Proyecto Final

Etiquetas	En curso
Fecha de creación	@2 de diciembre de 2024 14:10

Sugerencias

- Si el objetivo principal es emular un entorno lo más cercano posible al hardware real de dispositivos IoT (como routers, cámaras o sistemas embebidos), QEMU sería más adecuado debido a su capacidad para emular arquitecturas específicas como ARM y MIPS.
- Si el objetivo es simplemente probar estrategias de *hardening* en sistemas operativos genéricos o ligeros, VirtualBox es más sencillo y rápido de configurar, ideal para un enfoque experimental básico sin la necesidad de emular hardware específico de IoT.

Para este proyecto, que busca analizar sistemas operativos en dispositivos IoT, QEMU sería más ideal si se necesita precisión en la simulación del hardware. Sin embargo, si los recursos o el tiempo son limitados, puedes optar por VirtualBox para comenzar.

Kali-Linux

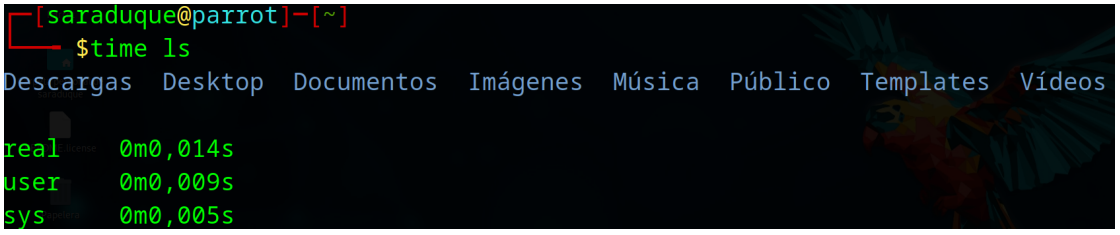
Tiempos Sin Hardening

Comandos

```
//Listar archivos
time ls
time ls -l
time ls -a
time ls -lh
//Cambiar de directorio
time cd Documentos
time cd ..
//Crear directorios
time mkdir ejemplo
//Eliminar archivos y directorios
time rm -r ejemplo
```

```
sudo apt update

sudo apt install sysbench

sysbench cpu --cpu-max-prime=20000 run
```

`time ls`



`time ls -l`

`time ls -a`

```
┌──[saraduque@parrot]─[~]
└─── $time ls -a
.                   .msf4
..                  Música
.bashrc             .profile
.BurpSuite          Público
.cache              .sudo_as_admin_successful
.config             Templates
.dbeaver4           .vboxclient-clipboard-tty7-control.pid
Descargas           .vboxclient-clipboard-tty7-service.pid
Desktop             .vboxclient-display-svga-x11-tty7-control.pid
.dmrc               .vboxclient-display-svga-x11-tty7-service.pid
Documentos          .vboxclient-draganddrop-tty7-control.pid
.emacs              .vboxclient-draganddrop-tty7-service.pid
.face               .vboxclient-hostversion-tty7-control.pid
.face.icon          .vboxclient-seamless-tty7-control.pid
.gtkrc-2.0          .vboxclient-seamless-tty7-service.pid
Imágenes            .vboxclient-vmsvga-session-tty7-control.pid
.java               Vídeos
.kde                .Xauthority
.last-updated       .xsession-errors
.local              .xsession-errors.old
.mozilla

real    0m0,033s
user    0m0,010s
sys     0m0,023s
```

`time ls -lh`

```
┌──[saraduque@parrot]─[~]
└─── $time ls -lh
total 0
drwxr-xr-x 1 saraduque saraduque  0 dic  3 11:32 Descargas
drwxr-xr-x 1 saraduque saraduque 28 oct 23 08:49 Desktop
drwxr-xr-x 1 saraduque saraduque 56 dic  4 13:50 Documentos
drwxr-xr-x 1 saraduque saraduque  0 dic  3 11:32 Imágenes
drwxr-xr-x 1 saraduque saraduque  0 dic  3 11:32 Música
drwxr-xr-x 1 saraduque saraduque  0 dic  3 11:32 Público
drwxr-xr-x 1 saraduque saraduque 22 oct 23 08:49 Templates
drwxr-xr-x 1 saraduque saraduque  0 dic  3 11:32 Vídeos

real    0m0,008s
user    0m0,003s
sys     0m0,005s
```

`time cd Documentos` y `time cd ..`

```
┌─[saraduque@parrot]─[~]
└──╼ $time cd Documentos

real    0m0,000s
user    0m0,000s
sys     0m0,000s
┌─[saraduque@parrot]─[~/Documentos]
└──╼ $time cd ..

real    0m0,000s
user    0m0,000s
sys     0m0,000s
```

