

TALLER: Hacking Ético

Luis Felipe Narváez Gómez. E-mail: luis.narvaez@usantoto.edu.co. Cod: 2312660. Facultad de Ingeniería de Sistemas.

Lo primero que debemos corroborar antes de hacer esta práctica es la conexión a la misma red de las maquinas, la maquina anfitrión Windows 10 y la Maquina Virtualizada Kali Linux. Para esto basta con ver la configuración de la conexión de red y compararla con la conexión en puente de la Máquina virtual en general de Virtual Box.

La Imagen de la izquierda es la información de la conexión de red de la Maquina anfitrión Windows 10 y la imagen de la derecha corresponde a la conexión de red del Virtual Boc para la maquina virtualizada Kali Linux.

Propiedades

Velocidad de vínculo (recepción/transmisión): 1000/1000 (Mbps)

Dirección IPv6 local de vínculo: fe80::f875:795c:71fd:af69%7

Dirección IPv4: 172.21.103.208

Servidores DNS IPv4: 200.14.205.2
200.14.207.210

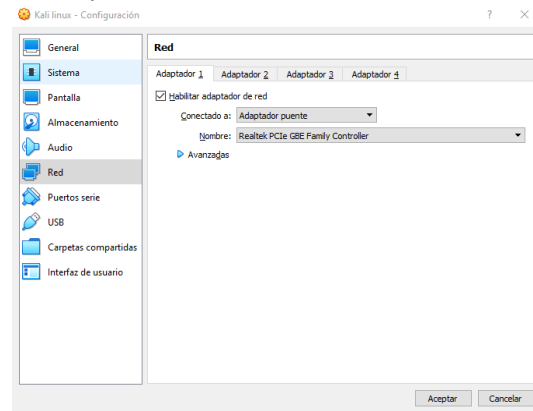
Fabricante: Realtek

Descripción: Realtek PCIe GBE Family Controller

Versión del controlador: 10.23.1003.2017

Dirección física (MAC): 54-E1-AD-AC-0A-94

Copiar



Una vez hecho esto confirmaremos que las IP correspondan a maquinas conectadas a la misma red y mandaremos ping entre ellas. Las configuraciones de red correspondientes son las siguientes:

```
C:\Users\ruiiso>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufixo DNS específico para la conexión. . . : fe80::f875:795c:71fd:af69%7
    Vínculo: dirección IPv6 local. . . . . : fe80::f875:795c:71fd:af69%7
    Dirección IPv4. . . . . : 172.21.103.208
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 172.21.103.1

Adaptador de Ethernet VirtualBox Host-Only Network:

    Sufixo DNS específico para la conexión. . . : fe80::b9f6:bce4:48e4:4d8d%12
    Vínculo: dirección IPv6 local. . . . . : fe80::b9f6:bce4:48e4:4d8d%12
    Dirección IPv4. . . . . : 192.168.56.1
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . :

Adaptador de LAN inalámbrica Conexión de área local* 1:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . . :

Adaptador de Ethernet Ethernet 2:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Wi-Fi 2:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . . :

Adaptador de Ethernet Conexión de red Bluetooth:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . . :

C:\Users\ruiiso>
```

```
(root@machineonruiiso)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.21.103.140 netmask 255.255.255.0 broadcast 172.21.103.255
    inet6 fe80::a00:27ff:fe07:df8 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:07:0d:f8 txqueuelen 1000 (Ethernet)
    RX packets 1071 bytes 105021 (102.5 KiB)
    RX errors 0 dropped 107 overruns 0 frame 0
    TX packets 15 bytes 1960 (1.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@machineonruiiso)-[~]
#
```

Ahora bien, comprobaremos la conexión entre maquinas utilizando el PING.

```
C:\Users\ruiiso>ping 172.21.103.208

Haciendo ping a 172.21.103.140 con 32 bytes de datos:
Respuesta desde 172.21.103.140: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.21.103.140: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.21.103.140: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.21.103.140: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 172.21.103.140:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\ruiiso>
```

