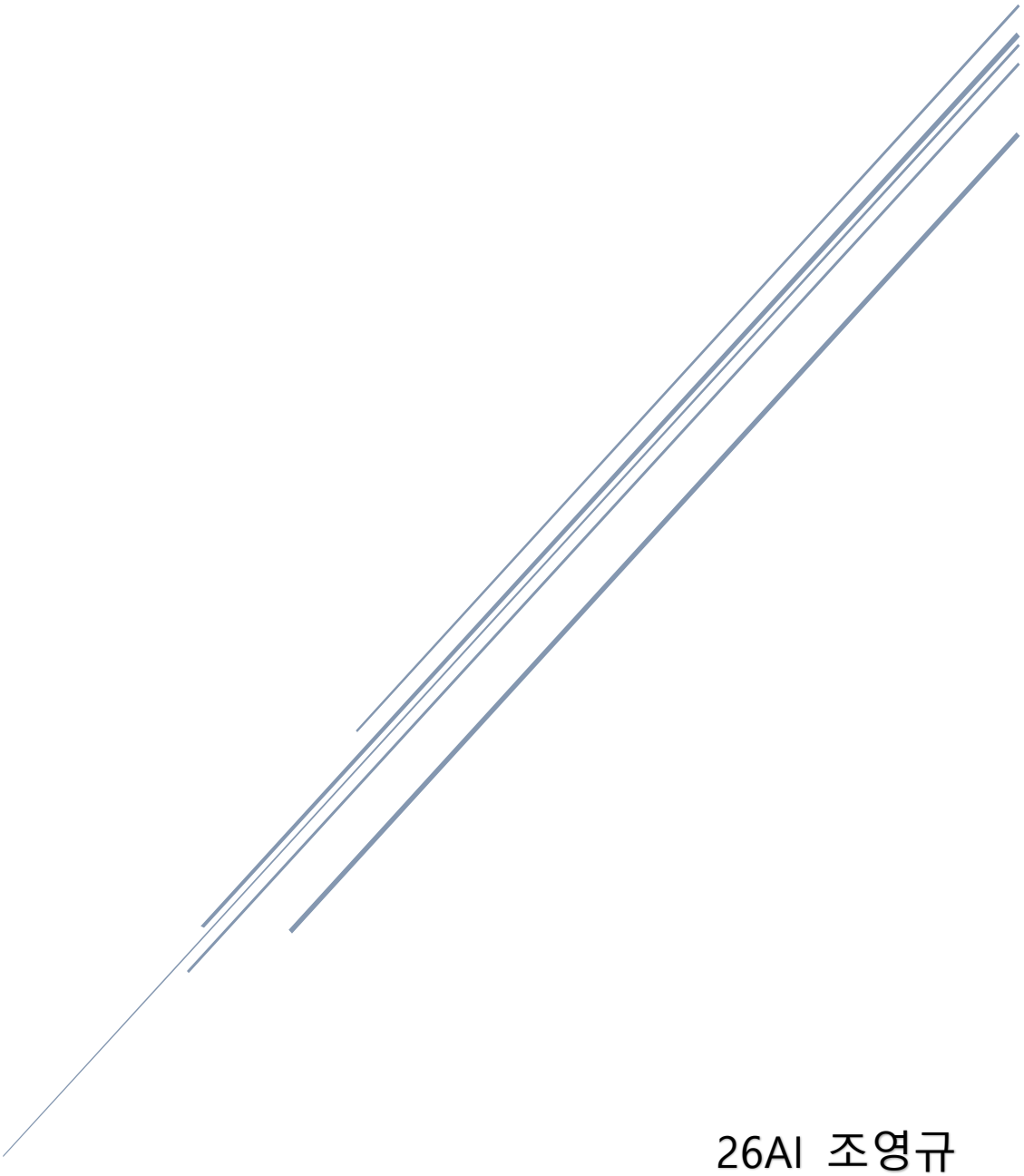
Ping of Death 공격 탐지 정책 생성

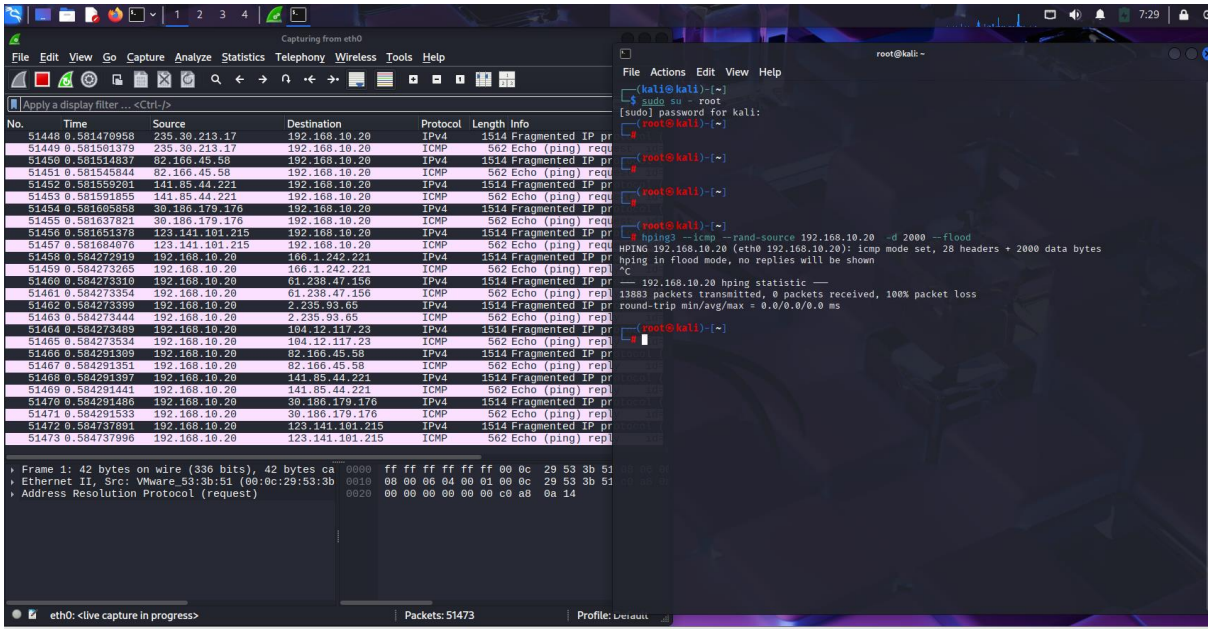
공격 패턴 분석을 통한 탐지 룰 생성 및 로그 확인



26AI 조영규

목차

1. Ping of Death 공격



