Politécnico costa atlántica
INSTITUCIÓN DE EDUCACIÓN SUPERIOR

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

REVISTA GESTIÓN, COMPETITIVIDAD E INNOVACIÓN

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 maquina servidor web, una maquina atacante con una instalación de kalilinux y un sevidor 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

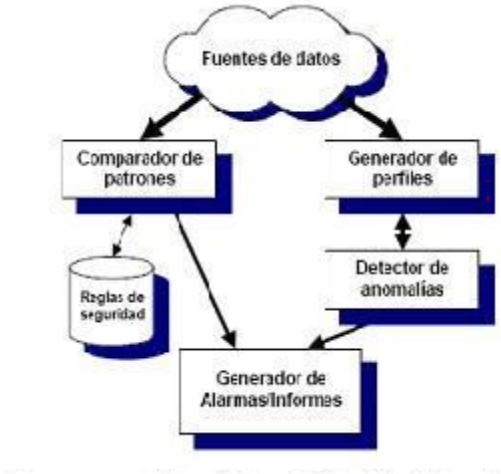

Figura 1 Esquema general de un IDS. Fuente: Propia

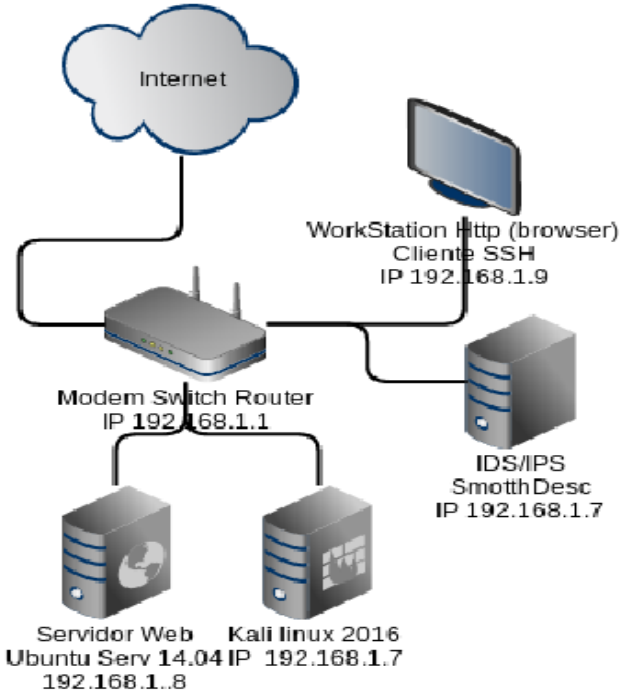

Figura 2 Diagrama de la topología utilizada para la práctica. Fuente: Propia

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/ en formato ISO. Se creó una máquina virtual en Virtualbox (eta 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.

