

## Implementación de un IDS

Implementation of an IDS

Mario Ávila Pérez \*

\* Ingeniero de Sistemas. Especialista en Pedagogía para el desarrollo del Aprendizaje autónomo. Especialista en Seguridad Informática. Docente Escuela De Ciencias Básicas, Tecnologías e Ingenierías. Universidad Nacional Abierta y a Distancia UNAD, Barranquilla. mavilap@gmail.com

**Fecha de recepción:** 27 de Noviembre de 2019

**Fecha de aceptación:** 13 de Julio de 2020

**Citación:**

Ávila Pérez, M. (2020). Implementación de un IDS. Gestión, Competitividad e innovación(Enero-Junio 2020), 11-23.

## **RESUMEN**

*En este artículo se presenta la actividad individual correspondiente a la práctica 2 del curso Seguridad Avanzada en Redes de Datos, evidenciando la instalación, configuración y pruebas de un sistema de detección de intrusos IDS. La práctica se realiza en un ambiente controlado, en una red LAN aislada, las máquinas utilizadas para las pruebas se virtualizaron usando la herramienta VirtualBox. La prueba se basó en la instalación de una máquina servidor web, una máquina atacante con una instalación de kalilinux y un servidor IDS con el IDS Snort.*

**Palabras Claves:** Modelo de medición, diagnostico, procesos logísticos, parámetros, sistemas de información, Balanced Score Card, supply chain, planeación estratégica, indicadores estratégicos..

## **ABSTRACT**

*This article presents the individual activity corresponding to practice 2 of the Advanced Security in Data Networks course, evidencing the installation, configuration and testing of an IDS intrusion detection system. The practice is done in a controlled environment, in an isolated LAN network, the machines used for the tests were virtualized using the VirtualBox tool. The test was based on the installation of a web server machine, an attacking machine with a kali linux system and an IDS server with the IDS Snort.*

**Keywords:** IDS, snort, terminal, kali, linux, snorby, command.

### **1. Introducción**

Las organizaciones de hoy están incorporado a sus procesos elementos que permitan hacer medición para poder evaluar si las metas se están cumpliendo, poder conocer en tiempo real los avances en materia de resultados y poder aplicar los correctivos si son necesarios con el propósito de reencaminar acciones y esfuerzos dirigidos. Los resultados obtenidos a través de la medición sirven como herramientas para identificar oportunidades y/o debilidades presentes en los procesos controlados.

La amplia utilización que tienen las redes hoy en día, y la cantidad de servicios de aplicaciones y servicios que se brindan a través de las redes, hace necesario que se establezcan mecanismos que garanticen la seguridad de dichas redes. Un sistema detección de intrusos IDS, constituye un mecanismo de monitoreo constante a una red, con la finalidad de detectar actividad inusual, sospechosa o maliciosa, proveniente de una fuente externa o de internet, o proveniente de un dispositivo interno de la red monitorizada.

### **2. IDS (Sistema de Detección de Intrusos)**

Un IDS es un sistema de detección de intrusos que consiste en monitorear el tráfico de la red para someterlo a un análisis con el propósito de detectar actividad sospechosa y de esta manera proceder a generar una alarma o una acción correctiva. El análisis del tráfico de la red se realiza mediante la utilización de mecanismos de identificación de patrones y métodos estadísticos. Los sistemas de detección de intrusos se fundamentan en tres pilares que son:

- Una fuente de información que proporciona eventos del sistema
- Un motor de análisis que busca evidencias de intrusiones
- Un mecanismo de respuesta que actúa según los resultados del motor de análisis

