Snort 설치

1) 설치 전 네트워크 카드명 변경

```
#apt-get update
#apt-get install –y net-tools
#nano /etc/default/grub
   GRUB_CMDLINE_LINUX="find_pressed=/preseed.cfg auto noprompt
   priority=critical locale=en_US net.ifnames=0 biosdevname=0"
#grub-mkconfig -o /boot/grub/grub.cfg
#reboot
```

Snort의 랜카드를 항상 동일하게 인식시키는 과정

- net.ifnames=0 //eth0, eth1 형태의 옛 네이밍 유지
- biosdevname=0 //BIOS 가 자동으로 네트워크 장치 이름 지정하는 것을 비활성화
- grub-mkconfig -o /boot/grub/grub.cfg //설정 파일을 갱신

2) Snort 설치

```
#apt-get install -y snort
#snort –V
```

3) Snort 재시작 또는 룰 적용

```
#systemctl restart snort
```

4) Snort 설정 파일

/etc/snort/snort.conf

✓ Snort의 주요 설정 파일

✓ Snort의 전체 동작 방식을 제어

✓ Snort가 동작 시 필요한 환경변수 정의, 로그 위치, rule 파일, 탐지 옵션 등을 지정

- 네트워크 주소 범위나 포트 등의 환경 변수 지정
- Rule 포함 영역 정의, 어떤 rule 파일을 사용할 지를 지정 하는 부분
- 로깅 경로 설정, snort가 탐지 로그를 저장할 기본 경로

5) Snort Rule 생성 관련 파일

/etc/snort/rules

✓ Snort가 탐지에 사용하는 rule 파일들이 저장되어 있음

✓ 여러 개의 룰 파일들이 존재하며, 각 파일은 **탐지하려는 공격 유형 또는 프로토콜별로 분류**되어 있음

/etc/snort/rules/local.rules

✓ 새 rule 추가 시 사용

✓ 사용자가 직접 작성하는 custom rule 파일

6) Snort 설정 파일

snort -T -c /etc/snort/snort.conf

- ✓ Snort IDS 테스트
- ✓ 옵션 –T는 테스트 모드, 옵션 –C는 설정 파일을 지정하여 설정 오류를 확인
- ✓ Snort successfully validated the configuration 문구가 뜨면 관제 시 문제 없음을 의미
- ✓ 문법적 오류가 발생 시 문제 발생원인 확인 가능
- ✓ 실제 패킷 캡처는 하지 않음

snort -i eth0 -c /etc/snort/snort.conf

- ✓ 생성된 룰 적용 후 IDS 실행
- ✓ 옵션 -i은 분석할 네트워크 인터페이스를 지정
- ✓ Snort를 침입 탐지 시스템(IDS) 모드로 실행하는 기본적인 명령
- ✓ 실제 네트워크 트래픽을 캡처하고 분석 , 룰(rule)에 따라 실시간 탐지 수행

7) Snort 탐지 로그 확인

snort -A console -c /etc/snort/snort.conf

- ✓ 콘솔에서 실시간 로그 확인
- ✓ Snort가 탐지한 경고를 터미널 화면에 바로 출력
- ✓ 로그 파일 대신 즉시 결과를 확인 가능

tail -f /var/log/snort/snort.alert.fast

- ✓ Snort가 남긴 로그 파일을 실시간으로 출력
- ✓ -f : 파일이 갱신될 때마다 실시간으로 추가 내용 출력
- ✓ Snort가 탐지한 경로를 실시간으로 모니터링