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.

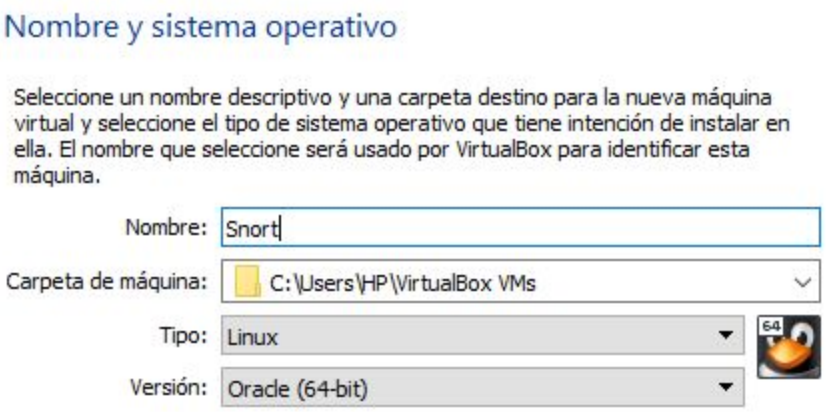
https://www.virtualbox.org/wiki/Downloads

- Ubuntu 18.10

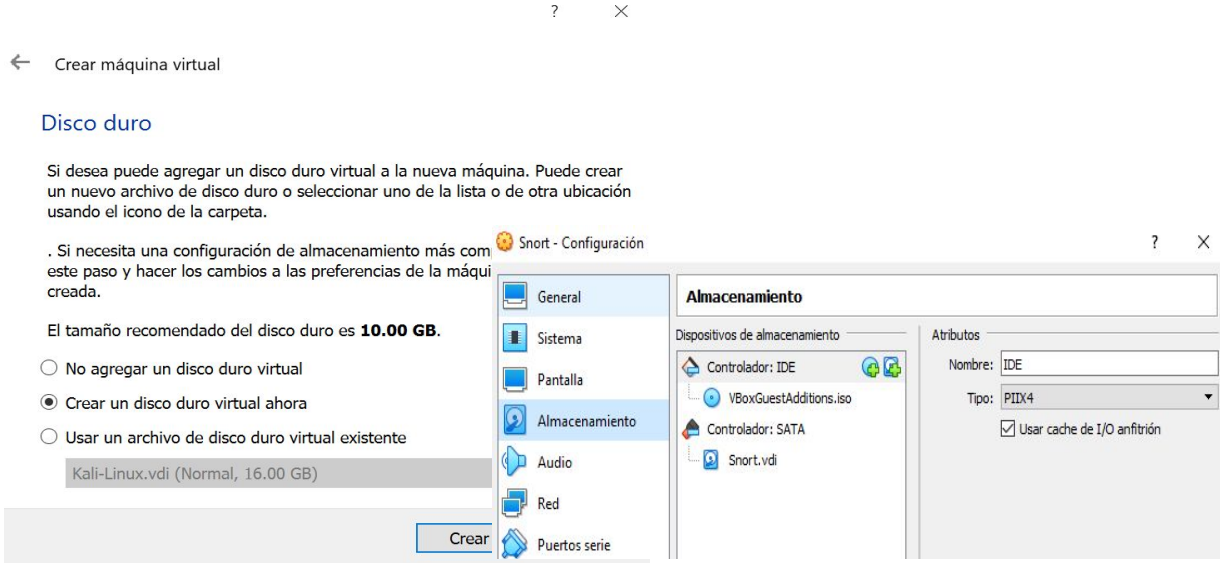
https://www.ubuntu.com/download/server

A. Instalación de Snort.

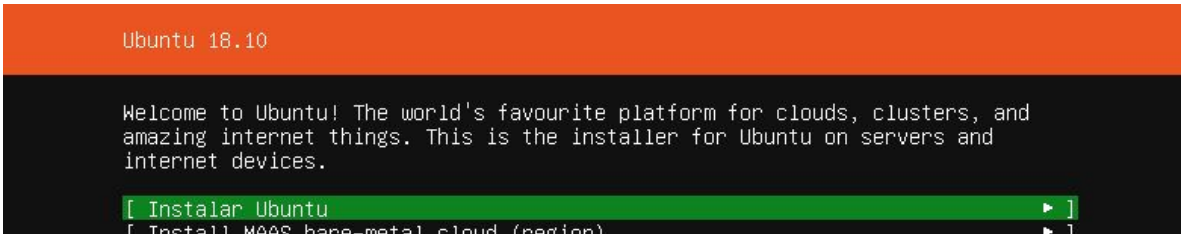
1. Se crea una nueva máquina virtual.



