

Universidad Paraguay Aleman



UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN



Seguridad TICs

Prof.: Chrystian Ruiz Diaz

Contenido

Nota de Uso Académico.....	3
Guía para Instalar Snort IDS en Kali Linux.....	4
Consideraciones	4
Preparación: Eliminar Instalaciones Previas de Snort	4
Paso 1: Actualizar el Sistema.....	4
Paso 2: Instalar Dependencias.....	4
Paso 3: Crear Enlaces Simbólicos para Bibliotecas RPC	5
Paso 4: Configurar Variables de Entorno para la Compilación	5
Paso 5: Instalar DAQ	5
Paso 6: Descargar y Compilar Snort	5
Paso 7: Crear Directorios Necesarios.....	6
Paso 8: Descargar el Archivo <code>unicode.map</code>	6
Paso 9: Configurar Snort.....	6
Paso 10: Crear Reglas Básicas	7
Regla para detectar ICMP (ping):	7
Reglas para detectar nmap:.....	7
Paso 11: Agregar la Ruta de las Bibliotecas a <code>ld.so.conf</code>	7
Paso 12: Actualizar el Caché de las Bibliotecas Dinámicas	8
Paso 13: Probar Snort.....	8
Paso 14: Generar Tráfico ICMP y Nmap	8
Paso 15: Verificar los Logs	8
Paso 16: Configuración de Snort como un Servicio (Opcional)	9

Nota de Uso Académico

Este documento ha sido preparado exclusivamente para el uso académico del docente. Este documento no puede ser distribuido a ninguna otra parte ni utilizado para ningún otro propósito, diferente al establecido como alcance en el proyecto académico de la **UNIVERSIDAD PARAGUAYO ALEMANA**. El uso indebido del material fuera del ámbito académico no representa ninguna responsabilidad del docente.

USO EXCLUSIVO EN LABORATORIO

Guía para Instalar Snort IDS en Kali Linux

Consideraciones

I. Compatibilidad de Módulos y Librerías: Este material es una guía referencial para la instalación y pruebas a realizarse. Es responsabilidad del usuario verificar e instalar las versiones de los módulos, librerías y dependencias que sean compatibles con el entorno de trabajo.

II. Manejo de Copia y Pegado de Código entre PC Física y VM: Al copiar y pegar sentencias desde la PC física a la máquina virtual (VM), es común que se copien caracteres no visibles (como saltos de línea `\r\n` u otros). Para evitar problemas, se recomienda pegar el código en un editor de texto dentro de la VM y ajustar manualmente los espacios, tabulaciones y saltos de línea según sea necesario para cada sentencia.

III. Corrección de Errores: Detectar, investigar y corregir errores de sintaxis es una parte integral del trabajo. Los estudiantes deben estar preparados para identificar y solucionar estos problemas como parte del proceso de aprendizaje y desarrollo.

Aplicación	Versión
Kali GNU/Linux Rolling	2024.2
Snort	snort-2.9.20.tar.gz
DAQ	daq-2.0.7.tar.gz

Preparación: Eliminar Instalaciones Previas de Snort

Antes de comenzar con la instalación, elimina cualquier versión previa de Snort:

```
sudo apt-get remove --purge snort
sudo apt-get autoremove
sudo apt-get autoclean
```

Paso 1: Actualizar el Sistema

Asegúrate de que tu sistema esté completamente actualizado.

```
sudo apt update && sudo apt upgrade -y
```

Paso 2: Instalar Dependencias

Instala todas las dependencias necesarias, incluyendo LuaJIT y las bibliotecas RPC:

```
sudo apt install -y build-essential libpcap-dev libpcres3-dev  
libdumbnet-dev bison flex zlib1g-dev liblzma-dev openssl libssl-dev  
pkg-config libhwloc-dev liblua5.1-dev libtirpc-dev libnfs-dev
```

Paso 3: Crear Enlaces Simbólicos para Bibliotecas RPC

En algunas distribuciones, la biblioteca `rpc/rpc.h` y otros archivos pueden estar en una ubicación diferente. Crea enlaces simbólicos para resolver este problema:

```
sudo ln -s /usr/include/tirpc/rpc/rpc.h /usr/include/rpc/rpc.h  
sudo ln -s /usr/include/tirpc/rpc /usr/include/rpc
```

Paso 4: Configurar Variables de Entorno para la Compilación

Al compilar Snort, asegúrate de que las bibliotecas TIRPC sean reconocidas configurando las variables de entorno adecuadas:

```
export CPPFLAGS="-I/usr/include/tirpc"  
export LDFLAGS="-ltirpc"
```

Paso 5: Instalar DAQ

Descarga e instala la biblioteca DAQ:

```
cd /tmp  
wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz  
tar -xzf daq-2.0.7.tar.gz  
cd daq-2.0.7  
./configure  
make  
sudo make install
```

Paso 6: Descargar y Compilar Snort

Descarga la última versión de Snort y compílala:

```
cd /tmp  
wget https://www.snort.org/downloads/snort/snort-2.9.20.tar.gz  
tar -xzf snort-2.9.20.tar.gz  
cd snort-2.9.20
```

```
./configure --enable-sourcefire --disable-open-appid  
make  
sudo make install
```

Paso 7: Crear Directorios Necesarios

Crea los directorios necesarios para la configuración y los logs de Snort:

```
sudo mkdir /etc/snort /etc/snort/rules /var/log/snort  
sudo touch /etc/snort/snort.conf /etc/snort/rules/local.rules  
sudo mkdir /usr/local/lib/snort_dynamicrules
```

Paso 8: Descargar el Archivo `unicode.map`

Descarga el archivo `unicode.map` y colócalo en el directorio de Snort:

```
sudo wget -O /etc/snort/unicode.map  
https://raw.githubusercontent.com/eldondev/Snort/master/etc/unicode.map  
p
```

