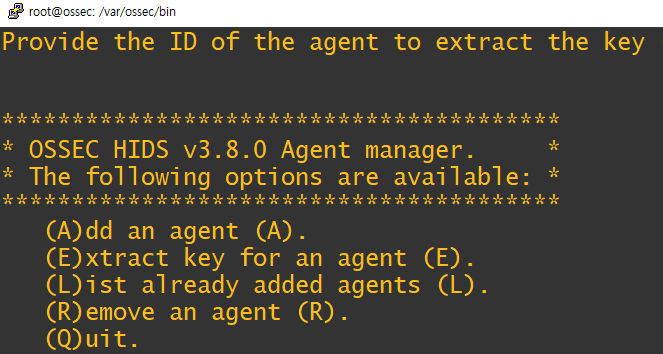
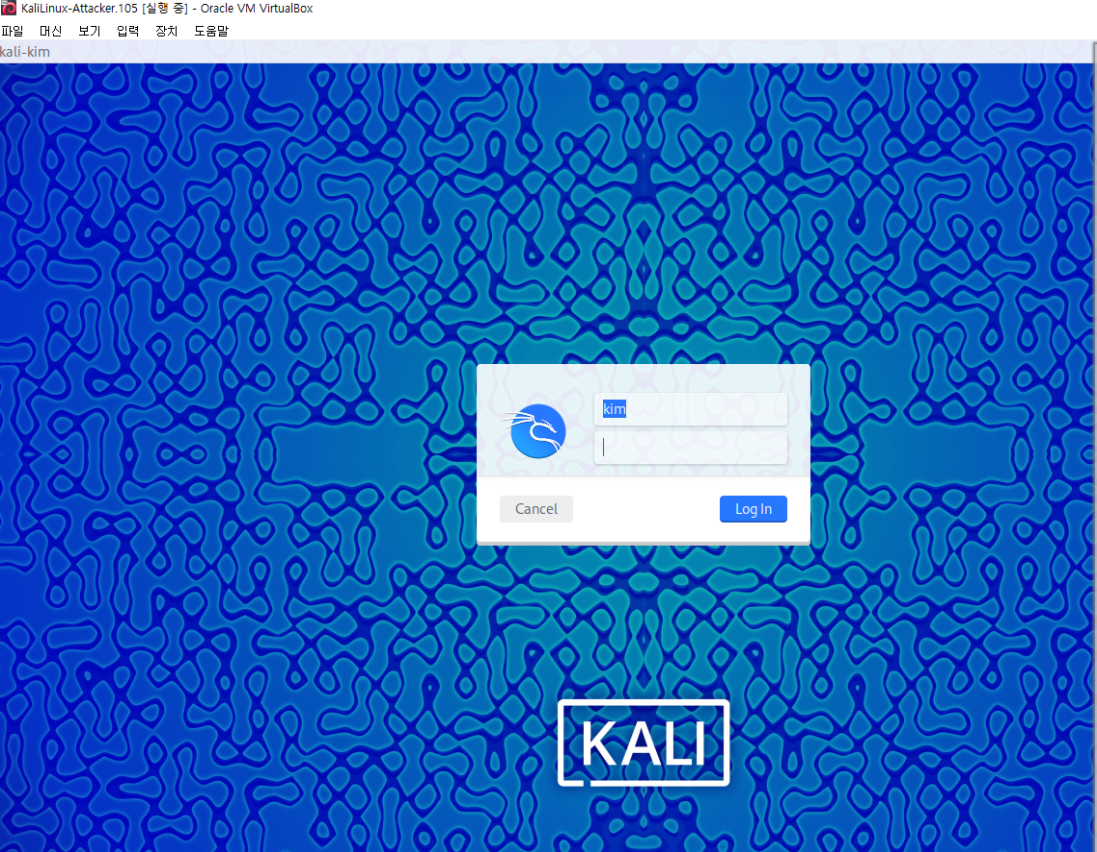
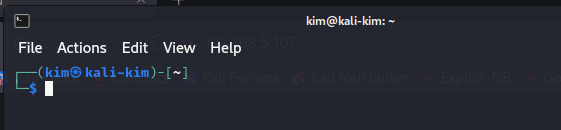
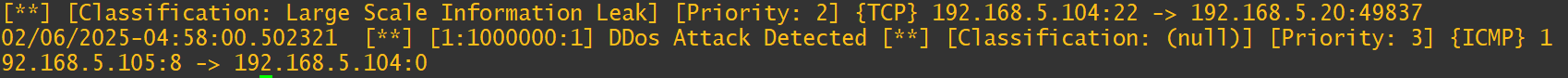
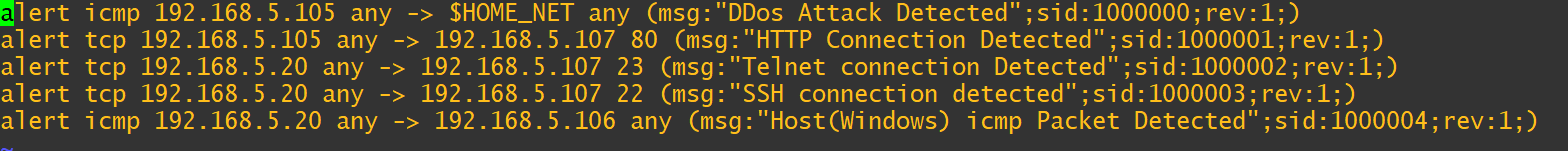
**1.1 ~ 1.3 Kali, Web Server, OSSEC, Suricata를 설치하여 정상 동작이 가능하도록 하시오.  
OSSEC 동작화면**  
 **1.4 Kali 시스템에 사용자(본인이름)를 추가하고 패스워드를 설정하도록 하시오.  
Kali 동작화면  
  
