**UNIVERSIDAD DE LOS ANDES**

**FACULTAD DE INGENIERÍA**

**MAESTRÍA EN SEGURIDAD DE LA INFORMACIÓN**

**CURSO: MSIN – 4102 Infraestructura Segura**

**Héctor Mauricio Sánchez Cod 200918684**

**Fredy Alonso Cardona Cod 200519139**

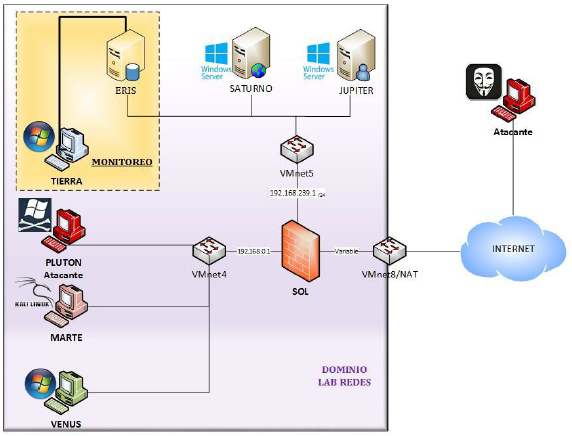
**Felipe Rivera Cod 201214786**

**Joan Torres Cod 201315711**

# Informe Proyecto IDS

## Configuración inicial del Ambiente

Para el desarrollo de las actividades propuestas para el proyecto, se realiza la configuración del ambiente de acuerdo a la topología de red mostrada a continuación.



*Arquitectura Ambiente Proyecto IPS*

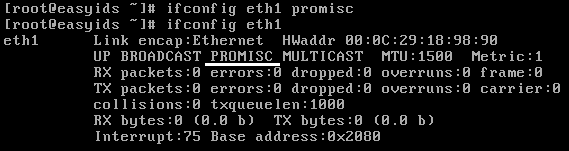
Para el desarrollo de la implementación del Proyecto, se definieron los siguientes segmentos de Red, los cuales se configuración a través del Firewall:

* Zonas de Red
  + Verde: Zona Segura
  + Naranja: Red DMZ
  + Roja: Zona Insegura (Internet)

## Aislamiento del Snort

Según la definición de la página oficial de Snort, éste se define como un software abierto y gratuito para la detección y prevención de intrusiones en tiempo real y registro de los paquetes de tráfico. “What is Snort? It is an open source intrusion prevention system capable of real-time traffic analysis and packet logging”.

La instalación de la máquina con Snort, se realiza en el servidor ***ERIS*** del ambiente, el cual se configura con dos (2) interfaces de red, una conectada a una interfaz de red independiente para la administración de la solución y otra tarjeta de red conectada a la Zona Segura (Verde) en ***modo promiscuo***, para el monitoreo de los del tráfico hacia los servidores víctima.

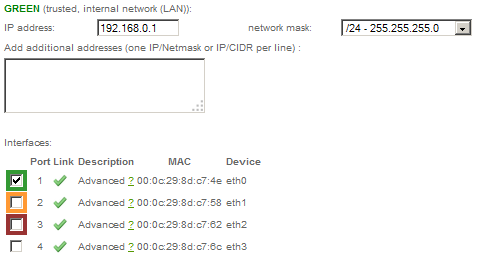


## Configuración de las Zonas en el Firewall Endian

El desarrollo de la configuración de la Topología de red se realiza la configuración de 3 zonas de Firewall, las cuales se describen a continuación:

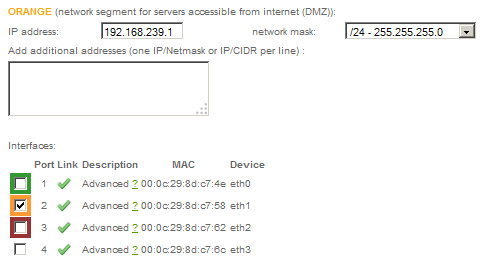
***Zona Verde:***

El segmento de red correspondiente a los servidores internos de la red **LABREDES**. El direccionamiento utilizado para la zona es **192.168.0.0/24**, la dirección IP de la Interfaz del firewall es 192.168.0.1.



