Práctica Evaluable Módulo IV

Responsable técnico: Brian Latham

Responsable de documentación: Amadou Diallo

Responsable de demo: Daniel Stix

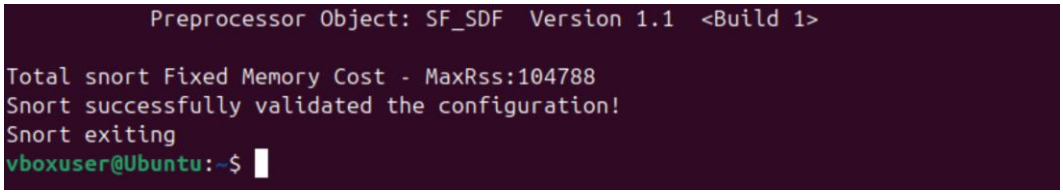
Implementación de Snort en Ubuntu - Sistema de Detección de Intrusos (NIDS). En un primer intento, se consideró el uso de Kali Linux para esta práctica debido a su orientación a la ciberseguridad. Sin embargo, tras evaluar las necesidades específicas de instalación y configuración de Snort, se optó por utilizar Ubuntu, ya que esta ultima proporcionó un entorno más estable y compatible para ejecutar Snort de manera efectiva, especialmente al manejar dependencias y servicios de red necesarios para este tipo de implementación.

1. Investigación y Selección del IDS

Para esta práctica se investigó sobre los sistemas de detección de intrusos en red (NIDS). Se eligió Snort por ser un IDS open-source robusto, ampliamente utilizado y con buena documentación.Un IDS (Intrusion Detection System) es un sistema que monitoriza el tráfico de red o actividad en sistemas para detectar comportamientos maliciosos o no autorizados. Analiza paquetes y eventos en tiempo real usando firmas o técnicas heurísticas. Su objetivo es alertar sobre intrusiones o anomalías, ayudando a prevenir ataques o violaciones de seguridad. Existen IDS basados en red (NIDS) y en host (HIDS).

2. Montaje del Laboratorio

Se instaló Snort sobre una máquina virtual con Ubuntu. Tras la instalación, se procedió a su configuración y se puso en marcha para comenzar con la detección de tráfico de red.



Snort funcionando correctamente tras la instalación inicial.

```
vboxuser@Ubuntu:~$ sudo systemctl status snort
● snort.service - LSB: Lightweight network intrusion detection system
     Loaded: loaded (/etc/init.d/snort; generated)
     Active: active (running) since Fri 2025-05-09 06:59:26 UTC; 6min ago
       Docs: man:systemd-sysv-generator(8)
    Process: 1348 ExecStart=/etc/init.d/snort start (code=exited, status=0/SUCCESS)
      Tasks: 2 (limit: 6827)
     Memory: 89.1M (peak: 104.8M)
        CPU: 1.007s
     CGroup: /system.slice/snort.service
             └─1543 /usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g snort --pid-path /run>

May 09 06:59:25 Ubuntu snort[1543]:            Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
May 09 06:59:25 Ubuntu snort[1543]:            Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
May 09 06:59:25 Ubuntu snort[1543]:            Preprocessor Object: SF_FTPTELNET  Version 1.2  <Buil>
May 09 06:59:25 Ubuntu snort[1543]:            Preprocessor Object: SF_POP  Version 1.0  <Build 1>
May 09 06:59:25 Ubuntu snort[1543]:            Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
May 09 06:59:25 Ubuntu snort[1543]:            Preprocessor Object: SF_DCERPC2  Version 1.0  <Build >
May 09 06:59:25 Ubuntu snort[1543]:            Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
May 09 06:59:25 Ubuntu snort[1543]: Commencing packet processing (pid=1543)
May 09 06:59:26 Ubuntu snort[1348]:     ...done.
```

Verificación de que el servicio Snort se encuentra activo y ejecutándose en el sistema.

