Instituto Politécnico Nacional

Unidad Profesional Interdisciplinaria en Ingeniería y Tecnologías Avanzadas

Seguridad de Redes

Profesor. Polanco Montelongo Francisco Antonio

Alumno: Hernández Guzmán Bryan Alexis

Grupo: 3TV4

Práctica: SNORT

INTRODUCCION

¿Qué es SNORT?

Snort es un sistema de detección de intrusos en red, libre y gratuito. Ofrece la capacidad de almacenamiento

de bitácoras en archivos de texto y en bases de datos abiertas, como MySQL. Implementa un motor de detección

de ataques y escaneo de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente

definida.

Este IDS implementa un lenguaje de creación de reglas flexible, potente y sencillo. Durante su instalación,

provee de cientos de filtros o reglas para backdoor, DDoS, finger, FTP, ataques web, CGI, Nmap, entre otros.1

Puede funcionar como sniffer y registro de paquetes. Cuando un paquete coincide con algún patrón establecido

en las reglas de configuración, se logea. Así se sabe cuándo, de dónde y cómo se produjo el ataque.

Snort tiene una base de datos de ataques que se actualiza constantemente a través de internet. Los usuarios

pueden crear firmas basadas en las características de los nuevos ataques de red y enviarlas a la lista de correo

de firmas de Snort, esta ética de comunidad y compartir ha convertido a Snort en uno de los IDS basados en

red más populares, actualizados y robustos.

Características principales

Estas son las principales características de Snort:

- Monitor de tráfico en tiempo real
- Registro de paquetes
- Análisis de protocolo
- Coincidencia de contenido
- Huellas digitales del SO
- Puede instalarse en cualquier entorno de red.

• Crea registros

• Fuente abierta

• Las reglas son fáciles de implementar

Snort funciona en Windows y en Linux.

Desarrollo:

Primeramente instalamos Snort con sudo apt-get install snort y creamos dentro de la carpte /etc/snort/rules el archivo custom.rules que nos resvira para agregar reglas si se requiere, o en todo caso se puede usar las reglas por defecto que son las local rules, haremos ambos procedimientos:

```
bryan@bryan-VirtualBox:~$ sudo touch /etc/snort/rules/custom.rules
[sudo] contraseña para bryan:
Lo siento, pruebe otra vez.
[sudo] contraseña para bryan:
bryan@bryan-VirtualBox:~$ ls /etc/snort/rules/
attack-responses.rules          community-web-dos.rules   p2p.rules
backdoor.rules                  community-web-iis.rules   policy.rules
bad-traffic.rules               community-web-misc.rules  pop2.rules
chat.rules                      community-web-php.rules   pop3.rules
community-bot.rules             custom.rules              porn.rules
community-deleted.rules         ddos.rules                rpc.rules
community-dos.rules             deleted.rules             rservices.rules
```

Se usara un editor de texto para entrar al archivo de texto /etc/snort/snort.conf

Para configurar la red local y la externa antes ejecutando el comanod ifconfig para conocer nuestra red local:

```
  GNU nano 6.2                    /etc/snort/snort.conf
# 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 10.0.2.15

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
```

Dentro del archivo local rules se agregaran las siguientes reglas icmp ping si hay un ping de la maquina virtual a la maquina física:

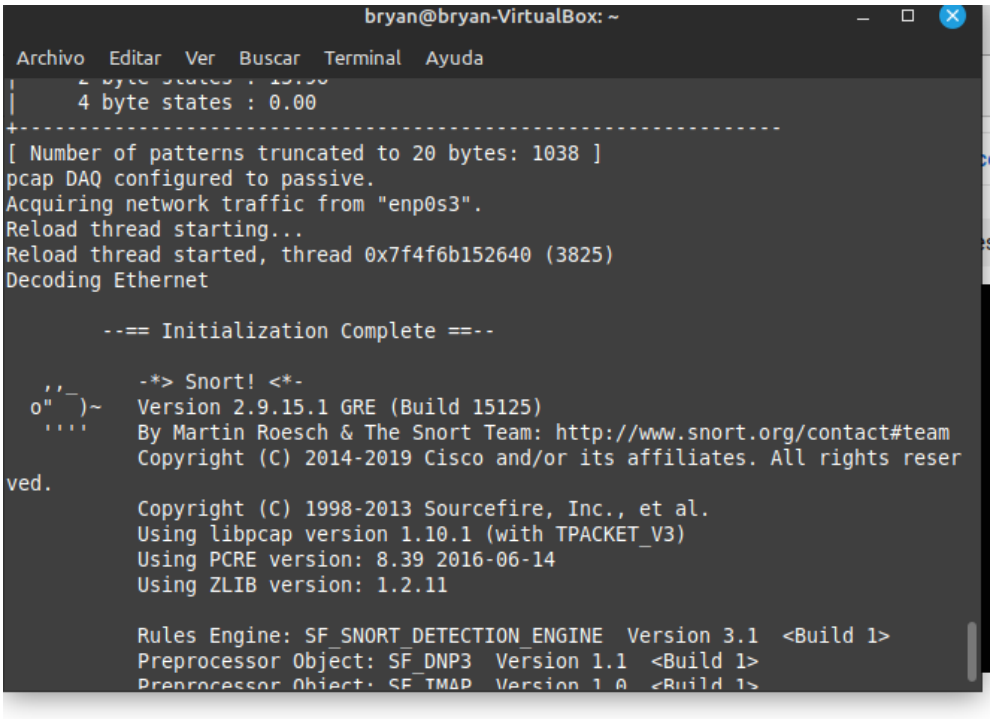
```
/etc/snort/rules
1 # $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
2 # ----------------
3 # LOCAL RULES
4 # ----------------
5 # This file intentionally does not come with signatures.  Put your local
6 # additions here.
7
8 alert icmp  10.0.2.15/24 any -> any any (msg:"Alguien esta haciendo ping"; sid: 19910316; rev:
  1;)
```

