Revista Nexos Científicos *ISSN: 2773-7489*
Julio –Diciembre 2019 pp. 20-27 *Correo: editor@istvidanueva.edu.ec*
Volumen 3, Número 2 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: septiembre 2019 *Fecha de aceptación: octubre 2019*

Detección de Intrusos con la Plataforma Open Source Snort

Galo Manuel Diaz [1]

[1] *Universidad Tecnológica Israel-Ciencias de la Ingeniería –Carrera de Sistemas, Quito, Ecuador, galodiaz@gmail.com*

Resumen: En el campo de las Tecnologías de la Información la seguridad de los sistemas es uno de los factores más importantes a tener en cuenta. Sin una buena estrategia de seguridad, una de las partes más importantes y a la vez más vulnerables del sistema, los datos, podrían verse seriamente amenazados. Entre los componentes que ayudan a los administradores en las tareas de seguridad se encuentran los Sistemas de Detección de Intrusiones (IDS). Actualmente existen varios programas mediante los cuales se puede implementar un IDS, entre los que se destaca el Snort; este es un software muy flexible que ofrece la posibilidad de almacenar sus bitácoras tanto como en archivo de texto o en una base de datos. Este trabajo está enfocado en analizar y evaluar el desempeño del Snort como un IDS; para ello se llevan a cabo una serie de pruebas que consisten en escaneos desde diversas localizaciones mediante la utilización de herramientas como GFI Languard y Nmap.

Palabras clave: Tecnología, Software, Snort.

Intruder Detection With The Platform Open Source Snort

Abstract: In the field of Information Technology, the security of systems is one of the most important factors to consider. Without a good security strategy, one of the most important and most vulnerable parts of the system, data, could be seriously threatened. Components that help administrators with security tasks include Intrusion Detection Systems (IDS). Currently there are several programs through which an IDS can be implemented, among which the Snort stands out; This is a very flexible software that offers the possibility of storing your logs both as a text file or in a database. This work is focused on analyzing and evaluating the performance of the Snort as an IDS; For this, a series of tests are carried out, consisting of scans from various locations using tools such as GFI Languard and Nmap.

Keywords: Technology, Server, Linux, Radius.

1. INTRODUCCIÓN

De manera general, se puede describir la relación entre amenazas, vulnerabilidad y control de la siguiente manera: una amenaza puede ser bloqueada aplicando un control a una vulnerabilidad. (Kaufman, Perlman et al. 2002).

Los sistemas de protección convencionales como los firewalls y antivirus, entre otros, empiezan a ser insuficientes ante la gran variedad de ataques que día a día son cada vez más devastadores (Cheswick, Bellovin et al. 2003), esto muestra que es necesario crear una nueva línea de defensa que les evite a los administradores la tarea de estar pendientes en todo momento de su red.

Los atacantes están evolucionando y aparecen nuevas técnicas como los Troyanos, gusanos y escaneos silenciosos que atraviesan los cortafuegos mediante protocolos permitidos como HTTP, ICMP o DNS. Los atacantes buscan vulnerabilidades en

1. Estudiante de 8vo Sistemas Informáticos, galodiaz@gmail.com

los pocos servicios que el cortafuego permite y enmascaran sus ataques dentro de estos protocolos, quedando la red expuesta de nuevo.
Una buena forma de mejorar la seguridad de la red es la instalación de mecanismos de detección, capaces de avisar al administrador de la red en el momento en que se produzcan estos ataques (casi en tiempo real).
En esta línea, surgen los sistemas de detección de intrusos, como uno de los campos más investigados en los últimos años.
La Detección de Intrusos es uno de los métodos utilizados para proporcionar seguridad a una red de ordenadores; es la comprobación, a través del proceso de monitoreo, que un ordenador, una red o un sistema completo con varias subredes funcionan correctamente desde el punto de vista de las políticas de seguridad definidas por la organización. (Vigo 2005).