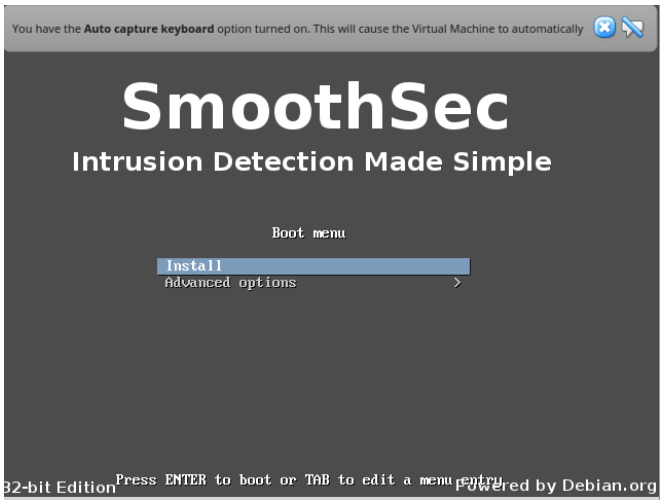

Figura 3. Instalación de SmoothSec. Fuente: Propia

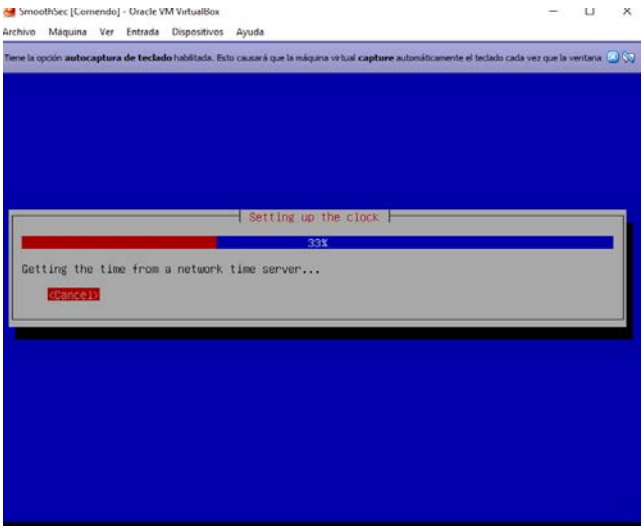

Figura 4. Inicio del script de instalación. Fuente: Propia

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 omita 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.

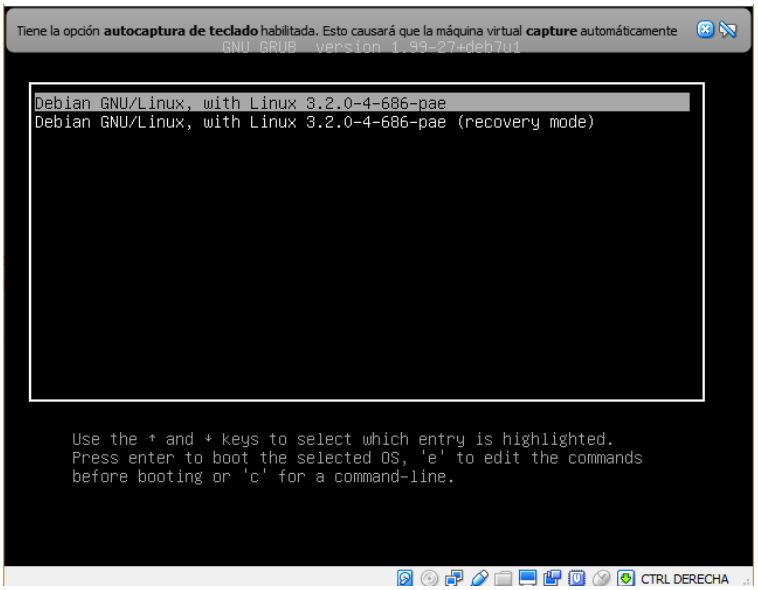

Figura 5. Inicio del SmoothSec. Fuente: Propia

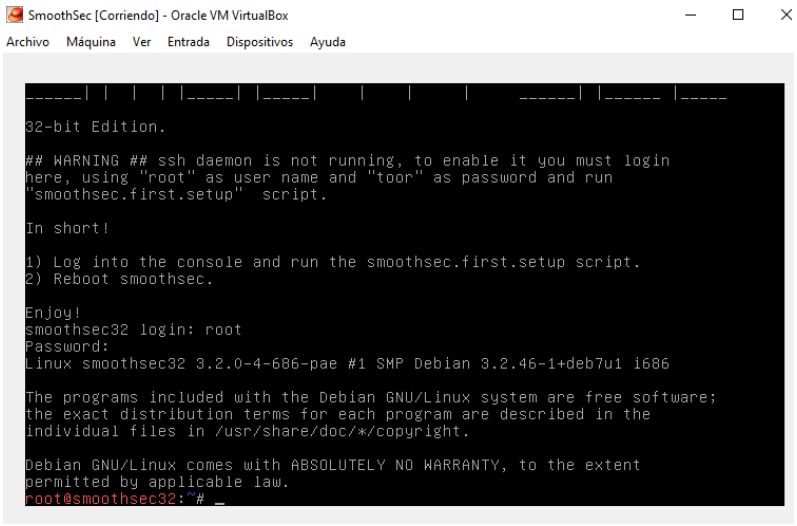

Figura 6. Primer Login. Fuente: Propia

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]

