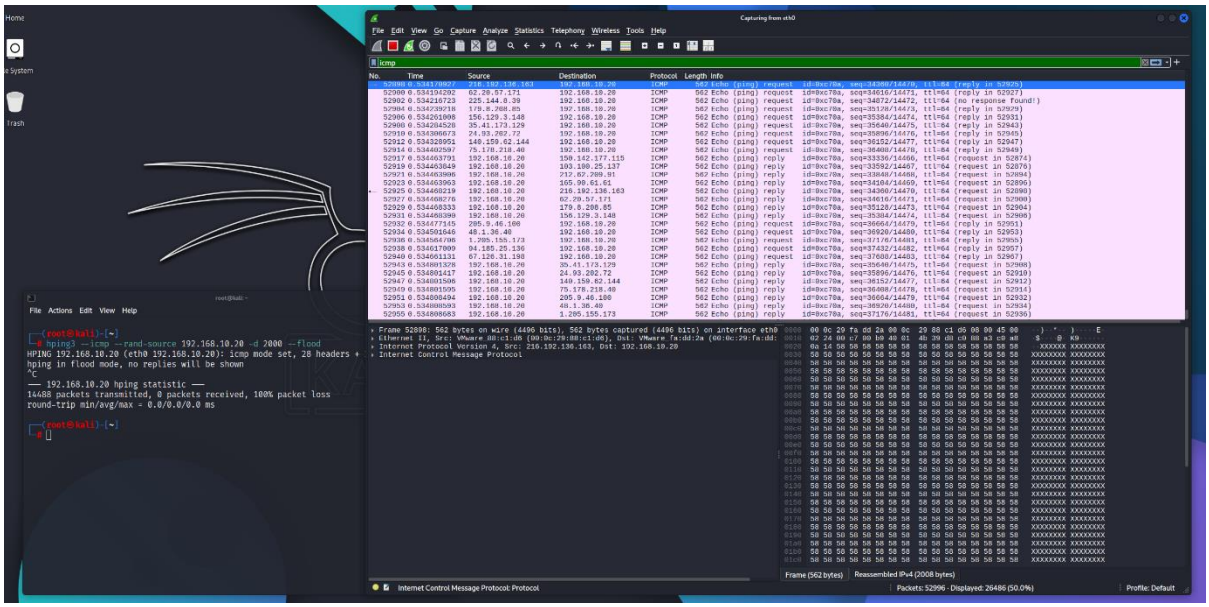
Ping of Death 공격 탐지 정책 생성

공격 패턴 분석을 통한 탐지 룰 생성 및 로그 확인

Ping of Death 공격에 대한 탐지 정책을 생성합니다. 공격 패턴을 파악하여 관제 룰을 생성하고 생성된 룰을 통해 실제 공격 시 탐지된 로그를 확인합니다.

1. **[Kali] Ping of Death 공격**

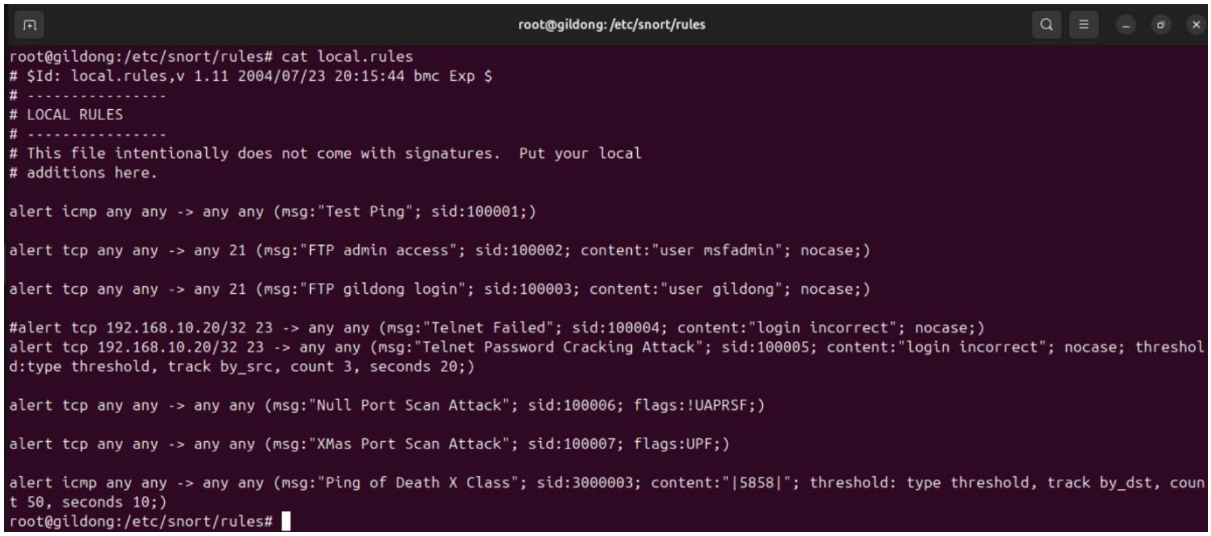
   #hping3 –icmp –rand-source 192.168.10.20 -d 2000 –flood 명령어를 통해 Ping of Death 공격을 수행합니다. Wireshark에서 해당 공격의 패킷을 분석한 결과 패킷 바이트에서 58이 반복되는 공격 패턴을 탐지합니다.



