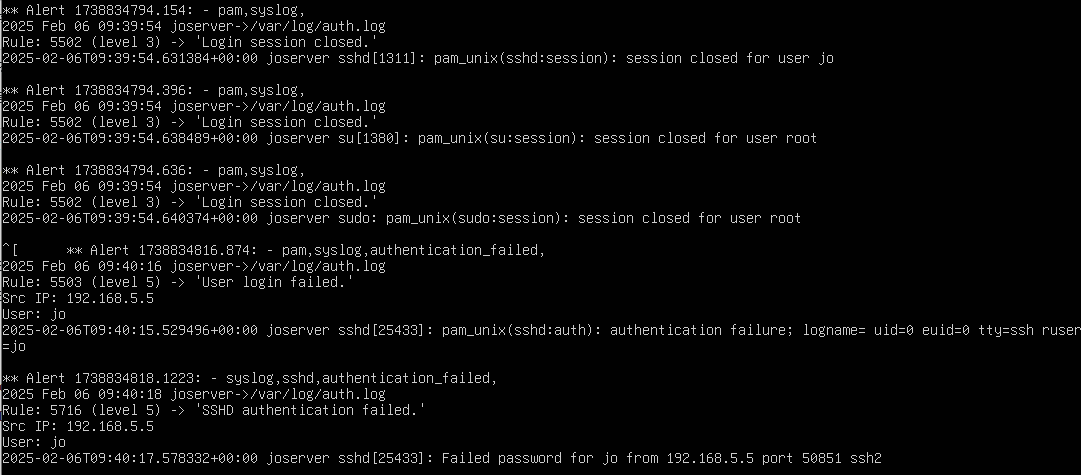
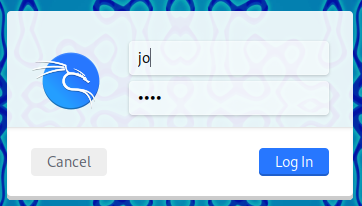
* 1. **~ 1.3 Kali, Web Server, OSSEC, Suricata를 설치하여 정상 동작이 가능하도록 하시오. (Kali, Web Server는 제외)**