`time mkdir ejemplo` y `time rm -r ejemplo`

```
┌─[saraduque@parrot]─[~]
└──╼ $time mkdir ejemplo

real    0m0,012s
user    0m0,007s
sys     0m0,005s
┌─[saraduque@parrot]─[~]
└──╼ $time rm -r ejemplo

real    0m0,020s
user    0m0,016s
sys     0m0,002s
```

`sudo apt update`

```
┌─[✗]─[saraduque@parrot]─[~]
└──╼ $sudo apt update
Obj:1 https://deb.parrot.sh/parrot lory InRelease
Obj:2 https://deb.parrot.sh/direct/parrot lory-security InRelease
Obj:3 https://deb.parrot.sh/parrot lory-backports InRelease
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 157 paquetes. Ejecute «apt list --upgradable» para verlos.
```

`sudo apt install sysbench`

```
┌─[saraduque@parrot]─[~]
└──╼ $sudo apt install sysbench
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  sysbench
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 157 no actualizados.
```

`sysbench cpu --cpu-max-prime=20000 run`

```
┌─[saraduque@parrot]─[~]
└──╼ $sysbench cpu --cpu-max-prime=20000 run
sysbench 1.0.20 (using system LuaJIT 2.1.0-beta3)

Running the test with following options:
Number of threads: 1
Initializing random number generator from current time


Prime numbers limit: 20000

Initializing worker threads...

Threads started!

CPU speed:
    events per second:   444.93

General statistics:
    total time:                          10.0012s
    total number of events:              4451

Latency (ms):
         min:                                    1.88
         avg:                                    2.24
         max:                                    5.76
         95th percentile:                        2.71
         sum:                                 9990.59

Threads fairness:
    events (avg/stddev):           4451.0000/0.00
    execution time (avg/stddev):   9.9906/0.00
```

▼ Utilizar shodan

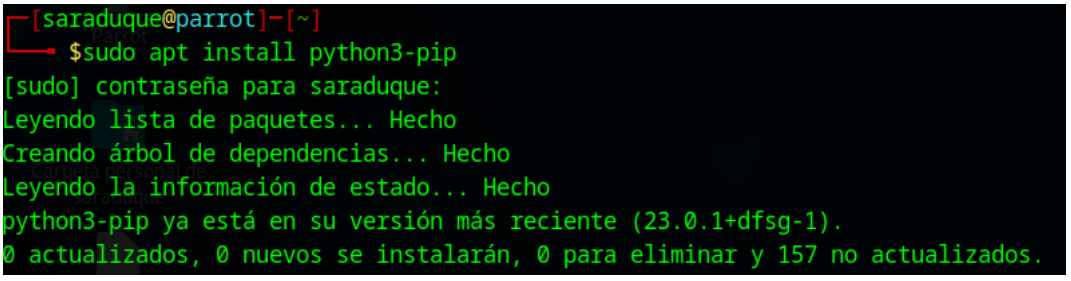
▼ Comandos a ejecutar

```
//Averiguamos si tenemos shodan instalado
pip list | grep shodan

//Configurar shodan
sudo apt install python3-pip  # Si aún no tienes pip i
pip3 install shodan
```

```
//archivo a condigurar
nano shodan_analysis.py

//ejecutar el script
python3 shodan_analysis.py

shodan init 'my_api_key'

shodan host 8.8.8.8

shodan count apache

shodan info

shodan myip

shodan radar

shodan scan submit

shodan search apache

shodan stats apache

shodan stream

shodan version
```

▼ Capturas de pantalla

`sudo apt install python3-pip`



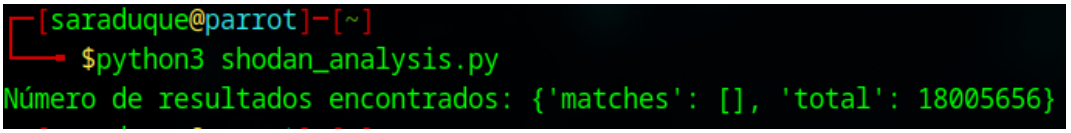
`pip list | grep shodan`

`shodan init 'my_api_key'`

`nano shodan_analysis.py`

```
import shodan

SHODAN_API_KEY = 'EGYetoe97AyEiexORNMq73zxzJBw9C4p'

api = shodan.Shodan(SHODAN_API_KEY)

try:
    results = api.count("apache")
    print(f"Número de resultados encontrados: {results
except shodan.APIError as e:
    print(f"Error: {e}")
```

