



# Laboratorio: Configuración y Uso de un IDS (Sistema de Detección de Intrusos)

Module	IT - Cibersecurity
Teacher,-s	Chrystian Ruiz Diaz
Student,-s	Tobías Emanuel González Vera
Career,-s	Ingeniería en Tecnologías de la Información Empresarial
Date	@June 27, 2024
Wochentage	Donnerstag
Deadline	@July 2, 2024
Status	Sended
Attached files	<u><a href="#">Unidad_31_GuiaActividad_IDS_Snort_2920.pdf</a></u>

---

[Configuración y Uso de un IDS \(Snort\) en Kali Linux](#)

[Objetivo](#)

[Herramientas Necesarias](#)

[Pasos](#)

[Instalación de Snort](#)

[Instalación de dependencias](#)

[Instalar DAQ y compilar SNORT](#)

[PROBANDO SNORT](#)

[Configuración de Snort como servicio](#)

---

---

# Configuración y Uso de un IDS (Snort) en Kali Linux

## Objetivo

El objetivo de esta práctica es aprender a configurar y utilizar un IDS (Sistema de Detección de Intrusos) en Kali Linux para monitorear y analizar el tráfico de red en busca de actividades sospechosas o maliciosas.

## Herramientas Necesarias

- Kali Linux
- Snort (una herramienta IDS)

---

## Pasos

### Instalación de Snort

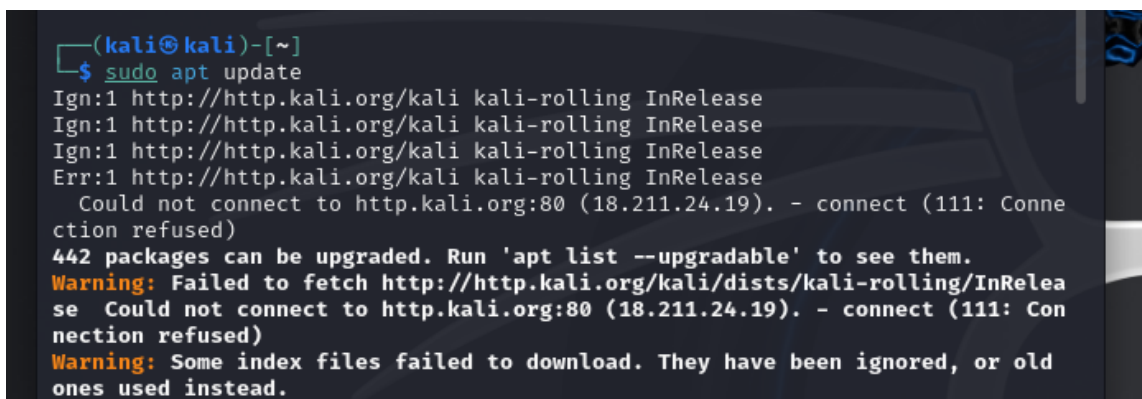
#### 1. Abrir una terminal en Kali Linux:

- Primero, actualizo los repositorios para asegurarme de tener las últimas versiones de los paquetes:

```
sudo apt update
```