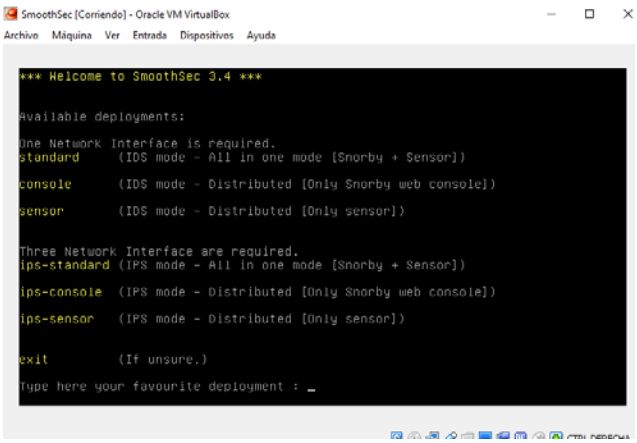

Figura 7. smoothsec.first.setup. Fuente: Propia

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

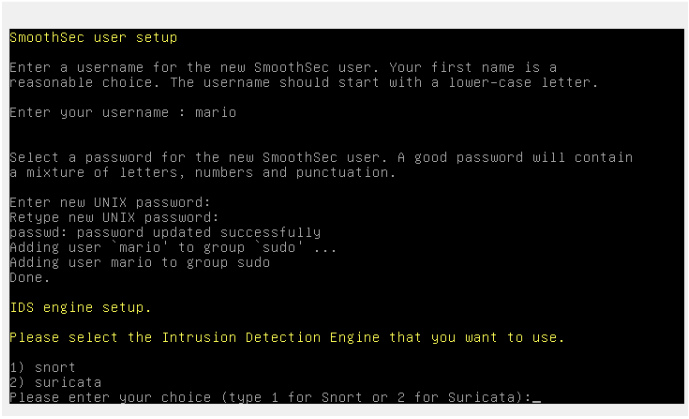

Figura 8 Configuración de SmoothSec. Fuente: Propia

Configuración

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

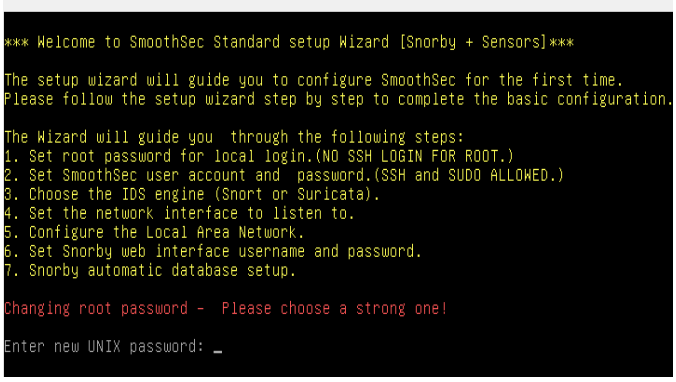

Figura 9 Configuración de SmoothSec. Fuente: Propia

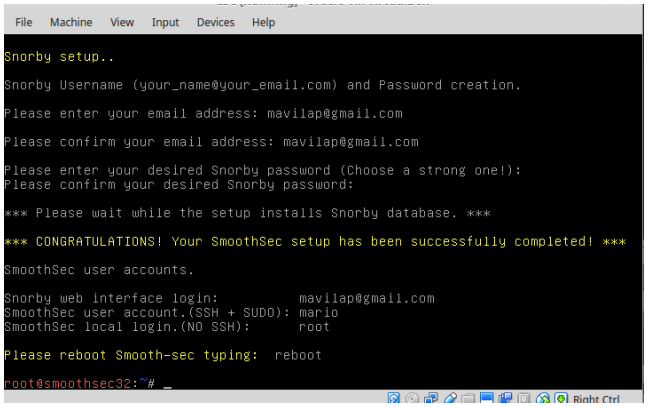

Figura 10. Configuración de SmoothSec. Fuente: Propia

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 > atacched to Bridge Adapter), para que las maquinas queden visibles en la red local.