La elección del Snort se basa en que ha alcanzado un estado de madurez y desarrollo, donde su funcionalidad permite despliegues exitosos; por otra parte, su gran difusión a lo largo del mundo (más de 3, 000,000 de descargas y de 150,000 usuarios activos según (Scott, Wolfe et al. 2004)) permite tener una comunidad de usuarios lo suficientemente amplia como para advertir de nuevas amenazas y vulnerabilidades, y para generar y compartir reglas. En Snort, además, disponen de un amplio rango de herramientas y programas para su análisis, como, por ejemplo, BASE, Snortlog, Snortreport, Snortsam, etc. (Staff 2005).

2. METODOLOGÍA

Para la instalación y configuración del Snort e implementación como IDS; se ilustran los principales pasos a seguir y se configuran los elementos esenciales tales como: la red a la cual se desea proteger, las reglas y preprocesadores a utilizar, así como el formato que se desea que sea guardada la información recopilada en el fichero de salida.

2.1 Herramientas auxiliares para el funcionamiento del NIDS

Para la realización de esta investigación se realiza la instalación de una máquina virtual mediante el VMware con la última distribución de Ubuntu, la cual presenta la versión 2.9.6.0 del Snort en su gestor de paquetes disponible para esta distribución, aunque si se desea usar la versión más actual se puede descargar desde la página Web oficial (http:\\www.snort.org). La forma más sencilla es instalarlo directamente a través del gestor de paquetes debido a que de forma manual su instalación es más compleja y consta de muchos pasos.

En esta investigación, Snort registra la información de las alertas en una base de datos mysql, denominada Snort. La elección de Mysql radica en que es el gestor de base de datos Open Source más popular, que permite dar la posibilidad de crear y configurar usuarios, asignando a cada uno de ellos permisos diferentes (Harper, 2004). Además, da la opción de exportar e importar datos fácilmente, incluso una base de datos completa.

Esta información que brinda Snort y que es almacenada en Mysql, es posible acceder a ella de forma ordenada y sencilla a través de la aplicación Web escrita en Php denominada BASE (del inglés Basic Analysis and Security Engine). BASE es el sucesor de otro sistema denominado ACID (del inglés Analysis Console for Instruction Databases), surge debido a la dificultad de analizar los cientos de alertas que se generan en redes con alto tráfico.

Entre las facilidades que ofrece BASE, y que se convirtieron en los aspectos considerados para su uso en el proyecto, se tiene la opción de hacer búsquedas de alertas específicas ya sean por IP fuente/destino, por fecha, por ataque, por protocolo, realizar informes, gráficas, y permite además observar de una forma gráfica los paquetes capturados y la generación de gráficas estadísticas.

```
Apt-get install apache2 php5
libapache2-mod-php5
Apt-get install mysql-server mysql-
client php5-mysql
Apt-get install phpmyadmin
Apt-get install Snort-mysql
```

Revista Nexos Científicos *ISSN: 2773-7489*
Julio –Diciembre 2019 pp. 20-27 *Correo: editor@istvidanueva.edu.ec*
Volumen 3, Número 2 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: septiembre 2019 *Fecha de aceptación: octubre 2019*

Configuración de mysql.

```
root@simulator-virtual-machine:~# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 59
Server version: 5.1.49-1ubuntu8.1 (Ubuntu)

Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL v2 license

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
root@simulator-virtual-machine:~# mysql -uroot -p snort
Enter password:
mysql> grant all on snort.* to snort@localhost identified by '123456';
Query OK, 0 rows affected (0.00 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)
```

Ilustración 1: Creación de un usuario para la base de datos Snort.

2.2 Configuración de Snort

Después de preparar la base de datos, se comienza a configurar el Snort. Para que Snort funcione como un IDS de redes es necesario definir y estructurar su comportamiento en su archivo de configuración, snort.conf (véase figura 2.8), el cual se encuentra ubicado por defecto en el directorio /etc/ snort. (Belmonte, 2002).