로그인 후 화면**

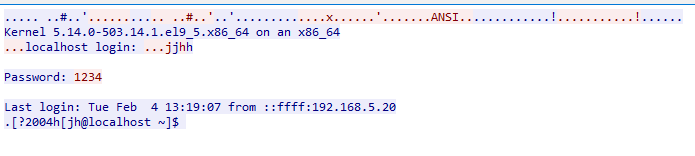
****  
  
  
**2.1 ~ 2.5 Suricata Rule을 정책 조건에 맞게 설정하고 탐지 테스트를 진행하시오.**1. Kali(.105) -> suricata(.104) : DDoS 공격 탐지 ****2. Kali(.105) -> Web Server(.107) : HTTP 접속 탐지

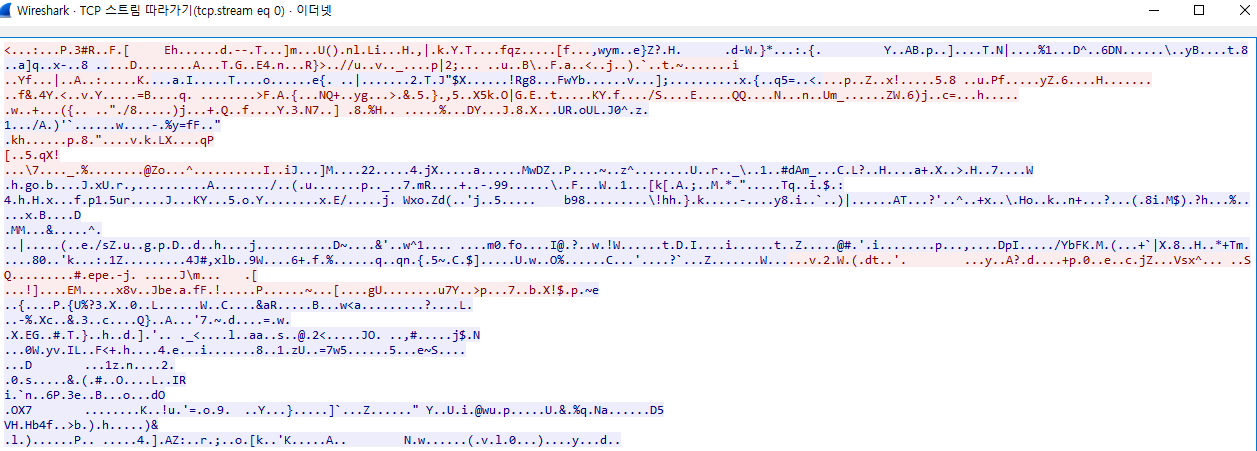
  
3. Host(Windows)(.20) -> Web Server(.107) : Telnet 접속 탐지  
  
4. Host(Windows)(.20) -> Web Server(.107) : ssh 접속 탐지  
  
5. Host(Windows)(.20) -> OSSEC(.106) : ICMP 패킷 탐지  
  
  
Suricata Rule  


[[IP 할당]]  
Kali: 192.168.5.105  
Suricata: $HOME\_NET(192.168.5.104)