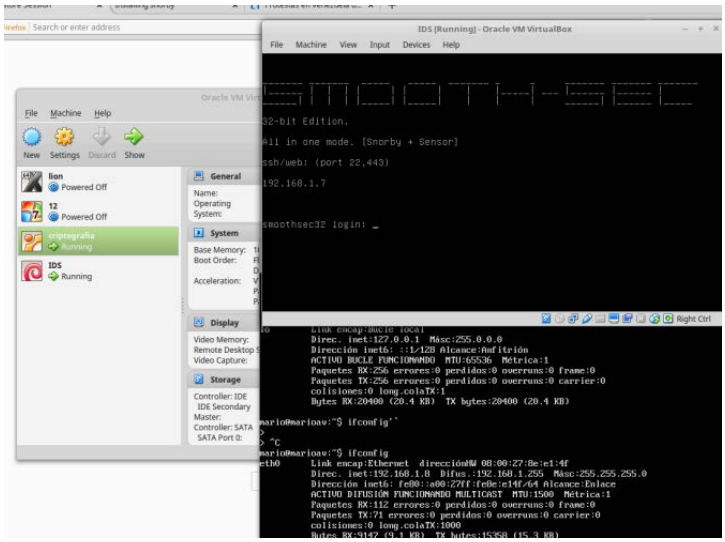

Figura 11. Vista de las máquinas en virtualBox. Fuente: Propia

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.

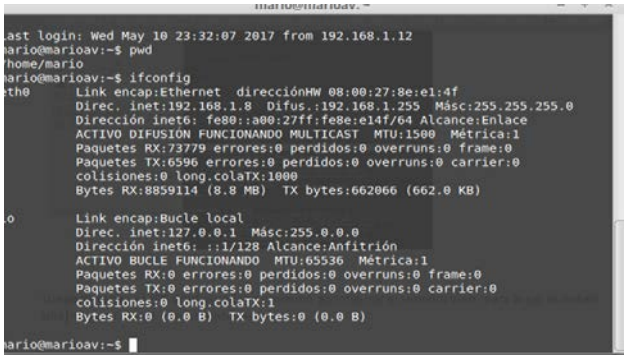

Figura 12. Servidor Web. Fuente: Propia

Una vez instalado el servidor con Ubuntu se procedió a instalar el servidor web apache, con el comando sudo apt-get apache2

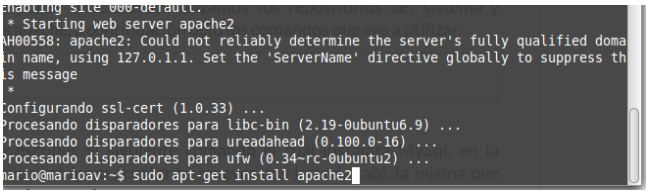

Figura 13. Instalación de Apache. Fuente: Propia

En el directorio /var/www/html Se publicó una página html cualquiera denominada prueba.html, como se aprecia en la Figura 14