2. **[NIDS] Ping of Death 공격 탐지 정책**

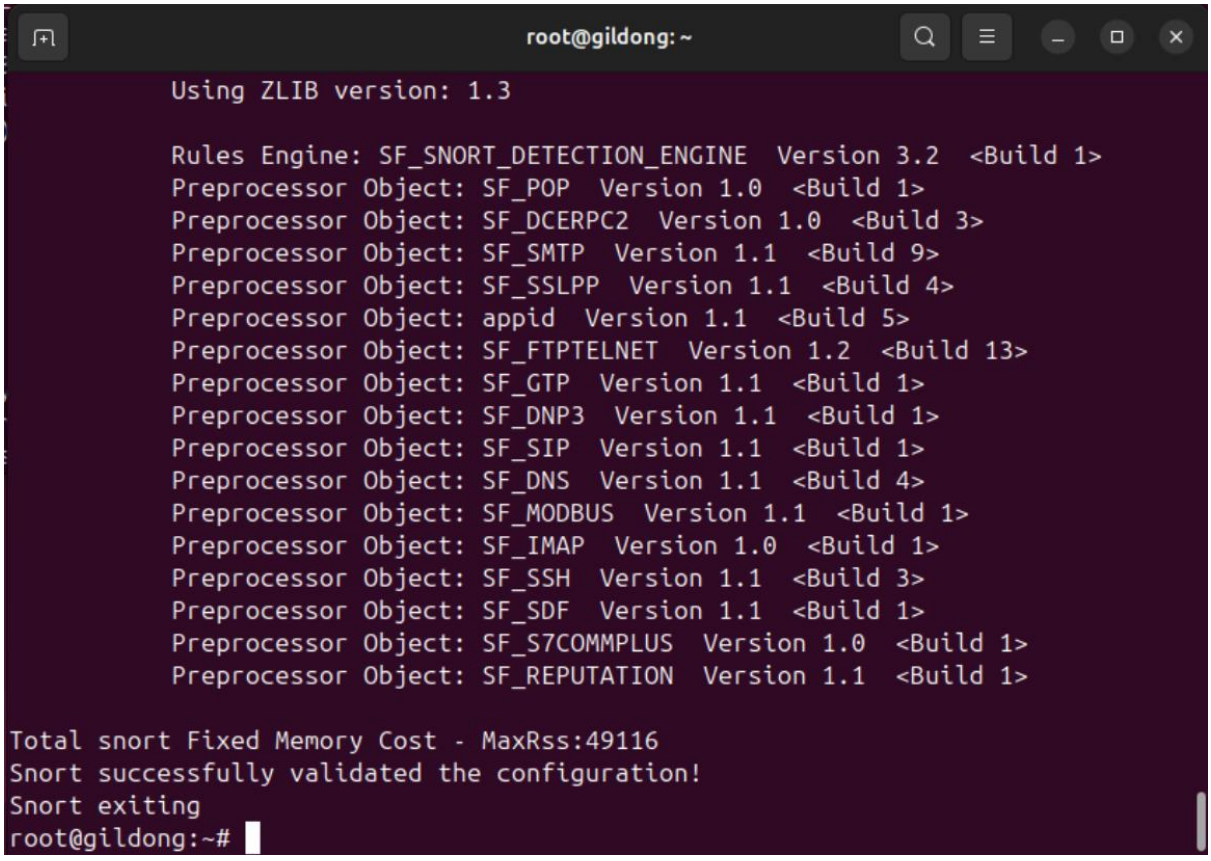
   #nano local.rules 명령어를 통해 관제 룰을 생성합니다. local.rules 파일 내 alert icmp any any -> any any (msg:"Ping of Death X Class"; sid:3000003; content:"|5858|"; threshold: type threshold, track by_dst, count 50, seconds 10;)을 입력하고 저장합니다.