***Zona Naranja:***

El segmento de red correspondiente a los servicios expuestos de la red **LABREDES**. El direccionamiento utilizado para la zona es **192.168.239.0/24**, la dirección IP de la Interfaz del firewall es 192.168.239.1.



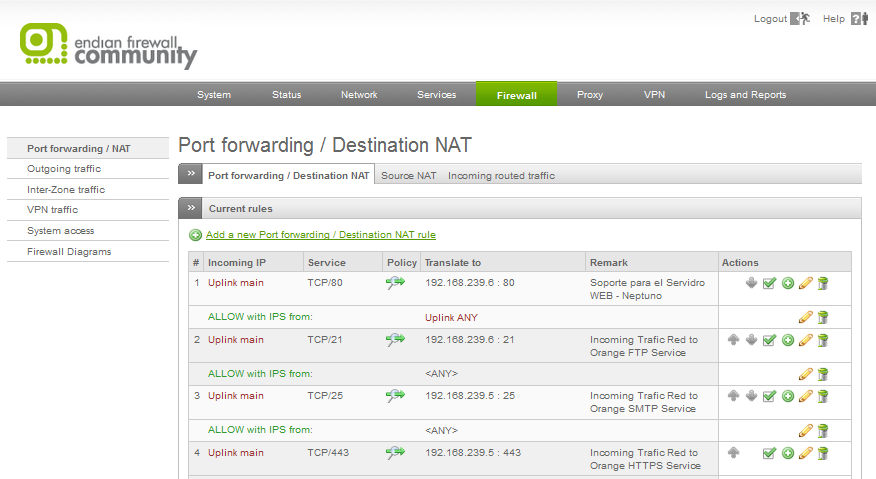
***Zona Roja:***

El segmento de red correspondiente a la conexión hacia **internet**.

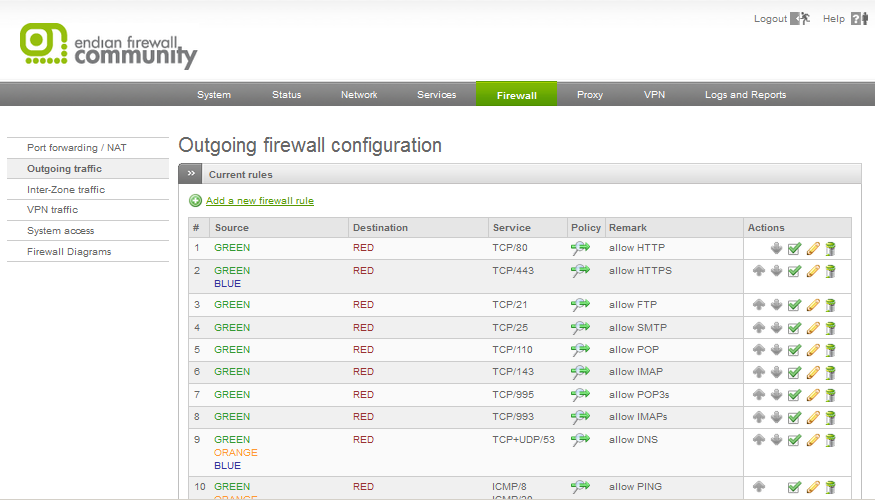
## Políticas de Seguridad Implementadas en el Firewall

En la implementación del Firewall para la topología de red de LABREDES se realizó la configuración de las siguientes políticas.

