

Paso a Paso

1. Verificamos que python esté instalado.
2. Actualizamos la lista de paquetes disponibles y sus versiones en los repositorios configurados, pero no instala ni actualiza paquetes.
3. Descargamos e instalamos la versión de Python 3 disponible en los repositorios del sistema junto con sus dependencias.
4. Verificamos la versión de Python3
5. Instalamos pip, el gestor de paquetes para Python 3, que permite instalar y administrar librerías de Python.
6. Instalamos las herramientas necesarias para crear y gestionar entornos virtuales en Python 3.
7. Creamos un entorno virtual aislado llamado mi_entorno, donde podemos gestionar dependencias sin afectar el sistema global.
8. Activamos el entorno virtual mi_entorno, cambiando al entorno aislado para instalar y usar dependencias específicas.
9. Instalamos la librería Shodan para interactuar con la API de Shodan desde Python.
10. Creamos un archivo vacío llamado consulta_shodan.py en el directorio actual.
11. Abrimos el editor de texto Nano para crear el archivo consulta_shoda.py desde la terminal.
12. Abrimos el archivo de configuración del servidor SSH (sshd_config) en el editor de texto Nano con privilegios de administrador para editar su configuración.
13. Reiniciamos el servicio SSH en el sistema, aplicando cualquier cambio en su configuración.
14. Instalamos UFW (Uncomplicated Firewall), una herramienta para gestionar el firewall en sistemas basados en Linux.
15. Listamos los paquetes instalados en el sistema y filtra los que contienen "ufw" en su nombre o descripción.
16. Ejecutamos el script de Python consulta_shodan.py en el entorno de Python y obtenemos el tiempo de respuesta.
17. Permitimos el tráfico de la red para conexiones SSH a través del firewall UFW, habilitando el acceso remoto por SSH.
18. Establecemos la política predeterminada del firewall UFW para bloquear todo el tráfico entrante no autorizado.
19. Establecemos la política predeterminada del firewall UFW para bloquear todo el tráfico saliente no autorizado.
20. Deshabilitamos el servicio avahi-daemon, impidiendo que se inicie automáticamente al arrancar el sistema.
21. Deshabilitamos el servicio CUPS (sistema de impresión), evitando que se inicie automáticamente al arrancar el sistema.

Configuración en Parrot

```
[saraduque@parrot]~$ python --version
bash: python: Orden no encontrada
[saraduque@parrot]~$ sudo apt-get update
[sudo] contraseña para saraduque:
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
[saraduque@parrot]~$ sudo apt-get install python3
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
python3 ya está en su versión más reciente (3.11.2-1+b1).
fijado python3 como instalado manualmente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 157 no actualizados.
[saraduque@parrot]~$ python3 --version
Python 3.11.2
[saraduque@parrot]~$ sudo apt-get install python3-pip
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
python3-pip ya está en su versión más reciente (23.0.1+dfsg-1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 157 no actualizados.
```

```
[x]-[saraduque@parrot]-[~]
└─$ sudo apt-get install python3-venv
  car en el chat
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
python3-venv ya está en su versión más reciente (3.11.2-1+b1).
fijado python3-venv como instalado manualmente arte
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 157 no actualizados.
[saraduque@parrot]-[~]
└─$ ls
Descargas Desktop Documentos Imágenes Música Público Templates Vídeos
[saraduque@parrot]-[~]
└─$ cd 2024-1/cmll -miércoles
.BurpSuite/.config/Avo/Descargas/.Documentos/jp.java/.local/.msf4/Público/Vídeos/
.cache/.dbeaver4/Desktop/Imágenes/.kde/.mozilla/Música/Templates/
[saraduque@parrot]-[~]
└─$ cd Documentos/
[saraduque@parrot]-[~/Documentos] ANDRES MARIN LOPERA: Buenos días muchachos. Estoy es perdiendo que me habiliten acc...
└─$ $ python -m venv mi_entorno
bash: python: orden no encontrada
[saraduque@parrot]-[~/Documentos]
└─$ python3 -m venv mi_entorno
[saraduque@parrot]-[~/Documentos]
└─$ source mi_entorno/bin/activate
(mi_entorno) [saraduque@parrot]-[~/Documentos]
└─$ pip install shodan
  las profe, profe ¿que temas entran para este primer parcial del jueves en gestión de proyectos?
Collecting shodan
  Downloading shodan-1.31.0.tar.gz (57 kB)
    57.9/57.9 kB 1.6 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Collecting XlsxWriter
  Downloading XlsxWriter-3.2.0-py3-none-any.whl (159 kB)
    159.0/159.0 kB 5.0 MB/s eta 0:00:00
[saraduque@parrot]-[~/Documentos]
```

```
(mi_entorno) [saraduque@parrot]-[~/Documentos]
└─$ touch consulta_shodan.py
  TU: Buenos días profe, profe ¿que temas entran para e...
(mi_entorno) [saraduque@parrot]-[~/Documentos]
└─$ nano consulta_shodan.py
  ANDRES MARIN LOPERA, JACKSON LEONARDO, JUAN DIEGO, ...
(mi_entorno) [saraduque@parrot]-[~/Documentos]
└─$ nano consulta_shodan.py
  LORENZO JOSE MOTA GARCIA
```

```

● ● ●

1 import shodan
2 import time
3
4 SHODAN_API_KEY = 'xcWxcPC2dEz81ZKn5ZpRVKpy7uBCfcUc'
5 api = shodan.Shodan(SHODAN_API_KEY)
6
7 def medir_tiempo_consulta(query):
8     inicio = time.time()
9     try:
10         resultados = api.search(query)
11     except shodan.APIError as e:
12         print(f"Error en la consulta: {e}")
13     fin = time.time()
14     return fin - inicio
15
16 query = 'apache'
17 tiempo_respuesta = medir_tiempo_consulta(query)
18 print(f"Tiempo de respuesta: {tiempo_respuesta:.2f} segundos")

