Snort3-Regeln verstehen

Inhalt

Einleitung

In diesem Dokument werden die Regeln für **Snort3** in Cisco **Secure Firewall Threat Defense (FTD)**.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Lizenzierung

Keine spezifischen Lizenzanforderungen, die Basislizenz ist ausreichend und die genannten Funktionen sind in der **Snort-**Engine innerhalb der FTD und in den **Snort3** Open-Source-Versionen enthalten.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco **Secure Firewall Threat Defense (FTD)**Cisco **Secure Firewall Management Center (FMC)** Version 7.0+ mit

Snort3.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Snort ist die Cisco IPS-Engine, die Datenverkehrsanalysen und Paketprotokollierung in Echtzeit ermöglicht.

Snort kann Protokollanalysen durchführen, Inhalte durchsuchen und Angriffe erkennen.

Snort3 ist eine aktualisierte Version des Snort2 IPS mit einer neuen Softwarearchitektur, die Leistung, Erkennung, Skalierbarkeit und Benutzerfreundlichkeit verbessert.

Snort3-Regeln

Sie verwenden dieses LUA-Format, um **Snort3** Regeln, die leichter zu lesen, zu schreiben und zu überprüfen sind.

Regelaktionen

Diese neue Version ändert die Regelaktionen. Die neuen Definitionen lauten wie folgt:

- **Pass**: Beenden der Auswertung nachfolgender Regeln für Pakete
- **Alert**: Nur Ereignis generieren
- **Block**: Paket verwerfen, Restsitzung blockieren
- **Drop**: Nur Paket verwerfen
- **Rewrite**: Erforderlich, wenn die Option replace verwendet wird.
- **React**: HTML-Block-Antwortseite senden
- **Reject**: Einspeisen von TCP-RST oder ICMP nicht erreichbar

Regelanatomie

Die Anatomie ist:

Der Regelheader enthält die Aktion, das Protokoll, das Quell- und das Zielnetzwerk sowie die Ports.

In **Snort3**verwenden, kann der Regelkopf eine der folgenden Optionen sein:

- Serviceregelkopf

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

- Header für Dateiregeln

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

- Überschrift für konventionelle Regel

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

Regelfunktionen

Zu den neuen Funktionen gehören:

- Beliebiger Leerraum (jede Option auf einer eigenen Zeile)

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

- konsistente Nutzung von `und ;`

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

- Netzwerke und Ports sind optional

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

- Fügt weitere Haftpuffer hinzu (Dies ist nicht die vollständige Liste)

```
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-Style-Kommentare

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

- Hinweis (rem)-Schlüsselwort

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

- appids-Schlüsselwörter

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

- sd_pattern für die Filterung vertraulicher Daten
- Regex-Schlüsselwort unter Verwendung von Hyperflex-Technologie
- Service-Schlüsselwort ersetzt Metadaten

Beispiele

Beispiel mit HTTP-Service-Header und Sticky-Puffer http_uri

Aufgabe: Schreiben Sie eine Regel, die das Wort erkennt **malicious** im HTTP-URI.

Lösung:

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

Beispiel mit Dateiservice-Header

Aufgabe: Schreiben Sie eine Regel, die PDF-Dateien erkennt.

Lösung:

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

Verwandte Links

Snort Rules und IDS Software-Download

Github

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.