REPORT

보안시스템운영및실습

학 번 : 2021671029
이 름 : 박예서
제출일 : 2023년 4월 30일

1. 스노트의 Rule Header에 대해 설명하시오.

Rule Header						
Action	Protocol	Source IP Address	Source Port	->	Dest IP Address	Dest Port

- Action : 동작 방식
  - alert(alert 발생과 기록)
  - log(패킷 기록)
  - pass(패킷 무시)
- Protocol : 프로토콜
  - TCP, UDP, ICMP, IP
- Source IP Address : 송신자 IP 주소
- Source IP Port : 송신자 포트 번호
- -> : 패킷 방향
  - ->
  - <>(송수신자 구별없이 지정 IP간 모든 패킷을 탐지)
- Dest IP : 수신자 IP 주소
- Dest Port : 수신자 포트 번호
- Rule Option : 옵션
  - content
  - msg
  - dept
  - sid
  - threshold

2. Content 옵션의 depth, within, distance에 대해서 설명하시오.

depth 옵션 : 전송되는 파일을 조사하여 파일 내부 옵셋 0-N 범위에서 지정된 시그니처를 조사한다.

within 옵션 : 이전 content가 매칭된 경우, 매칭된 지점 이후부터 탐색할 범위를 지정할 때 사용한다.

distance 옵션 : 매칭된 지점 이후부터 무시할 범위를 지정한 수 현재 content를 찾는다.