El fichero se divide en 4 partes fundamentales:

- Configuración de las variables de red para nuestro entorno.
- Configuración de los preprocesadores. Configuración de los plugins de salida.
- Personalización de las reglas.

```
  GNU nano 2.2.4            File: snort.conf

#--------------------------------------------------
#   http://www.snort.org     Snort 2.8.5.2 Ruleset
#     Contact: snort-sigs@lists.sourceforge.net
#--------------------------------------------------
# $Id$
#
##################################################
# This file contains a sample snort configuration.
# You can take the following steps to create your own custom configuration:
#
#  1) Set the variables for your network
#  2) Configure dynamic loaded libraries
#  3) Configure preprocessors
#  4) Configure output plugins
#  5) Add any runtime config directives
#  6) Customize your rule set
#
##################################################
# Step #1: Set the network variables:
                          [ Read 935 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

Ilustración 2:Archivo de configuración del Snort.

Para garantizar que el sistema monitoriza el tráfico adecuado, las variables HOME_NET y EXTERNAL_NET deben reflejar la infraestructura de la red. En una red simple, HOME_NET se define un rango de IP privado, como 192.168.0.0/24. Esto implica que todo el tráfico originado en el rango de IP 192.168.0.1- 255 es considerado tráfico interno (Belmonte, 2002). Estos detalles varían dependiendo de cada configuración. Si en nuestra red interna hay varias subredes, se puede añadir todas separándolas con comas. La entrada EXTERNAL_NET es un listado de direcciones específicas que se consideran externas. La forma más sencilla de configurarla es usando el valor !$HOME_NET, que Snort entenderá como "cualquier dirección distinta de HOME_NET".

```
# var HOME_NET [10.1.1.0/24,192.168.1.0/24]
#
# MAKE SURE YOU DON'T PLACE ANY SPACES IN YOUR LIST!
#
# or you can specify the variable to be any IP address
# like this:

var HOME_NET [10.12.20.1/50,10.12.22.1/40,10.12.23.240]
```

Ilustración 3:Configuración de la red interna en el snort.conf.

```
# List of DNS servers on your network
var DNS_SERVERS [10.12.20.1,10.12.20.2]

# List of SMTP servers on your network
var SMTP_SERVERS $HOME_NET

# List of web servers on your network
var HTTP_SERVERS 10.12.20.5

# List of sql servers on your network
var SQL_SERVERS $HOME_NET

# List of telnet servers on your network
var TELNET_SERVERS $HOME_NET
```

Ilustración 4: Configuración de los servidores en el fichero snort.conf.

Configuración de los preprocesadores

A partir de la versión 1.5 aparecieron los preprocesadores que permiten que las funcionalidades de Snort sean extendidas por los usuarios proporcionando un sistema de acceso a los paquetes antes de que sean procesados por el motor de detección de Snort y las reglas. Las configuraciones predeterminadas para estos subsistemas son muy generales, a medida que se experimente con Snort, se puede ajustar para obtener un mejor rendimiento y resultados.

Revista Nexos Científicos *ISSN: 2773-7489*
Julio –Diciembre 2019 pp. 20-27 *Correo: editor@istvidanueva.edu.ec*
Volumen 3, Número 2 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: septiembre 2019 *Fecha de aceptación: octubre 2019*

```
preprocessor sfportscan: proto  { all } \
                         memcap { 10000000 } \
                         scan_type { all } \
                         sense_level { medium } \
                         logfile { portscan.log } \
```

Ilustración 5: Prepocesador sfportscan configurado en el fichero snort.conf.

Opciones de configuración del Sfportscan:

Proto: Indica que protocolo se desea que inspeccione para detectar un scan. Se puede usar tcp, udp, ip, all.

Memcap: Máxima cantidad de memoria a usar por sfportscan expresada en bytes. A mayor cantidad, mayor capacidad de detección.

Sense_level: Ajusta el nivel de sensibilidad de la detección. Puede ser low, medium o high: Es importante este ajuste para no generar falsos positivos / negativos. Dependiendo del nivel indicado, se podrá en el preprocesador detectar un mayor número de escaneos, pero a cambio de la generación de falsas alertas.

Scan_type: Indica el tipo de escaneo a detectar. Se puede usar portsweep, decoy_portscan, distributed_portscan, o all (todos).

logfile: Nombre del fichero donde sfportscan almacenará los logs de alertas.

