Actividad 2: Sistema de detección de intrusos

Objetivos

Reforzar los conocimientos del estudiante relativos a mecanismos de defensa de redes y el uso de sistemas de detección de intrusos.

Pautas de elaboración

El entorno es el mismo que el utilizado en la actividad «Mecanismo de defensa en redes». Ante cualquier duda, se recomienda revisar la preparación del entorno de dicha actividad.

Otras herramientas útiles:

Con el objetivo de comprobar que las reglas que les pediremos en la actividad son correctas pueden hacer uso de algunas herramientas dentro del entorno de NETinVM.

La primera recomendación es que temporalmente cambien la política del cortafuegos (Iptables) a una política permisiva, para asegurarse que no está bloqueando sus pruebas.

La segunda es que creen un fichero de configuración específico para sus reglas (por ejemplo, pruebas snort.conf) y ejecuten Snort para que monitorice cada una de las interfaces del cortafuegos, tal y como se muestra en el siguiente gráfico.

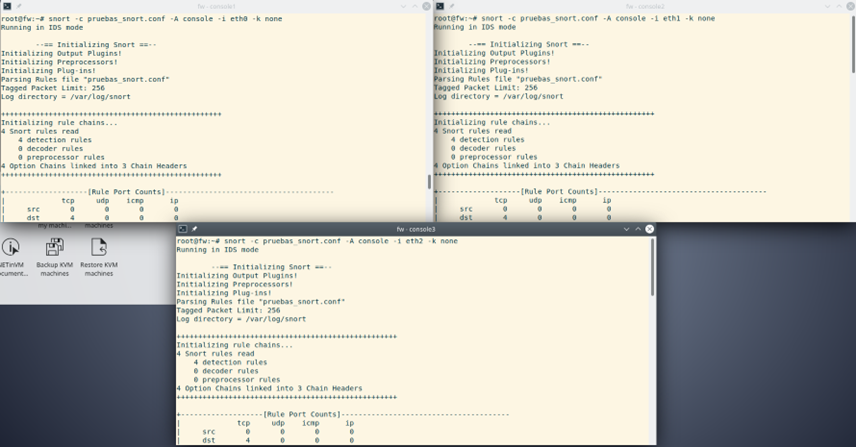


Figura 1. Ejecución de Snort. Fuente: elaboración propia.

Finalmente, de nuevo les recomendamos utilizar el comando netcat, tanto para crear peticiones como para simular servicios (cuando estos no estén desplegados en la arquitectura). La sintaxis de netcat es muy sencilla. Por ejemplo:

* Para crear un servicio que escuche en el puerto 80 TCP: nc -l -p 80.
* Para crear un servicio que escuche en el puerto 53 UDP: nc -lu -p 53.
* Para comunicarse con un servicio que escucha en el puerto 80 TCP: nc [IP o nombre del host] 80.
* Para comunicarse con un servicio que escucha en el puerto 53 UDP: nc -u [IP o nombre del host] 53.

El siguiente gráfico muestra un ejemplo de una comunicación desde **exta** con el servidor web en **dmza** y como Snort en **fw** muestra una alerta al detectar uno de los patrones buscado (GET /pass.html).

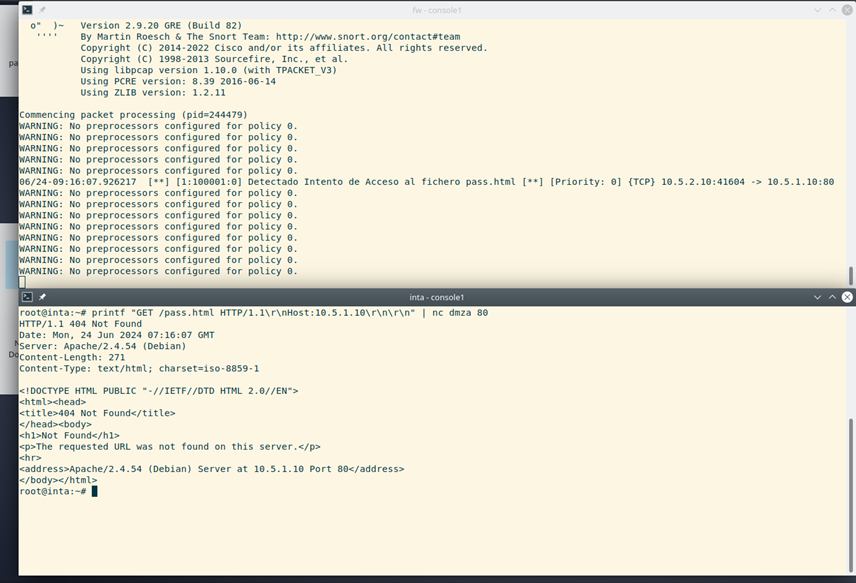


Figura 2. Alerta de Snort. Fuente: elaboración propia.