- Luego, instalo Snort utilizando el siguiente comando:

```
sudo apt install snort
```



```
(kali㉿kali)-[~]  
$ sudo apt update  
Ign:1 http://http.kali.org/kali kali-rolling InRelease  
Ign:1 http://http.kali.org/kali kali-rolling InRelease  
Ign:1 http://http.kali.org/kali kali-rolling InRelease  
Err:1 http://http.kali.org/kali kali-rolling InRelease  
      Could not connect to http.kali.org:80 (18.211.24.19). - connect (111: Connection refused)  
442 packages can be upgraded. Run 'apt list --upgradable' to see them.  
Warning: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease  
      Could not connect to http.kali.org:80 (18.211.24.19). - connect (111: Connection refused)  
Warning: Some index files failed to download. They have been ignored, or old ones used instead.
```

```
(kali㉿kali)-[~]
$ sudo apt install snort
Installing:
  snort

Installing dependencies:
  libdaq3      liblognorm5  snort-common
  libestr0     oinkmaster  snort-common-libraries
  libfastjson4 rsyslog      snort-rules-default

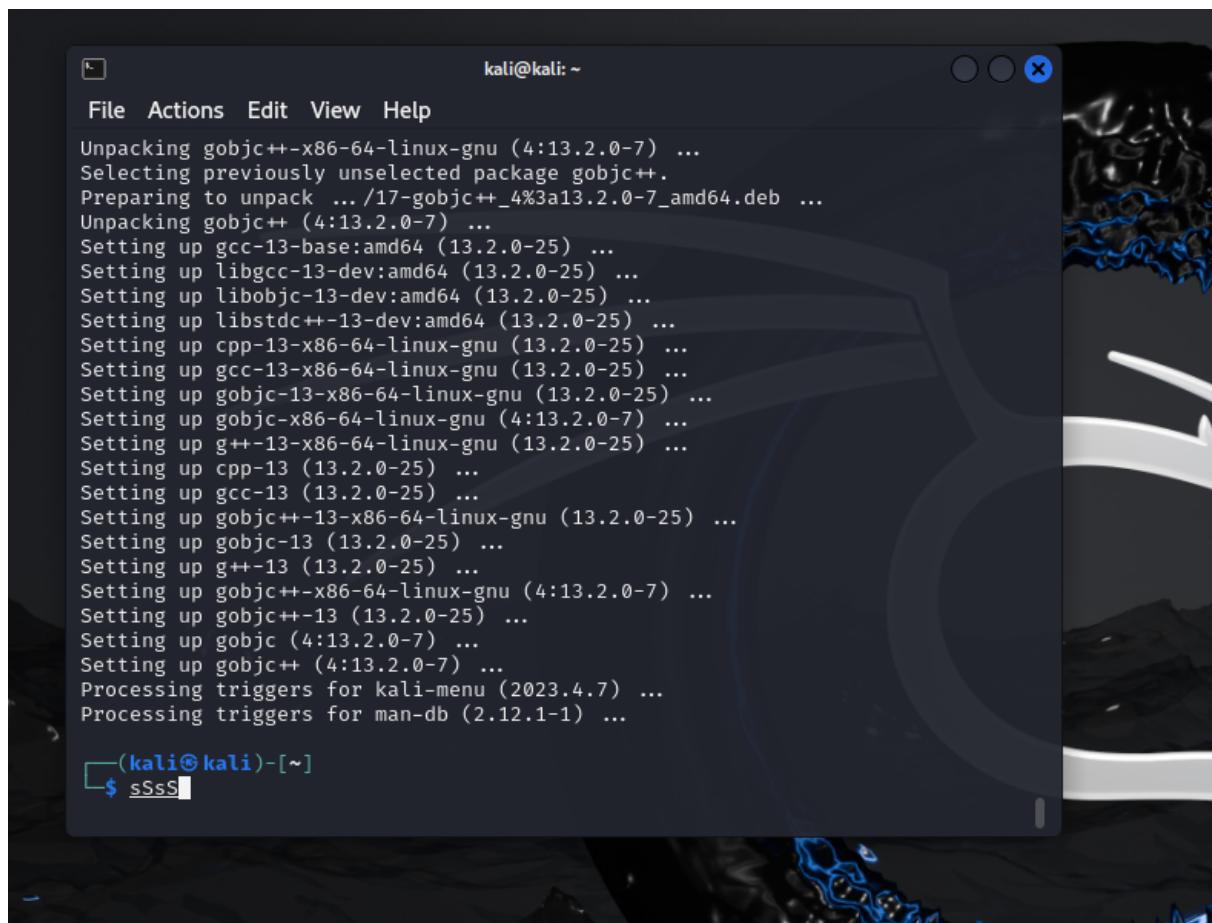
Suggested packages:
  rsyslog-mysql  rsyslog-doc  rsyslog-gssapi
  | rsyslog-pgsql rsyslog-openssl rsyslog-relp
  rsyslog-mongodb | rsyslog-gnutls snort-doc

Summary:
  Upgrading: 0, Installing: 10, Removing: 0, Not Upgrading: 442
  Download size: 9,236 B / 3,664 kB
  Space needed: 15.7 MB / 64.6 GB available

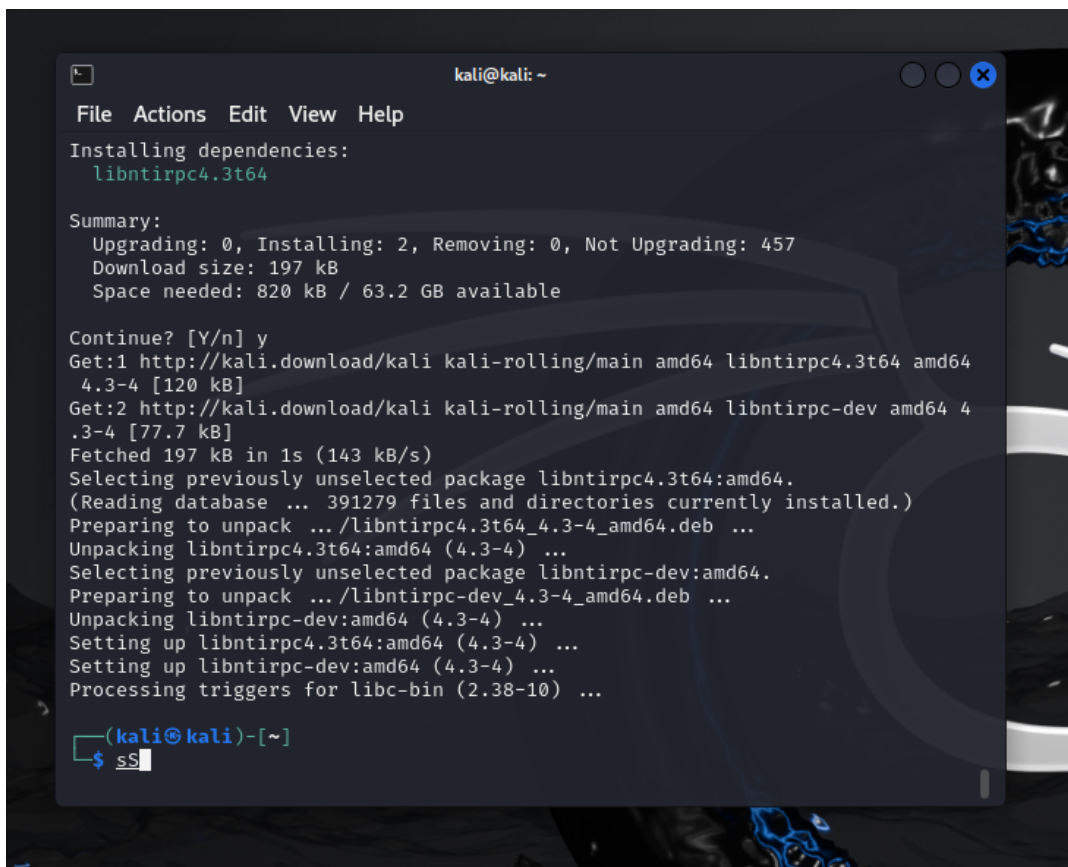
Continue? [Y/n] Y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libestr0 amd64 0.1.11-1+b1 [9,236 B]
Fetched 9,236 B in 1s (8,221 B/s)
Selecting previously unselected package snort-common-libraries.
(Reading database ... 391259 files and directories currently installed.)
Preparing to unpack .../0-snort-common-libraries_3.1.82.0-0kali1+b1_amd64.deb
...
Unpacking snort-common-libraries (3.1.82.0-0kali1+b1) ...
```