`python3 shodan_analysis.py`

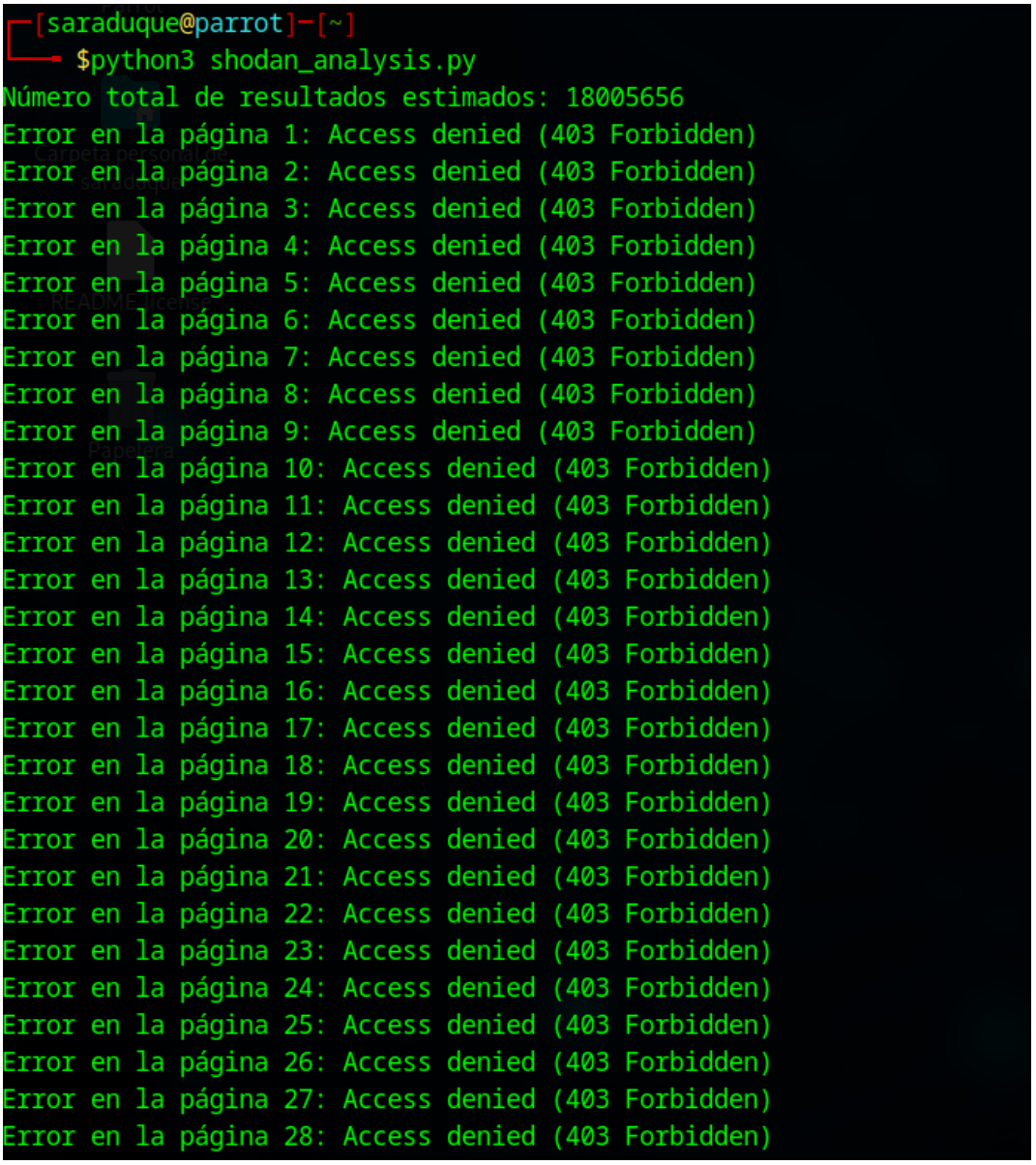


`nano shodan_analysis.py`

```
import shodan

SHODAN_API_KEY = 'EGYetoe97AyEiexORNMq73zxzJBw9C4p'

# Inicializa la API de Shodan
api = shodan.Shodan(SHODAN_API_KEY)
```

```
# Parámetros de búsqueda
query = 'apache'
page_size = 100
max_results = 10  # Número máximo de resultados a most

# Obtén el número total de resultados
total_results = api.count(query)['total']
print(f"Número total de resultados estimados: {total_r

# Variable para contar los resultados procesados
results_shown = 0

# Itera sobre las páginas de resultados
for page in range(1, (total_results // page_size) + 2)
    try:
        # Realiza la búsqueda en la página actual
        results = api.search(query, page=page)

        # Procesa los resultados de la página
        for result in results['matches']:
            if results_shown < max_results:
                print(f"IP: {result['ip_str']}")
                print(f"Puerto: {result['port']}")
                print(f"Data: {result['data']}")
                results_shown += 1
            else:
                break

        if results_shown >= max_results:
            break

    except shodan.APIError as e:
        print(f"Error en la página {page}: {e}")

print("Fin de la búsqueda")
```

