

Introducción:

En esta práctica se instalará el software necesario para instalar Snort y conocer su implementación y poder resolver el reto #9 del SANS Holiday Hack Challenge 2018.

Los sistemas IDS es un programa que permite detectar accesos no autorizados a un equipo informático a una red.

Permiten la detección de ataques de:

- Versión de software
- Sistemas operativos
- Hosts activos
- Escáner de vulnerabilidades
- Acceso a sistemas
- Ataques de denegación de servicio.

En función de la forma como obtiene sus datos se pueden clasificar en dos tipos los IDS:

- **Sistemas de detección de intrusos basados en equipo (HIDS):** Utilizan programas instalados en los equipos para intentar detectar modificaciones en equipos afectados por un ataque, y hace un reporte de sus conclusiones
- **Sistemas de detección de intrusos basados en red (NIDS):** Detecta accesos no deseados a la red, este tipo de IDS suele incorporar un analizador de paquetes de red (sniffer) con los que el núcleo del NIDS puede obtener información sobre el tráfico que circula por la red.

Herramientas necesarias:

- VirtualBox 6.0.4.

<https://www.virtualbox.org/wiki/Downloads>

- Ubuntu 18.10

<https://www.ubuntu.com/download/server>

A. Instalación de Snort.

1. Se crea una nueva máquina virtual.

Nombre y sistema operativo

Seleccione un nombre descriptivo y una carpeta destino para la nueva máquina virtual y seleccione el tipo de sistema operativo que tiene intención de instalar en ella. El nombre que seleccione será usado por VirtualBox para identificar esta máquina.

Nombre:

Carpeta de máquina:

Tipo:

Versión:

2. Con las especificaciones mínimas si no se cuenta con muchos recursos en como memoria RAM y disco duro. Además de agregar al controlador IDE de disco la imagen de Ubuntu y adaptador en modo “Red NAT” y la red con el nombre de “Platzi”.

← Crear máquina virtual

Disco duro

Si desea puede agregar un disco duro virtual a la nueva máquina. Puede crear un nuevo archivo de disco duro o seleccionar uno de la lista o de otra ubicación usando el icono de la carpeta.

. Si necesita una configuración de almacenamiento más com Snort - Configuración

El tamaño recomendado del disco duro es **10.00 GB**.

☐ No agregar un disco duro virtual

☒ Crear un disco duro virtual ahora

☐ Usar un archivo de disco duro virtual existente

General

Sistema

Pantalla

Almacenamiento

Audio

Red

Puertos serie

Almacenamiento

Dispositivos de almacenamiento

- Controlador: IDE
- VBoxGuestAdditions.iso
- Controlador: SATA
- Snort.vdi

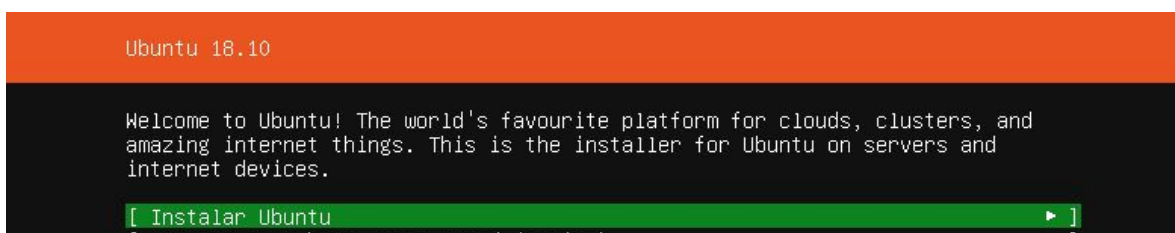
Atributos

Nombre:

Tipo:

☒ Usar cache de I/O anfitrión

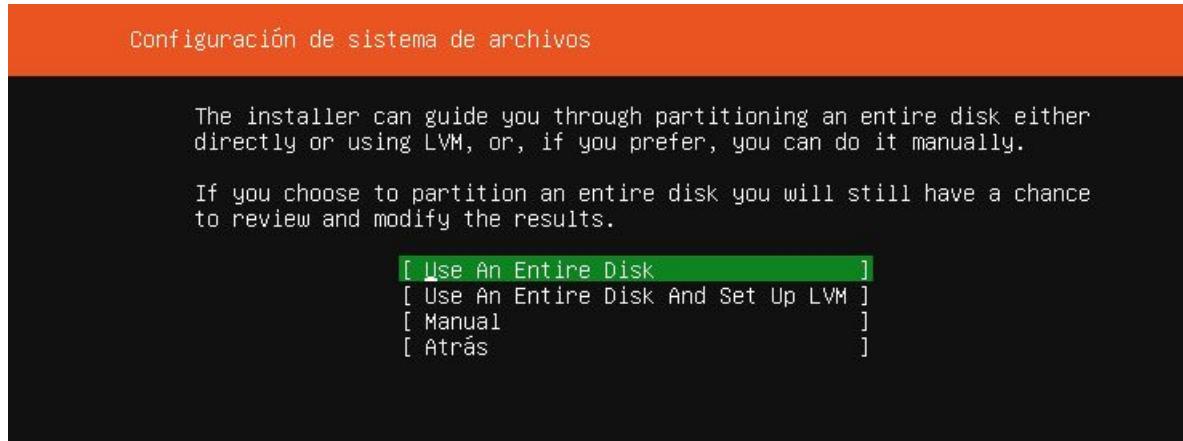
3. Se procede a la instalación usando una configuración similar a la de Mutillidae.



- La interfaz de red para la instalación y puesta en marcha se configurará como “Red NAT”.



- Sin proxy y el espejo quedara el default, además de la utilización del disco completo.



- Lo siguiente es configurar el nombre, usuario y la contraseña del equipo. Sin ninguna aplicación adicional.



7. Una vez instalado correctamente, reiniciar la máquina en la opción que se muestra y al momento de iniciar ejecutar:

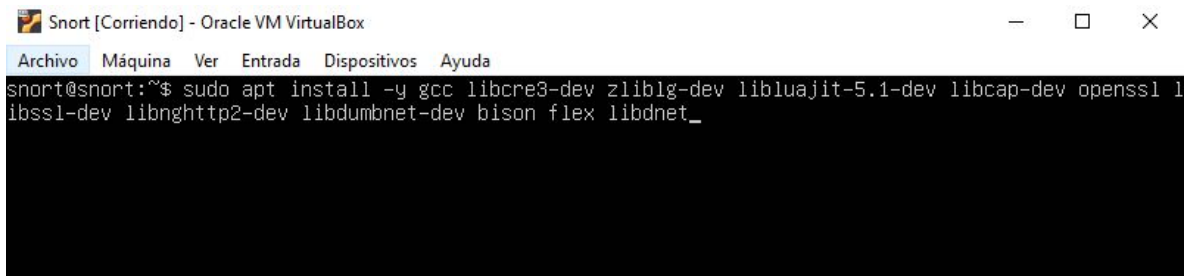
```
sudo apt-get update
```

```
[ 25.038586] cloud-init[1895]: Cloud-init v. 18.4-7-g4652b196-0ubuntu1
9 22:02:11 +0000. Datasource DataSourceNoCloud [seed=/var/lib/cloud/seed/
Up 25.02 seconds
[ OK ] Started Execute cloud user/final scripts.
[ OK ] Reached target Cloud-init target.

Ubuntu 18.10
```

8. Es necesario instalar las librerías requeridas por Snort con el comando.

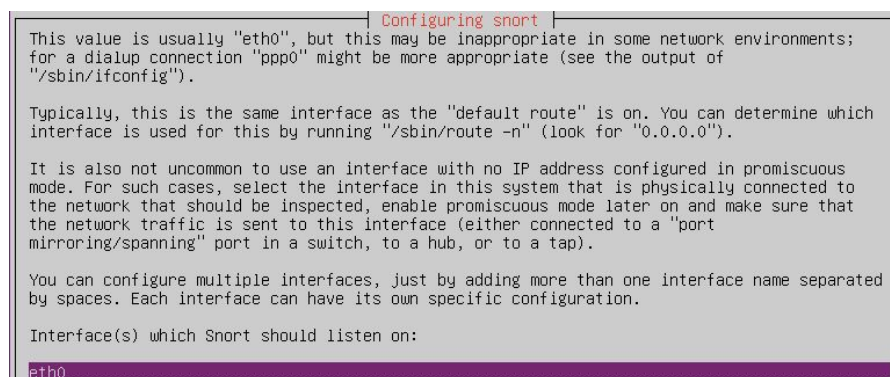
```
sudo apt install -y gcc libpcap-dev zlib1g-dev liblua5.1-dev libpcap-dev openssl
libssl-dev libnghttp2-dev libdumbnet-dev bison flex libdnet
```



9. Teniendo Ubuntu listo, para instalar Snort se ejecuta el comando.

```
Sudo apt-get install snort
```

10. Preguntar la interfaz que utilizará la herramienta, en este caso `enp0s3`.



11. El intervalo de direcciones para la red local es 192.168.2.0/24.

Configuración de snort

Tiene que utilizar el formato CIDR, esto es, 192.168.1.0/24 para un bloque de 256 IPs o 192.168.1.42/32 para sólo una dirección. Debe separar múltiples direcciones por «,» (comas) y sin espacios.