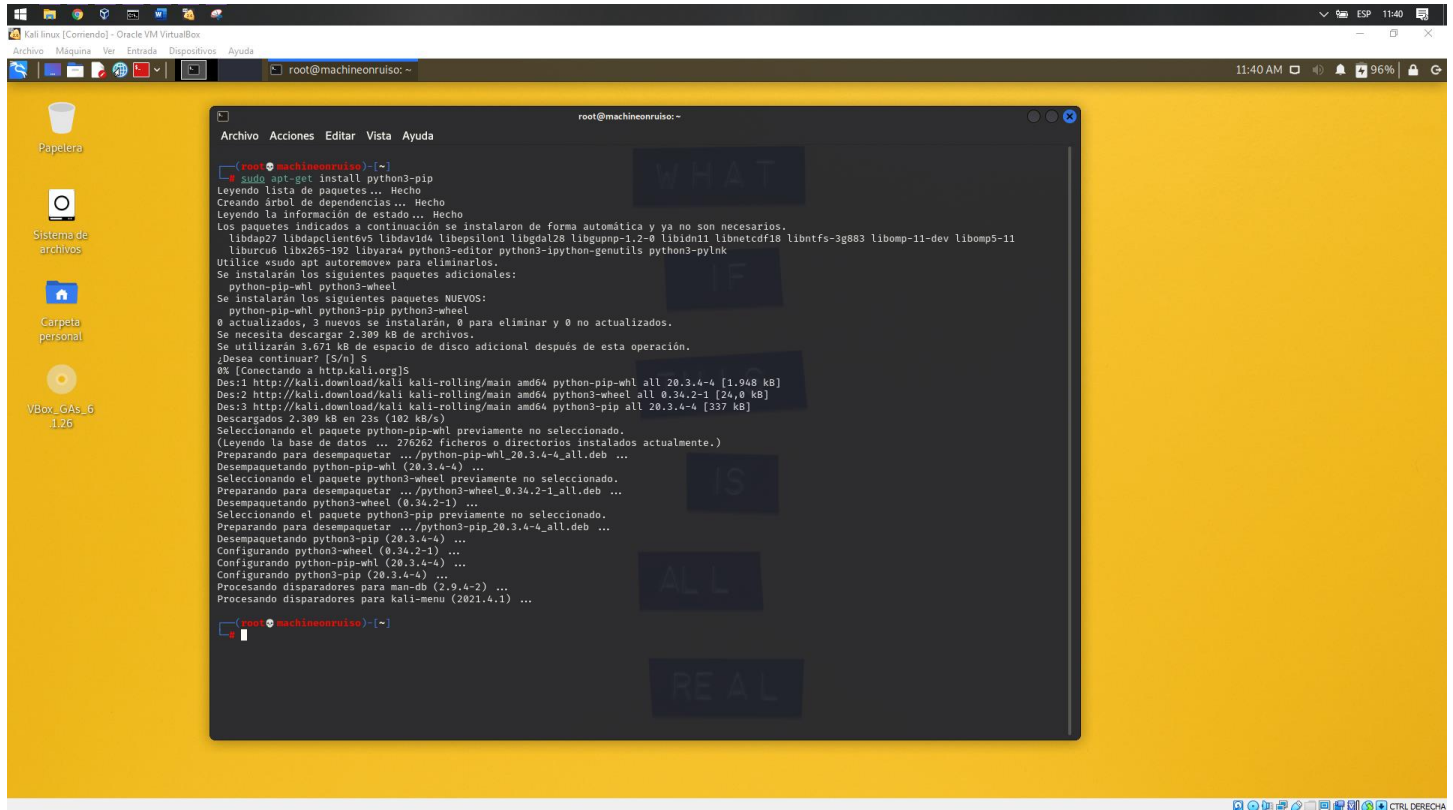
```
(root@machineonruiiso)-[~]
# ping 172.21.103.208
PING 172.21.103.208 (172.21.103.208) 56(84) bytes of data.
64 bytes from 172.21.103.208: icmp_seq=1 ttl=128 time=0.289 ms
64 bytes from 172.21.103.208: icmp_seq=2 ttl=128 time=0.302 ms
64 bytes from 172.21.103.208: icmp_seq=3 ttl=128 time=0.319 ms
64 bytes from 172.21.103.208: icmp_seq=4 ttl=128 time=0.312 ms
64 bytes from 172.21.103.208: icmp_seq=5 ttl=128 time=0.436 ms
64 bytes from 172.21.103.208: icmp_seq=6 ttl=128 time=0.307 ms
64 bytes from 172.21.103.208: icmp_seq=7 ttl=128 time=0.344 ms
^C
--- 172.21.103.208 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6138ms
rtt min/avg/max/mdev = 0.289/0.329/0.436/0.046 ms

(root@machineonruiiso)-[~]
#
```