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”.

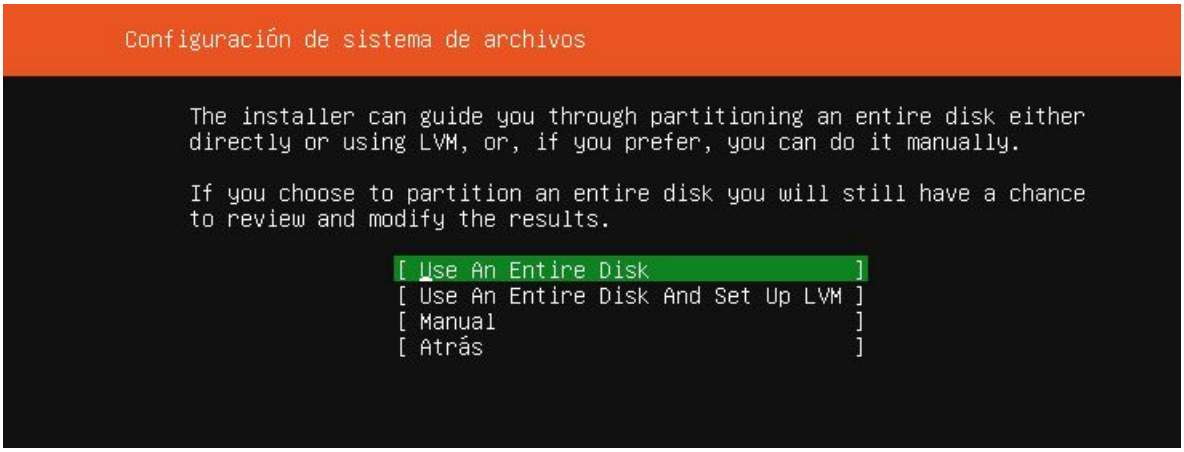


3. Se procede a la instalación usando una configuración similar a la de Mutillidae.



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

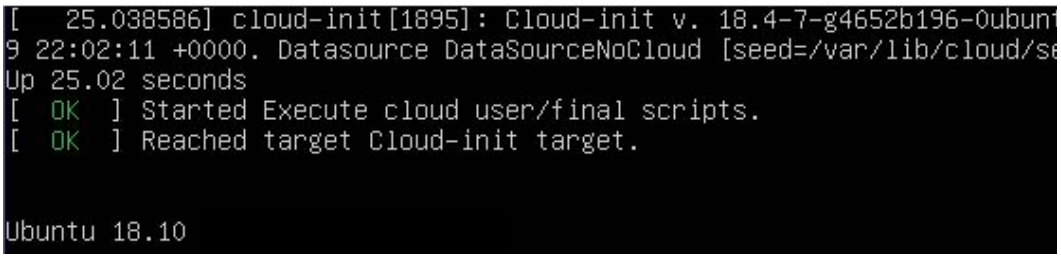
5. Sin proxy y el espejo quedara el default, además de la utilización del disco completo.



