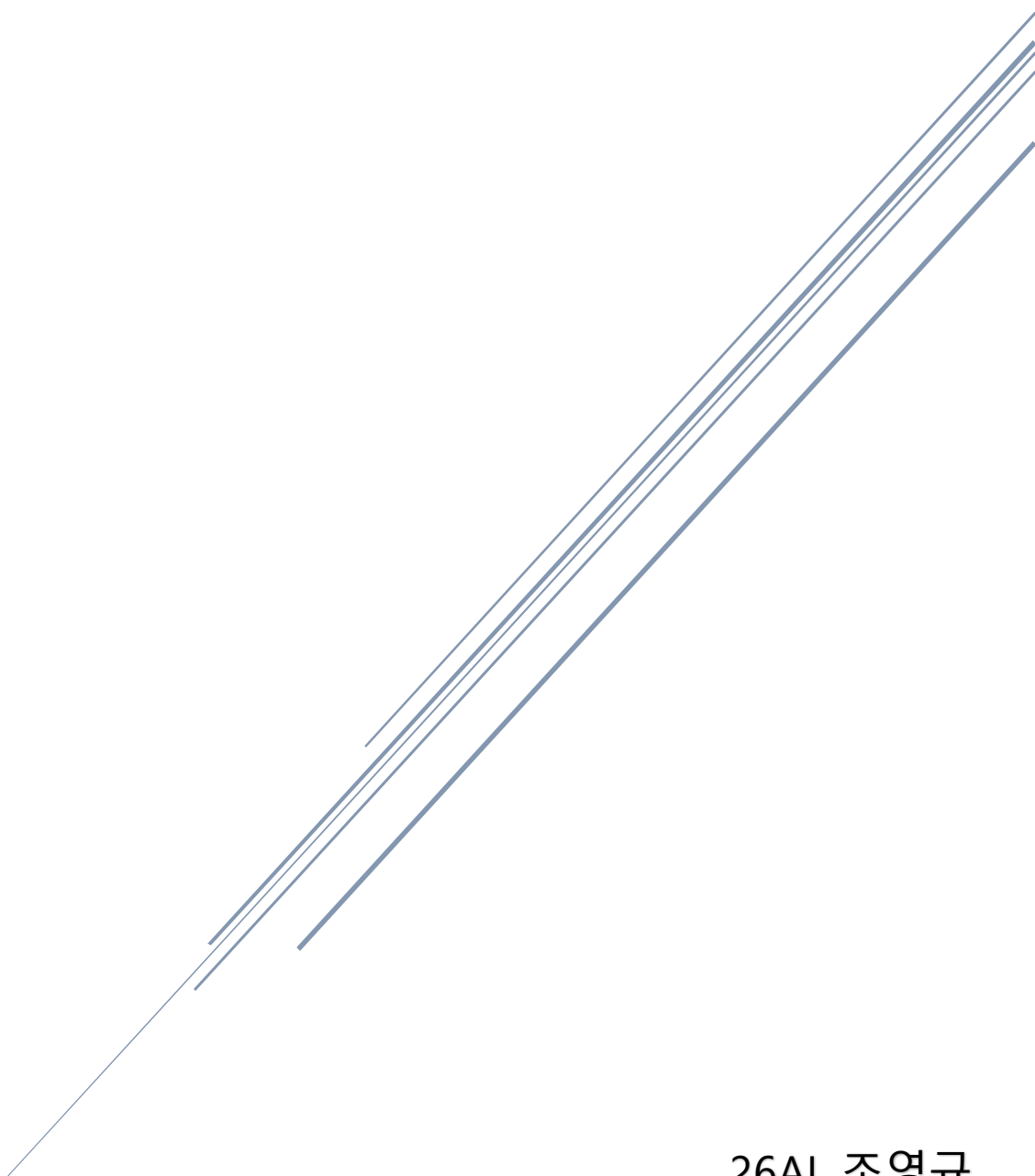


Ping of Death 공격 탐지 정책 생성

공격 패턴 분석을 통한 탐지 룰 생성 및 로그 확인

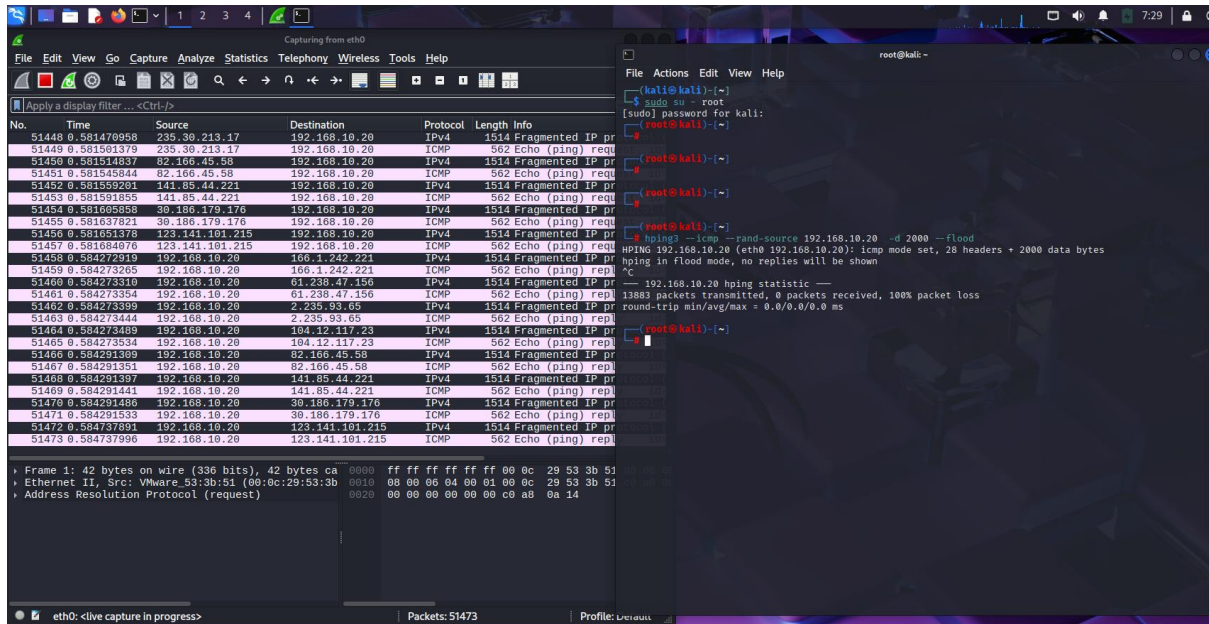


26AI 조영규

목차

1. Ping of Death 공격	2
1.2 공격 패턴 탐지	2
2. 공격에 대한 탐지 Rule 생성 및 적용	2
3. Rule 적용 후 공격 탐지	3
3.1 Threshold: type both	3
3.2 Threshold: type threshold	3

1. Ping of Death 공격



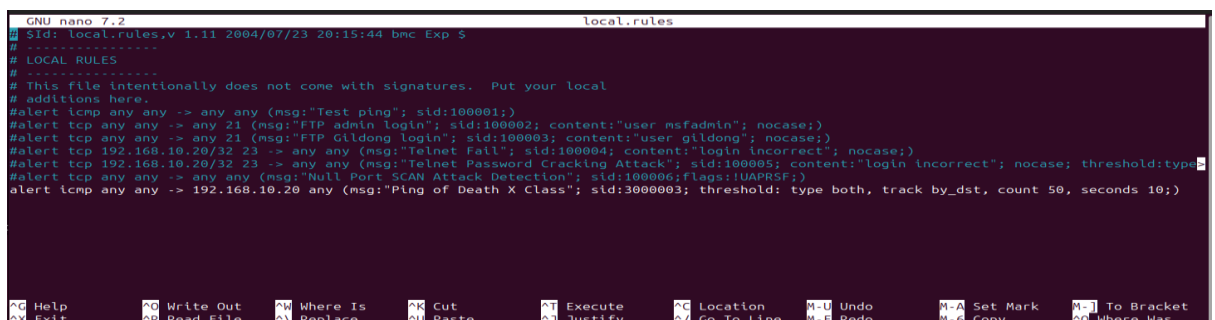
- Hping3 --icmp --random-source 192.168.10.20 -d 2000 --flood 명령어를 통해 서버에게 Ping of Death 공격을 하고, 와이어 샤크를 통해 패킷을 캡처한다.

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

```
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Commencing packet processing (pid=3344)
07/20-20:36:17.449509  [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 105.124.250.183 -> 192.168.10.20
```

- 이벤트에 대해 로그가 1개만 생성되는 것을 확인할 수 있다.

3.2 Threshold: type threshold

```
root@powder: ~
87/20-20:39:23.706471 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 139.96.152.161 -> 192.168.10.20
87/20-20:39:23.708261 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 245.14.173.149 -> 192.168.10.20
87/20-20:39:23.709833 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 50.58.27.18 -> 192.168.10.20
87/20-20:39:23.711240 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 205.98.245.38 -> 192.168.10.20
87/20-20:39:23.713237 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 40.102.194.27 -> 192.168.10.20
87/20-20:39:23.715167 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 144.212.255.185 -> 192.168.10.20
87/20-20:39:23.717522 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 14.87.233.142 -> 192.168.10.20
87/20-20:39:23.719898 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 27.93.204.3 -> 192.168.10.20
