Configuración de la variable SNORT_BPF en un centro de la defensa

Contenido

Introducción

Usted puede utilizar el filtro de paquete de Berkeley (BPF) para excluir un host o una red de la inspección por un centro de la defensa. El Snort utiliza la variable de **`Snort_BPF`** para excluir el tráfico de una directiva de la intrusión. Este documento proporciona las instrucciones en cómo utilizar la variable de **`Snort_BPF`** en los diversos escenarios.

> Consejo: Se recomienda fuertemente para utilizar una regla de la confianza en una directiva del control de acceso para determinar cuál es y no se examina el tráfico, bastante que un BPF en la directiva de la intrusión. La variable de **`Snort_BPF`** está disponible en la versión de software 5.2, y se desaprueba en la versión de software 5.3 o más alto.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento en las reglas del centro de la defensa, de la directiva de la intrusión, del filtro de paquete de Berkeley, y del Snort.

Componentes Utilizados

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

- Centro de la defensa
- Versión de software 5.2

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Pasos de configuración

Para configurar la variable de **Snort_BPF**, siga los pasos abajo:

1. Acceda la interfaz del Web User de su centro de la defensa.
2. Navegue a las **directivas > a la intrusión > a la directiva de la intrusión**.
3. Haga clic el icono del *lápiz* para editar su directiva de la intrusión.
4. Haga clic en las **variables del** menú a la izquierda.
5. Una vez que se configuran las variables, usted necesitará salvar los cambios, y reaplica su directiva de la intrusión para que tome el efecto.

Figura: Tiro de pantalla de la página de la Configuración variable de Snort_BPF

Ejemplos de Configuración

Algunos ejemplos básicos se proporcionan abajo para la referencia:

Escenario 1: Ignore todo el tráfico, a y desde un escáner de vulnerabilidad

1. Tenemos un escáner de vulnerabilidad en la dirección IP 10.1.1.1
2. Queremos ignorar todo el tráfico a y desde el escáner
3. El tráfico puede o no puede tener una etiqueta (vlan) 802.1q

El SNORT_BPF es:
not host 10.1.1.1 and not (vlan and host 10.1.1.1)COMPARACIÓN: el not* de los *is del tráfico VLA N-marcado con etiqueta, pero las puntas 1 y 2 sigue siendo verdades sería: **not host 10.1.1.1**Sin rodeos, esto ignoraría el tráfico donde está 10.1.1.1 uno de los puntos finales (el escáner).

Escenario 2: Ignore todo el tráfico, a y desde dos escáneres de vulnerabilidad

1. Tenemos un escáner de vulnerabilidad en la dirección IP 10.1.1.1

2. Tenemos un segundo escáner de vulnerabilidad en la dirección IP 10.2.1.1
3. Queremos ignorar todo el tráfico a y desde el escáner
4. El tráfico puede o no puede tener una etiqueta (vlan) del 802.11

El SNORT_BPF es:
not (host 10.1.1.1 or host 10.2.1.1) and not (vlan and (host 10.1.1.1 or host 10.2.1.1)) Comparación: El not* de los *is del tráfico VLA N-marcado con etiqueta, pero las puntas 1 y 2 sigue siendo verdades sería: **not (host 10.1.1.1 or host 10.2.1.1)**En resumen, esto ignoraría el tráfico donde está 10.1.1.1 O 10.2.1.1 uno de los puntos finales.

> Nota: Es importante observar que la etiqueta vlan debe, en casi todos los casos, ocurrir solamente una vez en un BPF dado. Los únicos tiempos usted debe verlo más de una vez, es si sus usos de la red jerarquizaron marcar con etiqueta del VLA N (designado a veces “QinQ ").

Escenario 3: Ignore el tráfico con Tag del VLA N, a y desde dos escáneres de vulnerabilidad

1. Tenemos un escáner de vulnerabilidad en la dirección IP 10.1.1.1
2. Tenemos un segundo escáner de vulnerabilidad en la dirección IP 10.2.1.1
3. Queremos ignorar todo el tráfico a y desde el escáner
4. El tráfico es 802.11 (vlan) marcado con etiqueta, y usted desea utilizar una etiqueta (vlan) específica, como en el VLAN 101

El SNORT_BPF es:

not (host 10.1.1.1 or host 10.2.1.1) and not (vlan 101 and (10.1.1.1 or host 10.2.1.1))

Escenario 4: Ignore el tráfico de un servidor de backup

1. Tenemos un servidor del backup de la red en la dirección IP 10.1.1.1
2. Las máquinas en la red conectan con este servidor en el puerto 8080 para funcionar con su respaldo nocturno
3. Deseamos ignorar este tráfico de reserva, pues es cifrado y en grandes cantidades

El SNORT_BPF es:
not (dst host 10.1.1.1 and dst port 8080) and not (vlan and (dst host 10.1.1.1 and dst port 8080)) Comparación: El not* de los *is del tráfico VLA N-marcado con etiqueta, pero las puntas 1 y 2 sigue siendo verdades sería: **not (dst host 10.1.1.1 and dst port 8080)**
Traducido, esto significa que el tráfico a 10.1.1.1 (nuestro servidor de backup hipotético) en el puerto 8080 (puerto de escucha) no se debe examinar por el motor de la detección IPS.

Es también posible utilizar la `red` en el lugar del `host` para especificar un bloque de la red, bastante que un solo host. Por ejemplo:

```
not net 10.1.1.0/24
```

Es generalmente una práctica adecuada hacer el BPF tan específico como sea posible; excepto el tráfico del examen que necesita ser excluido, mientras que no excepto cualquier tráfico sin relación que pudiera contener las tentativas del exploit.

Escenario 5: Para usar los rangos de red bastante que los host individuales

Usted puede especificar los rangos de red en la variable BPF bastante que los host para acortar la longitud de la variable. Para hacerle tan utilizará la palabra clave `neta` en lugar del host y especificará un rango CIDR. Debajo tiene un ejemplo:

```
not (dst net 10.8.0.0/16 and dst port 8080) and not (vlan and (dst net 10.8.0.0/16
and dst port 8080))
```

> Nota: Asegúrese por favor de que usted ingrese a la dirección de red que usa la notación de CIDR y un direccionamiento usable dentro del espacio de la dirección del bloque CIDR. Por ejemplo utilice la red 10.8.0.0/16 bastante que la red 10.8.2.16/16.

La variable **SNORT_BPF** se utiliza para evitar que cierto tráfico sea examinado por un motor de la detección IPS; a menudo por las cuestiones de rendimiento. Esta variable utiliza el formato estándar de los filtros del paquete de Berkeley (BPF). El tráfico que corresponde con la variable **SNORT_BPF** será examinado; mientras que el tráfico que no corresponde con la variable **SNORT_BPF** no será examinado por el motor de la detección IPS.