`python3 shodan_analysis.py`

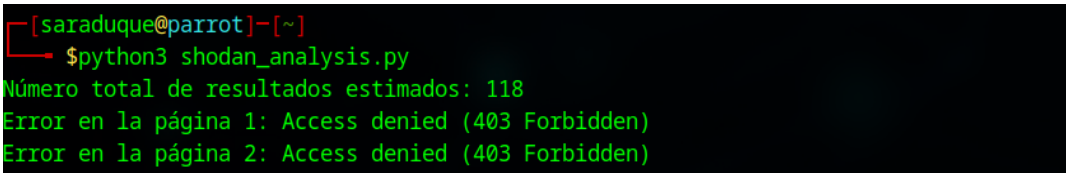


`nano shodan_analysis.py` Buscar Camaras Web

```
import shodan

SHODAN_API_KEY = 'EGYetoe97AyEiexORNMq73zxzJBw9C4p'

# Inicializa la API de Shodan
api = shodan.Shodan(SHODAN_API_KEY)

# Parámetros de búsqueda
query = 'title:"webcamXP"'
page_size = 100  # Número de resultados por página
```

```
try:
    # Obtener el número total de resultados
    total_results = api.count(query)['total']
    print(f"Número total de resultados estimados: {tot

    # Iterar sobre las páginas de resultados
    for page in range(1, (total_results // page_size)
        try:
            # Realizar la búsqueda en la página actual
            results = api.search(query, page=page)

            # Procesar los resultados de la página
            for result in results['matches']:
                print(f"IP: {result['ip_str']}")
                print(f"Puerto: {result['port']}")
                print(f"Data: {result['data']}")
                print("-" * 20)

        except shodan.APIError as e:
            print(f"Error en la página {page}: {e}")

except shodan.APIError as e:
    print(f"Error al obtener el número total de result
```

`python3 shodan_analysis.py`



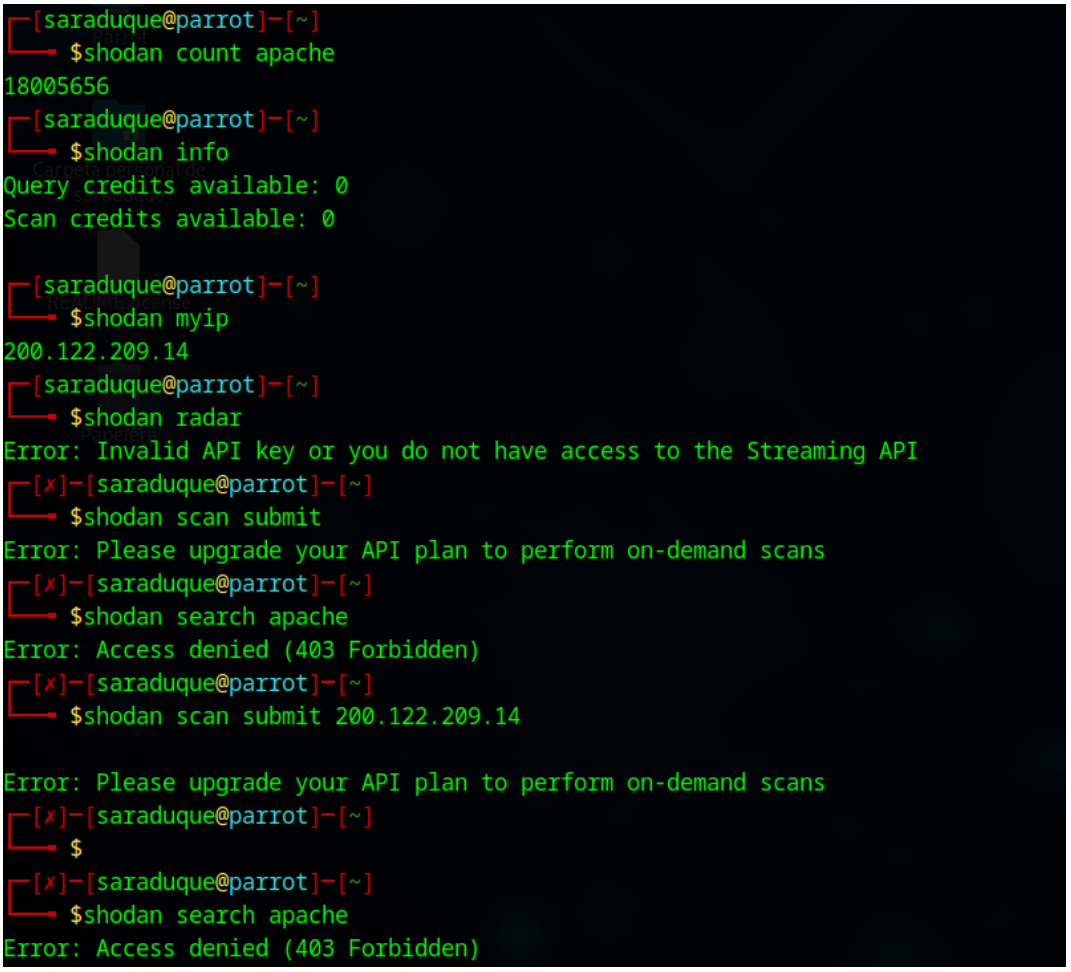
Comandos de shodan

```
Commands:
  alert       Manage the network alerts for your account
  convert     Convert the given input data file into a different format.
  count       Returns the number of results for a search
  data        Bulk data access to Shodan
  domain      View all available information for a domain
  download    Download search results and save them in a compressed JSON...
  honeyscore  Check whether the IP is a honeypot or not.
  host        View all available information for an IP address
  info        Shows general information about your account
  init        Initialize the Shodan command-line
  myip        Print your external IP address
  org         Manage your organization's access to Shodan
  parse       Extract information out of compressed JSON files.
  radar       Real-Time Map of some results as Shodan finds them.
  scan        Scan an IP/ netblock using Shodan.
  search      Search the Shodan database
  stats       Provide summary information about a search query
  stream      Stream data in real-time.
  version     Print version of this tool.
```