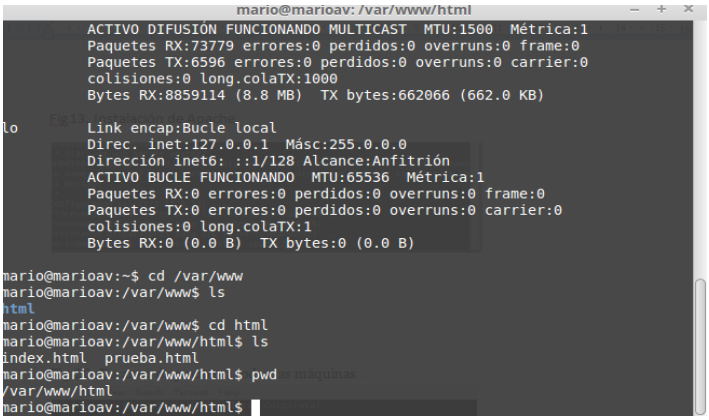

Figura 14. /var/www/html . Fuente: Propia

Se ejecutó el comando para subir el apache

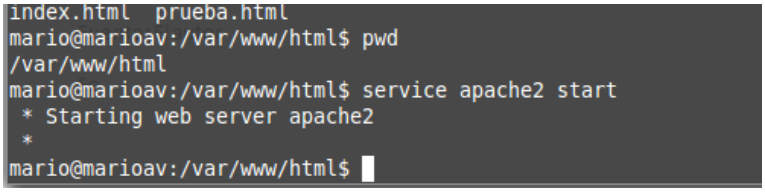

Figura 15. Htmls. Fuente: Propia

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

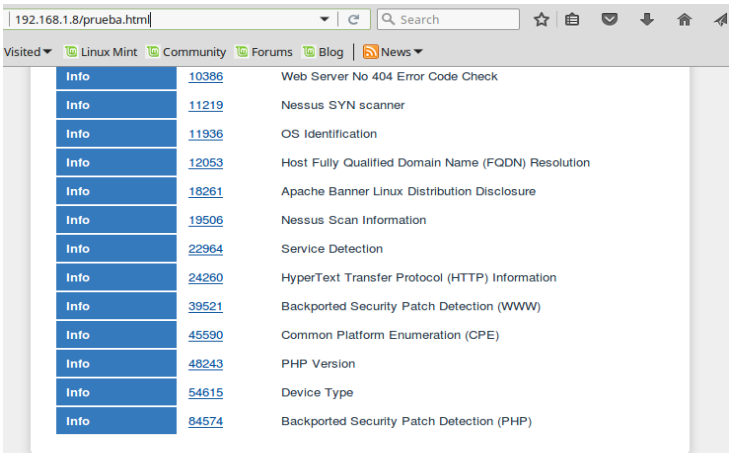

Figura 16. http://192.168.1.18/prueba.html. Fuente: Propia

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 .

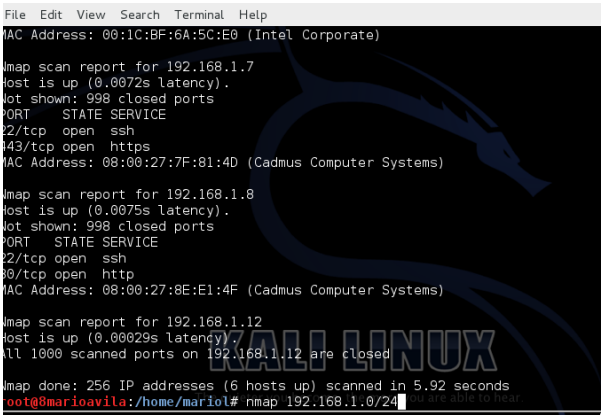

Figura 17. Escaneo de puertos a todas las máquinas. Fuente: Propia

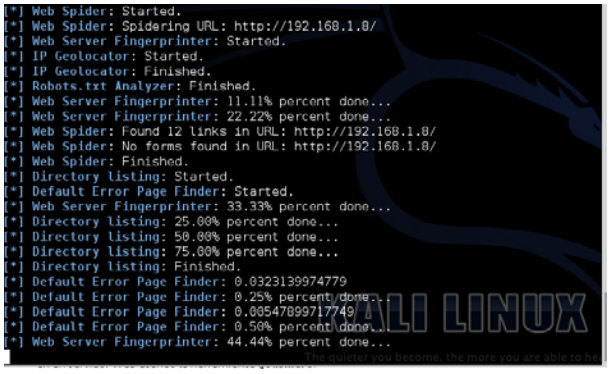

Figura 18. Escaneo. Fuente: Propia

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

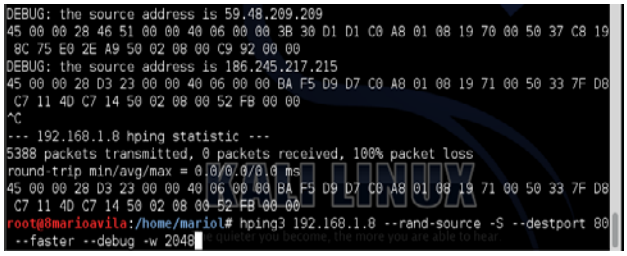

Figura 19. Escaneo con hping. Fuente: Propia

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.