Después de guardar la configuración se irá al archivo /etc/snort/snort.conf para comprobar que las reglas estén habilitadas:

```
bryan@bryan-VirtualBox: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
 GNU nano 6.2                  /etc/snort/snort.conf *
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/community-sql-injection.rules
include $RULE_PATH/community-web-client.rules
include $RULE_PATH/community-web-dos.rules
include $RULE_PATH/community-web-iis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/custom.rules

##################################################
# Step #8: Customize your preprocessor and decoder alerts
# For more information, see README.decoder_preproc_rules
##################################################

# decoder and preprocessor event rules
# include $PREPROC_RULE_PATH/preprocessor.rules
# include $PREPROC_RULE_PATH/decoder.rules
# include $PREPROC_RULE_PATH/sensitive-data.rules

##################################################
```

Por ultimo se ejecutara el comando snort -A console -c snort.conf -i enp0s3

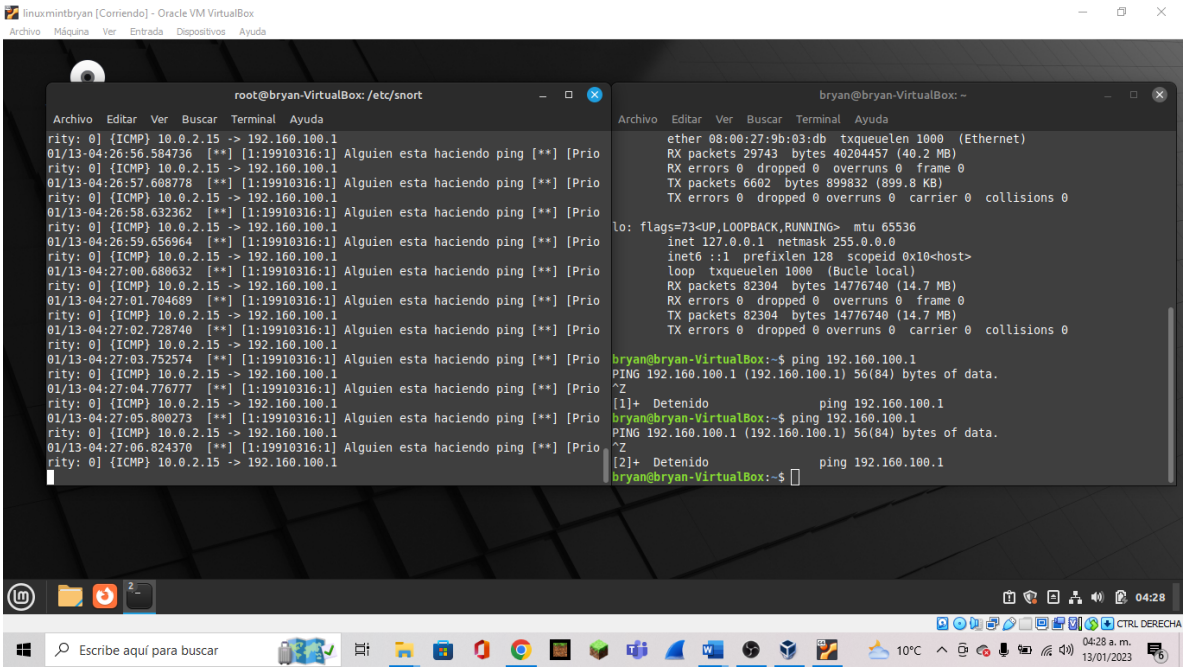
Para empezar a visualizar los contenidos



De nuestra maquina física tomaremos en cuenta nuestra puerta de enlace predeterminada:

```
Adaptador de Ethernet Ethernet 2:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::8988:9663:34e3:fb53%5
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.56.1
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :

Adaptador de LAN inalámbrica Conexión de área local* 1:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Dirección IPv6 . . . . . . . . . . . . . . : 2806:2f0:90c1:dc13:3a56:1bb8:c4f0:3030
   Dirección IPv6 temporal. . . . . . . . . . : 2806:2f0:90c1:dc13:69c9:fe0d:93a7:afc3
   Vínculo: dirección IPv6 local. . . : fe80::8837:39d:36f0:982%17
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.100.244
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::1%17
                                       192.168.100.1
```

Se puede observar que cuando se envía un ping a la maquina física, saltan las alertas:



Conclusiones:

Dentro de esta practica pudimos observar el uso de snort y la importancia de este, el crear las reglas, meterse en el tema es formar un sistema libre de intrusos, actualmente hay una versión de paga que es muy recomendable tener debido a su alta eficiencia, ya que al tener un código abierto las personas puede seguir agregando y actualizando las reglas en caso de ser necesario, como practica de seguridad me parece muy importante conocer que incluso para evitar palabras o paginas aunque no sean maliciosas, el tener un control de todo esto es muy beneficioso a la hora en el que tienes un trabajo como administrador de algún lugar.