Paso 9: Configurar Snort

Edita el archivo de configuración principal de Snort:

```
sudo nano /etc/snort/snort.conf
```

Asegúrate de que las siguientes líneas estén configuradas correctamente:

```
var RULE_PATH /etc/snort/rules  
var SO_RULE_PATH /etc/snort/so_rules  
var PREPROC_RULE_PATH /etc/snort/preproc_rules  
var WHITE_LIST_PATH /etc/snort/rules  
var BLACK_LIST_PATH /etc/snort/rules  
  
preprocessor frag3_global: max_fragments 65536  
preprocessor frag3_engine: policy first detect_anomalies  
preprocessor stream5_global: track_tcp yes, track_udp yes  
preprocessor stream5_tcp: policy first, ports both 80 443  
preprocessor stream5_udp: ignore_any_rules  
preprocessor http_inspect: global iis_unicode_map  
/etc/snort/unicode.map 1252  
preprocessor http_inspect_server: server default profile all ports {  
80 8080 8180 } oversize_dir_length 500  
  
output alert_fast: stdout  
output log_tcpdump: /var/log/snort/tcpdump.log
```

```
include $RULE_PATH/local.rules
```

Paso 10: Crear Reglas Básicas

Edita el archivo `local.rules` para agregar las reglas básicas para ICMP y detección de nmap:

```
sudo nano /etc/snort/rules/local.rules
```

Añade las siguientes líneas:

Regla para detectar ICMP (ping):

```
alert icmp any any -> any any (msg:"ICMP Packet Detected";  
sid:1000001; rev:1;)
```

Reglas para detectar nmap:

```
# Detectar escaneo de puertos TCP SYN  
alert tcp any any -> any any (flags:S; msg:"Nmap TCP SYN Scan  
Detected"; sid:1000002; rev:1;)  
  
# Detectar escaneo de puertos TCP FIN  
alert tcp any any -> any any (flags:F; msg:"Nmap TCP FIN Scan  
Detected"; sid:1000003; rev:1;)  
  
# Detectar escaneo de puertos TCP NULL  
alert tcp any any -> any any (flags:0; msg:"Nmap TCP NULL Scan  
Detected"; sid:1000004; rev:1;)  
  
# Detectar escaneo de puertos TCP Xmas  
alert tcp any any -> any any (flags:SF; msg:"Nmap TCP Xmas Scan  
Detected"; sid:1000005; rev:1;)  
  
# Detectar escaneo de puertos UDP  
# alert udp any any -> any any (msg:"Nmap UDP Scan Detected";  
sid:1000006; rev:1;)
```

Paso 11: Agregar la Ruta de las Bibliotecas a `ld.so.conf`

Usa el siguiente comando para agregar `/usr/local/lib` a `ld.so.conf`:

```
echo "/usr/local/lib" | sudo tee /etc/ld.so.conf.d/snort.conf
```

Paso 12: Actualizar el Caché de las Bibliotecas Dinámicas

Luego, actualiza el caché de las bibliotecas dinámicas:

```
sudo ldconfig
```

Paso 13: Probar Snort

Ejecuta Snort con permisos de superusuario para probar su funcionamiento con las nuevas reglas y configuraciones de preprocessors:

```
sudo snort -v -c /etc/snort/snort.conf -i eth0
```

Nota: Asegúrate de reemplazar `eth0` con el nombre de tu interfaz de red.

Paso 14: Generar Tráfico ICMP y Nmap

Abre otra terminal y genera tráfico ICMP utilizando el comando `ping`:

```
ping -c 4 8.8.8.8
```

Genera tráfico de escaneo `nmap`:

```
sudo nmap -sS 192.168.0.1  
sudo nmap -sF 192.168.0.1  
sudo nmap -sN 192.168.0.1  
sudo nmap -sX 192.168.0.1
```

Nota: Asegúrate de reemplazar `192.168.0.1` con la IP de destino adecuada.

Paso 15: Verificar los Logs

Snort debe haber registrado los paquetes ICMP y las detecciones de `nmap` en su log. Revisa los logs para verificarlo:

```
sudo cat /var/log/snort/alert
```

Deberías ver entradas similares a estas en el archivo de logs:


```
less
```

```
[**] [1:1000001:1] ICMP Packet Detected [**]
[Priority: 0]
06/29-14:15:32.567890 IP 192.168.1.2 -> 8.8.8.8
ICMP TTL:64 TOS:0x0 ID:54321 IpLen:20 DgmLen:84
Type:8 Code:0 ID:12345 Seq:1 ECHO

[**] [1:1000002:1] Nmap TCP SYN Scan Detected [**]
[Priority: 0]
06/29-14:16:45.123456 IP 192.168.1.3 -> 192.168.1.1
TCP TTL:64 TOS:0x0 ID:54321 IpLen:20 DgmLen:40
Flags:S Seq:0x0 Ack:0x0 Win:0

...
```

Paso 16: Configuración de Snort como un Servicio (Opcional)

Para que Snort se ejecute como un servicio, puedes crear un archivo de servicio systemd:

```
sudo nano /etc/systemd/system/snort.service
```

Añade lo siguiente:

```
[Unit]
Description=Snort NIDS
After=network.target

[Service]
ExecStart=/usr/local/bin/snort -c /etc/snort/snort.conf -i eth0

[Install]
WantedBy=multi-user.target
```

Luego, habilita y comienza el servicio:

```
sudo systemctl enable snort
sudo systemctl start snort
sudo systemctl status snort
```

Esto debería configurar Snort para que se inicie automáticamente con el sistema y se ejecute en segundo plano.