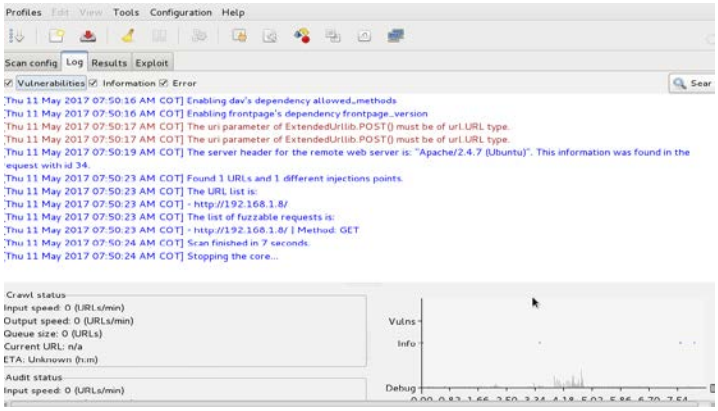

Figura 19. Escaneo con w3af [3]. Fuente: Propia

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.

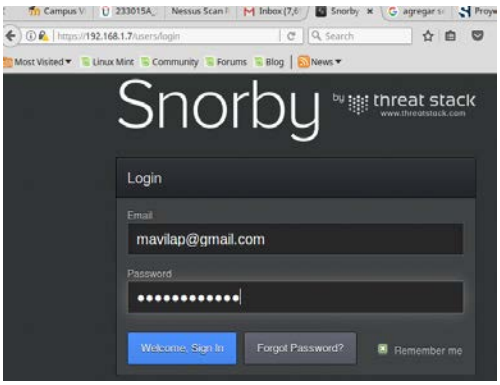

Figura 21 Ingreso a Snorby. Fuente: Propia

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.

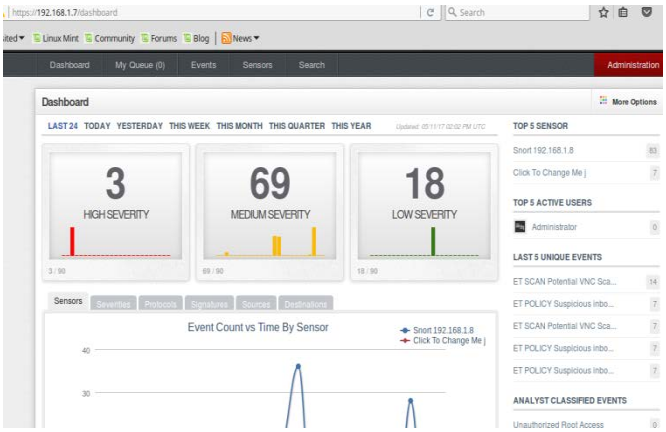

Figura 22. Pantalla de inicial de snorby. Fuente: Propia

En la figura 22 Se pueden apreciar unas 90 eventos para ese momento, y en la figura 23 a raves 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.