Example ha quedado muy satisfecha con tu último trabajo y ha decidido llamarte de nuevo. Parece que tu recomendación sobre que un cortafuegos no es suficiente por sí solo hoy en día, para proteger una red adecuadamente, no ha caído en saco roto. En Example ha gustado la idea de defensa en profundidad que les explicaste, por lo que han decidido empezar a desarrollarla añadiendo un sistema de detección de intrusos (IDS) a su arquitectura. La solución escogida ha sido **Snort.**

Tras una reunión donde te explican todos los detalles dibujas un gráfico de la arquitectura. No ha cambiado respecto a tu último trabajo para ellos.

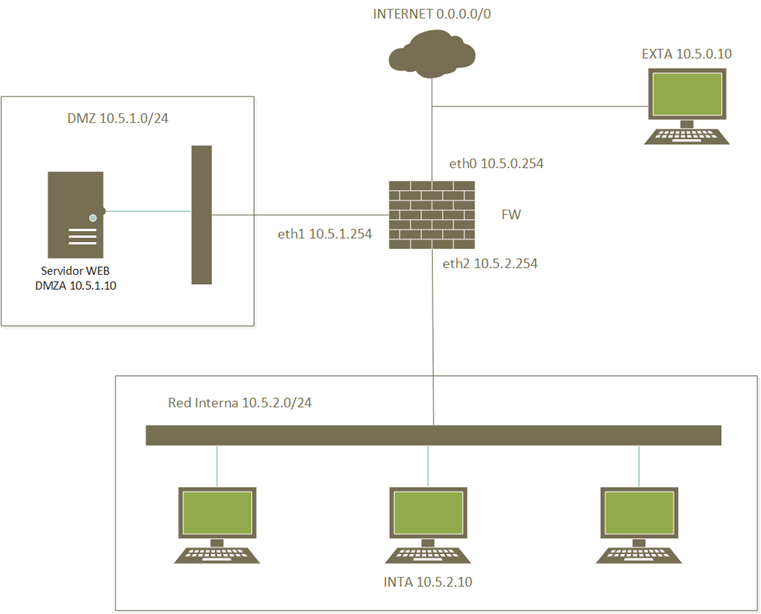


Figura 3. Gráfico de la arquitectura a proteger. Fuente: elaboración propia.

Un cortafuegos **FW** con tres interfaces interconecta tres segmentos de red: la red interna de la empresa, la DMZ y el acceso a internet. Dentro de la DMZ se encuentra un servidor web **(DMZA).** Además, tienes acceso a uno de los equipos de la red local **(INTA)** y a otro en internet **(EXTA),** que te permite tener una visión de la red desde el exterior.

Decides que la mejor localización para el IDS es el cortafuegos FW y te pones manos a la obra:

1. Para facilitar la creación de reglas y mejorar su entendimiento decides crear algunas variables. Defines una **variable para la red local (RED\_LOCAL),** otra **para el servidor web (SERV\_WEB),** otra **para la DMZ (RED\_DMZ)** y otra para **todo lo que no sea ni red local ni DMZ (RED\_EXTERNA).**
2. En Example están preocupados porque creen que se puede estar intentando explotar una vulnerabilidad del servidor Apache Tomcat, que está en el servidor WEB DMZ en el puerto 8180. Decides añadir una regla que detecte el método GET /manager/html en los primeros caracteres de todos los paquetes HTTP (puerto 8180) dirigidos desde Internet al servidor WEB. Cuando se detecte el patrón indicado la regla lanzará una alerta con el mensaje «Detectado acceso al Manager de Tomcat».
3. Ahora quieren añadir una nueva regla que permita detectar si se está intentando ejecutar un exploit en el mismo servidor Apache Tomcat. Hay que **crear una nueva regla que detecte los comandos PUT** en los primeros caracteres y que entre los siguientes 256 caracteres de todos los paquetes HTTP (puerto 8180) desde internet al servidor WEB DMZ tengan estos contenidos:

* /manager/deploy/?path=/.
* WEB-INF.
* metasploit.