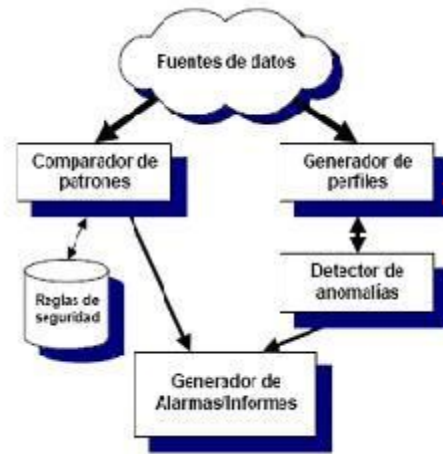


Figura 1 Esquema general de un IDS. Fuente: Propia

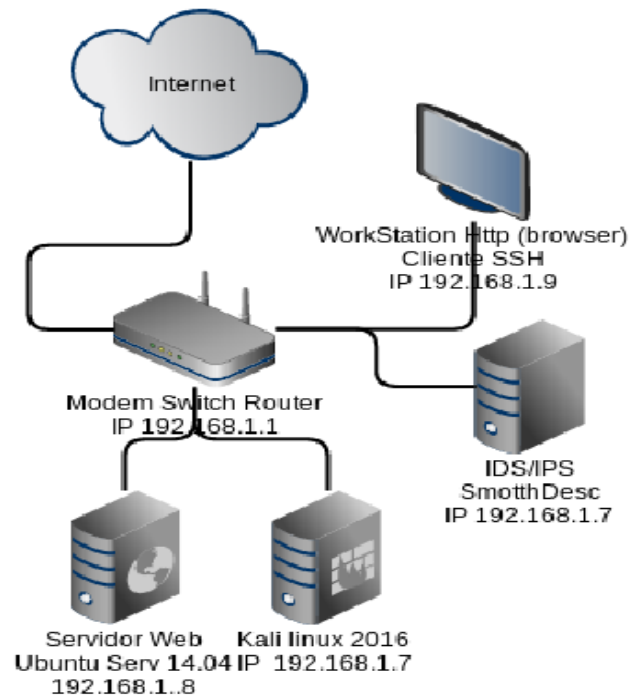


Figura 2 Diagrama de la topología utilizada para la práctica. Fuente: Propia

## Instalación del IDS

Se tomó la decisión de descargar una distribución Linux basada en debían denominada SmoothSec, la cual según lo investigado es uno de las mejores distribuciones, que ofrece versatilidad, facilidad de configuración y proporciona seguridad a una red determinada con una rápida implementación del software de monitoreo Snort [1].

Se descargó la distribución desde el sitio [wb para desarrollo sourceforge](https://sourceforge.net/projects/smoothsec/), <https://sourceforge.net/projects/smoothsec/> en formato ISO. Se creó una máquina virtual en Virtualbox (esta instalación se tenía previamente desde la práctica 1. Se procedió a inicializar la máquina virtual con boot desde la ISO smoothsec descargada, como se aprecia en la Figura 3y 4.