Tenga en cuenta que si Snort está configurado para utilizar múltiples interfaces se utilizará esta definición como valor de «HOME_NET» para todos ellos.

Intervalo de direcciones para la red local:

192.168.2.0/24

<Ok>

12. Vuelve a preguntar la interfaz donde escuchara Snort.

Configuración de snort

Este valor suele ser «eth0», pero puede no ser correcto para algunos entornos de red. Si está utilizando una conexión de marcación telefónica mediante PPP a Internet puede ser más apropiado utilizar «ppp0» (consulte la salida de «/sbin/ifconfig»).

Generalmente la interfaz que se añade aquí es generalmente la misma que tiene definida la ruta por omisión. Para determinar qué interfaz se está utilizando para esto, ejecute «/sbin/route -n» (busque aquellos valores asociados a «0.0.0.0»).

Tampoco es infrecuente ejecutar Snort en una interfaz sin dirección IP que esté configurada en modo promiscuo. Para estos casos, seleccione la interfaz en el sistema que está físicamente conectada a la red debería inspeccionarse, active el modo promiscuo más adelante y asegúrese que el tráfico de dicha red se está enviado a esa interfaz (bien conectándola a un puerto de un conmutador en modo «port mirroring/spanning», bien conectado a un concentrador o a un tap)

Puede configurar múltiples interfaces simplemente añadiendo más de un nombre de interfaz y separándolos por espacios. Cada interfaz puede tener su propia configuración.

Interfaz/ces donde debería escuchar Snort:

enp0s3

<Ok>

13. Para comprobar que se instaló correctamente.

Snort -V

```
snort@snort:~$ snort -V
o''~
  ''~
  ''~
  ''~

-*> Snort! <*-
Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
```

14. Ingresar a la carpeta /etc/snort y editar el archivo snort.conf.

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
snort@snort:/etc/snort/rules$ nano /etc/snort/snort.conf
```

15. Es importante dejar las opciones HOME_NET y EXTERNAL_NET de la siguiente forma.

```
GNU nano 2.9.8 /etc/snort/snort.conf
# Note to Debian users: this value is overridden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.2.0/24_
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
```

16. Se valida la configuración con el comando.

```
Snort -T -i enp0s3 -c /etc/snort/snort.conf
```

```
Snort successfully validated the configuration!
Snort exiting
snort@snort:/etc/snort/rules$ snort -T -i enp0s3 -c /etc/snort/snort.conf
```

17. Para ingresar una regla personalizada editar el archivo local.rules en la carpeta /etc/snort/rules.

```
snort@snort:/etc/snort/rules$ nano /etc/snort/rules/local.rules _
```

18. Se agrega una regla que detecte el protocolo ICMP.

```
GNU nano 2.9.8 /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.

alert icmp any any -> $HOME_NET any (msg: "ICMP detectado"; sid:1000001; rev:1;)
```

19. Para iniciar Snort, se debe escribir lo siguiente.

Sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3

```
snort@snort:/etc/snort/rules$ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
```

Las opciones con las que se cuenta al iniciar son las siguientes:

- A console: imprime alertas de modo rápido a la salida estándar.
- q: modo silencioso. No mostrar banner ni informe de estado.
- c: la ruta a nuestro archivo snort.conf.
- i: La interfaz para escucha.

20. Se manda un ping de la máquina donde se encuentra instalado Kali hacia la ip 192.168.2.8.


```
root@kali:~# ping 192.168.2.8
PING 192.168.2.8 (192.168.2.8) 56(84) bytes of data.
64 bytes from 192.168.2.8: icmp_seq=1 ttl=64 time=0.423 ms
64 bytes from 192.168.2.8: icmp_seq=2 ttl=64 time=0.228 ms
```

21. Automáticamente Snort muestra la alerta establecida.

```
ICMP} 192.168.2.5 -> 192.168.2.8
04/08-04:46:40.855024  [**] [1:1000001:1] ICMP detectado [**] [Priority: 0] {ICMP} 192.168.2.8 -> 192.168.2.5
04/08-04:46:40.855024  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.2.8 -> 192.168.2.5
04/08-04:46:41.879840  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.2.5 -> 192.168.2.8
04/08-04:46:41.879840  [**] [1:1000001:1] ICMP detectado [**] [Priority: 0] {ICMP} 192.168.2.5 -> 192.168.2.8
```