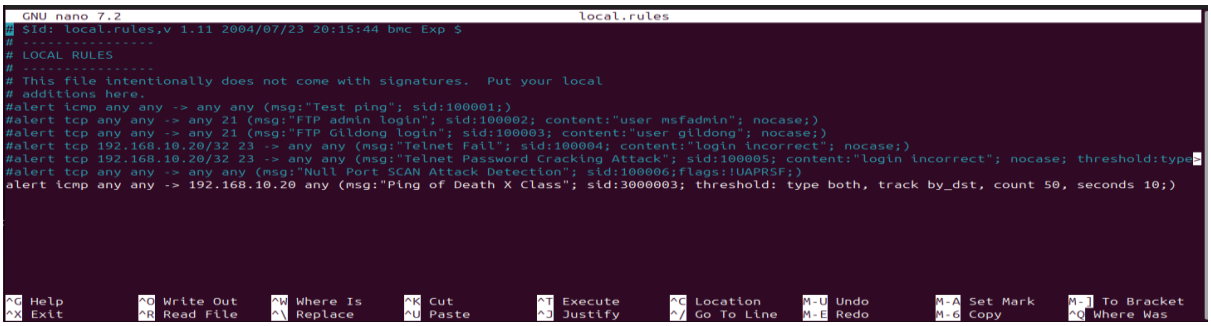
- Hping3 --icmp –random-source 192.168.10.20 -d 2000 --flood 명령어를 통해 서버에게 Ping of Death 공격을 하고, 와이어 샤크를 통해 패킷을 캡처한다.