OSSEC 감지 정상 동작 화면



Suricata 감지 정상 동작 화면

**1.4 Kali 시스템에 사용자(본인이름)를 추가하고 패스워드를 설정하도록 하시오.**

칼리 본인이름으로 로그인

**2.1 ~ 2.5 Suricata Rule을 정책 조건에 맞게 설정하고 탐지 테스트를 진행하시오.**

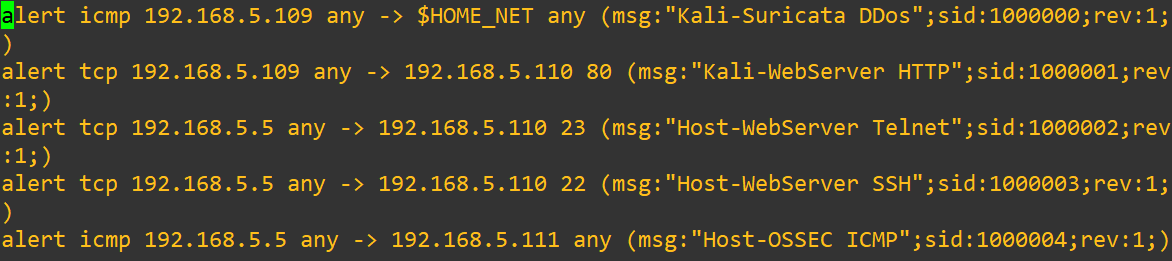
HOST(Window) IP - 192.168.5.5

Suricata IP - 192.168.5.108

Kali IP - 192.168.5.109

WebServer IP - 192.168.5.110

OSSEC IP - 192.168.5.111

Suricata rules 설정

 1. Kali -> Suricata : DDoS 공격 탐지

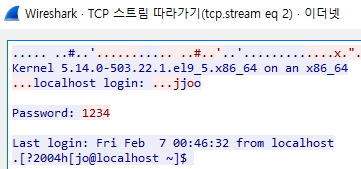
 2. Kali -> Web Server : HTTP 접속 탐지

 3. Host(Windows) -> Web Server : Telnet 접속 탐지

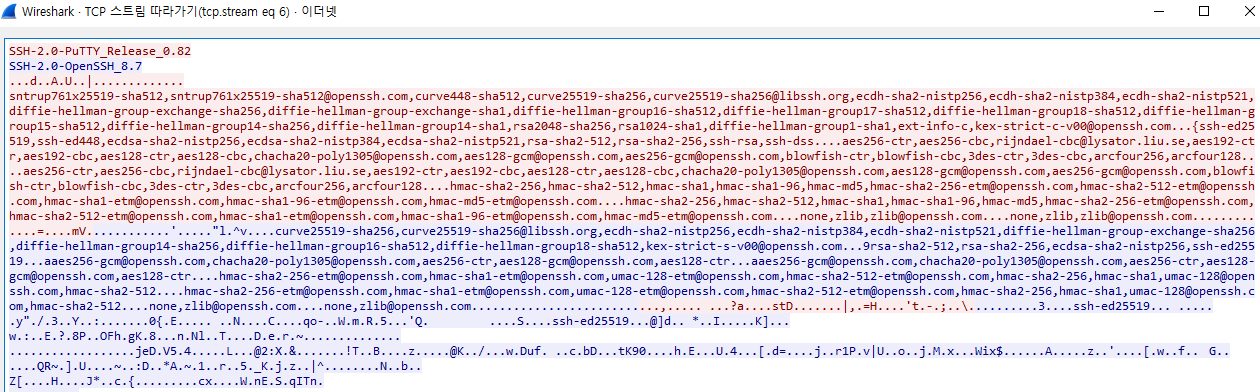
 4. Host(Windows) -> Web Server : ssh 접속 탐지