## Instalat dependencias

```
sudo apt install gobjc++
```

A terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The terminal output shows the installation of glibc++-x86-64-linux-gnu (4:13.2.0-7) and its dependencies. The packages being installed include gcc-13-base:amd64 (13.2.0-25), libgcc-13-dev:amd64 (13.2.0-25), libobjc-13-dev:amd64 (13.2.0-25), libstdc++-13-dev:amd64 (13.2.0-25), cpp-13-x86-64-linux-gnu (13.2.0-25), gcc-13-x86-64-linux-gnu (13.2.0-25), glibc-13-x86-64-linux-gnu (13.2.0-25), glibc-x86-64-linux-gnu (4:13.2.0-7), g++-13-x86-64-linux-gnu (13.2.0-25), cpp-13 (13.2.0-25), gcc-13 (13.2.0-25), glibc++-13-x86-64-linux-gnu (13.2.0-25), glibc++-13 (13.2.0-25), g++-13 (13.2.0-25), glibc++-x86-64-linux-gnu (4:13.2.0-7), glibc++-13 (13.2.0-25), glibc (4:13.2.0-7), and glibc++ (4:13.2.0-7). The terminal also shows the processing of triggers for kali-menu (2023.4.7) and man-db (2.12.1-1). The prompt is '(kali@kali)-[~]' and the user has entered '\$ sSsS'.

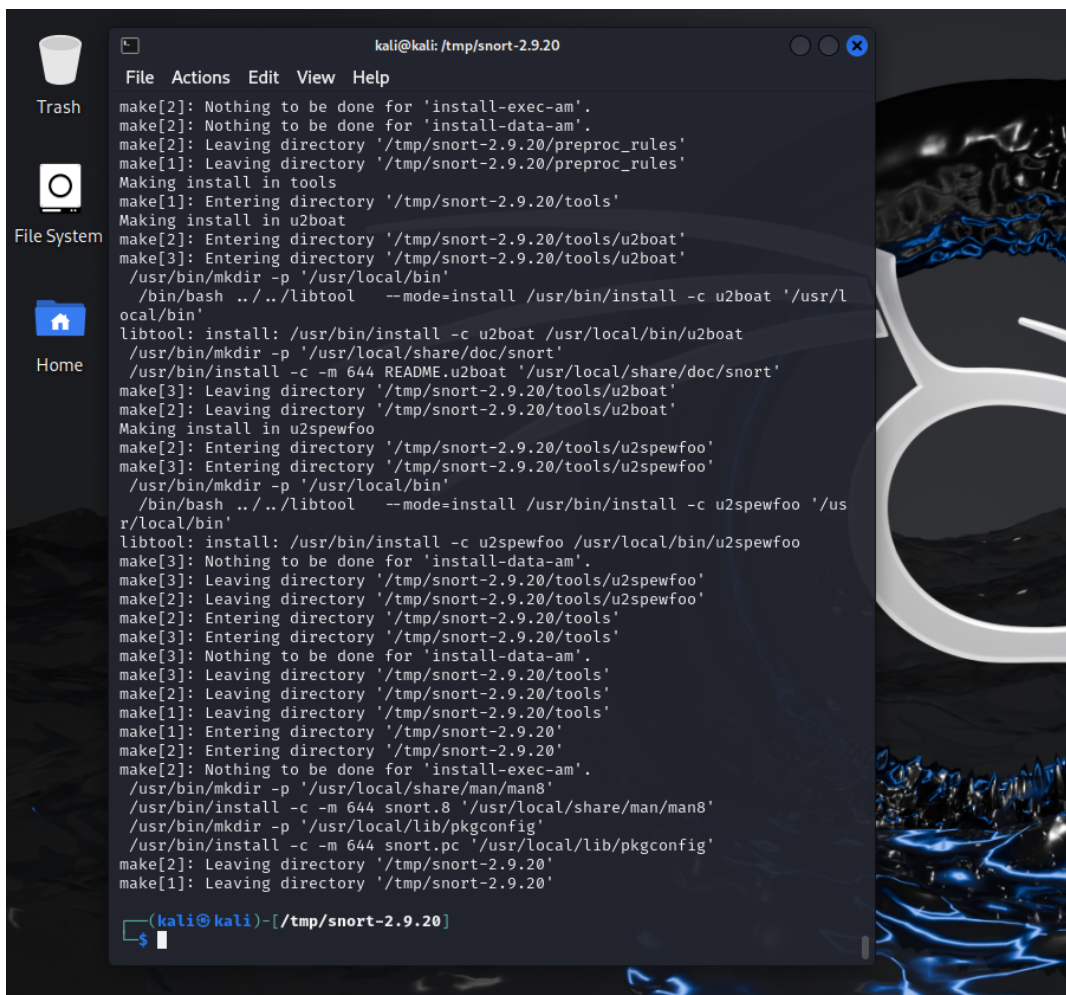
```
sudo apt install libntirpc-dev
```



```
kali@kali: ~  
File Actions Edit View Help  
Installing dependencies:  
  libntirpc4.3t64  
  
Summary:  
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 457  
  Download size: 197 kB  
  Space needed: 820 kB / 63.2 GB available  
  
Continue? [Y/n] y  
Get:1 http://kali.download/kali kali-rolling/main amd64 libntirpc4.3t64 amd64 4.3-4 [120 kB]  
Get:2 http://kali.download/kali kali-rolling/main amd64 libntirpc-dev amd64 4.3-4 [77.7 kB]  
Fetched 197 kB in 1s (143 kB/s)  
Selecting previously unselected package libntirpc4.3t64:amd64.  
(Reading database ... 391279 files and directories currently installed.)  
Preparing to unpack .../libntirpc4.3t64_4.3-4_amd64.deb ...  
Unpacking libntirpc4.3t64:amd64 (4.3-4) ...  
Selecting previously unselected package libntirpc-dev:amd64.  
Preparing to unpack .../libntirpc-dev_4.3-4_amd64.deb ...  
Unpacking libntirpc-dev:amd64 (4.3-4) ...  
Setting up libntirpc4.3t64:amd64 (4.3-4) ...  
Setting up libntirpc-dev:amd64 (4.3-4) ...  
Processing triggers for libc-bin (2.38-10) ...  
  
(kali@kali)-[~]  
$ sS
```

```
sudo apt update  
sudo apt install libc-dev-bin libc6-dev libtirpc-dev  
sudo ln -s /usr/include/tirpc/rpc /usr/include/rpc  
ls /usr/include/rpc/rpc.h
```