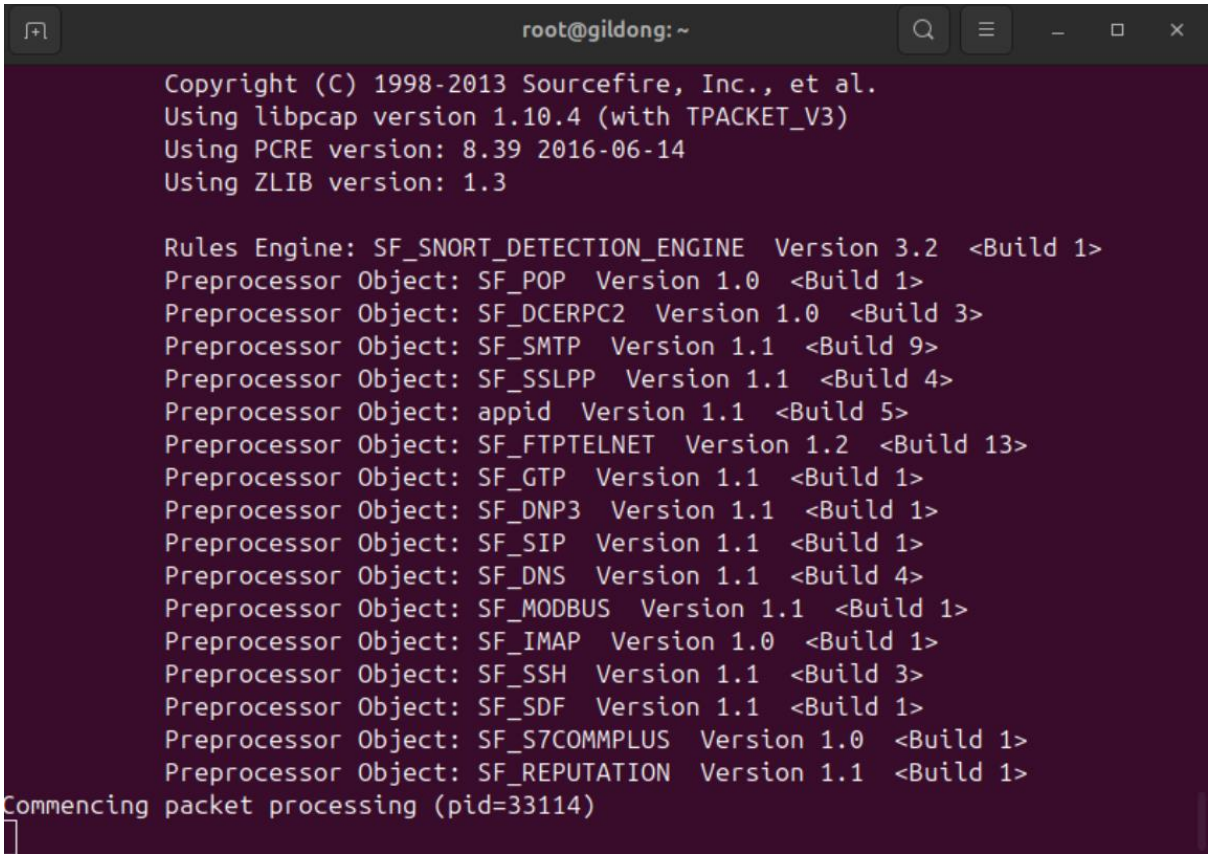
   #snort -T -c /etc/snort/snort.conf 명령어를 통해 오탈자나 문법 오류가 없는지 확인한 후 #snort -i eth0 -c /etc/snort/snort.conf 명령어를 통해 관제 룰을 적용합니다.


