3 -I eth0 --syn 192.168.20.200 -p 80 --flood --spoof 119.119.112.112]

확인



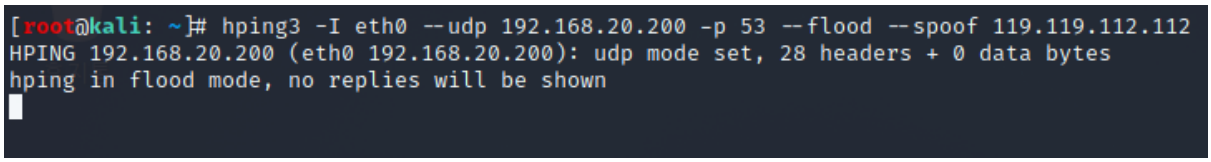
- UTM 방화벽 설정으로 부하가 발생하지 않는다.

3. UDP Flooding 공격 방지



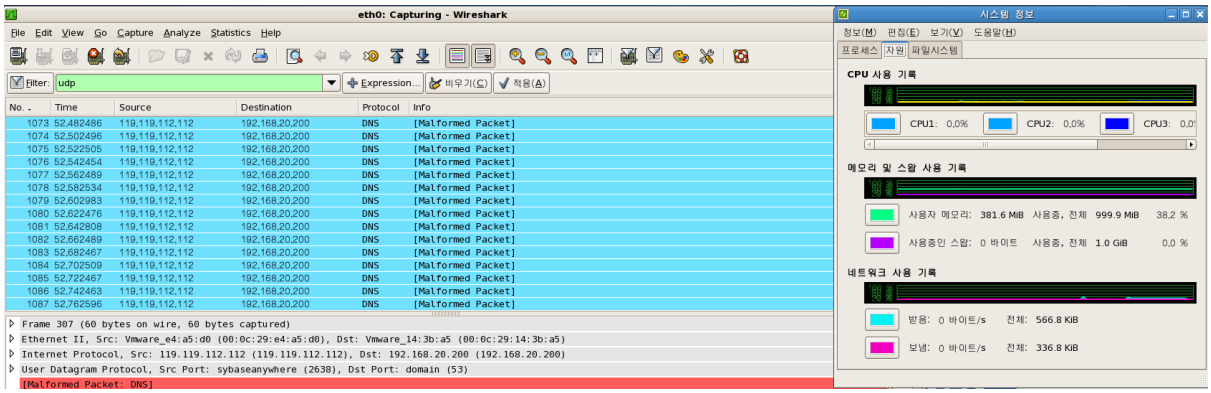
- 네트워크 보호 → 침입 방지 → Dos&플러딩 방지 → UDP 플러드 방지 사용

공격



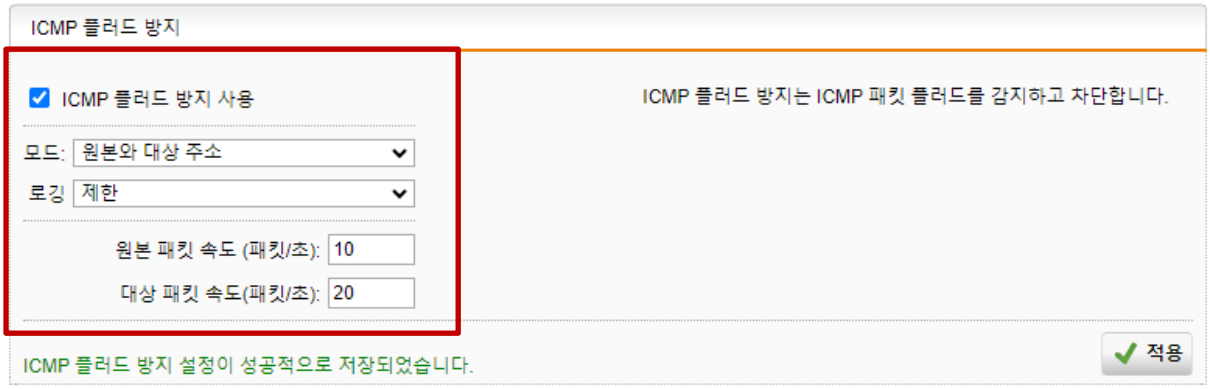
[hping3 -I eth0 --udp 192.168.20.200 -p 53 --flood --spoof 119.119.112.112]

확인



- - UTM 방화벽 설정으로 부하가 발생하지 않는다.

4. ICMP Flooding 공격 방지



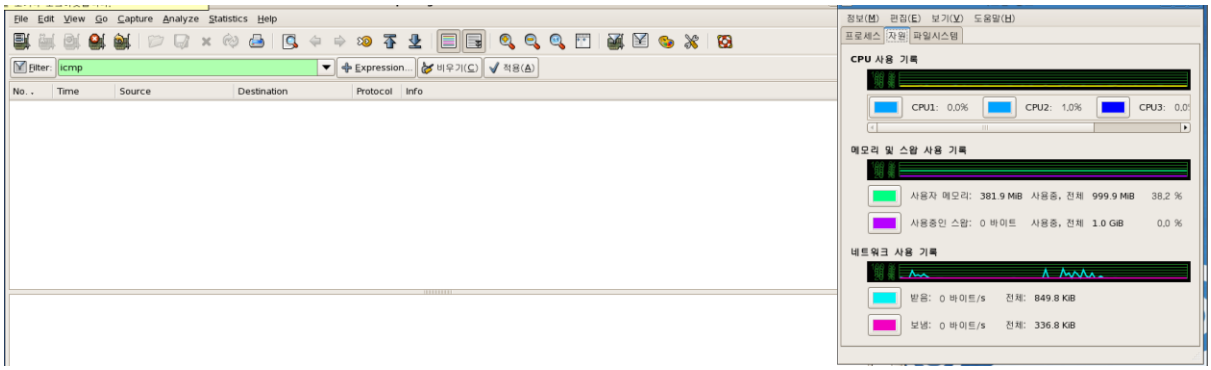
- 네트워크 보호 → 침입 방지 → Dos&플러딩 방지 → ICMP 플러드 방지 사용

공격

```
[root@kali: ~]# hping3 -I eth0 --icmp 192.168.20.200 --flood --spoof 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 --spoof 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.