## Instalar DAQ y compilar SNORT



The image shows a terminal window on a Kali Linux desktop. The window title is 'kali@kali: /tmp/snort-2.9.20'. The terminal output shows the progress of installing Snort 2.9.20. It includes steps for installing tools, u2boat, u2spewfoo, and setting up man pages and pkgconfig files. The installation is completed successfully.

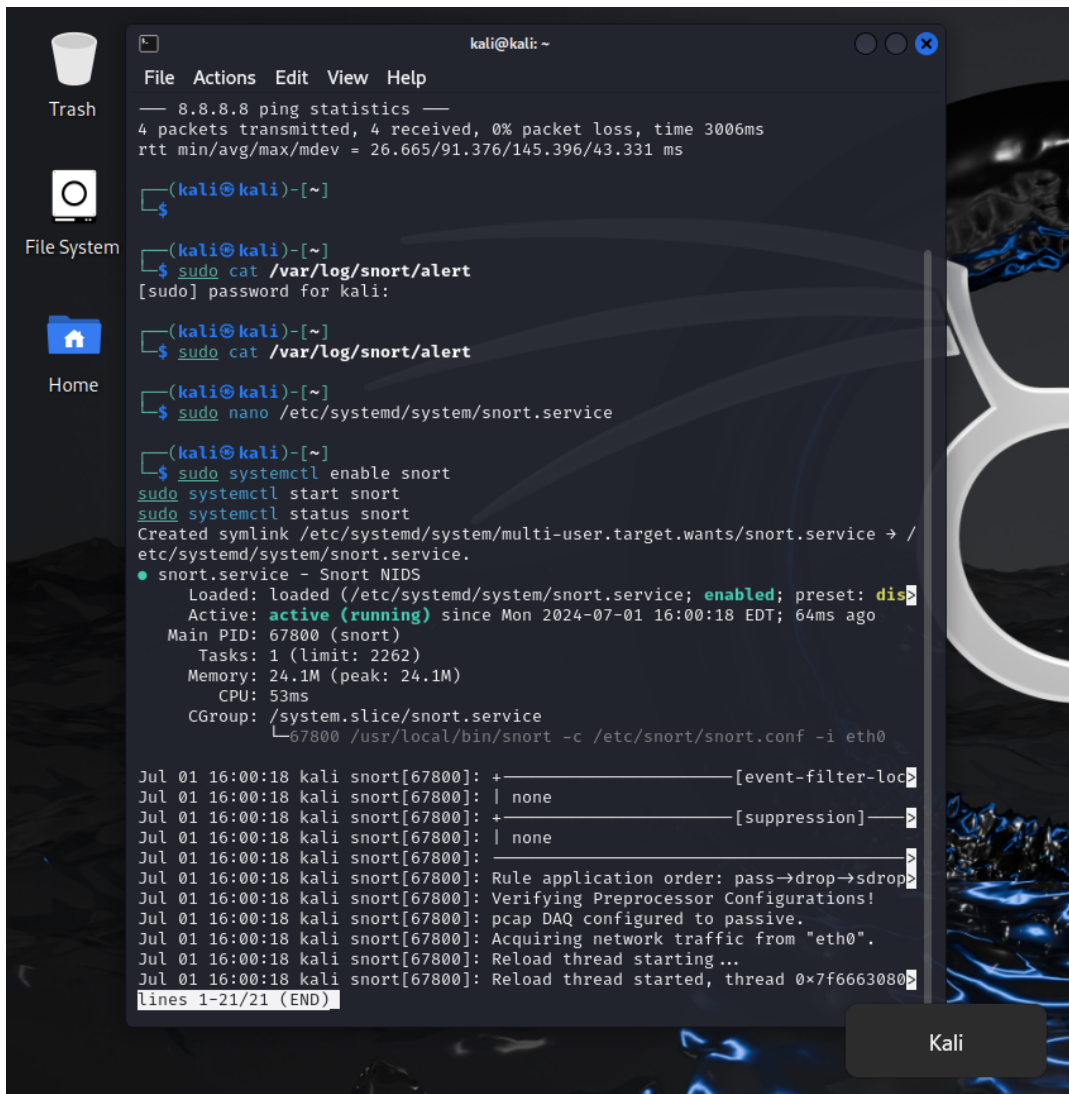
```
kali@kali: /tmp/snort-2.9.20
File Actions Edit View Help
make[2]: Nothing to be done for 'install-exec-am'.
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/tmp/snort-2.9.20/preproc_rules'
make[1]: Leaving directory '/tmp/snort-2.9.20/preproc_rules'
Making install in tools
make[1]: Entering directory '/tmp/snort-2.9.20/tools'
Making install in u2boat
make[2]: Entering directory '/tmp/snort-2.9.20/tools/u2boat'
make[3]: Entering directory '/tmp/snort-2.9.20/tools/u2boat'
/usr/bin/mkdir -p '/usr/local/bin'
/bin/bash ../libtool --mode=install /usr/bin/install -c u2boat '/usr/local/bin'
libtool: install: /usr/bin/install -c u2boat /usr/local/bin/u2boat
/usr/bin/mkdir -p '/usr/local/share/doc/snort'
/usr/bin/install -c -m 644 README.u2boat '/usr/local/share/doc/snort'
make[3]: Leaving directory '/tmp/snort-2.9.20/tools/u2boat'
make[2]: Leaving directory '/tmp/snort-2.9.20/tools/u2boat'
Making install in u2spewfoo