```
preprocessor http_inspect: global \
    iis_unicode_map unicode.map 1252

preprocessor http_inspect_server: server default \
    profile all ports { 80 8080 8180 } oversize_dir_length 500
    no_alerts
#
#  Example unique server configuration
#
preprocessor http_inspect_server: server 10.12.20.5 \
    ports { 80 3128 8080 } \
```

Ilustración 6: Prepocesador http_inspect configurado en el fichero snort.conf.

Ilustración 7:Orden de los preprocesadores en el fichero snort.conf.

Instalación y configuración de BASE

Apt-get install acidbase

Una vez concluido se ingresa por el navegador vía http://localhost/acidbase/.

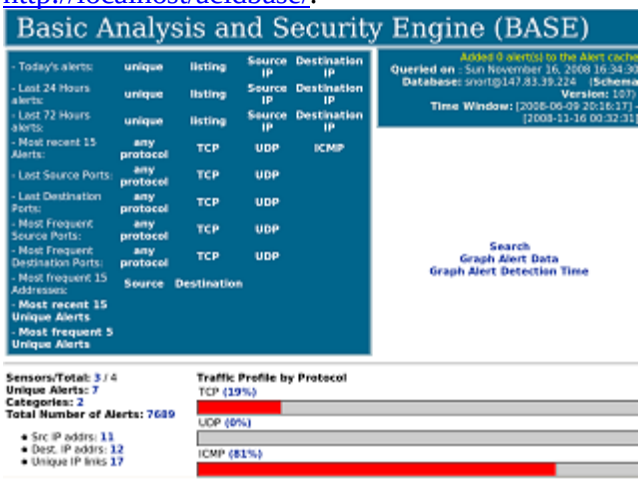

Ilustración 8: Interfaz Web del BASE.

Instalación y configuración de Pmgraph

/etc/snort/snort.conf
preprocesor perfmonitor: time 60 file /var/log/snort/snort.stats pktcnt 100

