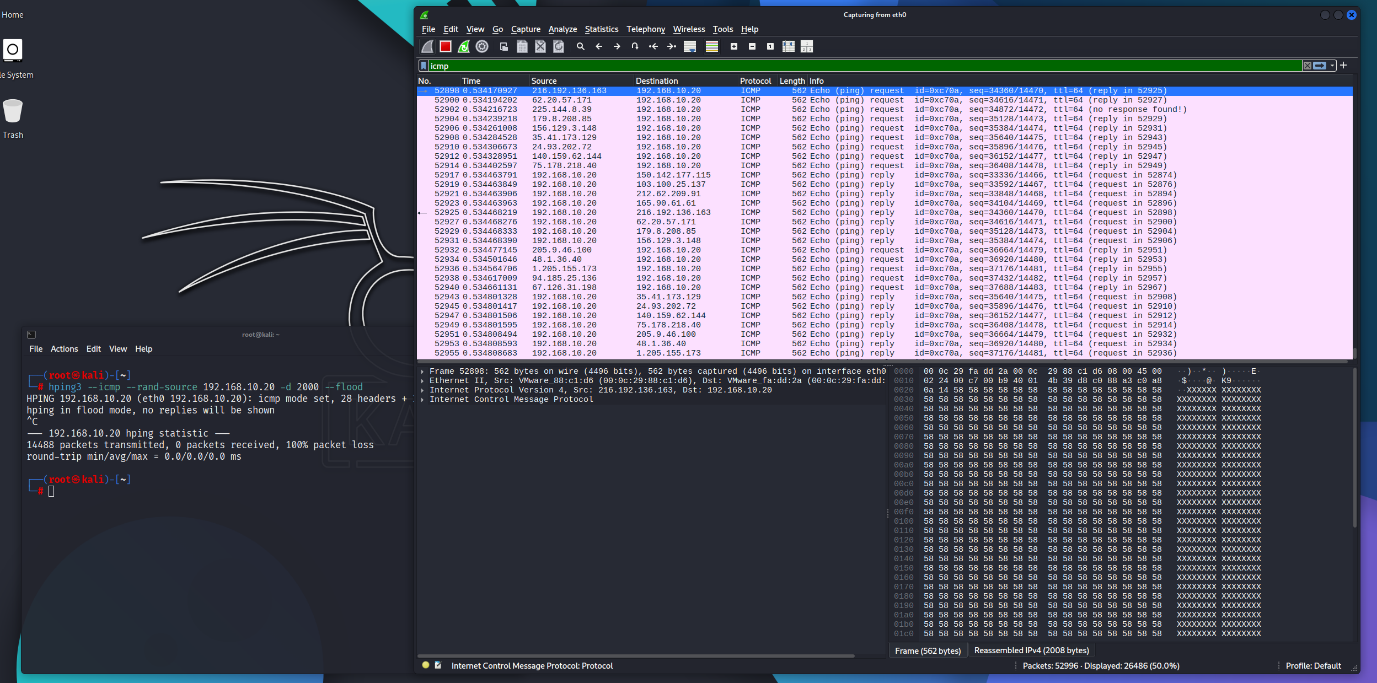
**Ping of Death 공격 탐지 정책 생성**

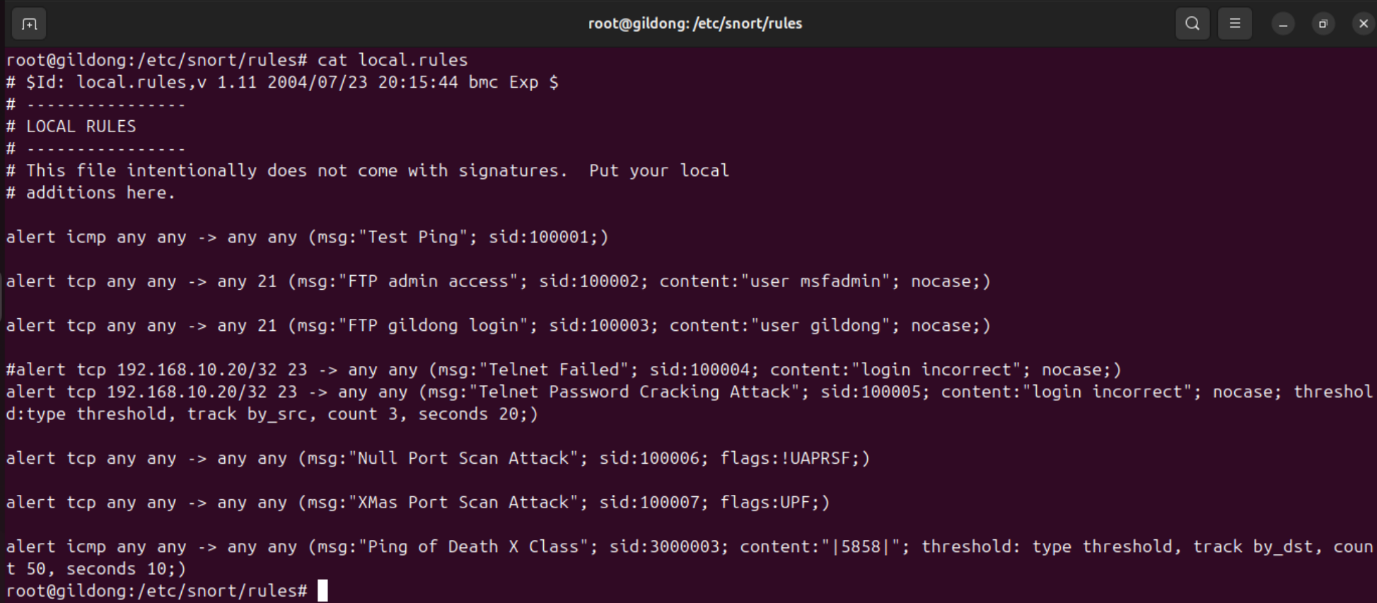
공격 패턴 분석을 통한 탐지 룰 생성 및 로그 확인