 5. Host(Windows) -> OSSEC : ICMP 패킷 탐지

**2.6 위의 탐지되는 패킷들 중 Telnet 및 ssh 트래픽을 Wireshark로 캡처하여 스트림 분석을 통해 차이점을 확인하시오.**

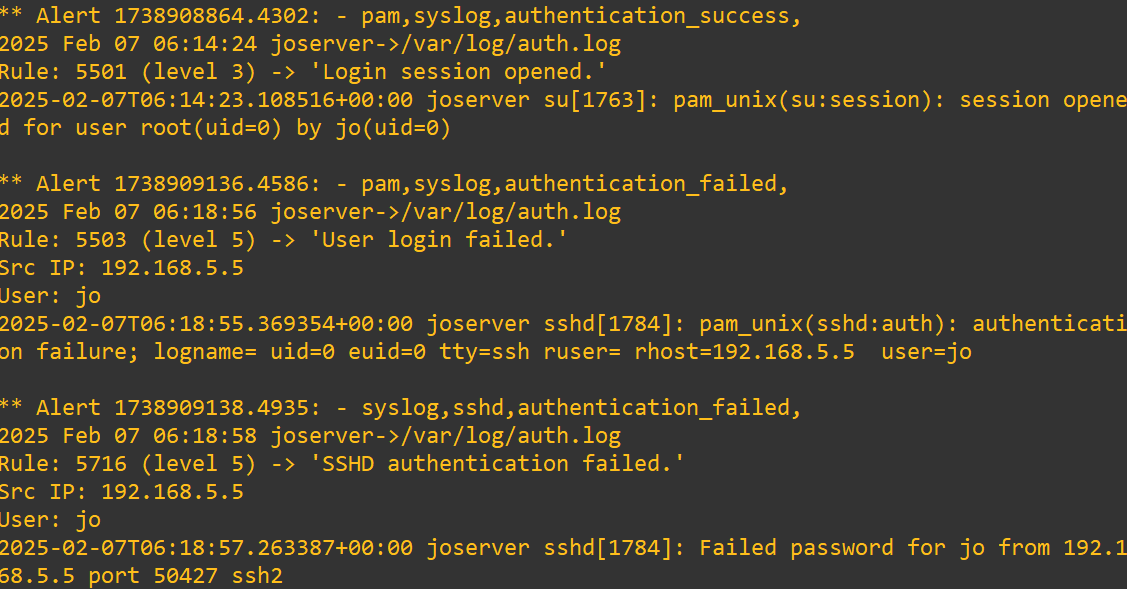


Telnet 분석 화면

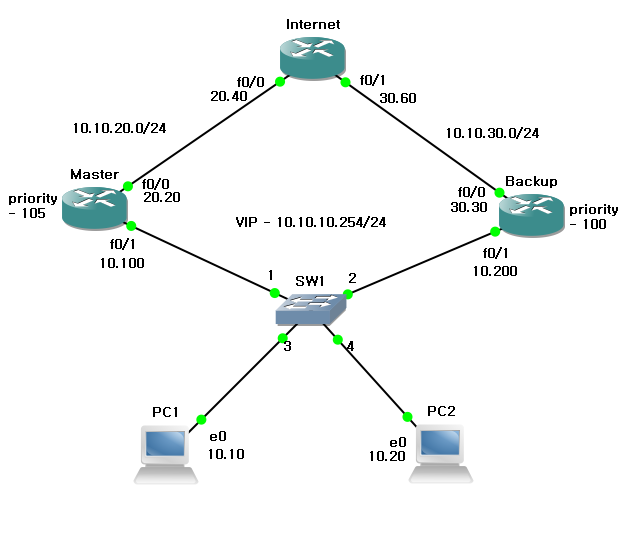
****SSH 분석 화면  
  
두 방법 분석 결과 Telnet은 보안성이 취약하여 아이디와 패스워드가 그대로 노출되는 반면 SSH는 암호화되어 출력되기 때문에 보안에 더 강하다는 것을 알 수 있다.

**3.1 ~ 3.4 OSSEC Agent 설정을 통해 Agent 시스템(Windosw 또는 Linux)의 트래픽 현황 및 하드웨어 사용량을 실시간 모니터링을 통해 운영 및 현황을 파악할 수 있고 로그를 확인하시오.**

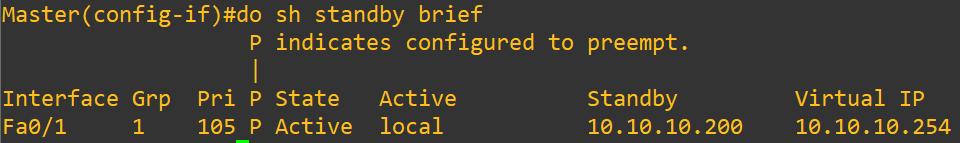


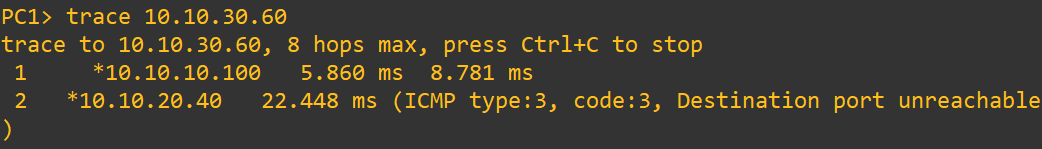
실시간 모니터링을 통해 이상이 있는 로그를 확인 (외부에서 putty로 원격 접속을 시도했으나 비밀번호 오류로 접근에 실패했다는 로그를 확인할 수 있음)

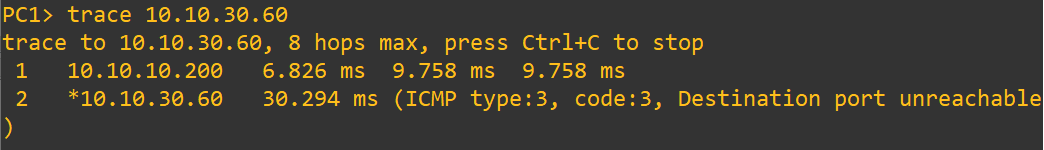
**3.5 FHRP(First Hops Redundancy Protocol) 중에서 HSRP를 통해 비정상 동작에 대응하기 위해 이중화를 설정하여 테스트를 진행하시오.**



토폴로지

이중화 세팅 상황(Master)

(정상) PC1에서 10.10.30.60으로 보냈을 때

(Master 라우터에 장애 발생 시) PC1에서 10.10.30.60으로 보냈을 때 - Backup 라우터로 돌아감