root@gildong: /etc/snort/rules
root@gildong:/etc/snort/rules# cat local.rules
$Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $

LOCAL RULES

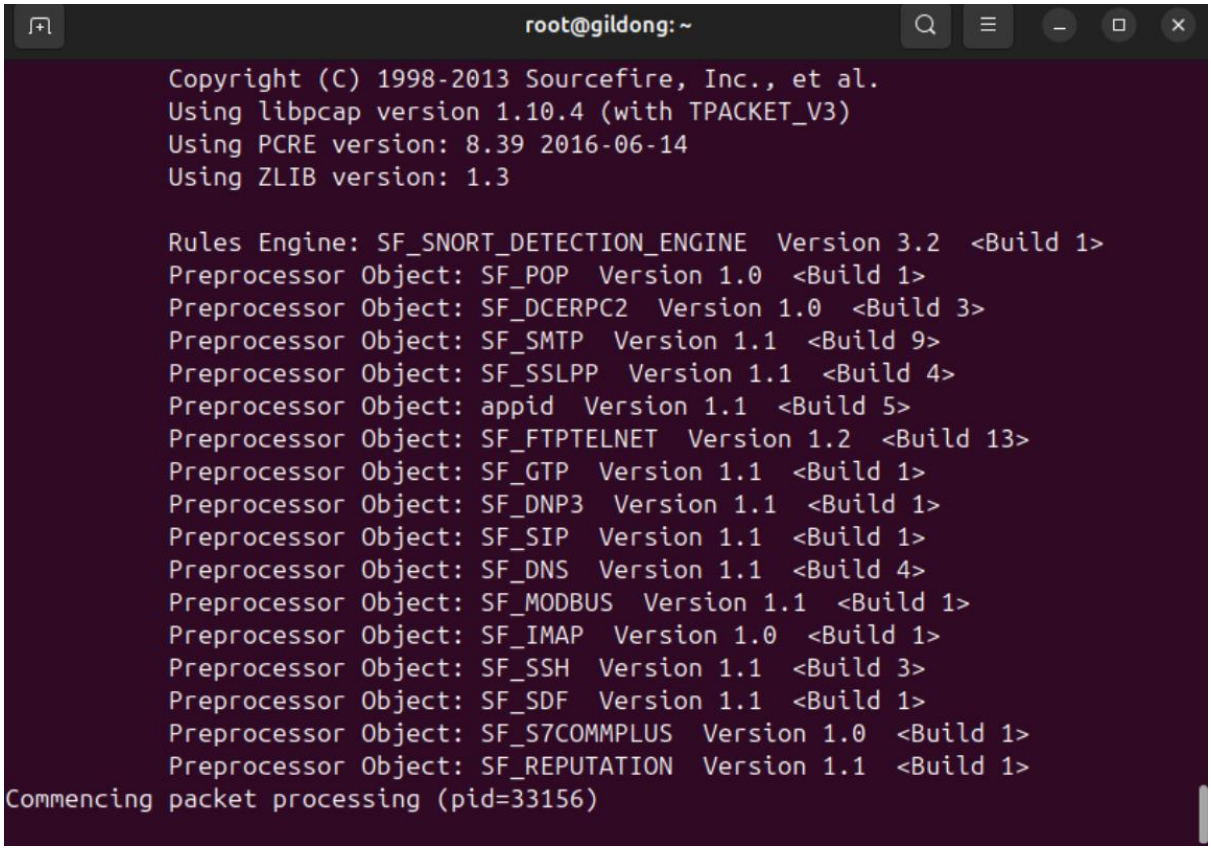
This file intentionally does not come with signatures. Put your local
additions here.
alert icmp any any -> any any (msg:"Test Ping"; sid:100001;)
alert tcp any any -> any 21 (msg:"FTP admin access"; sid:100002; content:"user msfadmin"; nocase;)
alert tcp any any -> any 21 (msg:"FTP gildong login"; sid:100003; content:"user gildong"; nocase;)
#alert tcp 192.168.10.20/32 23 -> any any (msg:"Telnet Failed"; sid:100004; content:"login incorrect"; nocase;)
alert tcp 192.168.10.20/32 23 -> any any (msg:"Telnet Password Cracking Attack"; sid:100005; content:"login incorrect"; nocase; threshol
d:type threshold, track by_src, count 3, seconds 20;)
alert tcp any any -> any any (msg:"Null Port Scan Attack"; sid:100006; flags:!UAPRSF;)
alert tcp any any -> any any (msg:"XMas Port Scan Attack"; sid:100007; flags:UPF;)
alert icmp any any -> any any (msg:"Ping of Death X Class"; sid:3000003; content:"|5858|"; threshold: type threshold, track by_dst, coun
t 50, seconds 10;)
root@gildong:/etc/snort/rules#