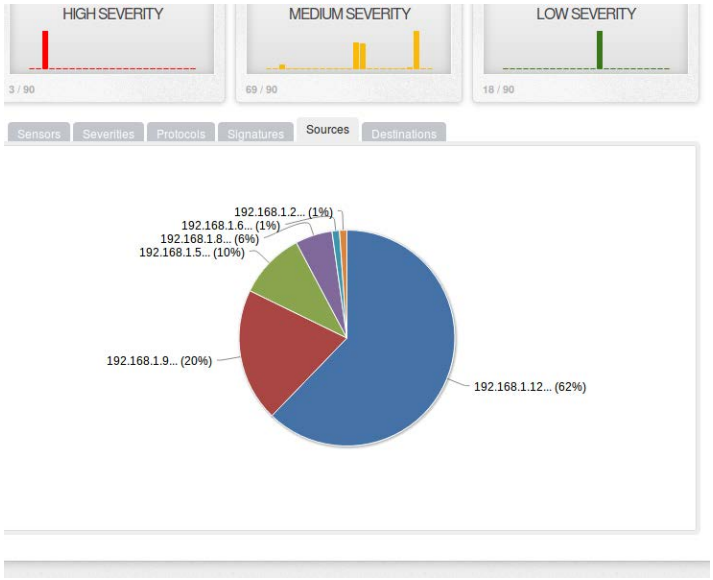

Figura 23. Origen de los eventos. Fuente: Propia

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.

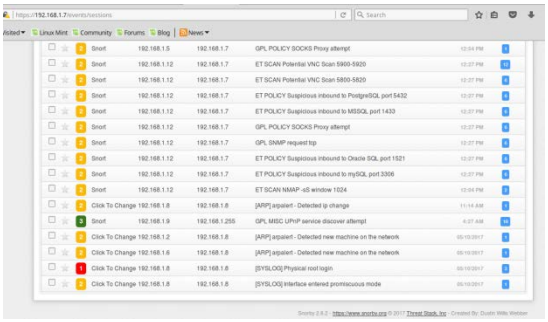

Figura.24. Eventos mostrados por snorby. Fuente: Propia

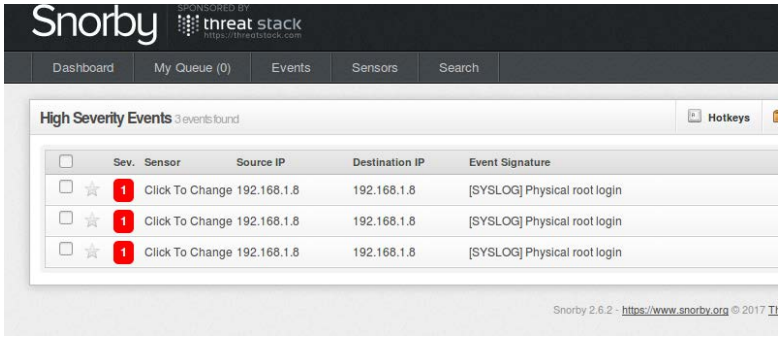

Figura 25. Eventos críticos. Fuente: Propia

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.

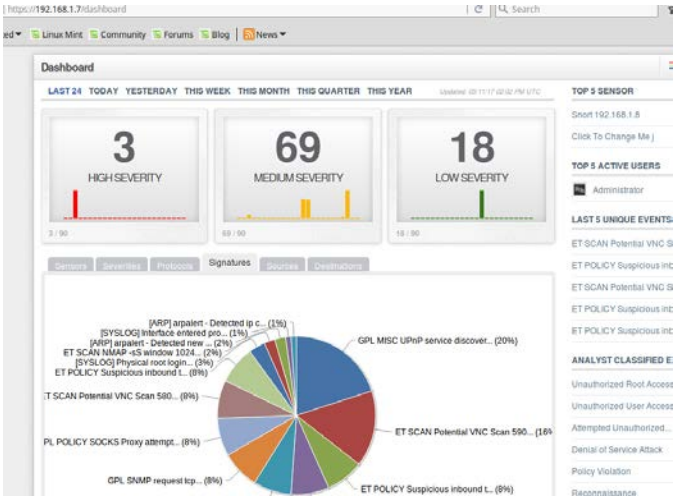

Figura 26 Estadísticas del tipo de ataque. Fuente: Propia

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

[4] Como instalar el servidor web en Ubuntu, Disponible en: http://www.vozidea.com/instalar-servidor-apache-ubuntu.