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

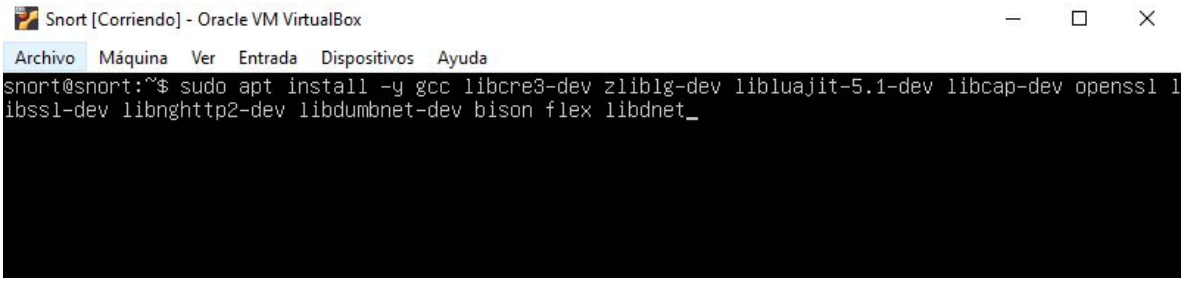
7. Una vez instalado correctamente, reiniciar la máquina en la opción que se muestra y al momento de iniciar ejecutar:

sudo apt-get update



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

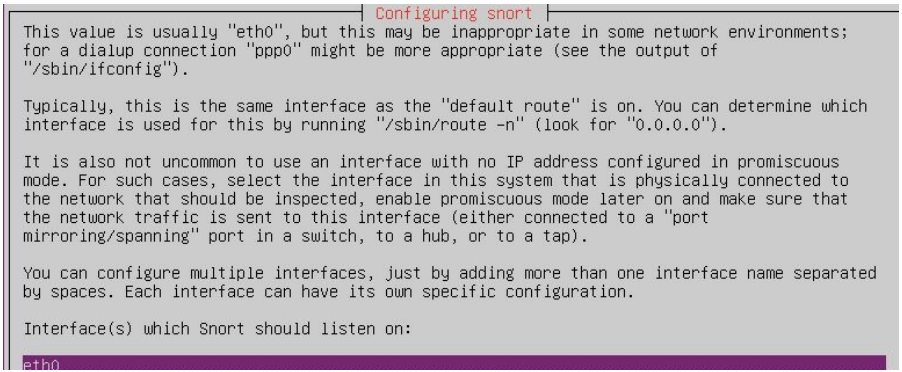
sudo apt install -y gcc libpcre3-dev zlib1g-dev libluajit-5.1-dev libpcap-dev openssl libssl-dev libnghttp2-dev libdumbnet-dev bison flex libdnet



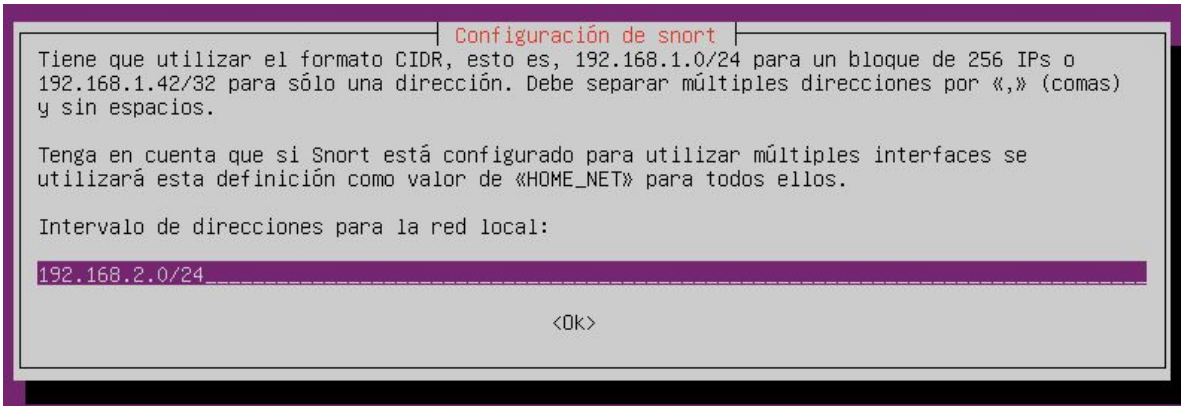
9. Teniendo Ubuntu listo, para instalar Snort se ejecuta el comando.

