

# Ping of Death 공격 탐지 정책 생성

## ❶ [Kali] Ping of Death 공격

```
#hping3 --icmp --rand-source 192.168.10.20 -d 2000 --flood
```

## ❷ 공격 시 와이어샤크를 이용하여 공격패턴탐지

## ❸ [NIDS] Ping of Death 공격에한 탐지 정책 생성과 적용

- Detection rule name : Ping of Death **X** Class

- SID : 3000004

- 해당 시그니처가 10초안에 50번 탐지될 경우 로그 생성

## ❹ [Kali] Ping of Death 공격

## ❺ [NIDS] Sguil을 통해 Ping of Death 공격 탐지 확인

제출화면

- Sguil 공격 탐지 확인

(show rule를 마크해서조이름이  
나와야 함)