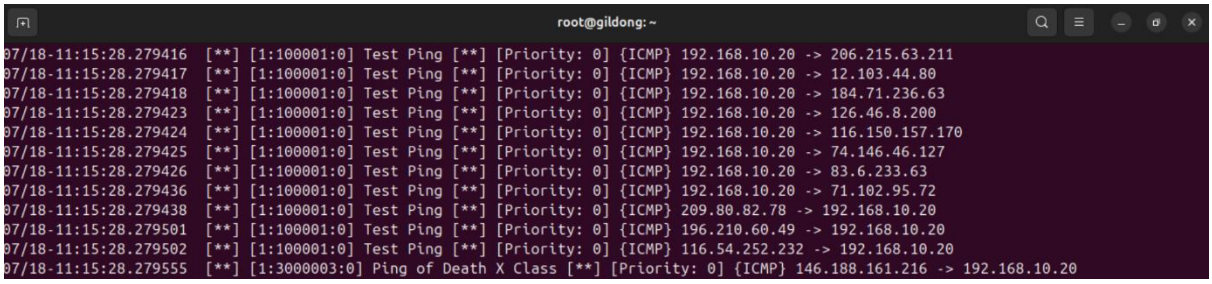

root@gildong: ~
Using ZLIB version: 1.3
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Total snort Fixed Memory Cost - MaxRss:49116
Snort successfully validated the configuration!
Snort exiting
root@gildong:~#



3. **[NIDS] Ping of Death 공격 탐지 확인**

   #snort -A console -c /etc/snort/snort.conf 명령어를 통해 콘솔에서 실시간으로 탐지를 확인합니다. 콘솔에서 정상적으로 탐지되었음을 확인합니다.


root@gildong: ~
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Commencing packet processing (pid=33156)


root@gildong: ~
07/18-11:15:28.279416 [**] [1:100001:0] Test Ping [**] [Priority: 0] {ICMP} 192.168.10.20 -> 206.215.63.211
07/18-11:15:28.279417 [**] [1:100001:0] Test Ping [**] [Priority: 0] {ICMP} 192.168.10.20 -> 12.103.44.80
07/18-11:15:28.279418 [**] [1:100001:0] Test Ping [**] [Priority: 0] {ICMP} 192.168.10.20 -> 184.71.236.63
07/18-11:15:28.279423 [**] [1:100001:0] Test Ping [**] [Priority: 0] {ICMP} 192.168.10.20 -> 126.46.8.200
07/18-11:15:28.279424 [**] [1:100001:0] Test Ping [**] [Priority: 0] {ICMP} 192.168.10.20 -> 116.150.157.170
07/18-11:15:28.279425 [**] [1:100001:0] Test Ping [**] [Priority: 0] {ICMP} 192.168.10.20 -> 74.146.46.127
07/18-11:15:28.279426 [**] [1:100001:0] Test Ping [**] [Priority: 0] {ICMP} 192.168.10.20 -> 83.6.233.63
07/18-11:15:28.279436 [**] [1:100001:0] Test Ping [**] [Priority: 0] {ICMP} 192.168.10.20 -> 71.102.95.72
07/18-11:15:28.279438 [**] [1:100001:0] Test Ping [**] [Priority: 0] {ICMP} 209.80.82.78 -> 192.168.10.20
07/18-11:15:28.279501 [**] [1:100001:0] Test Ping [**] [Priority: 0] {ICMP} 196.210.60.49 -> 192.168.10.20
07/18-11:15:28.279502 [**] [1:100001:0] Test Ping [**] [Priority: 0] {ICMP} 116.54.252.232 -> 192.168.10.20
07/18-11:15:28.279555 [**] [1:3000003:0] Ping of Death X Class [**] [Priority: 0] {ICMP} 146.188.161.216 -> 192.168.10.20