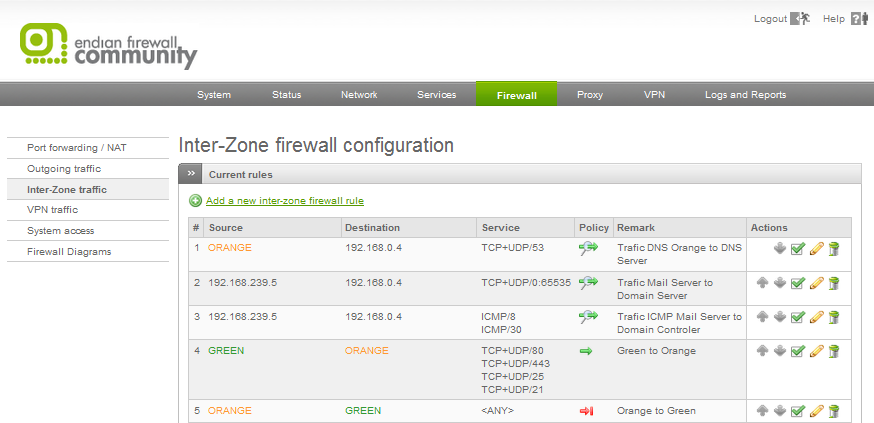
* ***Políticas de Redirección***



* ***Políticas de Entrada desde la Zona Roja (Internet)***



* ***Políticas entre Zonas***

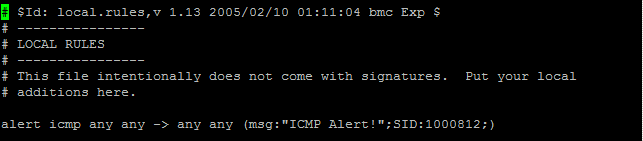


## Falla o en su defecto detección de los ataques en SNORT

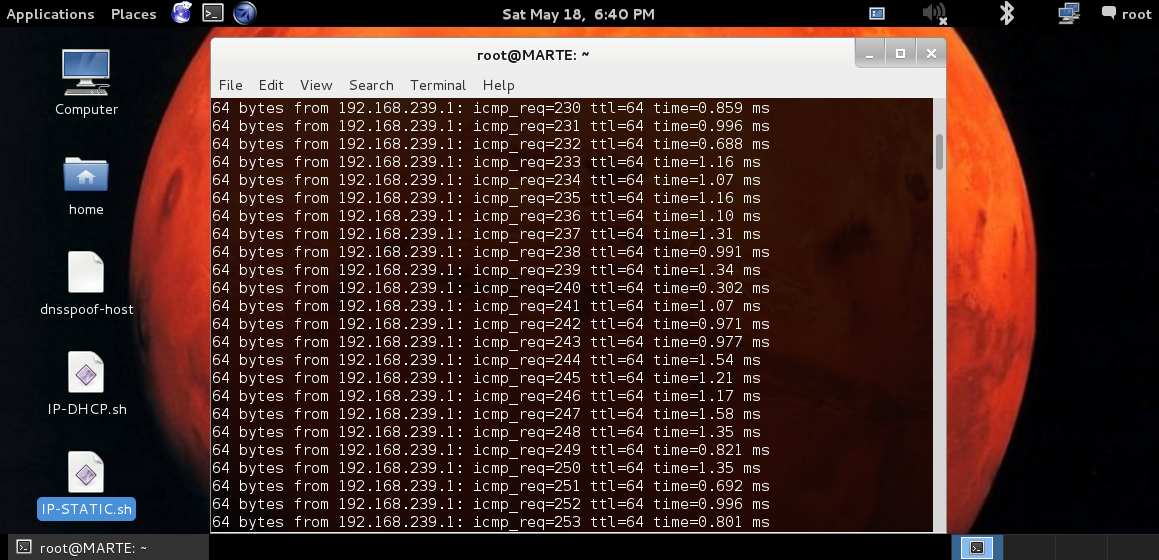
Luego de completar la implementación de la solución del SNORT, se realiza la configuración de las reglas de detección:

### Detección ICMP

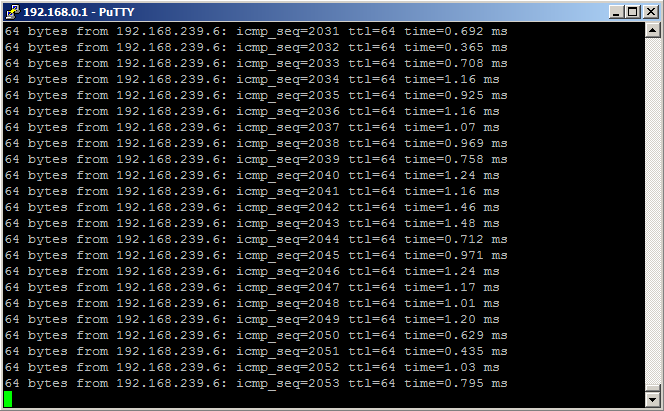
En la configuración del IDS, se realiza la implementación de reglas de detección del tráfico ICMP.



