Comprensión de las reglas de Snort3

Contenido

Introducción

En este documento se describen las reglas de **Snort3** en el sistema **Secure Firewall Threat Defense (FTD).**

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Licencias

No se requiere una licencia específica, la licencia básica es suficiente y las funciones mencionadas se incluyen en el motor **Snort** en el FTD y en las versiones de código abierto de **Snort3**.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco **Secure Firewall Threat Defense (FTD)**,Cisco **Secure Firewall Management Center (FMC)** versión 7.0+

con **Snort3**.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Snort es el motor Cisco IPS capaz de analizar el tráfico en tiempo real y registrar paquetes.

Snort puede realizar análisis de protocolos, búsquedas de contenido y detectar ataques.

Snort3 es una versión actualizada de Snort2 IPS con una nueva arquitectura de software que mejora el rendimiento, la detección, la escalabilidad y la facilidad de uso.

Reglas de Snort3

Utilizan el formato LUA para crear la **Snort3** reglas más fáciles de leer, escribir y verificar.

Acciones de regla

Esta nueva versión cambia las acciones de la regla, las nuevas definiciones son:

- **Pass**: detiene la evaluación de las reglas subsiguientes en relación con el paquete
- **Alert**: sólo generar evento
- **Block**: descartar paquete, bloquear sesión restante
- **Drop**: solo descartar paquete
- **Rewrite**: requerido si se utiliza la opción replace.
- **React**: Enviar página de respuesta de bloque HTML
- **Reject**: Inyecte TCP RST o ICMP inalcanzable

Anatomía de regla

La anatomía es:

El encabezado de regla contiene la acción, el protocolo, las redes de origen y destino y los puertos.

IN **Snort3**, el encabezado de regla puede ser una de las siguientes opciones:

- Encabezado de regla de servicio

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

- Encabezado de regla de archivo

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

- Encabezado de regla convencional

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

Funciones de regla

Algunas de las nuevas funciones son:

- Espacios en blanco arbitrarios (cada opción en su propia línea)

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

- Uso coherente de , y ;

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

- Las redes y los puertos son opcionales

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

- Agrega más búferes persistentes (esta no es la lista completa)

```
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
```

- Comentarios de estilo C

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

- Palabra clave Remark (rem)

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

- palabras clave appids

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

- sd_pattern para el filtrado de datos confidenciales
- Palabra clave Regex con el uso de la tecnología hyperflex
- La palabra clave Service reemplaza los metadatos

Examples

Ejemplo con encabezado de servicio http y búfer fijo http_uri

Tarea: Escribir una regla que detecte la palabra **malicious** en el URI HTTP.

Solución:

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

Ejemplo con encabezado de servicio de archivos

Tarea: Escribir una regla que detecte archivos PDF.

Solución:

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

Enlaces relacionados

Descarga de software IDS y reglas Snort

Github

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).