make[2]: Entering directory '/tmp/snort-2.9.20/tools/u2spewfoo'
make[3]: Entering directory '/tmp/snort-2.9.20/tools/u2spewfoo'
/usr/bin/mkdir -p '/usr/local/bin'
/bin/bash ../libtool --mode=install /usr/bin/install -c u2spewfoo '/usr/local/bin'
libtool: install: /usr/bin/install -c u2spewfoo /usr/local/bin/u2spewfoo
make[3]: Nothing to be done for 'install-data-am'.
make[3]: Leaving directory '/tmp/snort-2.9.20/tools/u2spewfoo'
make[2]: Leaving directory '/tmp/snort-2.9.20/tools/u2spewfoo'
make[2]: Entering directory '/tmp/snort-2.9.20/tools'
make[3]: Entering directory '/tmp/snort-2.9.20/tools'
make[3]: Nothing to be done for 'install-data-am'.
make[3]: Leaving directory '/tmp/snort-2.9.20/tools'
make[2]: Leaving directory '/tmp/snort-2.9.20/tools'
make[1]: Leaving directory '/tmp/snort-2.9.20/tools'
make[1]: Entering directory '/tmp/snort-2.9.20'
make[2]: Entering directory '/tmp/snort-2.9.20'
make[2]: Nothing to be done for 'install-exec-am'.
/usr/bin/mkdir -p '/usr/local/share/man/man8'
/usr/bin/install -c -m 644 snort.8 '/usr/local/share/man/man8'
/usr/bin/mkdir -p '/usr/local/lib/pkgconfig'
/usr/bin/install -c -m 644 snort.pc '/usr/local/lib/pkgconfig'
make[2]: Leaving directory '/tmp/snort-2.9.20'
make[1]: Leaving directory '/tmp/snort-2.9.20'

(kali@kali)-[/tmp/snort-2.9.20]
$
```

