Asignatura	Datos del alumno	Fecha
Seguridad en redes	Apellidos: Paz López	23/07/2021
	Nombre: Angel Ramón	

INTRODUCCION

Los sistemas de detección de intrusos (IDS) permiten la detección de ataques a una red o sistemas, ya sean Ataques de denegación de Servicios, ataques de accesos a sistemas entre otros, el Snort es un sistema IDS, es el sistema más popular para detección de intrusiones en la red, es capaz de realizar un análisis de tráfico en la red de un alto nivel utilizando un lenguaje de creación de reglas en la cual se pueden definir los parámetros a la hora analizar o monitorizar el sistema, estas reglas constan de dos partes: El encabezado de la regla y las opciones de la regla. Los elementos básicos del sistema Snort son: Decodificador de paquetes, motor de detección y sistema de logueo y alerta.

Un servidor en el que se encuentra instalado *Snort* está monitorizando todo el tráfico de la subred 172.16.0.0 con máscara 255.255.0.0. En adelante nos vamos a referir a esta subred como subred_A. El alumno debe escribir las reglas de *Snort* que permitan registrar los siguientes eventos:

Para todas las reglas que utilizaremos en cada inciso propuesto utilizaremos esta estructura para no explicarla en cada inciso: **Acción Protocolo IP puerto -> IP puerto**

Las direcciones de IP puerto del lado izquierdo corresponden al trafico provenientes del host de origen y del lado derecho al host destino (Gómez, s. f.)

Las Opciones de las reglas irán dentro de paréntesis después del encabezado (**Acción Protocolo IP puerto -> IP puerto)** y cada opción ira separado de ";"

1. **La palabra GET se utiliza en el protocolo HTTP para indicar un recurso a descargar y aparece siempre al inicio de los mensajes. Introduce una regla en snort que detecte el patrón «GET» en la parte de datos de todos los paquetes TCP que abandonan la subred_A y van a una dirección que no forma parte de la subred_A. Cuando se detecte el patrón indicado la regla debe lanzar una alerta con el mensaje «Detectado GET».**

   El primer elemento de la estructura ya mencionada es la acción la cual en este caso usaremos **alert** después seguimos el protocolo que vamos a usar y es **tcp** seguido la subred (IP) **172.16.0.0/16** para el puerto utilizaremos **any** porque puede definir cualquier numero de puerto seguido del operador bidireccional **->** Ahora colocamos la información del host destino donde el IP no tiene que estar en la misma red entonces colocamos la misma IP **!172.16.0.0/16** con un sigo de negación "!" lo cual significa cualquier dirección excepto la especificada, seguido colocamos el puerto lo cual colocamos **80** porque es el puerto que corresponde al protocolo HTTP, después definiremos las opciones de la regla utilizando paréntesis usando el comando **msg** que nos imprime un mensaje en las alertas y bitácoras en nuestro caso imprimirá "Detectado GET", después usamos **content** la cual busca por un contenido específico dentro del payload del paquete en nuestro caso buscamos **"GET"** y por ultimo utilizamos el método **http_method** que es un modificador de contenido que restringe la búsqueda al método extraído de una solicitud de cliente HTTP (*3.5 Payload Detection Rule Options*, s. f.). Si hay más de una configuración dentro del paréntesis van separadas por ";"

   alert tcp 172.16.0.0/16 any -> !172.16.0.0/16 80 (msg: "Detectado GET"; content: "GET"; http_method;)

2. **Introduce una regla que intente buscar la palabra «HTTP» entre los caracteres 4 y 40 de la parte de datos de cualquier paquete TCP con origen en la subred_A y van a una dirección que no forma parte de la subred_A. En el fichero de log, el registro debe contener el mensaje «Detectado HTTP».**

