11 de Julio de 2024

LABORATORIO DE REDES
Y
SISTEMAS OPERATIVOS

GRUPO N°6

TEMA: Capirca

PROFESOR: Di Biase, José Luis

ALUMNOS: Gomez, Nahuel
Lascar, Agustín
Redonda, Julián

1. Introducción

Capirca es una herramienta de código abierto y multiplataforma diseñada para facilitar la creación, gestión e implementación de listas de control de acceso (ACLs) en redes.
Los ACL son archivos de configuración que poseen reglas para permitir o denegar la entrada o salida de conexiones en las distintas redes.

Este proyecto realizado en Python y llevado a cabo por Google tenía como objetivo automatizar la creación de estos ACL, para los miles de routers que poseen.

Sus principales características son:

- Mejora en seguridad.
- Soporte multiplaforma.
- Validación de políticas.
- Simulación de políticas.
- Acoplamiento a otras ACL's.
- Escalabilidad.

2. ¿Qué es un ACL?

Las ACL (por sus siglas en inglés, Access Control List) son mecanismos que permiten definir y gestionar permisos de acceso a recursos como archivos, directorios, impresoras o servicios de red. Ayudan a especificar qué usuarios o grupos de usuarios se les otorga permiso para acceder a ciertos recursos y qué tipo de operaciones pueden realizar sobre ellos (por ejemplo, lectura, escritura, ejecución). Esto ayuda a gestionar la seguridad y la eficiencia de la red.

3. Instalación

Como prerrequisitos, al ser un proyecto basado en Python, se requiere instalar los siguientes paquetes:

python3

python3-pip

python3-setuptools

git

Para eso se debe ejecutar los siguientes comandos:

sudo apt update

sudo apt-get install python3 python3-pip python3-setuptools

sudo apt install git

La instalación de Capirca se lleva a cabo por terminal empezando por clonar el repositorio del proyecto de Github en un directorio a elección.

Para clonar el proyecto e instalarlo ejecutar:

git clone https://github.com/google/capirca.git

cd capirca/

python3 -m venv venv

source venv/bin/activate

pip install -r requirements.txt

pip install .

Para ejecutar y utilizar la herramienta hay que comenzar a generar nuestros archivos de configuración declarando nuestra política.

Éstas utilizan una extensión “.pol” y un “header” que siga la siguiente estructura:

header {

comment:: "Comentario de referencia"

target:: iptables OUTPUT

}

Además cada política debe ser declarada de la siguiente manera:

nombreDeTuPolítica {

comment:: "Comentario de referencia"

*source-address:: ***El puntero de tu IP****

protocol::

*destination-port:: *NOMBRE DE LOS SERVICIOS* (no los puertos)*

action:: accept/deny

}

Éste archivo se debe almacenar en la siguiente ruta: “capirca/policies/pol”

Dentro de la ruta: “capirca/def/” se van a alojar DOS archivos.

- *network.net*
- *services.svc.*

Donde en “network.net” vas a guardar las redes afectadas por tu política por ej:

“local-networks = 10.0.2.0/24”

Y en el “services.svc” van los servicios afectados en las políticas por ej:

MS_138 = 138/udp

MS_139 = 139/tcp

IMAP = 143/tcp

Tener en cuenta que estos archivos son necesarios dado que en el archivo “.pol” hacemos referencia a cada cosa por su puntero y no por su puerto o ip.

Una vez tengamos todo esto seteado vamos a ejecutar el comando

aclgen -o iptables --policy_file ./policies/pol/iptables_rules.pol --output_directory ./salida

con el flag “--policy_file” va la ruta de nuestra política específica “.pol”.Si tenemos más de una, no es necesario aclarar y en el output (aunque ya el nombre lo spoilea)

se requiere la ruta de la carpeta que va a almacenar los archivos y en caso de no existir, la crea.

4. Dependencias, Problemas y Soluciones

Como problemas en un principio fue que el readme del repo de git no está actualizado y al menos a nosotros no nos funcionó de forma correcta la guia tal cual, recurrimos a foros y wikis y dimos con los comandos que nos permitieron usar capirca.

Por otro lado al ser una herramienta de nicho no fue fácil encontrar soporte por fuera de la documentación dado que no existen tutoriales, o paso a paso de como recrear un ejemplo o un escenario posible

Otro de los problemas que tuvimos es que Capirca genera correctamente el txt para las tablas de IP pero, desconocemos si es por cuestiones de versionado y demás falta agregar “*filter” al comienzo y “COMMIT” al final del .TXT

Nos dimos cuenta que la iptables necesitan tanto output como input pero que Capirca rompía cada vez que le pasamos ambos parámetros en las políticas, como veíamos en algunos foros hasta que encontramos un ejemplo dentro del repo de git donde utiliza varios headers en varias partes de una misma política

5. Fuentes

https://github.com/google/capirca