87/20-20:39:23.722205 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 44.232.170.128 -> 192.168.10.20
87/20-20:39:23.724147 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 176.204.140.0 -> 192.168.10.20
87/20-20:39:23.726368 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 232.142.216.231 -> 192.168.10.20
87/20-20:39:23.729207 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 24.209.71.72 -> 192.168.10.20
87/20-20:39:23.731746 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 245.22.44.200 -> 192.168.10.20
87/20-20:39:23.734036 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 212.85.157.222 -> 192.168.10.20
87/20-20:39:23.736223 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 233.197.176.231 -> 192.168.10.20
87/20-20:39:23.739075 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 80.249.66.0 -> 192.168.10.20
87/20-20:39:23.740934 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 80.128.170.139 -> 192.168.10.20
87/20-20:39:23.743098 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 191.90.230.21 -> 192.168.10.20
87/20-20:39:23.744480 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 212.14.142.30 -> 192.168.10.20
87/20-20:39:23.746406 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 253.227.209.209 -> 192.168.10.20
87/20-20:39:23.748068 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 137.189.208.228 -> 192.168.10.20
87/20-20:39:23.749679 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 76.33.115.197 -> 192.168.10.20
87/20-20:39:23.751790 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 209.175.127.126 -> 192.168.10.20
```

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