1.2 공격 패턴 탐지

- 와이어 샤크를 보면 단기간 내에 다량의 ICMP 패킷이 전송된 것을 확인할 수 있다. DOS 공격으로, 단기간에 많은 ICMP 패킷을 전송하는 것을 시그니처로, 이를 이용해 공격에 대한 탐지 정책을 생성하여 적용한다.

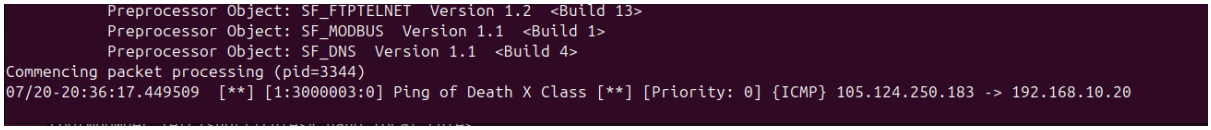
2. 공격에 대한 탐지 Rule 생성 및 적용

- Detection Rule Name: Ping if Death X Class
- SID: 3000003
- 해당 시그니처가 10초 안에 50번 탐지될 경우 로그 생성
- 생성한 rule:



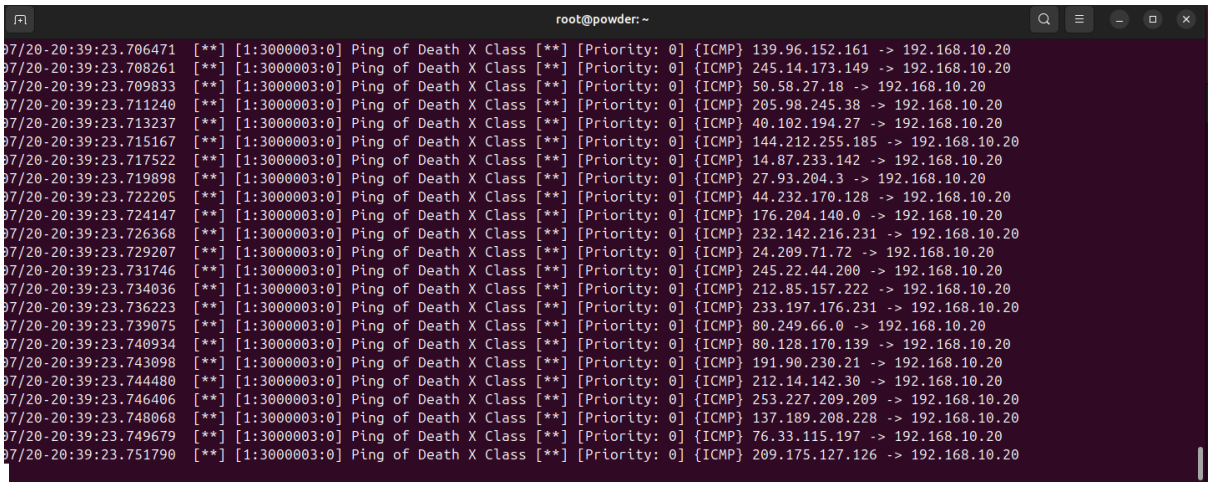
3. Rule 적용 후 공격 탐지

3.1 Threshold: type both



- 이벤트에 대해 로그가 1개만 생성되는 것을 확인할 수 있다.

3.2 Threshold: type threshold



- 로그 발생 기준을 만족하면 모두 로그 생성되는 것을 확인할 수 있다.