```

```

(mi_entorno) └─[saraduque@parrot]─[~/Documentos]
└─ $python consulta_shodan.py
Error en la consulta: Access denied (403 Forbidden)
Tiempo de respuesta: 0.71 segundos
(mi_entorno) └─[saraduque@parrot]─[~/Documentos]
└─ $

```

```

(mi_entorno) └─[saraduque@parrot]─[~/Documentos]
└─ $sudo nano /etc/ssh/sshd_config

```

```

(mi_entorno) └─[saraduque@parrot]─[~/Documentos]
└─ $sudo systemctl restart ssh
(mi_entorno) └─[saraduque@parrot]─[~/Documentos]
└─ $sudo apt-get install ufw
Leyendo lista de paquetes... Hecho MARIN LOPERA: Buenos días muchachos. Estoy es perando que me habiliten acc...
Creando árbol de dependencias... Hecho LOPERA
Leyendo la información de estado... Hecho
ufw ya está en su versión más reciente (0.36.2-1).
fijado ufw como instalado manualmente.
          https://www.microsoft.com/en-us/collections/qdn3cg01zk10d7sharingId=81BD9974A8BFFD25&WT.mc_id=cloud...
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 157 no actualizados.
(mi_entorno) └─[saraduque@parrot]─[~/Documentos]
└─ $sudo ufw status
Status: inactive
          Atención M CESPEDESTRO
          Un luengos de proto, proto, que temas entra para este primer parcial del jueves en gestión de proyectos?
(mi_entorno) └─[saraduque@parrot]─[~/Documentos]
└─ $dpkg -l | grep ufw
          JUAN DIEGO, JACKSON LEONARDO, JUAN DIEGO, ...
ii  gufw                         2024-1-Gmail...          22.04.0-1           all      graphical user interface for ufw
ii  ufw                          2024-1-Gmail...          0.36.2-1            all      program for managing a Netfilter firewall

```

```
(mi_entorno) [saraduque@parrot]-(~/Documentos]
└─ $sudo ufw allow ssh
Rules updatedcio
Rules updated (v6)
(mi_entorno) [saraduque@parrot]-(~/Documentos]
└─ $ping google.com
PING google.com (142.250.78.78) 56(84) bytes of data.
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=1 ttl=255 time=24.1 ms
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=2 ttl=255 time=19.3 ms
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=3 ttl=255 time=17.8 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2012ms
rtt min/avg/max/mdev = 17.801/20.401/24.056/2.660 ms
(mi_entorno) [saraduque@parrot]-(~/Documentos]nas días muchachos. Estoy esperando que me habiliten acc...
└─ $sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
(mi_entorno) [saraduque@parrot]-(~/Documentos]
└─ $ping google.com
PING google.com (142.250.78.46) 56(84) bytes of data.
64 bytes from bog02s15-in-f14.1e100.net (142.250.78.46): icmp_seq=1 ttl=255 time=31.5 ms
64 bytes from bog02s15-in-f14.1e100.net (142.250.78.46): icmp_seq=2 ttl=255 time=18.8 ms
^C
CATALINA M CESPEDES TORO
--- google.com ping statistics 
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 18.781/25.149/31.518/6.368 ms
```

```
(mi_entorno) [saraduque@parrot]-(~/Documentos]
└─ $ufw default deny outgoing
bash: ufw: orden no encontrada
(mi_entorno) [x]-[saraduque@parrot]-(~/Documentos]
└─ $sudo ufw default deny outgoing
Default outgoing policy changed to 'deny'
(be sure to update your rules accordingly)
(mi_entorno) [saraduque@parrot]-(~/Documentos]
└─ $ping google.com
PING google.com (142.250.78.78) 56(84) bytes of data.
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=1 ttl=255 time=20.3 ms
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=2 ttl=255 time=17.5 ms
64 bytes from bog02s16-in-f14.1e100.net (142.250.78.78): icmp_seq=3 ttl=255 time=18.9 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2009ms
rtt min/avg/max/mdev = 17.485/18.892/20.304/1.150 ms
```

```
(mi_entorno) [saraduque@parrot]-(~/Documentos]
└─ $python consulta_shodan.py
Error en la consulta: Access denied (403 Forbidden)
Tiempo de respuesta: 2.56 segundos
```