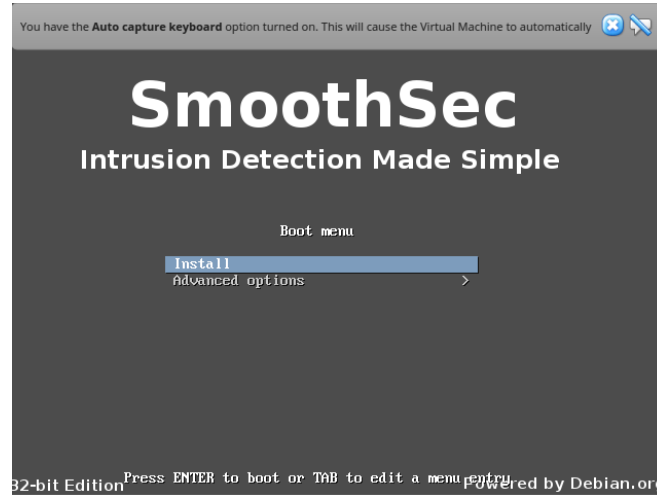


Figura 3. Instalación de SmoothSec. Fuente: Propia

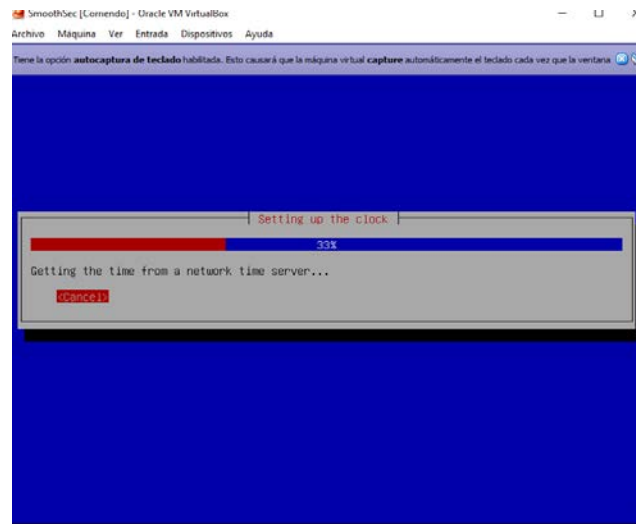


Figura 4. Inicio del script de instalación. Fuente: Propia

Luego de ingresar los parámetros necesarios, comunes a una instalación debían tales como idioma, país teclado nombre del host, del dominio, configuración, de los cuales se omite evidencia por ahorro de espacio en el documento, el script de instalación solicita autorización para la escritura del grub en el boot del disco principal, a lo que se responde afirmativamente. Con lo cual finaliza la instalación y el sistema pide confirmación para el reinicio.

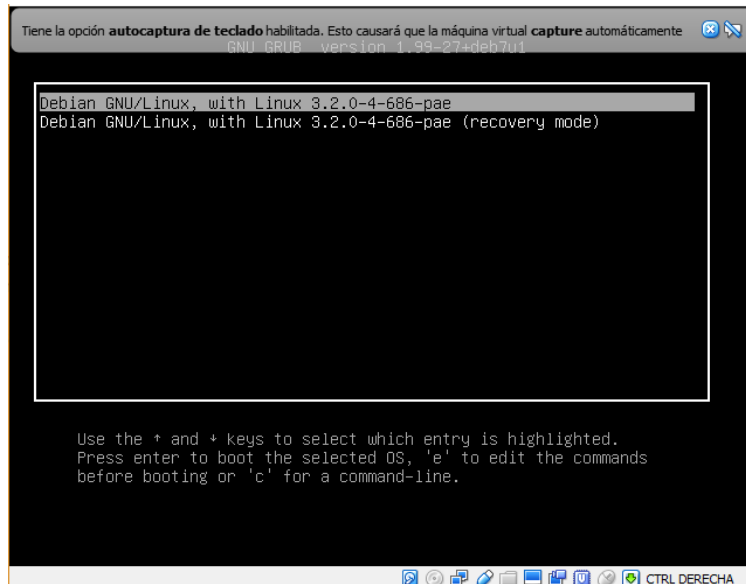


Figura 5. Inicio del SmoothSec. Fuente: Propia

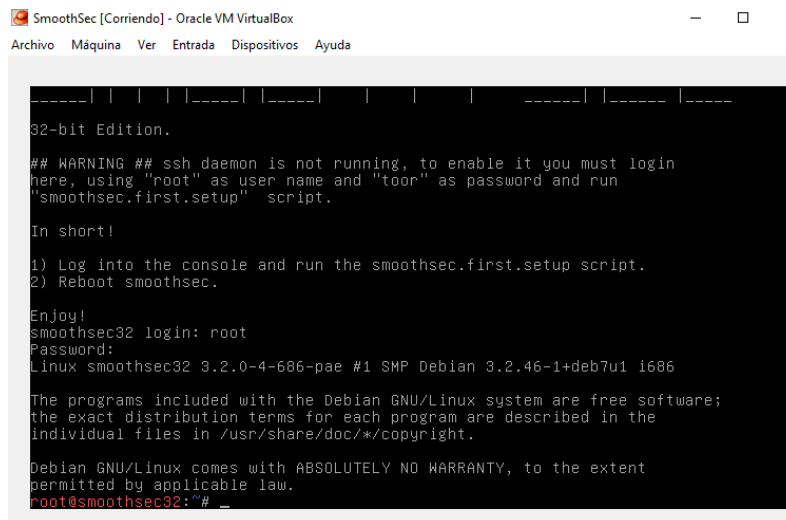


Figura 6. Primer Login. Fuente: Propia

Una vez se ingresa al sistema con el usuario root, contraseña toor, se procede a ejecutar el script smoothsec.first.setup. Este script realiza la configuración del IDS como se muestra en la figura 7. [2]

```

SmoothSec [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

*** Welcome to SmoothSec 3.4 ***

Available deployments:

One Network Interface is required.
standard  (IDS mode - All in one mode [Snorby + Sensor])
console   (IDS mode - Distributed [Only Snorby web console])
sensor    (IDS mode - Distributed [Only sensor])

Three Network Interface are required.
ips-standard (IPS mode - All in one mode [Snorby + Sensor])
ips-console  (IPS mode - Distributed [Only Snorby web console])
ips-sensor   (IPS mode - Distributed [Only sensor])

exit      (If unsure.)

Type here your favourite deployment : _