```
root@simulator-virtual-machine:~# pmgraph.pl /var/www/perfstats/ /var/log/snort/
snort.stats
Processing data from "/var/log/snort/snort.stats".
Got stats from 1 CPU
Inserting values into temporary RRD database
Generating images
Generating /var/www/perfstats//perfstats.html.
root@simulator-virtual-machine:~#
```

Ilustración 9:Resultado de la ejecución de pmgraph.pl.

Para concluir, se visita la página Web http://localhost/perfstats/perfstats.tml, donde se observa el funcionamiento de Pmgraph

Ilustración 10: Funcionamiento de Pmgraph.

2.3 Herramientas de propósitos generales

Con el objetivo de evaluar el desempeño del IDS implementado con el Snort se utilizan una serie de herramientas para realizar las pruebas de seguridad,

estas consisten en la realización de ataques (principalmente escaneos de puertos) desde diferentes localizaciones. Las características de cada una de dichas herramientas se muestran a continuación.

2.3.1 Network mapper o Nmap

Nmap es una de las utilidades de código libre más integras para el escaneo de redes y su uso es el más extendido. Está diseñado para permitir a los administradores de sistemas y en general, a quien lo desee, escanear redes a gran escala para determinar que dispositivos están activos y/o disponibles y qué tipo de servicio (nombre, versión, etc.) están ofreciendo en ese momento. De esta forma es posible explorar las redes y auditar su seguridad. (Lyon 2009).
Características:

- Disponible para Unix y Windows.
- Soporta una amplia variedad de técnicas de escaneo (aproximadamente quince), además de unas veinte configuraciones para cada una de ellas.
- Utiliza huellas TCP para la identificación del sistema operativo del equipo escaneado.

En la tabla I se pueden observar algunas de técnicas de escaneos de Nmap. (Ney 2006.).

Técnicas de escaneo	Sintáxis	Uso
TCP SYN	-sS	Escáner Sigiloso
TCP Connect ()	-sT	Escaneo sin privilegios de root
FIN	-sF	Escáner Sigiloso
Xmas	-sX	Escáner Sigiloso
Null	-sN	Escáner Sigiloso
Ping	-sP	Identificación de equipos en funcionamiento
Version Detection	-sV	Identificación de servicios
UDP	-sU	Encuentra los servicios UDP
IP Protocol	-sO	Descubre los protocolos soportados
ACK	-sA	Identifica cortafuegos
Windows	-sW	Escáner ACK avanzado
RPC	-sR	Información de los servicios RPC
List	-sL	Para realizar pruebas
Idle	-sI	Escaneando a través de terceros
FTP Bounce	-b	Histórico

Ilustración 11: Técnicas de escaneaos en Nmap.

Además ofrece otras varias prestaciones como detección de sistemas operativos (y sus versiones) vía TCP/IP fingerprinting, escaneo paralelo, detección de dispositivos no activos vía pings paralelos, deco y scanning, port filtering detection, direct (non-portmapper) RPC scanning, fragmentation Scanning y flexible target y port specification. (Orebaugh and Pinkard, 2008).
Hace uso de paquetes IP para determinar los tipos de firewalls o filtradores de paquetes en empleo.
El resultado del escaneo es usualmente una lista de puertos de interés en las máquinas escaneadas, mostrando el número, estado, protocolo y el más probable nombre del servicio. Los estados son abiertos, filtrado, sin filtrar y cerrado.

Abierto: La máquina objetivo aceptara conexiones en ese puerto sin restricciones
Filtrado: Posiblemente un firewall, filtro u otro obstáculo está bloqueando el puerto.
Sin filtrar: Puertos sin filtrar detectados por escáneres ACK o de ventanas.
Cerrado: El puerto está correctamente bloqueado o sin servicio a la escucha.
La sintaxis básica de nmap es:

Nmap [tipo de scan] [opciones] [especificación de objetivos]

2.4 GFI LANguard

GFI LANguard Network Security Scanner (GFI LANguard N.S.S.) es una herramienta de auditoría de seguridad, la cual proactivamente informa, y soporta la reparación de las vulnerabilidades de red puntualmente.

Es una solución empresarial esencial y rentable para salvaguardar sus sistemas y redes de ataques hacker y brechas de seguridad. El producto analiza toda la red, realiza más de 15.000 evaluaciones de vulnerabilidad e identifica todas las posibles amenazas de seguridad. Cuando se finaliza el análisis, GFI LANguard proporciona a los administradores las líneas maestras sobre cómo pueden ser dirigidas y proporciona toda la funcionalidad necesaria para instalar y administrar eficazmente parches en los 38 idiomas soportados por los productos Microsoft.

Permite realizar auditorías de seguridad en ordenadores basados tanto en Windows como en Linux. Durante una auditoría, el motor de escaneo recopila varias informaciones hardware y software de los equipos escaneados. Esto incluye el nivel de service pack de cada equipo objetivo, dispositivos

Revista Nexos Científicos *ISSN: 2773-7489*
Julio –Diciembre 2019 pp. 20-27 *Correo: editor@istvidanueva.edu.ec*
Volumen 3, Número 2 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: septiembre 2019 *Fecha de aceptación: octubre 2019*

potencialmente vulnerables tales como puntos de acceso inalámbricos y dispositivos USB, aplicaciones instaladas, así como recursos compartidos abiertos y puertos abiertos. El escáner también enumera ajustes de configuración específicos del SO tales como los ajustes del registro y los detalles de configuración de la política de contraseñas que ayudan en la identificación de los problemas de seguridad comunes relacionados con un sistema operativo configurado inadecuadamente (tal como un SO funcionando con los ajustes por defecto).

GFI LANguard N.S.S. también está equipado con algoritmos que comprueban la presencia de software de seguridad particular (es decir, aplicaciones antivirus y antispyware).

3. RESULTADOS Y DISCUSIÓN

3.1. Realización de Pruebas de seguridad

Prueba 1

En esta prueba se realizó un ataque mediante el Nmap usando la técnica de escaneo de escaneo Idle en donde se escanea usando el IP del sistema zombie. En este caso se escogió la dirección IP 10.12.24.6 (véase figura 3.1) El escaneo fue realizado desde la dirección IP 10.12.24.180.