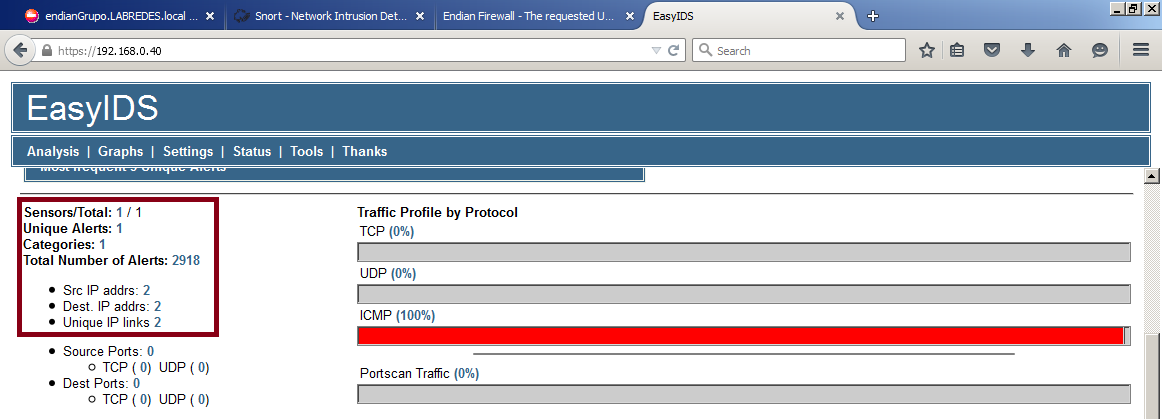
Desde diferentes hosts se realiza el envío de tráfico ICMP hacia la red monitoreada por el IDS.Para ello, se realiza la conexión de Marte a la Zona Naranja con el direccionamiento IP 192.168.239.6 y se realiza las peticiones de ping al servidor Júpiter, el cual tiene la IP 192.168.0.4.



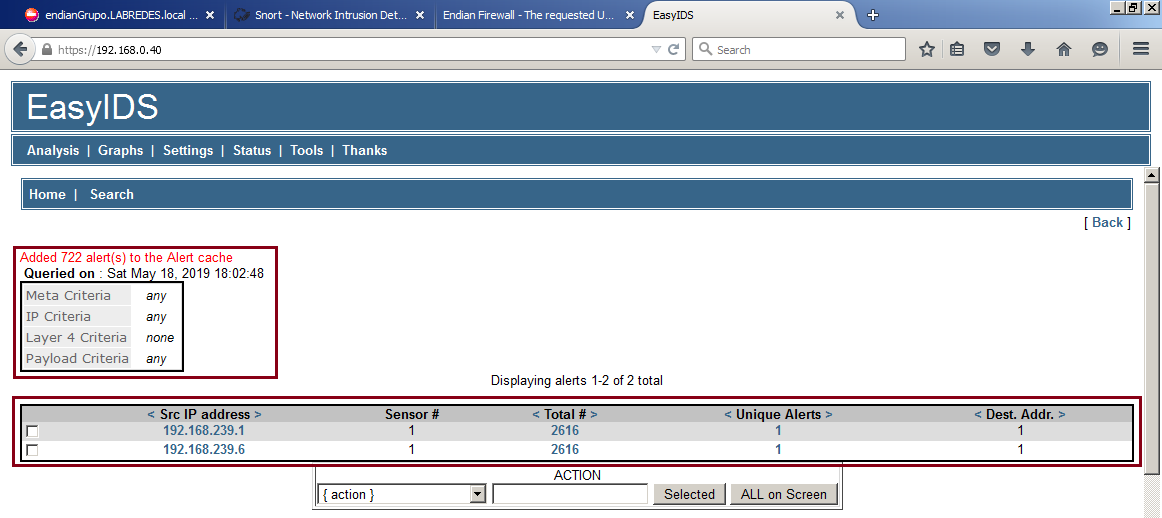
Así mismo, se realiza el envío de las peticiones ICMP desde el firewall Endian hacia el mismo host:



