Snort3 규칙 이해

목차

소개

이 문서에서는 **Snort3** Cisco의 엔진 **Secure Firewall Threat Defense (FTD).**

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco **Secure Firewall Threat Defense (FTD)**
- **Intrusion Prevention System (IPS)**
- **Snort2** 구문

라이센싱

특정 라이센스 요구 사항은 없으며, 기본 라이센스만으로도 충분하며, 언급된 기능은 FTD 내의 **Snort** 엔진 및 Snort**3** 오픈 소스 버전에 포함됩니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco **Secure Firewall Threat Defense (FTD)**, Cisco **Secure Firewall Management Center (FMC)** 버전 7.0 이상 **Snort3.**

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Snort 실시간 트래픽 분석 및 패킷 로깅이 가능한 Cisco IPS 엔진입니다.

Snort 프로토콜 분석, 콘텐츠 검색, 공격 탐지가 가능합니다.

Snort3 은(는) 성능, 탐지, 확장성 및 사용 편의성을 향상시키는 새로운 소프트웨어 아키텍처를 갖춘 Snort2 IPS의 업데이트 버전입니다.

Snort3 규칙

이 LUA 형식을 사용하여 **Snort3** 읽기, 쓰기 및 검증이 더 쉬운 규칙

규칙 작업

이 새 버전은 규칙 작업을 변경하며, 새 정의는 다음과 같습니다.

- **Pass**: 패킷에 대한 후속 규칙 평가 중지
- **Alert**: 이벤트만 생성
- **Block**: 패킷 삭제, 잔여 세션 차단
- **Drop**: 패킷 삭제만
- **Rewrite**: replaces 옵션을 사용하는 경우 필수
- **React**: HTML 블록 응답 보내기 페이지
- **Reject**: TCP RST 또는 ICMP 도달 불가 삽입

규칙 구조

해부학은 다음과 같습니다.

규칙 헤더에는 작업, 프로토콜, 소스 및 대상 네트워크, 포트가 포함됩니다.

수신 **Snort3**, 규칙 헤더는 다음 옵션 중 하나가 될 수 있습니다.

- 서비스 규칙 헤더

```
<iline" lang="lua">alert http ( msg:"Alert HTTP rule"; flow:to_client,established;
content:"evil", nocase; sid:1000001; )
```

- 파일 규칙 헤더

```
alert file ( msg: "Alert File example"; file_data; content:"malicious_stuff"; sid:1000006; )
```

- 일반 규칙 헤더

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"Alert HTTP rule";
flow:to_client,established; content:"evil", nocase; sid:1000001; )
```

규칙 기능

새로운 기능 중 일부는 다음과 같습니다.

- 임의 공백(각 옵션은 해당 줄에 있음)

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"Alert TCP rule";
flow:to_client,established; content:"evil", nocase; sid:1000000; )
```

- 및 일관된

```
content:"evil", offset 5, depth 4, nocase;
```

- 네트워크 및 포트는 선택 사항

```
alert http ( Rule body )
```

- 스티커 버퍼를 더 추가합니다(전체 목록이 아님).

```
http_uri http_raw_uri http_header http_raw_header http_trailer http_raw_trailer http_cookie
http_raw_cookie http_true_ip http_client_body http_raw_body http_method http_stat_code
http_stat_msg http_version http2_frama_header script_data raw_data
```

- C 스타일 주석

```
alert http ( msg:"Alert HTTP rule"; /* I can write a comment here */ ... )
```

- rem(remark) 키워드

```
alert http ( msg:"Alert HTTP rule"; flow:to_client,established; rem:"Put comments in the rule
anywhere"; content:"evil", nocase; sid:1000001; )
```

- appids 키워드

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any ( msg:"Alert on apps"; appids:"Google, Google
Drive"; content:"evil", nocase; sid:1000000; )
```

- 민감한 데이터 필터링을 위한 sd_pattern
- Hyperflex 기술을 사용하는 Regex 키워드
- Service 키워드가 메타데이터 대체

예

http 서비스 헤더 및 스티키 버퍼 http_uri의 예

작업: 단어를 탐지하는 규칙을 작성합니다. **malicious** HTTP URI에서

해결책:

```
alert http ( msg:"Snort 3 http_uri sticky buffer"; flow:to_server,established; http_uri;
content:"malicious", within 20; sid:1000010; )
```

파일 서비스 헤더의 예

작업: PDF 파일을 탐지하는 규칙을 작성합니다.

해결책:

```
alert file ( msg:"PDF File Detected"; file_type: "PDF"; sid:1000008; )
```

관련 링크

Snort 규칙 및 IDS 소프트웨어 다운로드

깃허브

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.