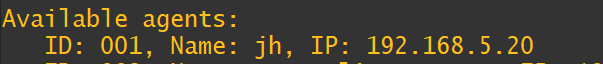
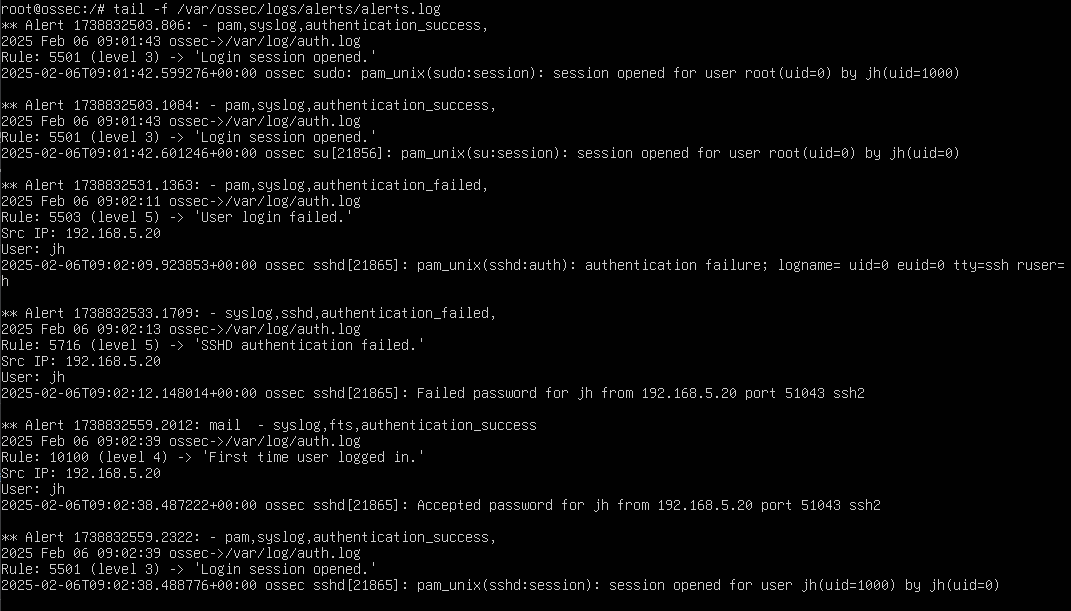
WebServer: 192.168.5.107  
Host(Windows): 192.168.5.20

OSSEC: 192.168.5.106

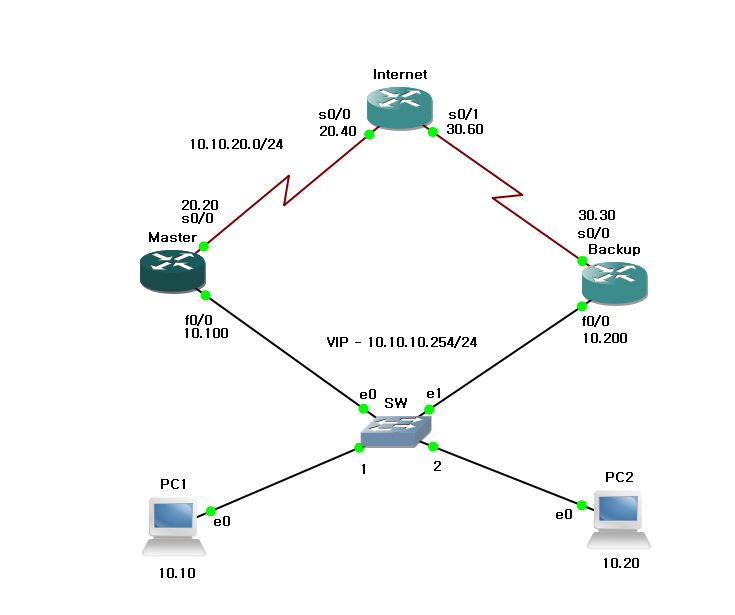
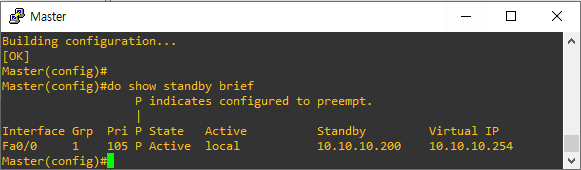
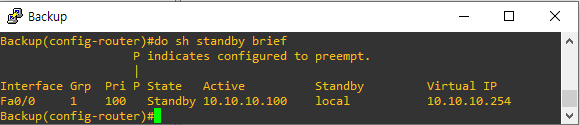
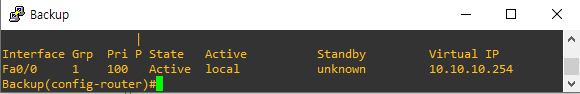
**2.6 위의 탐지되는 패킷들 중 Telnet 및 ssh 트래픽을 Wireshark로 캡처하여 스트림 분석을 통해 차이점을 확인하시오.  
  
3way handshake 거친 후  
  
와이어샤크 Telnet 접속 감지 – 유저 ID와 Password가 노출  
**

**와이어샤크 ssh 접속 감지 – 유저 ID와 Password가 암호화 된 모습**

**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.  
  
Agent 등록**

  
**Agent 모니터링(SSH 로그인 실패 및 성공화면)**  
 **실시간 모니터링을 통해 로그로 Window 환경의 트래픽 및 하드웨어 사용량을 확인 할 수 있다.**

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

  
Master(주회선 Active 상태)  
  
Backup(보조회선 Standby 상태)  
  
Master(주회선) 장애발생 시 Backup(보조회선->주회선으로 전환)  
  
standby 1 track 으로 장애 복구 시 다시 Master(주회선) Backup(보조회선)으로 복귀