`shodan host 8.8.8.8`

```
┌─[✗]─[saraduque@parrot]─[~]
└──╼ $shodan host 8.8.8.8
8.8.8.8
Hostnames:              dns.google
City:                   Mountain View
Country:                United States
Organization:           Google LLC
Updated:                2024-12-05T11:00:18.619519
Number of open ports:   2

Ports:
     53/tcp
     53/udp
    443/tcp
        |-- SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2, TLSv1.3
```

`shodan count apache, shodan info, shodan myip, shodan shodan radar`



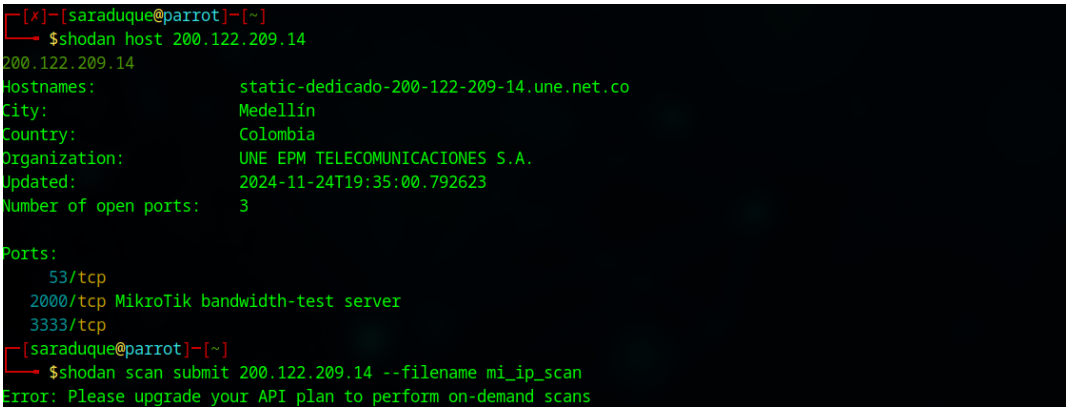
`shodan stats apache`

```
┌──[✗]─[saraduque@parrot]─[~]
└─► $shodan stats apache
Top 10 Results for Facet: country
US                                5,110,097
DE                                1,781,696
JP                                1,619,760
CN                                1,446,461
FR                                  765,568
IN                                  511,652
GB                                  459,666
NL                                  428,278
KR                                  392,211
CA                                  391,824

Top 10 Results for Facet: org
Amazon Technologies Inc.          738,400
China Education and Research Network     573,381
Amazon.com, Inc.                  527,167
DigitalOcean, LLC                 526,731
Hetzner Online GmbH               371,870
Aliyun Computing Co., LTD         340,773
GoDaddy.com, LLC                  280,619
Google LLC                        268,047
OVH SAS                           265,449
Unified Layer                     256,289
```

`shodan stream, shodan version, shodan search ip:myip`

```
┌──[saraduque@parrot]─[~]
└─► $shodan stream
Error: Invalid API key or you do not have access to the Streaming API
┌──[✗]─[saraduque@parrot]─[~]
└─► $shodan version
1.28.0
┌──[saraduque@parrot]─[~]
└─► $
┌──[saraduque@parrot]─[~]
└─► $shodan search ip:200.122.209.14

Error: Access denied (403 Forbidden)
```