Sudo apt-get install snort

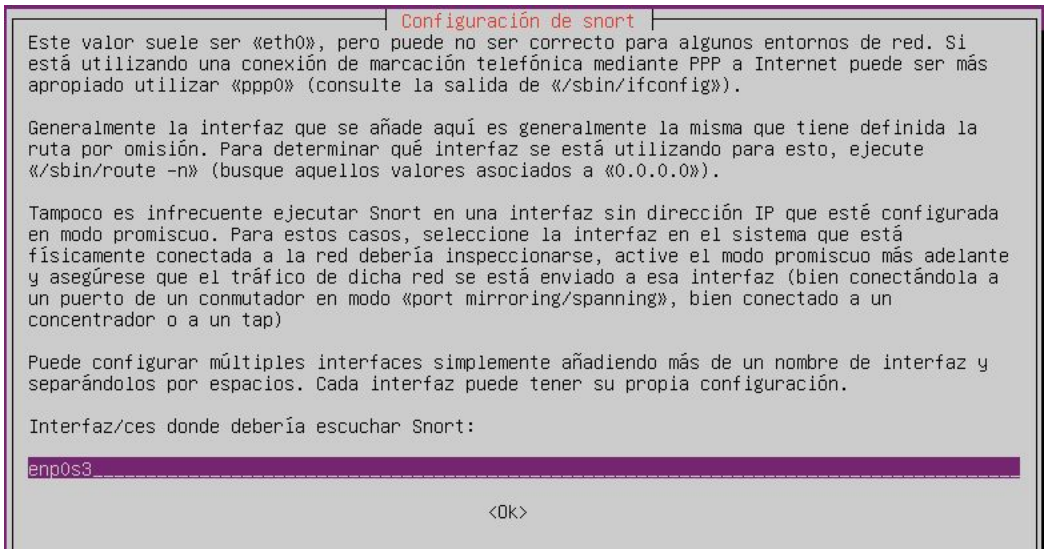
10. Pregunta la interfaz que utilizara la herramienta, en este caso enp0s3.