```

Figura 7. smoothsec.first.setup. Fuente: Propia

Se selecciona la opción Standard, luego se digita la contraseña para el usuario root, se crea un usuario adicional.

```

SmoothSec user setup

Enter a username for the new SmoothSec user. Your first name is a
reasonable choice. The username should start with a lower-case letter.
Enter your username : mario

Select a password for the new SmoothSec user. A good password will contain
a mixture of letters, numbers and punctuation.

Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Adding user 'mario' to group 'sudo' ...
Adding user mario to group sudo
Done.

IDS engine setup.

Please select the Intrusion Detection Engine that you want to use.

1) snort
2) suricata
Please enter your choice (type 1 for Snort or 2 for Suricata):_

```

Figura 8 Configuración de SmoothSec. Fuente: Propia

## Configuración

Se selecciona como motor para el IDS a SNORT también se puede seleccionar suricata.

```

*** Welcome to SmoothSec Standard setup Wizard [Snorby + Sensors]***

The setup wizard will guide you to configure SmoothSec for the first time.
Please follow the setup wizard step by step to complete the basic configuration.

The Wizard will guide you through the following steps:
1. Set root password for local login.(NO SSH LOGIN FOR ROOT.)
2. Set SmoothSec user account and password.(SSH and SUDO ALLOWED.)
3. Choose the IDS engine (Snort or Suricata).
4. Set the network interface to listen to.
5. Configure the Local Area Network.
6. Set Snorby web interface username and password.
7. Snorby automatic database setup.

Changing root password - Please choose a strong one!

Enter new UNIX password: _

```

Figura 9 Configuración de SmoothSec. Fuente: Propia

```

File Machine View Input Devices Help

Snorby setup..

Snorby Username (your_name@your_email.com) and Password creation.
Please enter your email address: mavilap@gmail.com
Please confirm your email address: mavilap@gmail.com
Please enter your desired Snorby password (Choose a strong one!):
Please confirm your desired Snorby password:

*** Please wait while the setup installs Snorby database. ***

*** CONGRATULATIONS! Your SmoothSec setup has been successfully completed! ***

SmoothSec user accounts.

Snorby web interface login:      mavilap@gmail.com
SmoothSec user account.(SSH + SUDO): mar1o
SmoothSec local login.(NO SSH):  root

Please reboot Smooth-sec typing:  reboot

root@smoothsec32:~# _

```

Figura 10. Configuración de SmoothSec. Fuente: Propia

Luego se solicita la configuración snorby, para lo cual se ingresa un Email válido y un password robusto. Una vez terminado el script de configuración se procede a reiniciar el servidor, con el comando reboot.

Se pueden apreciar las dos máquinas en la figura 11, cabe destacar que la configuración de la red en virtual box se hizo utilizando la opción puente (setting > network > attached to Bridge Adapter), para que las maquinas queden visibles en la red local.

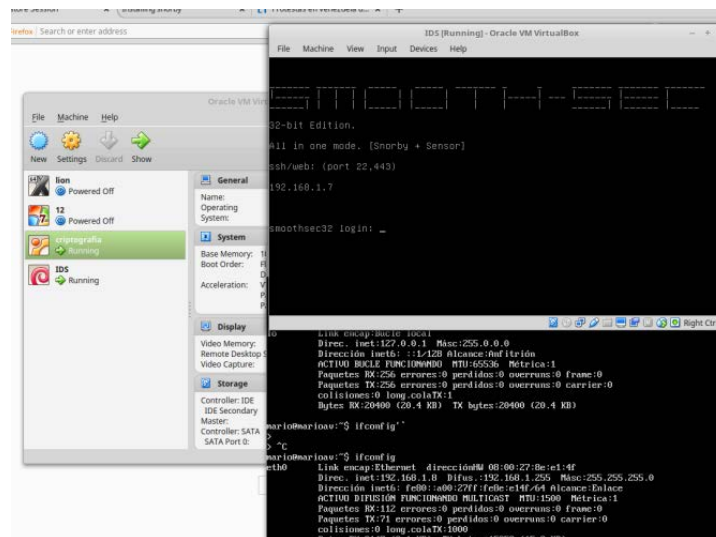


Figura 11. Vista de las máquinas en virtualBox. Fuente: Propia

Luego de tener el IDS Configurado se procedió a configurar el servidor web, para lo cual se instaló una máquina virtual con Ubuntu server, para alojar el servidor web.