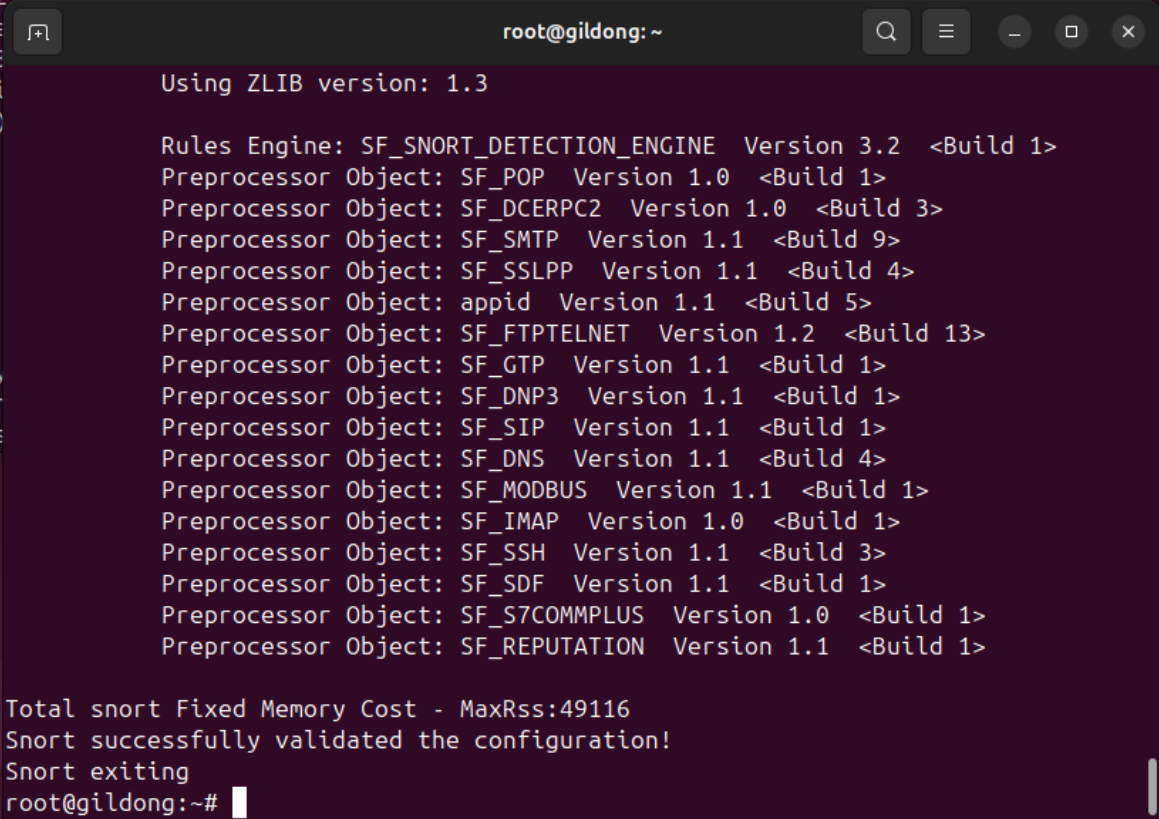
Ping of Death 공격에 대한 탐지 정책을 생성합니다. 공격 패턴을 파악하여 관제 룰을 생성하고 생성된 룰을 통해 실제 공격 시 탐지된 로그를 확인합니다.