Configuración en Kodachi

```
[15:10:18] kodachi@Secure-OS:~$ cd Documents
[15:10:28] kodachi@Secure-OS:~/Documents $ python3 -m venv mi_entorno
[15:11:17] kodachi@Secure-OS:~/Documents $ source mi_entorno/bin/activate
(mi_entorno) [15:11:51] kodachi@Secure-OS:~/Documents $ pip install shodan
Collecting shodan
  Downloading https://files.pythonhosted.org/packages/c5/06/c6dcc975a1e7d89bc7648e7f1acd2ab63df28/shodan-1.31.0.tar.gz (57kB)
    100% |██████████| 61kB 266kB/s
Collecting XlsxWriter (from shodan)
  Downloading https://files.pythonhosted.org/packages/a7/ea/53d1fe468e63e092cf16d12d6a66e0d7f0d02/XlsxWriter-3.2.0-py3-none-any.whl (159kB)
    100% |██████████| 163kB 588kB/s
Collecting click (from shodan)
  Downloading https://files.pythonhosted.org/packages/4a/a8/0b2ced25639fb20cc1c9
```

```
(mi_entorno) [15:12:30] kodachi@Secure-OS:~/Documents $ touch consulta_shodan.py
(mi_entorno) [15:12:56] kodachi@Secure-OS:~/Documents $ ls
consulta_shodan.py  mi_entorno
(mi_entorno) [15:12:59] kodachi@Secure-OS:~/Documents $ nano consulta_shodan.py
```

```
(mi_entorno) [15:15:47] kodachi@Secure-OS:~/Documents $ python consulta_shodan.py
Error en la consulta: Access denied (403 Forbidden)
Tiempo de respuesta: 1.19 segundos
(mi_entorno) [15:15:52] kodachi@Secure-OS:~/Documents $ python consulta_shodan.py
Error en la consulta: Access denied (403 Forbidden)
Tiempo de respuesta: 1.20 segundos
```

```
(mi_entorno) [15:16:20] kodachi@Secure-OS:~/Documents $ sudo nano /etc/ssh/sshd_config
(mi_entorno) [15:19:04] kodachi@Secure-OS:~/Documents $ ping google.com
PING google.com (216.58.212.238) 56(84) bytes of data.
64 bytes from ams16s22-in-f238.1e100.net (216.58.212.238): icmp_seq=1 ttl=116 time=173 ms
64 bytes from ams16s22-in-f238.1e100.net (216.58.212.238): icmp_seq=2 ttl=116 time=169 ms
64 bytes from ams16s22-in-f238.1e100.net (216.58.212.238): icmp_seq=3 ttl=116 time=171 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 169.135/171.237/173.556/1.842 ms
(mi_entorno) [15:19:18] kodachi@Secure-OS:~/Documents $ sudo systemctl restart ssh
```

```
(mi_entorno) [15:19:56] kodachi@Secure-OS:~/Documents $ sudo apt-get install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version (0.36-0ubuntu0.18.04.2).
0 upgraded, 0 newly installed, 0 to remove and 28 not upgraded.
1 not fully installed or removed.
After this operation, 0 B of additional disk space will be used.
Do you want to continue? [Y/n] y
Setting up cups-browsed (1.20.2-0ubuntu3.3) .
```

```
(mi_entorno) [15:20:33] kodachi@Secure-OS:~/Documents $ dpkg -l | grep ufw
ii  gufw      all        graphical user interface for ufw
ii  ufw       all        program for managing a Netfilter firewall
```

```
(mi_entorno) [15:22:42] kodachi@Secure-OS:~/Documents $ sudo ufw allow ssh
Rules updated
Rules updated (v6)
(mi_entorno) [15:23:32] kodachi@Secure-OS:~/Documents $ ping google.com
PING google.com (216.58.212.238) 56(84) bytes of data.
64 bytes from ams16s22-in-f238.1e100.net (216.58.212.238): icmp_seq=1 ttl=116 time=171 ms
64 bytes from ams16s22-in-f238.1e100.net (216.58.212.238): icmp_seq=2 ttl=116 time=170 ms
64 bytes from ams16s22-in-f238.1e100.net (216.58.212.238): icmp_seq=3 ttl=116 time=170 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2019ms
rtt min/avg/max/mdev = 170.223/170.864/171.528/0.533 ms
(mi_entorno) [15:23:42] kodachi@Secure-OS:~/Documents $ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
(mi_entorno) [15:23:58] kodachi@Secure-OS:~/Documents $ sudo ufw default deny outgoing
Default outgoing policy changed to 'deny'
(be sure to update your rules accordingly)
```

```
(mi_entorno) [15:24:34] kodachi@Secure-OS:~/Documents $ sudo systemctl disable avahi-daemon
Synchronizing state of avahi-daemon.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable avahi-daemon
Removed /etc/systemd/system/dbus-org.freedesktop.Avahi.service.
Removed /etc/systemd/system/sockets.target.wants/avahi-daemon.socket.
(mi_entorno) [15:25:35] kodachi@Secure-OS:~/Documents $ ping google.com
PING google.com (216.58.212.238) 56(84) bytes of data.
64 bytes from ams16s22-in-f238.1e100.net (216.58.212.238): icmp_seq=1 ttl=116 time=174 ms
64 bytes from ams16s22-in-f238.1e100.net (216.58.212.238): icmp_seq=2 ttl=116 time=173 ms
64 bytes from ams16s22-in-f238.1e100.net (216.58.212.238): icmp_seq=3 ttl=116 time=176 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2102ms
rtt min/avg/max/mdev = 173.816/174.767/176.466/1.296 ms
(mi_entorno) [15:25:58] kodachi@Secure-OS:~/Documents $ sudo systemctl disable cups
Synchronizing state of cups.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable cups
Unit /etc/systemd/system/cups.service is masked, ignoring.
```

```
(mi_entorno) [15:27:44] kodachi@Secure-OS:~/Documents $ python consulta_shodan.py
Error en la consulta: Access denied (403 Forbidden).
Tiempo de respuesta: 2.21 segundos
```