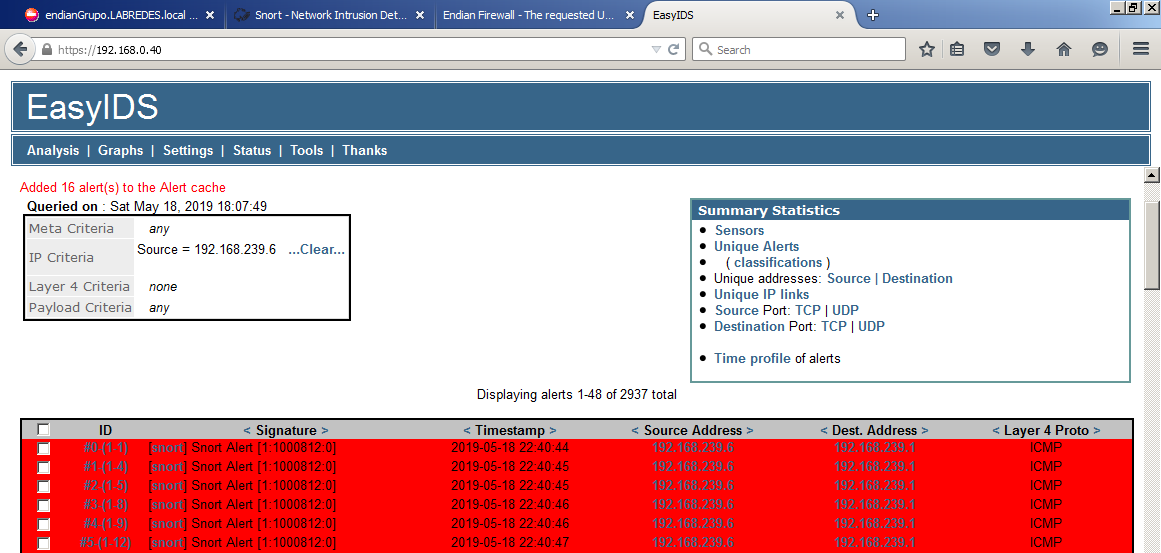
En la consola de gestión BASE proporcionada por la solución del SNORT, se evidencian las alertas de las peticiones ICMP hacia la red que está siendo monitoreada por el sensor.



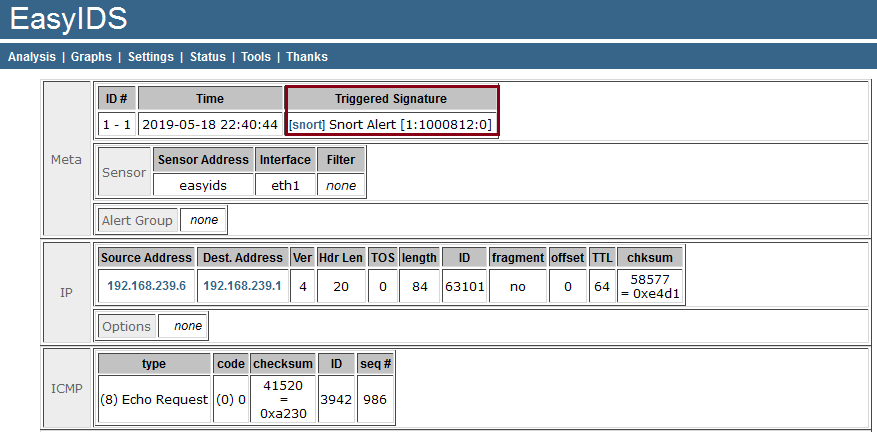
Al revisar en detalle los registros alertados por la solución, se ven los registros de las alertas generadas, con la información inicial desde donde se está realizando la solicitud y la cantidad de ocurrencias del evento.



