**SEGURIDAD INFORMÁTICA**

Imagen que contiene dibujo

Descripción generada automáticamente

**Docente:**

Carlos Aníbarro Zelaya.

**Alumno:**

Marco Antonio Roca Montenegro.

**Código:**

55995.

**IDS MARCORO**

Un IDS es un “sistema de detección de intrusiones”.

Detecta los accesos **No autorizados** que intentan acceder a nuestra red. El fin es el de tomar acciones analizando protocolos, logs y hasta *snMiffers*.

**Mi IDS:**

Es un H-IDS. – es un host el cual analiza los logs que se almacenan en **/var/log/auth.log; Detección de intrusión por SSH.**

Existen dos documentos: IDS\_MARCORO e IDS\_MARCORO2, las cadenas iptables que contienen bloquea todo acceso a la red, no solamente por ssh.

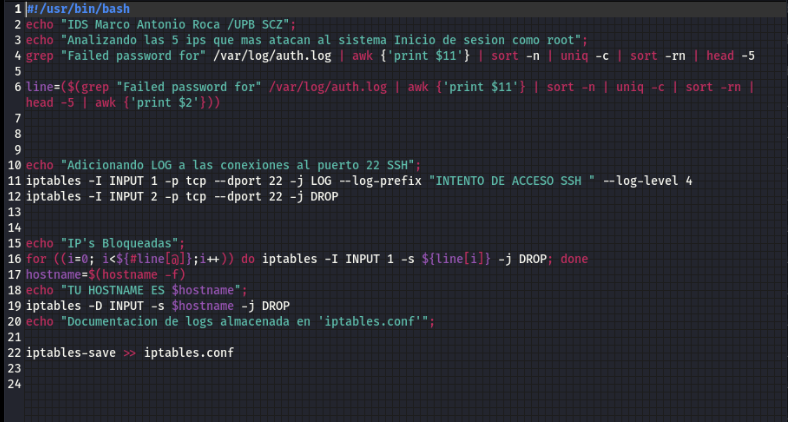
El primero bloquea IP’s para accesos no autorizados que intentan acceder como usuario “root”.

El segundo IDS bloquea cualquier IP que intente acceder con cualquier usuario.

**IDS\_MARCORO:**

El grep de la línea 4 analiza la coincidencia con “Failed password for”. Como está escrito anteriormente, analiza todos los accesos fallidos por ssh utilizando como usuario a **root**.

Pasa el grep a un array y luego los analiza como reglas DROP dentro de iptable.



**IDS\_MARCORO2:**

Utiliza un grep el cual analiza la sintaxis que concuerde con “ 3 números . 3 números . 3 números”.

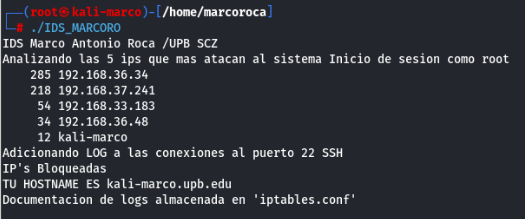
Transforma el grep a un array, procesa el array y los introduce como cadena INPUT que dropea. (No avisa que se está interrumpiendo el acceso).



**Nota:** Ambos documentos realizan una copia del sistema dentro del archivo “**iptables.conf**`”. Este almacena la serie de cadenas que maneja el sistema iptables y a su vez muestra el día, fecha y hora en la que se corrió el comando.

**Para correr el comando:** Descargue los documentos, posteriormente otorgue todos los permisos a ambos documentos utilizando **chmod 777 (**nombre del fichero**)**.

Corra el programa con: **./IDS\_MARCORO o ./IDS\_MARCORO2.**



**Como dentro de mis ips bloqueadas no se encuentra mi usuario o dominio, es que sale el mensaje “Bad rule”.  
Ambos IDS controlan para no bloquear TU PROPIO HOSTNAME.**

**Contenido dentro de iptables.conf:**