`shodan host 200.122.209.14`



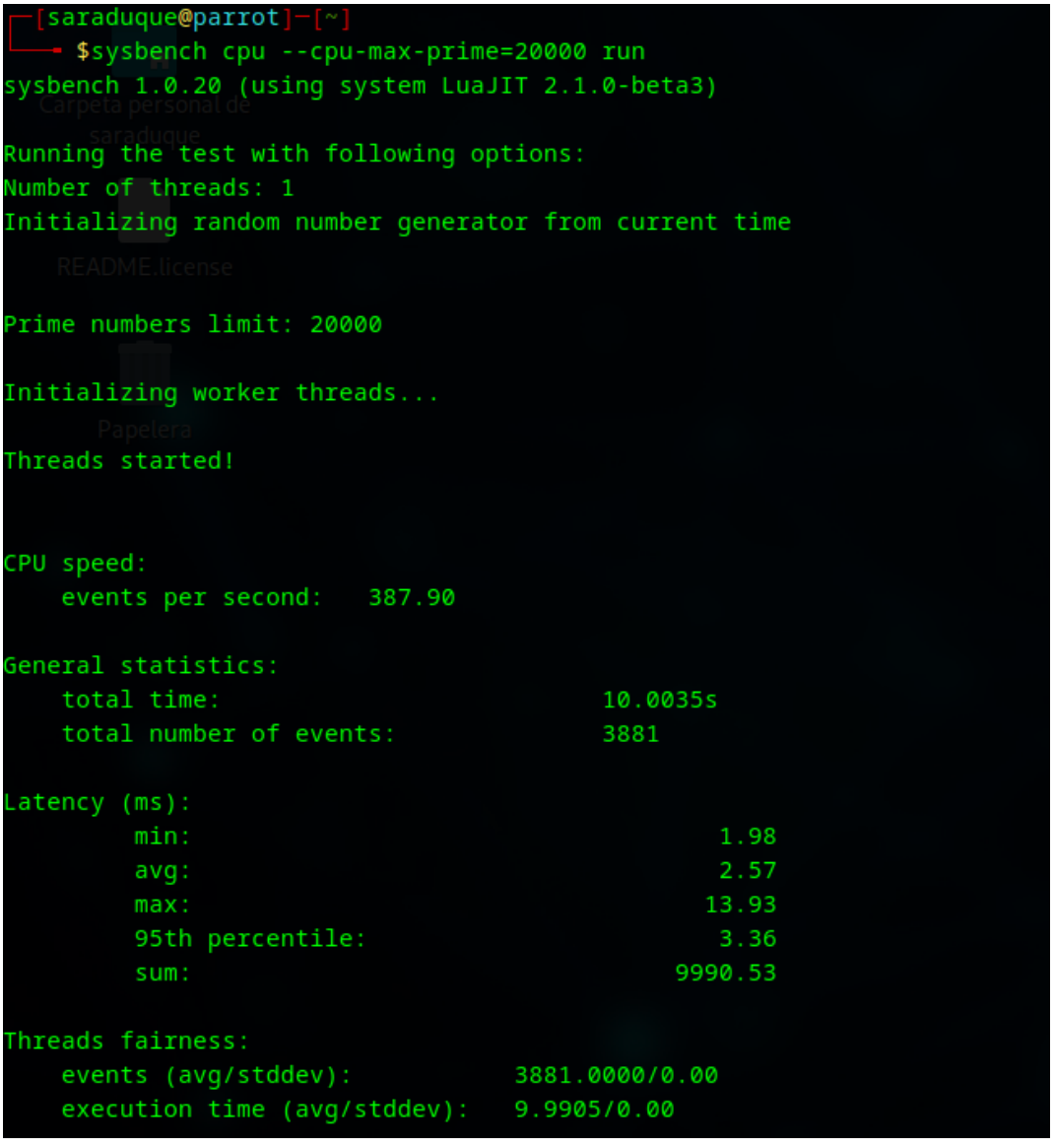
▼ Con Hardening

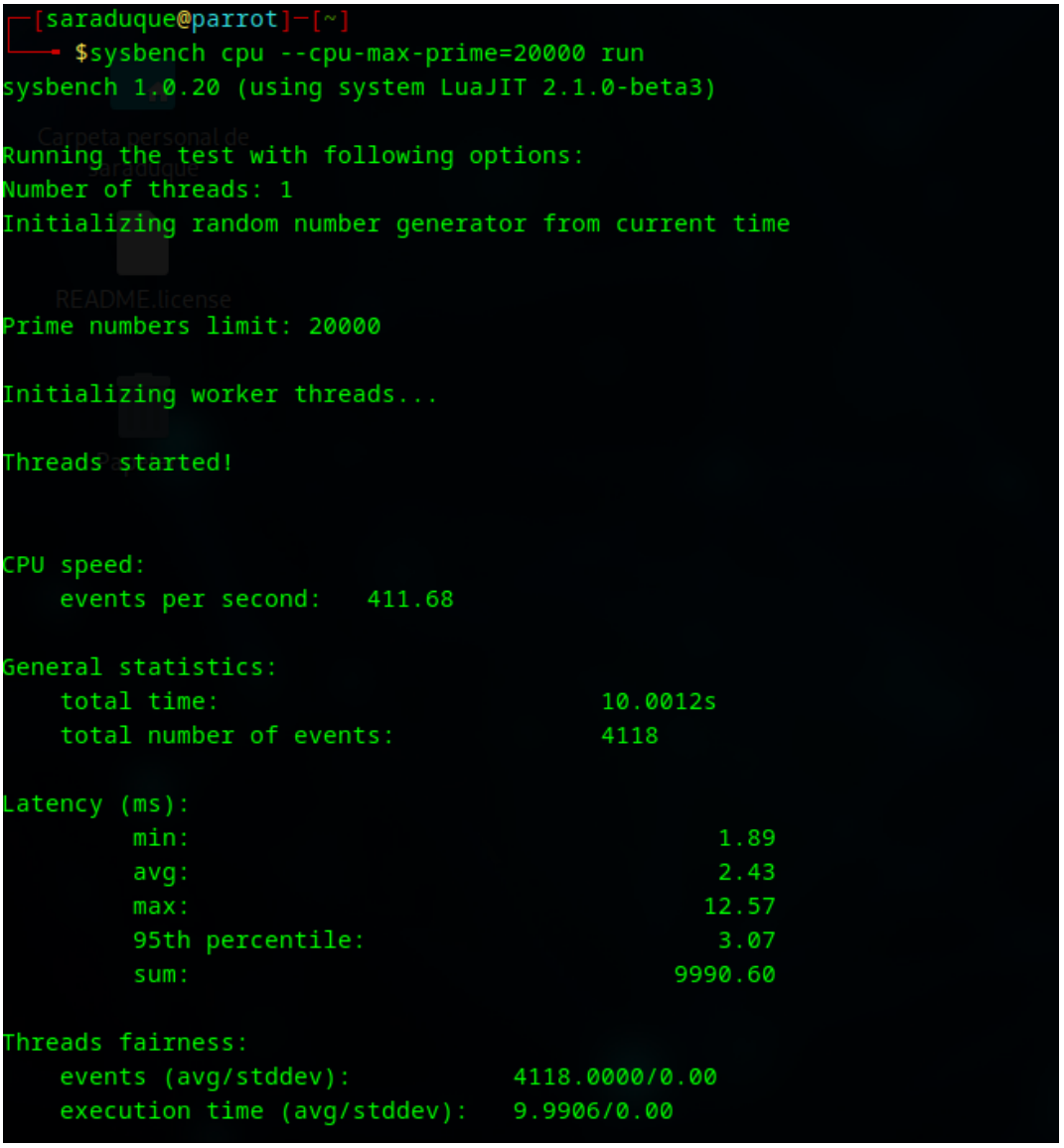
▼ Código

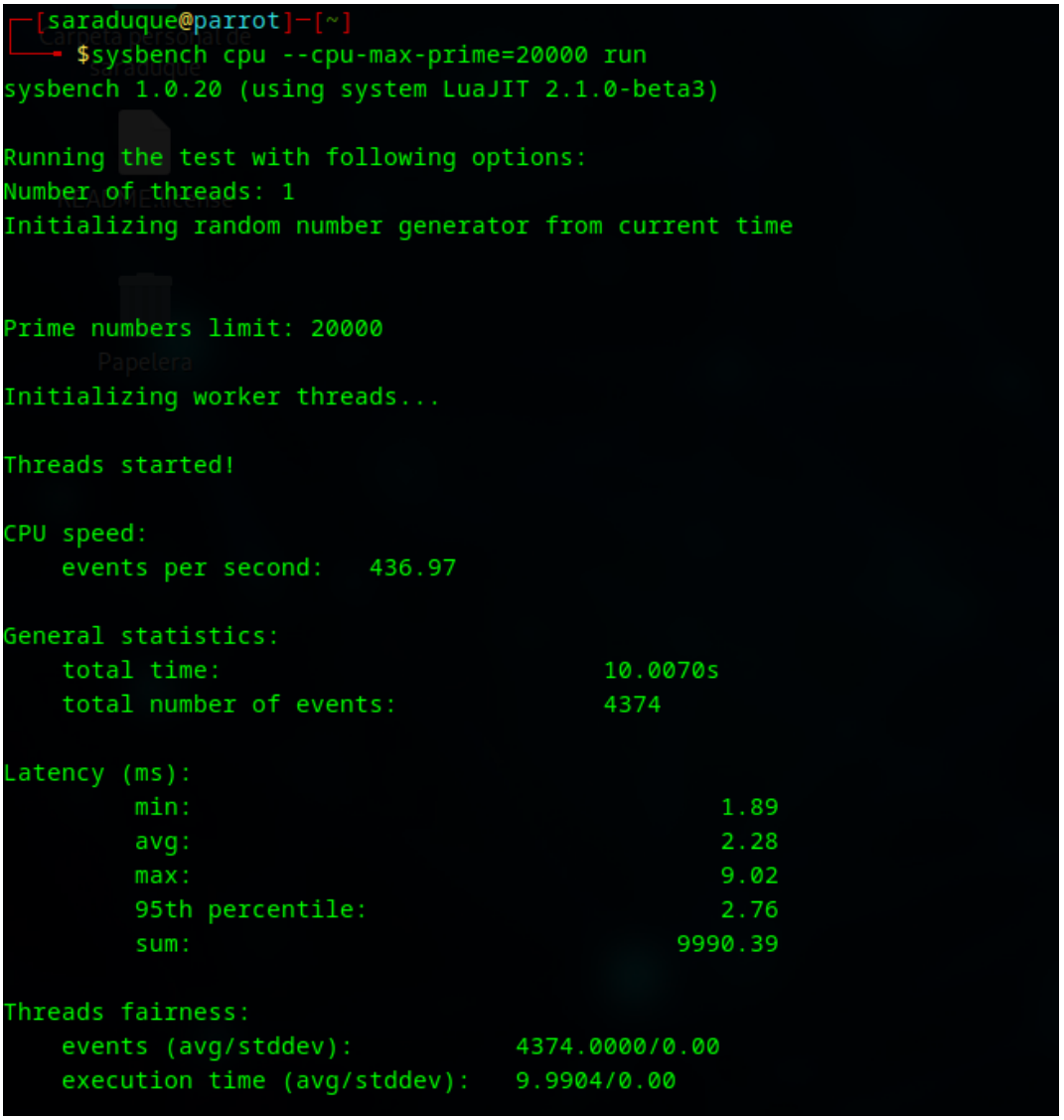
```
//Deshabilitar el inicio de sesión root mediante SSH m
PermitRootLogin no

//Mantén Kali actualizado
sudo apt install unattended-upgrades
sudo dpkg-reconfigure --priority=low unattended-upgrad

//Cortafuegos Firewall
sudo apt install ufw
sudo ufw enable
sudo ufw allow ssh
sudo ufw deny 80

//Cambia el puerto por defecto de SSH en /etc/ssh/sshd
Port 2222

//Deshabilita la autenticación por contraseña
PasswordAuthentication no

//Genera una clave SSH con
ssh-keygen -t rsa -b 4096

//Ajusta parámetros del kernel en /etc/sysctl.conf par