Configuración en Kali-Linux

```
(mi_entorno)-(saraduque@kali-linux)-[~]
$ touch consulta_shodan.py

(mi_entorno)-(saraduque@kali-linux)-[~]
$ nano consulta_shodan.py
```

```
(mi_entorno)-(saraduque@kali-linux)-[~]
$ python consulta_shodan.py
Error en la consulta: Access denied (403 Forbidden)
Tiempo de respuesta: 0.55 segundos
```

```
(mi_entorno)-(saraduque㉿kali-linux)-[~]
└─$ sudo nano /etc/ssh/sshd_config
[sudo] password for saraduque:
(mi_entorno)-(saraduque㉿kali-linux)-[~]
└─$ sudo systemctl restart ssh
(mi_entorno)-(saraduque㉿kali-linux)-[~]
└─$ sudo apt-get install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
libverbs-providers libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0 libibverbs1 libpython3.11-dev librados2
librdmacm1t64 python3-libb2to3 python3.11 python3.11-dev python3.11-minimal samba-vfs-modules
```

```
GNU nano 8.1                                     /etc/ssh/sshd_config

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile    .ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
```

```
GNU nano 8.1                                         /etc/ssh/sshd_config

# some PAM modules and threads)
KbdInteractiveAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
# the setting of "PermitRootLogin prohibit-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
ClientAliveInterval 300
ClientAliveCountMax 0
#UseDNS no
#PidFile /run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none
```

```
└─(mi_entorno)─(saraduque㉿kali-linux)─[~]  
└─$ sudo ufw allow ssh
```

Rules updated

Rules updated (v6)

```
└─(mi_entorno)─(saraduque㉿kali-linux)─[~]  
└─$ sudo ufw default deny incoming
```

Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

```
└─(mi_entorno)─(saraduque㉿kali-linux)─[~]  
└─$ sudo ufw default deny outgoing
```

Default outgoing policy changed to 'deny'
(be sure to update your rules accordingly)

```
└─(mi_entorno)─(saraduque㉿kali-linux)─[~]  
└─$ sudo systemctl disable avahi-daemon
```