Utilizando las mismas reglas del primer ejercicio siempre empezamos con la acción **alert** seguido con el protocolo **tcp** con el IP **172.16.0.0 / 16** que es el IP origen de la subred, después colocamos el puerto **any** para cualquier número de puerto, elegimos el flujo del tráfico con el operador bidireccional **->** con una IP que no forma parte de la subred_A por lo cual usamos el operador negación **"!"** lo cual significa cualquier dirección excepto la especificado por lo cual le especificamos la IP **!172.16.0.0/16** y el puerto **any** después usamos carácter " \ " para indicar carácter que pueda coincidir con las reglas de snort seguido de las opciones de la regla mediante los paréntesis las cual comenzamos a colocar **logto** lo que nos permite enviar paquete a archivo usuario en lugar de un archivo usual y el nombre del archivo **logto_log.txt,** seguimos con el **content** que en este caso será "HTTP", después utilizaremos **offset:** ya que nos especifica donde empezar a buscar dentro de del paquete y en nuestro caso empezaremos con **4,** luego usamos el **depth:** que nos especifica cuanto dentro del paquete debe ir a buscar el patrón especificado en nuestro caso seria **40** y para finalizar colocamos el mensaje con **msg: "Detectado HTTP"**

```
alert tcp 172.16.0.0/16 any -> !172.16.0.0/16 any \
(logto: logto_log.txt; content:"HTTP"; offset: 4; depth: 40; msg: " Detectado HTTP ";)
```

3. **Crea dos reglas para detectar cuando alguien está intentando acceder a una máquina situada en la subred_A cuya dirección IP es 172.16.1.3 al puerto 137 y los protocolos tanto UDP como TCP. Cuando se detecte el patrón indicado la regla debe lanzar una alerta con el mensaje «Intento de acceso al puerto 137 y el protocolo <TCP|UDP>».**

Comenzamos con la acción **alert** después con el protocolo **tcp** con la IP y el Puerto ambos con **any** después sigue el operador bidireccional -> a colocar la IP del destino en nuestro caso seria es **172.16.1.3** al puerto **137** después usamos carácter **"\"** y por último colocamos dentro del paréntesis las opciones de las reglas con el mensaje **msg: "**Intento de acceso al puerto 137 y el protocolo <TCP|UDP>**"**

```
alert tcp any any -> 172.16.1.3 137 \
(msg: "Attempt to access port 137 and protocol TCP";)
```

Comenzamos con la acción **alert** después con el protocolo **udp** con la IP y el Puerto ambos con **any** después sigue el operador bidireccional -> a colocar la IP del destino en nuestro caso seria es **172.16.1.3** al puerto **137** después usamos carácter **"\"** y por último colocamos dentro del paréntesis las opciones de las reglas con el mensaje **msg: "**Intento de acceso al puerto 137 y el protocolo <TCP|UDP>**"**

```
alert udp any any -> 172.16.1.3 137 \
(msg: "Attempt to access port 137 and protocol UDP";)
```

4. **Configura una única regla de *Snort* que permita capturar las contraseñas utilizadas (comando PASS) al conectarse a servicios de transferencia de ficheros (FTP) o de consulta de correo (POP3) desde la máquina con dirección IP 172.16.1.3 situada en la subred_A. Cuando se detecte el patrón indicado la regla debe lanzar una alerta con el mensaje «Detectada una contraseña».**

   Iniciamos con la acción **alert**, el protocolo **tcp,** la IP 172.16.1.3 seguido del puerto **any** seguido de la dirección usando el operador bidireccional **->** ahora colocamos para la IP **any** para que sea cualquier dirección IP, y los puertos serian para POP3 **110, 995,** para FTP usamos el puerto **20 y 21** (podemos colocarlo 20:21) luego usamos carácter **"\"** y después dentro del paréntesis las opciones de la regla con un mensaje **msg: "Detectada una contraseña"** con su respectivo contenido **content: "PASS"**

   **alert tcp 172.16.1.3 any -> any 110,995,20:21 **
   (msg:" Detectada una contraseña"; content:"PASS";)

CONCLUSION

Snort es una muy buena herramienta para la detección de intrusiones, es un sistema de código abierto la cual utiliza una serie de reglas que nos ayudan a definir los parámetros para limitar las actividades que se realizan en una red y mediante esas reglas poder analizar y detectar paquetes y generar alertas cuando sea necesario. Snort tiene tres usos principales: Para rastrear paquetes, para registrar paquetes que nos ayudara para la depuración del tráfico de red, y como un sistema de prevención de intrusiones en la red.

REFERENCIAS

- *3.5 Payload Detection Rule Options*. (s. f.). Recuperado 22 de julio de 2021, de http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node32.html
- Gómez, D. R. (s. f.). *Dr. Roberto Gómez Cárdenas*. 32. Obtenido de http://cryptomex.org/SlidesSeguridad/Herra3-snort.pdf
- *Reglas SNORT , detección de intrusos y uso no autorizado*. (2020, noviembre 22). CIBERSEGURIDAD .blog. https://ciberseguridad.blog/reglas-snort-deteccion-de-intrusos-y-uso-no-autorizado/