```
Nmap done: 3 IP addresses (2 hosts up) scanned in 16.432 seconds
SPARTAKUS:~# nmap -P0 -sI 10.12.24.6:3389 10.12.20.18

Starting Nmap 4.62 ( http://nmap.org ) at 2002-03-06 21:45 CET
Idle scan using zombie 10.12.24.6 (10.12.24.6:3389); Class: Incremental
Interesting ports on andromeda.fce.uclv.edu.cu (10.12.20.18):
Not shown: 1710 closed|filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
912/tcp  open  unknown
3389/tcp open  ms-term-serv
```

Ilustración 12: Escaneo con el Nmap.

[snort] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy 2011-06-08 07:29:30 10.12.24.6:3389 10.12.20.18:923 TCP

Ilustración 13: Resultados del IDS.

Prueba 2

En esta prueba se utilizó el decoys –D para tratar de engañar al host, haciéndole creer que el escaneo se está generando desde otros hosts.

```
root@simulator-virtual-machine:~# nmap -sS 10.12.20.18 -D 10.12.20.6,10.12.20.50
,10.12.20.5

Starting Nmap 5.21 ( http://nmap.org ) at 2011-06-08 11:05 CDT
Nmap scan report for andromeda.fce.uclv.edu.cu (10.12.20.18)
Host is up (0.00014s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
912/tcp  open  unknown
1688/tcp open  unknown
3389/tcp open  ms-term-serv
6129/tcp open  unknown
MAC Address: 00:15:17:44:6B:82 (Intel Corporate)
```

Ilustración 14: Escaneo con el Nmap.

[snort] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy 2011-06-08 11:03:20 10.12.20.6:55405 10.12.20.18:1088 TCP
[snort] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy 2011-06-08 11:03:20 10.12.20.50:55405 10.12.20.18:7921 TCP
[snort] COMMUNITY SIP TCP/IP message flooding directed to SIP proxy 2011-06-08 11:03:20 10.12.20.5:55405 10.12.20.18:32785 TCP

Prueba 3

En esta prueba se utilizó la opción del nmap de fragmentar los paquetes.