net.ipv4.tcp_syncookies = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.accept_redirects = 0
```

```
net.ipv4.conf.default.accept_redirects = 0

//Deshabilita USB automontado para evitar la ejecución
sudo apt install xscreensaver
```

▼ Capturas de pantalla




[saraduque@parrot]-[~]
$sysbench cpu --cpu-max-prime=20000 run
sysbench 1.0.20 (using system LuaJIT 2.1.0-beta3)
Running the test with following options:
Number of threads: 1
Initializing random number generator from current time
Prime numbers limit: 20000
Initializing worker threads...
Threads started!
CPU speed:
events per second: 411.68
General statistics:
total time: 10.0012s
total number of events: 4118
Latency (ms):
min: 1.89
avg: 2.43
max: 12.57
95th percentile: 3.07
sum: 9990.60
Threads fairness:
events (avg/stddev): 4118.0000/0.00
execution time (avg/stddev): 9.9906/0.00


[saraduque@parrot]-[~]
$sysbench cpu --cpu-max-prime=20000 run
sysbench 1.0.20 (using system LuaJIT 2.1.0-beta3)
Running the test with following options:
Number of threads: 1
Initializing random number generator from current time
Prime numbers limit: 20000
Initializing worker threads...
Threads started!
CPU speed:
events per second: 436.97
General statistics:
total time: 10.0070s
total number of events: 4374
Latency (ms):
min: 1.89
avg: 2.28
max: 9.02
95th percentile: 2.76
sum: 9990.39
Threads fairness:
events (avg/stddev): 4374.0000/0.00
execution time (avg/stddev): 9.9904/0.00