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

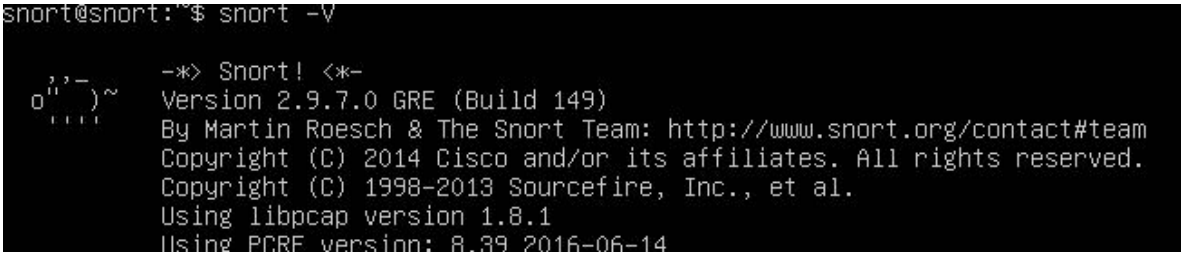


12. Vuelve a preguntar la interfaz donde escuchara Snort.

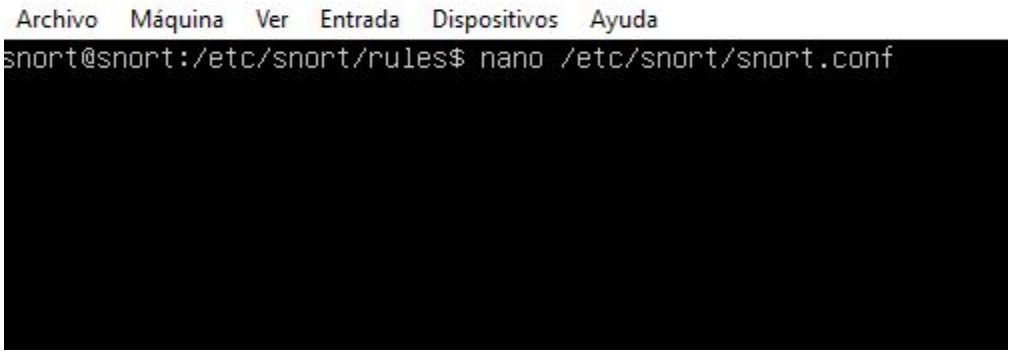


13. Para comprobar que se instaló correctamente.

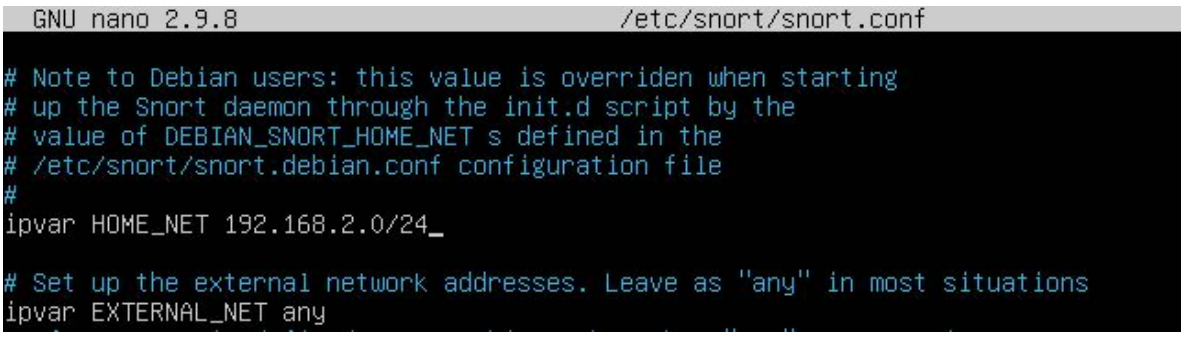
Snort -V



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

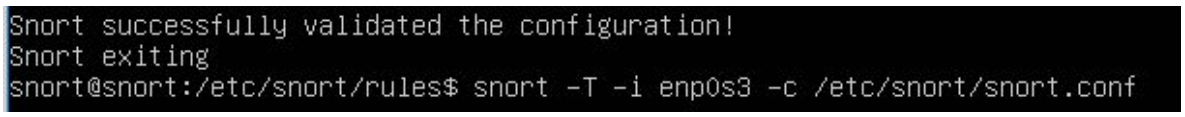


15. Es importante dejar las opciones HOME_NET y EXTERNAL_NET de la siguiente forma.

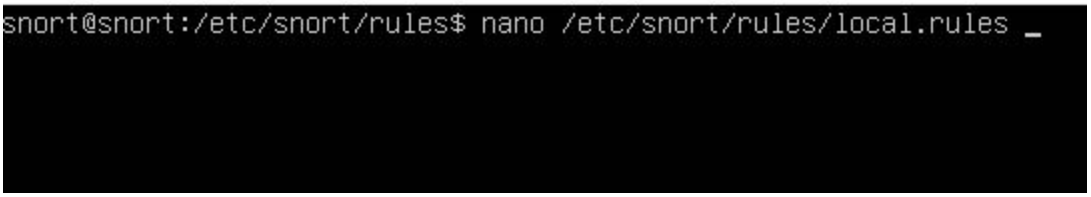


16. Se valida la configuración con el comando.

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.



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

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

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 -> 19
2.168.2.5
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 -> 19
2.168.2.8
```