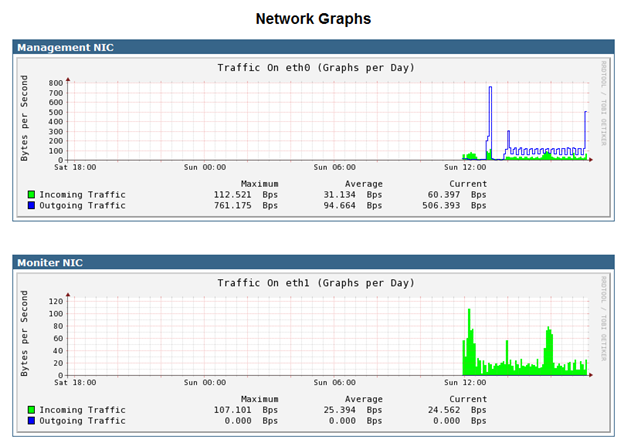
Al ingresar al detalle, se tiene el registro de cada uno de los eventos generados.



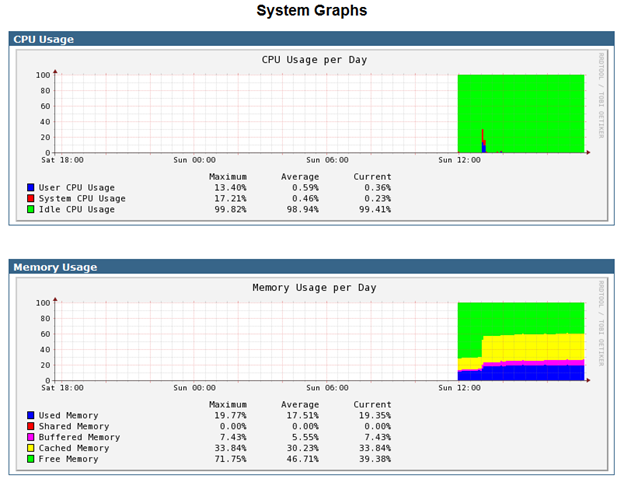
En la información del evento se encuentra el detalle de la información, incluyendo el ***ID de la alerta de detección*** creada inicialmente.



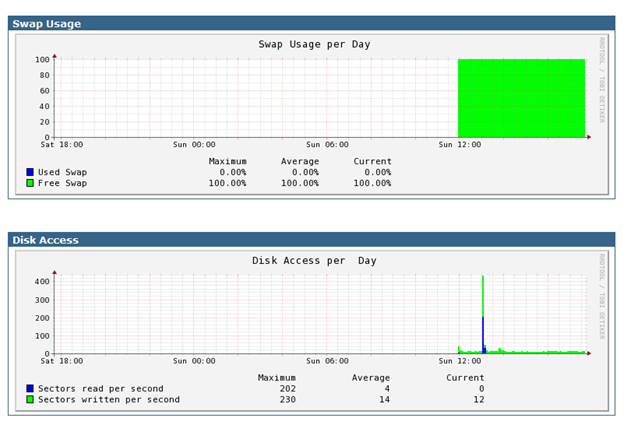
Se observo el tráfico de red en eth0 y en eth1 donde se puede ver que el incomming traffic es mucho mayor en la eth1 y el outgoing traffic es mayor en eth0.



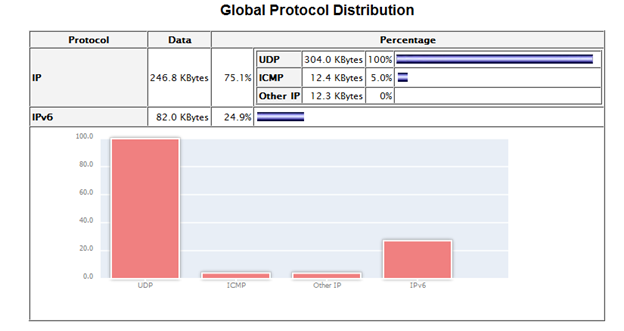
En los gráficos de sistema es posible monitorear el uso de las diferentes memorias y las cpus con el fin de descubrir comportamientos por fuera de los patrones ya determinados y de esta manera identificar posibles intrusos.



También es posible monitorear los accesos a disco ya sea de escritura o de lectura, esto con el fin de monitorear los movimientos de la información persistente almacenada dentro del sistema.



Es posible identificar los protocolos de conexión y de comunicación del sistema y el peso de la información que viaja por estos.