```
root@ASGARD:~# nmap -f 10.12.20.18

Starting Nmap 5.21 ( http://nmap.org ) at 2011-06-08 13:18 CDT
Nmap scan report for andromeda.fce.uclv.edu.cu (10.12.20.18)
Host is up (0.0019s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
912/tcp  open  unknown
1688/tcp open  unknown
3389/tcp open  ms-term-serv
6129/tcp open  unknown
```

Ilustración 15: Escaneo con el Nmap.

3.2 Análisis de los resultados de las pruebas realizadas

Luego de realizadas las distintas pruebas se pudo observar que la mayoría de los diferentes escaneos fueron detectados por el IDS, destacando las pruebas 1, 2 y 3 las cuales se utilizan para evasión de cortafuegos/IDS y falsificación.

En la prueba 3 se dividió la cabecera del paquete TCP para hacer más difícil su detección. En la figura 15 se puede observar que la trama que se obtuvo tiene un tamaño de 8 byte que es la división por defecto que realiza el Nmap, no obstante, el IDS fue capaz de detectarlo.

En las pruebas 1 y 2 se utilizaron IP señuelos para poder realizar el escáner, a lo que el IDS es incapaz de detectar la verdadera dirección de origen.

Revista Nexos Científicos
Julio –Diciembre 2019 pp. 20-27
Volumen 3, Número 2
Fecha de recepción: septiembre 2019
ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: octubre 2019

3.2.1 Algunos resultados obtenidos por el IDS

A continuación, se presentan algunos datos que brinda el IDS implementado con el Snort. Tipos de alertas detectadas.

< Firma >	< Clasificación >	< Total # >	Sensor #	< Dirección Origen >	< Dirección Dest >	< First >	< Ultimo >
[snort] COMMUNITY SIP TCP/IP essage flooding directed to SIP proxy	attempted-dos	1438(80%)	2	22	26	2011-06-07 12:57:03	2011-06-08 13:19:47
[snort] (portscan) Open Port	desclasificado	225(13%)	2	18	19	2011-06-07 12:43:32	2011-06-08 11:10:00
[snort] (portscan) TCP Portscan	desclasificado	113(6%)	2	59	18	2011-06-07 12:43:32	2011-06-08 13:17:32
[snort] (portscan) TCP Portsweep	desclasificado	8(0%)	1	1	4	2011-06-08 06:46:18	2011-06-08 10:17:32
[snort] (portscan) ICMP Sweep	desclasificado	4(0%)	1	1	2	2011-06-08 06:45:39	2011-06-08 11:19:26

Ilustración 16: Alertas más comunes.

Direcciones IP desde donde se reportaron las alertas.

10.12.25.170	1	65	3	1
10.12.34.43	1	38	1	1
10.12.26.180	1	37	4	1
10.12.26.181	1	37	3	1
10.12.18.5	1	37	3	1
10.12.23.233	1	34	3	4

Ilustración 17: Direcciones IP de origen que más veces se ha detectado.

3.2. Resultados obtenidos por el Pmgraph

A continuación, se muestran algunas de las gráficas que genera el Pmgraph

Ilustración 18: Alertas por segundo.

4. CONCLUSIONES

– Snort presenta una instalación cómoda y un funcionamiento adecuado para los propósitos de detección de actividad maliciosa como IDS, así como una interfaz amigable.

– Permite integrase con otras herramientas, como por ejemplo Pmgraph, para mejorar su rendimiento, y BASE, para facilitar el análisis de los resultados.

– A través de las pruebas realizadas se pudo ver la capacidad de detección del sistema, mediante el análisis de las alertas producidas y las direcciones de los equipos que intervinieron en dichas alertas. Además, se pudo evaluar el rendimiento del sistema durante un período de tiempo.

– Es posible ocultar ataques al IDS enviando el tráfico de forma especial. Este problema no aparece solo en Snort, sino que está presente en muchos de los IDS comerciales y es tema de investigación en la actualidad.

REFERENCIAS

Y.C. (s.f.). CIE Professional Development Series Network Security Technologies and Solutions. Cisco Press. Carter, G. (March 20, 2003). LDAP System Administration.

Anonymous (2002). Maximum Security, SAMS.

Belmonte, I. (2002.). Configuración de un sistema de detección de intrusiones. Configuración de Snort con interface ACID. Disponible en: http://www.redes-linux.com/manuales/seguridad/snort_assl.pdf. [Consultado el 16 de abril del 2011]

Castell, S. F. (2004). Métodos de seguridad en una red: cortafuegos y detección de intrusos (IDS), Valencia, España.

Center, N. C. S. (1988). A guide to understanding audit in trusted systems, Technical Report NCSC-TG-001, National Computer Security Center.

Chapman, D. B., E. D. Zwicky, et al. (1995). Building internet firewalls, O'Reilly & Associates, Inc.

Cheswick, W. R., S. M. Bellovin, et al. (2003). Firewalls and Internet security: repelling the wily hacker, Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA. [En línea]. Disponible en:

http://www.dannyreviews.com/h/Firewalls_and_Internet_Security.html. [Consultado el 15 de marzo del 2011]

Gregg, M. (2006). Hack the stack: using snort and ethereal to master the 8 layers of an insecure network, Syngress. [En línea]. Disponible en: http://www.ebookee.org/Hack-the-Stack-Using-Snort-and-Ethereal-to-Master-the-8-Layers-of-an-Insecure-N_873.html.[Consultado el 18 de mayo del 2011]