3. Implementación de Casos de Uso

Se definieron varias reglas de Snort para detectar comportamientos específicos en la red.

```
  GNU nano 7.2                        /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 -> 8.8.8.8 any (msg:"ALERTA: Ping a 8.8.8.8 detectado"; sid:1000001; rev:1;)
alert tcp any any -> any 80 (msg:"ALERTA: Acceso HTTP detectado"; sid:1000002; rev:1;)
alert tcp any any -> any 443 (msg:"ALERTA: Posible uso de Dropbox"; sid:1000003; rev:1;)
alert tcp any any -> any 22 (msg:"ALERTA: Conexion SSH saliente detectada"; sid:1000004; rev:1;)
```

Actualización de las reglas de Snort después de una primera prueba sin resultados.

```
vboxuser@Ubuntu:~$ sudo cat /var/log/snort/alert
05/08-19:07:22.541134  [**] [1:1000001:1] ALERTA: Ping a 8.8.8.8 detectado [**] [Priority: 0] {ICMP}
10.0.2.15 -> 8.8.8.8
05/08-19:07:23.543923  [**] [1:1000001:1] ALERTA: Ping a 8.8.8.8 detectado [**] [Priority: 0] {ICMP}
10.0.2.15 -> 8.8.8.8
05/08-19:07:24.546149  [**] [1:1000001:1] ALERTA: Ping a 8.8.8.8 detectado [**] [Priority: 0] {ICMP}
10.0.2.15 -> 8.8.8.8
05/08-19:07:25.547194  [**] [1:1000001:1] ALERTA: Ping a 8.8.8.8 detectado [**] [Priority: 0] {ICMP}
10.0.2.15 -> 8.8.8.8
05/08-19:07:26.549831  [**] [1:1000001:1] ALERTA: Ping a 8.8.8.8 detectado [**] [Priority: 0] {ICMP}
10.0.2.15 -> 8.8.8.8
```

Prueba para generar una alerta al hacer ping a 8.8.8.8. Las reglas personalizadas reaccionan ante este evento.

```
vboxuser@Ubuntu:~$ curl ssh test.rebex.net
curl: (6) Could not resolve host: ssh
<head><title>Document Moved</title></head>
<body><h1>Object Moved</h1>This document may be found <a HREF="https://test.rebex.net/">here</a></bod
```

Caso de uso: conexión saliente SSH detectada como alerta por la regla definida.

```
vboxuser@Ubuntu:~$ sudo  tcpdump -i enp0s3 port 80 or port 443 or port 22
```

Caso de uso: acceso a una web específico que genera alerta de navegación.

4. Verificación de Alertas

```
05/09-07:24:34.857606  [**] [1:1000001:1] ALERTA: Ping a 8.8.8.8 detectado [**] [Priority: 0] {ICMP}
10.0.2.15 -> 8.8.8.8
05/09-07:26:23.007138  [**] [1:1000003:1] ALERTA: Posible uso de Dropbox [**] [Priority: 0] {TCP} 10.
0.2.15:51214 -> 108.157.106.174:443
05/09-07:33:13.697679  [**] [1:1000002:1] ALERTA: Acceso HTTP detectado [**] [Priority: 0] {TCP} 10.0
.2.15:54738 -> 194.108.117.16:80
```

Verificación de las alertas generadas por Snort al activarse las reglas definidas.

```
05/09-07:24:34.857606  [**] [1:1000001:1] ALERTA: Ping a 8.8.8.8 detectado [**] [Priority: 0] {ICMP}
10.0.2.15 -> 8.8.8.8
05/09-07:26:23.007138  [**] [1:1000003:1] ALERTA: Posible uso de Dropbox [**] [Priority: 0] {TCP} 10.
0.2.15:51214 -> 108.157.106.174:443
05/09-07:33:13.697679  [**] [1:1000002:1] ALERTA: Acceso HTTP detectado [**] [Priority: 0] {TCP} 10.0
.2.15:54738 -> 194.108.117.16:80
05/09-07:37:15.016506  [**] [1:1000004:1] ALERTA: Conexion SSH saliente detectada [**] [Priority: 0]
{TCP} 10.0.2.15:47934 -> 194.108.117.16:22
```

Resumen donde se muestran las cuatro alertas generadas durante las pruebas: ping, web, SSH y Dropbox.

5. Conclusión

La práctica permitió familiarizarse con la instalación, configuración y uso de un IDS como Snort en un entorno Ubuntu. Se crearon y probaron reglas para detectar distintos tipos de tráfico en red, cumpliendo con los objetivos de detección de eventos. El trabajo en grupo y el uso de herramientas open-source fomentaron el aprendizaje práctico de ciberseguridad defensiva.