### Prueba Synflood

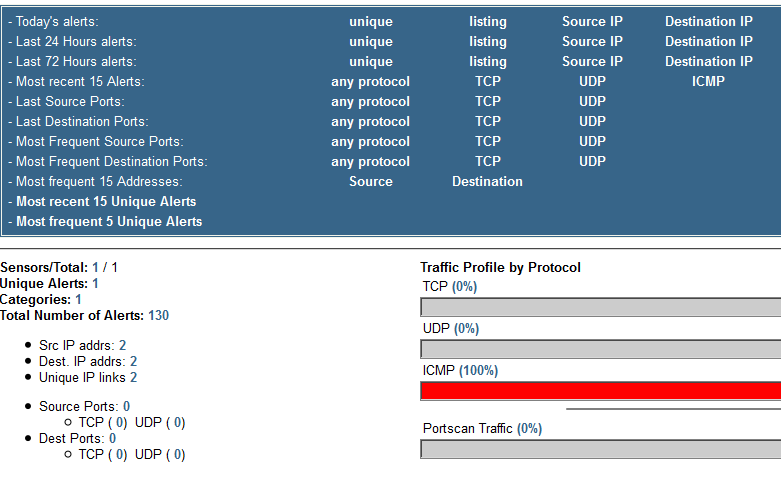
### Reglas activadas para evitar un ataque de DoS utilizando flood.

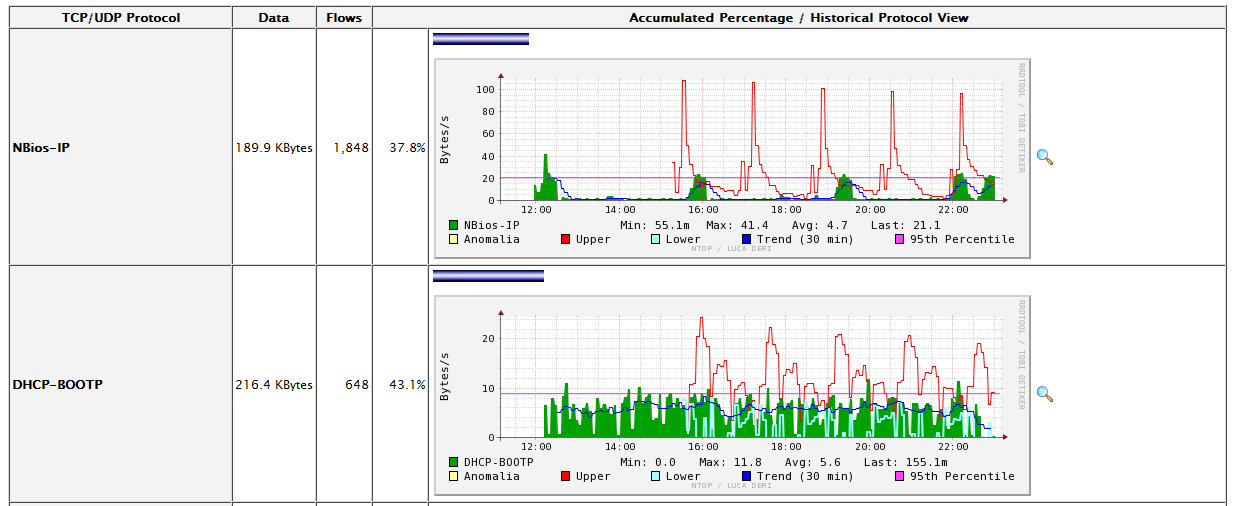
### 

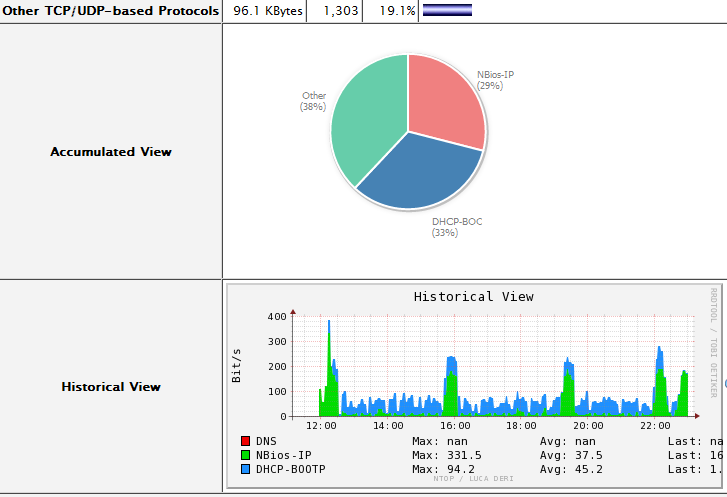
### Ataque Utilizando un archivo Python

### Inserting image...

### Respuesta del IDS







El IDS regulo las peticiones con éxito impidiendo que el servicio se cayera.