Desde la maquina Kali 192.168.1.12, se abrió el navegador digitando en la dirección: <http://192.168.1.18/prueba.html>

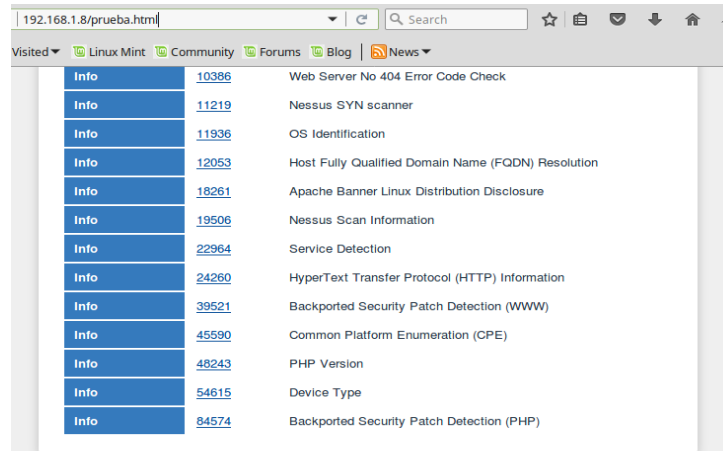


Figura 16. <http://192.168.1.18/prueba.html>. Fuente: Propia

Se procede a iniciar la máquina con kali Linux , previamente instalada, como se aprecia en la figura 17. Y comenzando a realizar un escaneo de puertos a todas las máquinas de la red , con el comando # nmap 192.168.1.0/24 .

```
File Edit View Search Terminal Help
MAC Address: 00:1C:BF:6A:5C:E0 (Intel Corporate)

Nmap scan report for 192.168.1.7
Host is up (0.0072s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp   open  https
MAC Address: 08:00:27:7F:81:4D (Cadmus Computer Systems)

Nmap scan report for 192.168.1.8
Host is up (0.0075s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:8E:E1:4F (Cadmus Computer Systems)

Nmap scan report for 192.168.1.12
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.1.12 are closed

Nmap done: 256 IP addresses (6 hosts up) scanned in 5.92 seconds
root@marioavila:/home/mario# nmap 192.168.1.0/24
```

Figura 17. Escaneo de puertos a todas las máquinas. Fuente: Propia

```
[*] Web Spider: Started.
[*] Web Spider: Spidering URL: http://192.168.1.0/
[*] Web Server Fingerprinter: Started.
[*] IP Geolocator: Started.
[*] IP Geolocator: Finished.
[*] Robots.txt Analyzer: Finished.
[*] Web Server Fingerprinter: 11.11% percent done...
[*] Web Server Fingerprinter: 22.22% percent done...
[*] Web Spider: Found 12 links in URL: http://192.168.1.0/
[*] Web Spider: No forms found in URL: http://192.168.1.0/
[*] Web Spider: Finished.
[*] Directory Listing: Started.
[*] Default Error Page Finder: Started.
[*] Web Server Fingerprinter: 33.33% percent done...
[*] Directory Listing: 25.00% percent done...
[*] Directory Listing: 50.00% percent done...
[*] Directory Listing: 75.00% percent done...
[*] Directory Listing: Finished.
[*] Default Error Page Finder: 0.022139974779
[*] Default Error Page Finder: 0.25% percent done...
[*] Default Error Page Finder: 0.60547899717749
[*] Default Error Page Finder: 0.50% percent done...
[*] Web Server Fingerprinter: 44.44% percent done...
```