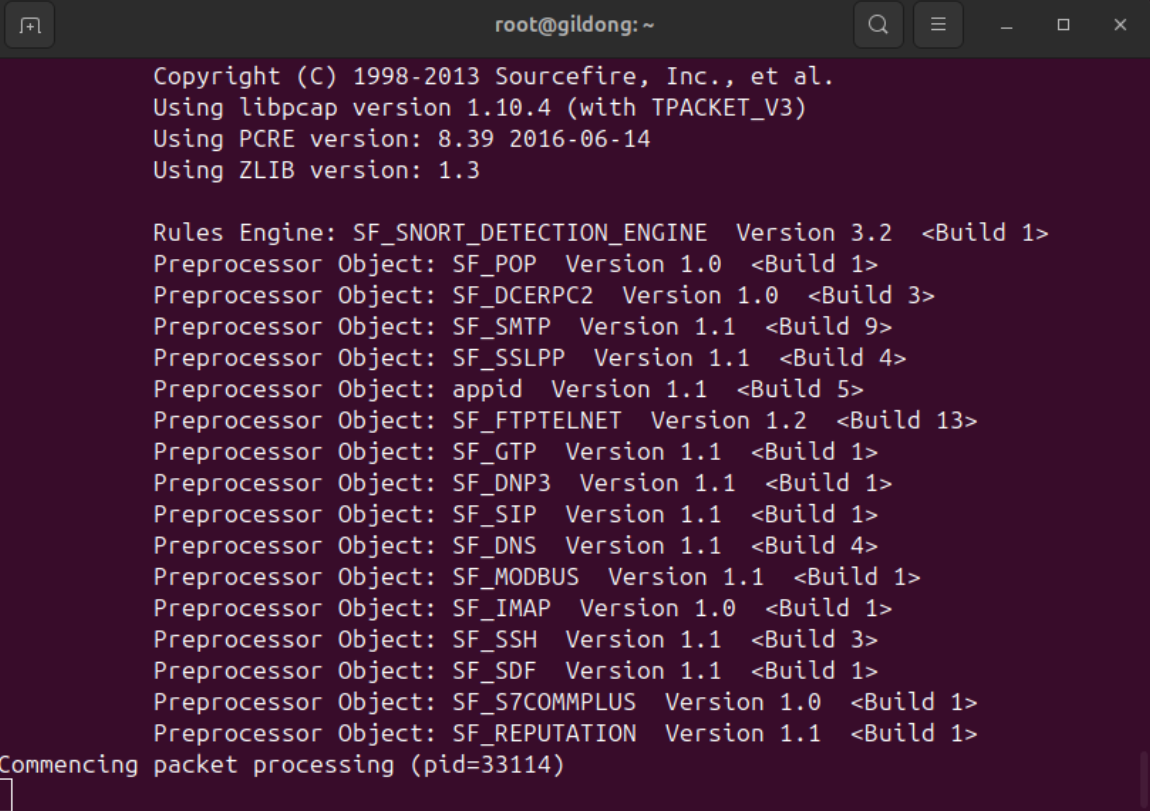
1. **[Kali] Ping of Death 공격**  
   #hping3 –icmp –rand-source 192.168.10.20 -d 2000 –flood 명령어를 통해 Ping of Death 공격을 수행합니다. Wireshark에서 해당 공격의 패킷을 분석한 결과 패킷 바이트에서 58이 반복되는 공격 패턴을 탐지합니다.



1. **[NIDS] Ping of Death 공격 탐지 정책**  
   #nano local.rules 명렁어를 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.







1. **[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.