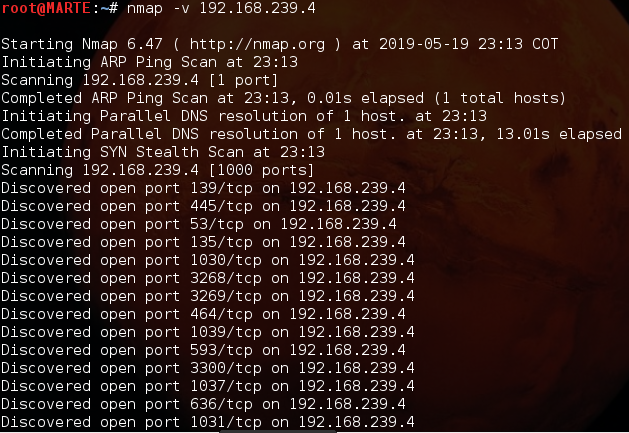
**Prueba Port Scan**

### Reglas activadas para evitar un ataque de análisis de puerto utilizando alguna herramienta tipo nMap.

### 

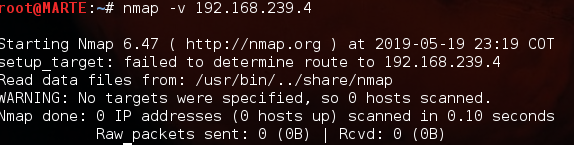
### Ataque usando nmap con kali Linux

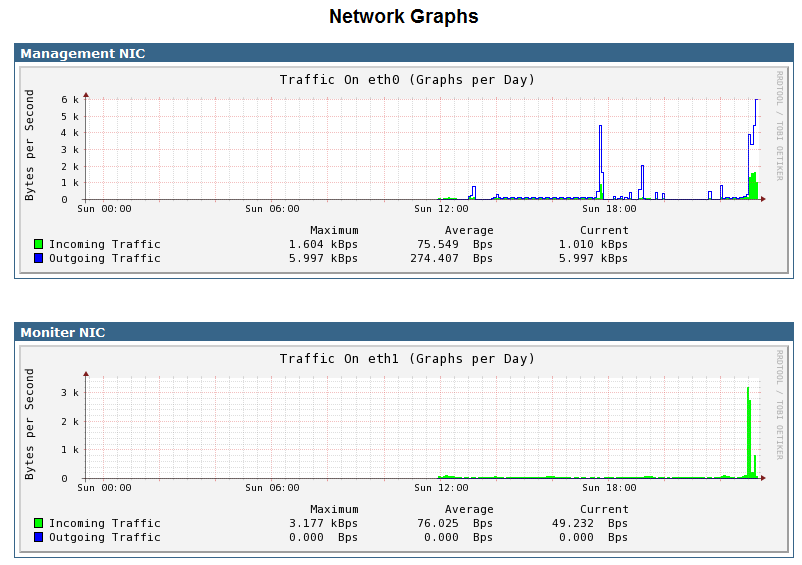
### 

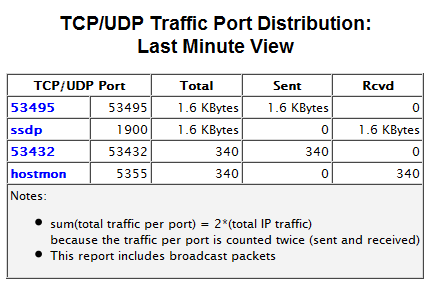


Respuesta del IDS

Después de activar las reglas anti port scan.







El IDS bloqueo el acceso a los puertos con éxito y no se puedo realizar el ataque una vez este se activó.