Figura 18. Escaneo. Fuente: Propia

También se realizó ataque con comando hping . Hping es una línea de comandos orientado TCP , es un ensamblador de paquetes IP y analizador.

```
DEBUG: the source address is 59.48.209.209
45 00 00 28 46 51 00 00 40 06 00 00 3b 30 d1 d1 c0 a8 01 08 19 70 00 50 37 c8 19
8c 75 e0 2e a9 50 02 08 00 c9 92 00 00
DEBUG: the source address is 186.245.217.215
45 00 00 28 d3 23 00 00 40 06 00 00 ba f5 d9 d7 c0 a8 01 08 19 71 00 50 33 7f d8
c7 11 4d c7 14 50 02 08 00 52 fb 00 00
^C
--- 192.168.1.8 hping statistic ---
5388 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
45 00 00 28 d3 23 00 00 40 06 00 00 ba f5 d9 d7 c0 a8 01 08 19 71 00 50 33 7f d8
c7 11 4d c7 14 50 02 08 00 52 fb 00 00
root@marloavila:~/home/mariol# hping3 192.168.1.8 --rand-source -S --destport 80
--faster --debug -w 2048
```

Figura 19. Escaneo con hping. Fuente: Propia

Se procedió a realizar un ataque desde la maquina kali Linux hacia el servidor web utilizando la herramienta w3af, la cual se lanzó desde la consola de kali Linux con el comando # w3af, configuró el escaneo hacia nuestro servidor web, como se aprecia en la figura 20.

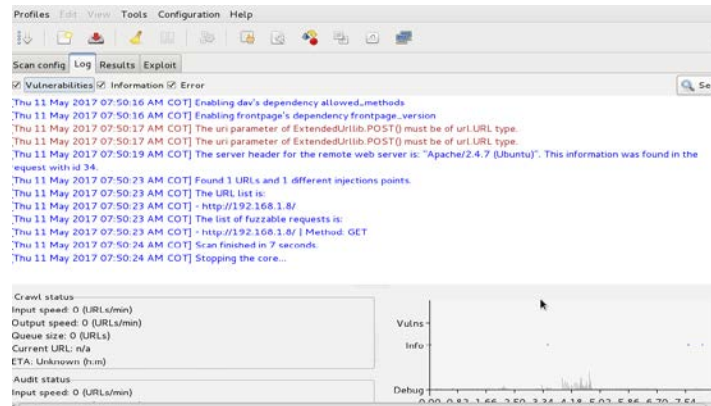


Figura 19. Escaneo con w3af [3]. Fuente: Propia

Se procedió a ingresar al servidor , desde la maquina host , para la cual se abrió el navegador web ingresando a la dirección https:// 192.168.1.7 , que apunta a snorby , la interfaz gráfica de administración de snort . Como se aprecia en la figura 21.

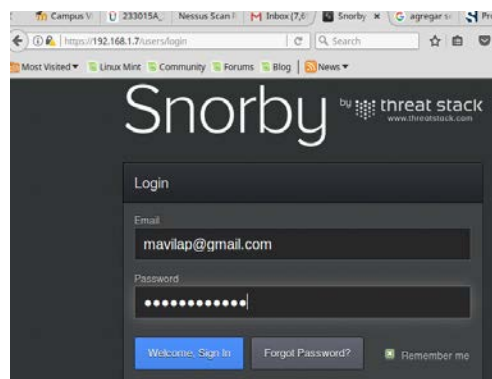


Figura 21 Ingreso a Snorby. Fuente: Propia

Se proporcionaron las credenciales que se seleccionaron durante la fase de configuración del IDS. El sistema despliega la página de inicio del monitor IDS como se puede observar en la figura 22.

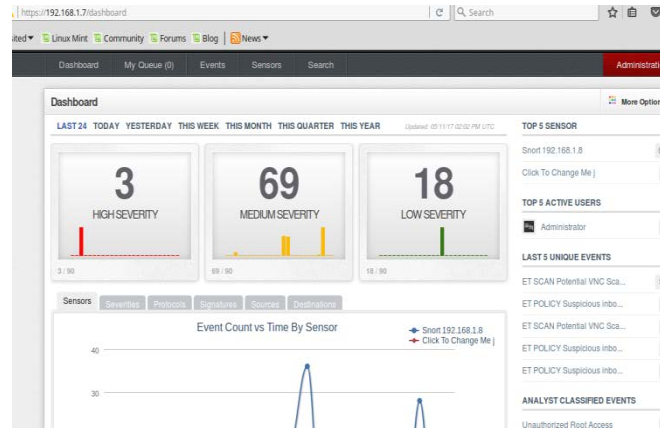


Figura 22. Pantalla de inicio de snorby. Fuente: Propia

En la figura 22 Se pueden apreciar unas 90 eventos para ese momento, y en la figura 23 a través de la pestaña source del monitor, se puede observar una estadística donde despliega un gráfico tipo torta, donde se muestra el origen de los eventos.