Cuando se cumpla la regla deberá mostrar una alerta con el mensaje «Detectado exploit de Apache Tomcat Manager Application Deployer».

1. El administrador de red de Example está preocupado por la exposición a ataques de tipo botnet y que haya comunicación IRC entre equipos locales y de internet. **Decides añadir una regla de Snort que detecte los comandos JOIN, NICK y SERVER de IRC** desde la red local al conectarse a servicios de IRC entre los puertos 6800 y 7000 en máquinas de internet. Cuando se detecte el patrón indicado la regla lanzará una alerta con el mensaje «Detectada conexión a servidores IRC».

Extensión y formato

Ya has configurado el IDS con las reglas adecuadas, has comprobado que todo sea correcto y crees que has terminado el trabajo, pero no es así. El responsable de seguridad de Example es de la vieja escuela y quiere todas las reglas documentadas. Además, es muy quisquilloso y solo aceptará la documentación si se la entregas en el formato concreto. Debes rellenar la Tabla 1 solo con las reglas de Snort que deberían aplicarse para llevar a cabo las acciones solicitadas, generar un PDF y hacer entrega de este a través de la plataforma facilitada dentro del plazo establecido. ¡Suerte!

Notas:

* Todas las acciones deben llevarse a cabo con una única regla (a excepción de la acción 1 para la que se requiere la definición de tres variables).
* La evaluación de la práctica se llevará a cabo únicamente evaluando la tabla de reglas que entreguen.
* Utilizad las variables definidas en el primer punto en el resto de apartados siempre que sea posible.
* Utilizad los [puertos](https://es.wikipedia.org/wiki/Anexo:Puertos_de_red) conocidos asociados a los protocolos:

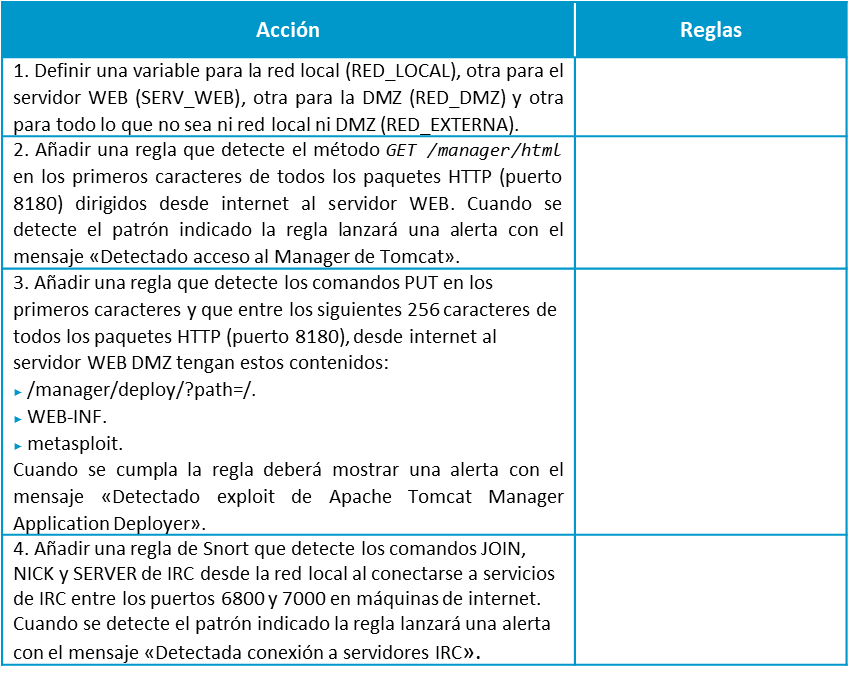


Tabla 1. Reglas Snort. Fuente: elaboración propia.

Rúbrica

|  |  |  |  |
| --- | --- | --- | --- |
| Sistema de detección de intrusos | Descripción | Puntuación máxima  (puntos) | Peso  % |
| Criterio 1 | Cada variable vale 0,75 puntos. | 2,5 | 25 % |
| Criterio 2 | Cada regla vale 2,5 puntos. | 7,5 | 75 % |
| Criterio 3 | Se resta 0,75 por cada fallo u omisión de un parámetro. |  |  |
| Criterio 4 | Tres o más fallos en una regla hacen que esa regla puntúe 0. |  |  |
|  |  | **10** | **100 %** |

**Solución**

