THE BRIDGE

CYBER SECURITY

Reglas IDS/IPS

Reglas IDS/IPS

- **IDS (Sistemas de Detección de Intrusos):**
  - Las reglas en IDS son esenciales para detectar actividades sospechosas o maliciosas en la red.
  - La sintaxis de las reglas puede variar según la herramienta utilizada, pero en general, sigue un patrón común.

  - Las reglas se dividen en 3 parte que son
    - **Action o Acción** en rojo
    - **Header o cabecera** en verde
    - **Rules option u opciones de la regla** en Azul.

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"HTTP GET Request
Containing Rule in URI"; flow:established,to_server; http.method;
content:"GET"; http.uri; content:"rule"; fast_pattern; classtype:bad-
unknown; sid:123; rev:1;)
```

https://docs.suricata.io/en/latest/rules/intro.html

Reglas IDS/IPS

- **Action o Acción**: Que está en color Rojo. Indica que se va a hacer con el paquete cuando la regla se cumple.
- Algunas acciones comunes son:
  - **Alert**: generar una alerta en el LOG.
  - **Pass**: Detiene la inspección de paquetes y lo deja continuar.
  - **Drop**: Elimina el paquete y genera una alerta.
  - **Reject**: Genera un error y envía un error de RST/ICMP al que envía el paquete.

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"HTTP GET Request
Containing Rule in URI"; flow:established,to_server; http.method;
content:"GET"; http.uri; content:"rule"; fast_pattern; classtype:bad-
unknown; sid:123; rev:1;)
```

https://docs.suricata.io/en/latest/rules/intro.html

Reglas IDS/IPS

- **Header o cabecera**: Este es el de color Verde y define los datos principales del paquete como lo es el protocolo, IP, puerto y dirección de la regla.
  - **Protocolo:** Indica el protocolo en que vendrá el paquete
    - **Algunos ejemplos que podríamos usar son:**
      - tcp (for tcp-traffic)
      - udp
      - icmp
      - http (either HTTP1 or HTTP2)
      - ssh
      - smtp

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"HTTP GET Request
Containing Rule in URI"; flow:established,to_server; http.method;
content:"GET"; http.uri; content:"rule"; fast_pattern; classtype:bad-
unknown; sid:123; rev:1;)
```

https://docs.suricata.io/en/latest/rules/intro.html

Reglas IDS/IPS

- **Origen y Destino**: Es la IP o el ALIAS que puedas utilizar para indicar el origen y el destino del paquete.
  - Algunos Ejemplos
    - **10.0.2.100** : Dirección IP especifica
    - **![1.1.1.1, 1.1.1.2]:** Todas las direcciones excepto la 1.1.1.1 y la 1.1.1.2
    - **$HOME_NET**: Variable Local que indica el Rango de RED que está en la zona LAN.
    - **$EXTERNAL_NET**: Variable Local que indica el Rango de RED que está en la zona WAN.
    - **[10.0.0.0/24, !10.0.0.5]**: todo el segmento 10.0.0.0/24 excepto la IP 10.0.0.5

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"HTTP GET Request
Containing Rule in URI"; flow:established,to_server; http.method;
content:"GET"; http.uri; content:"rule"; fast_pattern; classtype:bad-
unknown; sid:123; rev:1;)
```

https://docs.suricata.io/en/latest/rules/intro.html

Reglas IDS/IPS

- **Puerto:** Indica el puerto de comunicaciones que va a verificar.
- Algunas acciones comunes son:
  - **ANY**: para cualquier puerto.
  - **80:** puerto especifico
  - **[80, 81, 82]:** Indica que se aplica a los puertos 80, 81 y 82.
  - **[80:100]:** Indica que va desde el puerto 80 hasta el 100.
  - **!80:** Todos los puertos, pero se excluye el puerto 80
  - **[1:80,![2,4]]:** desde el 1 al 80 pero excluyendo el 2 y el 4.

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"HTTP GET Request
Containing Rule in URI"; flow:established,to_server; http.method;
content:"GET"; http.uri; content:"rule"; fast_pattern; classtype:bad-
unknown; sid:123; rev:1;)
```

https://docs.suricata.io/en/latest/rules/intro.html

Reglas IDS/IPS

- **Dirección o sentido de la comunicación:** Indica el sentido del paquete, ya sea que venga desde el origen o ambas direcciones.

- Algunas acciones comunes son:
  - ->**:** En el sentido del Origen al destino.
  - <>**:** En ambas direcciones sin importar desde donde se origina.

  - **Nota**: No existe el indicador que va desde el Destino al origen o sea "<-".

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"HTTP GET Request
Containing Rule in URI"; flow:established,to_server; http.method;
content:"GET"; http.uri; content:"rule"; fast_pattern; classtype:bad-
unknown; sid:123; rev:1;)
```

https://docs.suricata.io/en/latest/rules/intro.html

Reglas IDS/IPS

- **Rules option u opciones de la regla** que está en Azul.
  - Esta entre paréntesis
  - Separadas las diferentes opciones por el símbolo "**;**".
  - La opción va escrita y se separa por el símbolo "**:**" del valor que se le va a asignar.
  - La opción va escrita y si no hay que asígnale el valor va sola..

  - Algunos de los valores mínimos requeridos son:
    - **sid**: Indicador Único de la Regla
    - **rev** : Revisión o versión de la regla.
    - **msg**: Mensaje que va a aparecer cuando se cumpla la regla.

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"HTTP GET Request
Containing Rule in URI"; flow:established,to_server; http.method;
content:"GET"; http.uri; content:"rule"; fast_pattern; classtype:bad-
unknown; sid:123; rev:1;)
```

https://docs.suricata.io/en/latest/rules/intro.html

Ejemplos de Reglas IDS/IPS

- Algunos ejemplos de reglas explicadas
  - **SNORT**
    - **alert tcp any any -> any any (msg:"Posible ataque HTTP"; content:"GET /malware"; sid:100001)**
      - Explicación:
        - **alert**: Se va a escribir en el LOG del sistema.
        - **tcp**: Protocolo TCP/IP
        - **Any:** cualquier puerto
        - **-> :** dirección del paquete.
        - **Any:** cualquier puerto
        - **msg:"Posible ataque HTTP"**: Mensaje descriptivo.
        - **content:"GET /malware"** es el string que se va a va a buscar en el paquete**.**
        - **sid:100001** es el ID de la regla.

  - **SURICATA**
    - **alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Posible ataque HTTP"; content:"GET /malware"; sid:100001; rev:1;)**
      - Explicación:
        - **Alert:** Se va a escribir en el LOG del sistema.
        - **http:** Protocolo
        - **$HOME_NET:** Variable que indica la red LAN
        - **Any:** Cualquier Puerto
        - **->:** Dirección del paquete
        - **$EXTERNAL_NET:** Variable que indica la red WAN
        - **Any:** Cualquier Puerto
        - **msg:"Posible ataque HTTP"** mensaje que se muestra en el log
        - **content:"GET /malware"** es lo que se va a buscar en el paquete.
        - **sid:100001** es el ID de la regla
        - **rev:1** es el número de revisión.


THE
BRIDGE