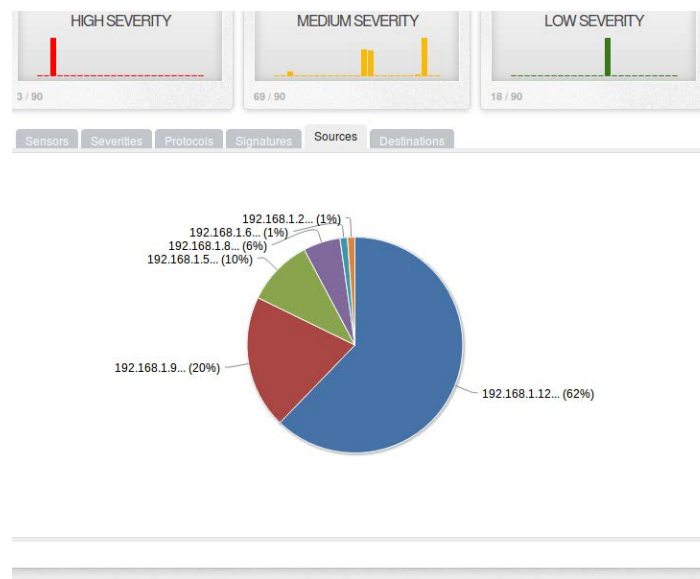


Figura 23. Origen de los eventos. Fuente: Propia

En la opción eventos de la interfaz de snorby, también es posible visualizar en detalle la naturaleza de los eventos, la firma del tipo de eventos, y otros datos que permitirán al administrador profundizar en la naturaleza del evento, como se puede ver en la figura 24.

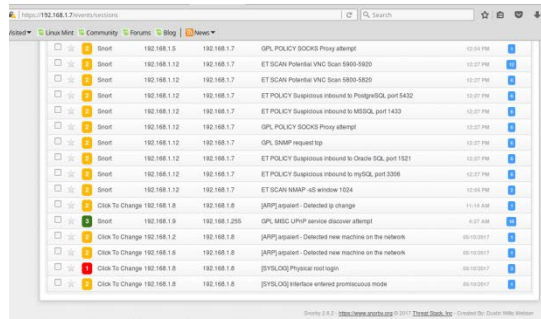


Figura.24. Eventos mostrados por snorby. Fuente: Propia



Figura 25. Eventos críticos. Fuente: Propia

Snorby posee una interfaz agradable, organizada y despliega información de diferentes formas, dependiendo de las características que se quieran observar., por ejemplo en la Figura 26 de puede observar un gráfico tipo torta donde se muestra los eventos por firmas.



Figura 26 Estadísticas del tipo de ataque. Fuente: Propia

## Conclusiones

Después de haber terminado la actividad se concluye que la protección de una red con un sistema de detección de intrusos IDS, es un paso fundamental a la hora de reducir el riesgo de vulneración de una red. Snort es un IDS de gran aceptación, robusto y gratuito, de código abierto. Su implementación ayuda disminuir el riesgo de vulneración de la red.

El monitoreo constante de una red mediante un IDS agrega capacidad de prevención y alerta a una organización, mediante la recopilación y análisis del tráfico de red. La realización de esta práctica deja como resultado una experiencia muy enriquecedora, que tiene mucha aplicabilidad en el campo de la seguridad informática.

## Referencias

- [1] Implementación de un servidor IDS para monitoreo de tráfico de red, Disponible en: <http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/10841/Informe.pdf?sequence=1>
- [2] SmoothSec IDS, Disponible en <https://techanarchy.net/2013/08/smoothsec-ids/>
- [3] Automated Audit using W3AF, Disponible en [https://www.owasp.org/index.php/Automated\\_Audit\\_using\\_W3AF](https://www.owasp.org/index.php/Automated_Audit_using_W3AF)
- [4] Como instalar el servidor web en Ubuntu, Disponible en: <http://www.vozidea.com/instalar-servidor-apache-ubuntu>.