## PROBANDO SNORT



## Configuración de Snort como servicio



The screenshot shows a Kali Linux desktop with a terminal window open. The terminal displays the following commands and output:

```
kali@kali: ~  
File Actions Edit View Help  
— 8.8.8.8 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3006ms  
rtt min/avg/max/mdev = 26.665/91.376/145.396/43.331 ms  
  
(kali@kali)-[~]  
$ sudo cat /var/log/snort/alert  
[sudo] password for kali:  
  
(kali@kali)-[~]  
$ sudo cat /var/log/snort/alert  
  
(kali@kali)-[~]  
$ sudo nano /etc/systemd/system/snort.service  
  
(kali@kali)-[~]  
$ sudo systemctl enable snort  
sudo systemctl start snort  
sudo systemctl status snort  
Created symlink /etc/systemd/system/multi-user.target.wants/snort.service →  
etc/systemd/system/snort.service.  
● snort.service - Snort NIDS  
   Loaded: loaded (/etc/systemd/system/snort.service; enabled; preset: disabled)  
   Active: active (running) since Mon 2024-07-01 16:00:18 EDT; 64ms ago  
     Main PID: 67800 (snort)  
       Tasks: 1 (limit: 2262)  
      Memory: 24.1M (peak: 24.1M)  
         CPU: 53ms  
    CGroup: /system.slice/snort.service  
            └─67800 /usr/local/bin/snort -c /etc/snort/snort.conf -i eth0  
  
Jul 01 16:00:18 kali snort[67800]: +-----[event-filter-loc  
Jul 01 16:00:18 kali snort[67800]: | none  
Jul 01 16:00:18 kali snort[67800]: +-----[suppression]-----  
Jul 01 16:00:18 kali snort[67800]: | none  
Jul 01 16:00:18 kali snort[67800]:  
Jul 01 16:00:18 kali snort[67800]: Rule application order: pass→drop→sdrops  
Jul 01 16:00:18 kali snort[67800]: Verifying Preprocessor Configurations!  
Jul 01 16:00:18 kali snort[67800]: pcap DAQ configured to passive.  
Jul 01 16:00:18 kali snort[67800]: Acquiring network traffic from "eth0".  
Jul 01 16:00:18 kali snort[67800]: Reload thread starting...  
Jul 01 16:00:18 kali snort[67800]: Reload thread started, thread 0x7f6663080  
lines 1-21/21 (END)
```

A "Kali" button is visible in the bottom right corner of the terminal window.