SACANDO INTRUSOS EN LA RED

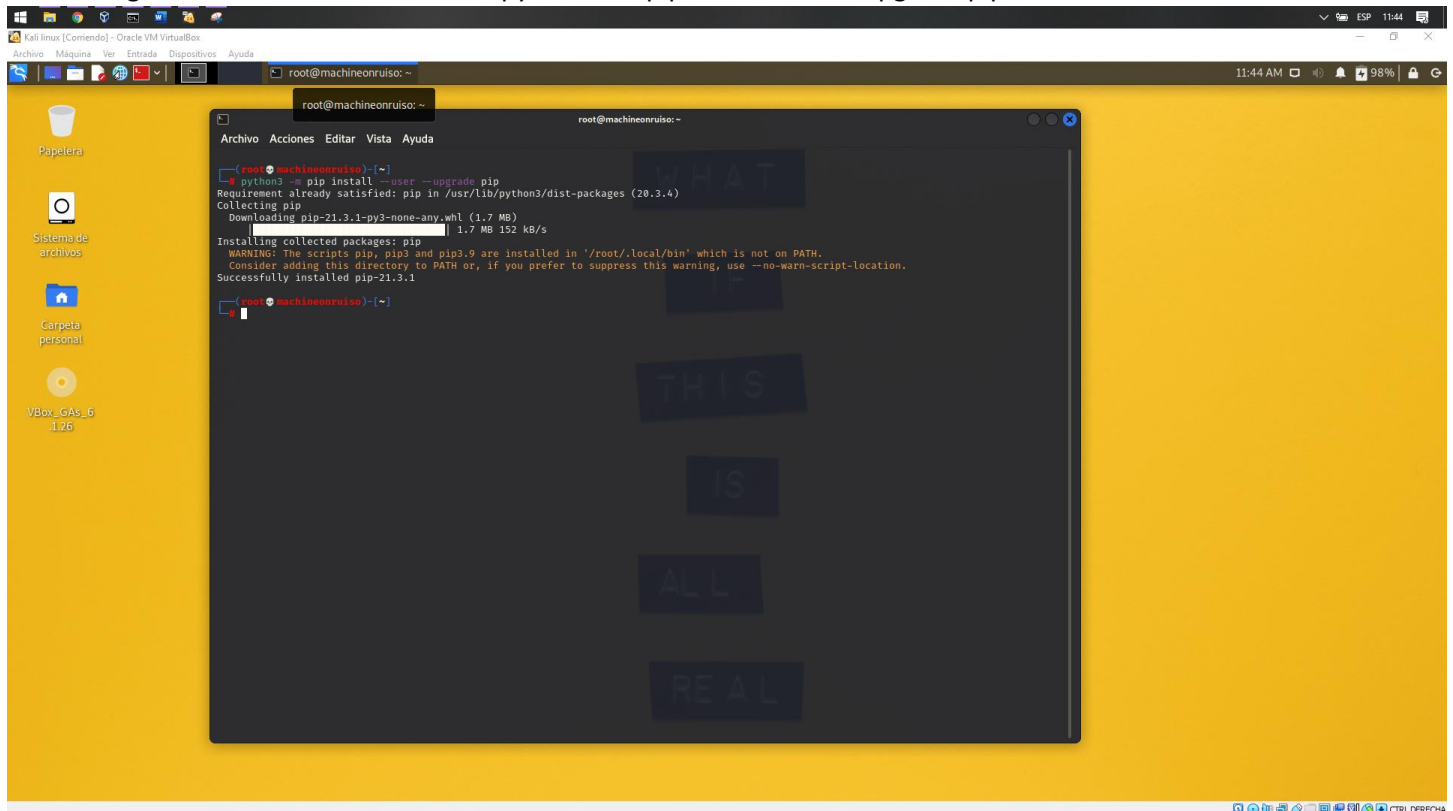
Para esta práctica utilizaremos la herramienta de KickThemOut, la cual esta desarrollada en Python y podemos ejecutar dentro de la consola con usuario root. Para ello primero debemos instalar Python en nuestro sistema y luego la herramienta.

Para instalar Python utilizaremos como primer comando: “sudo apt-get install python3-pip”.



```
root@machineonruiso: ~  
Archivo Acciones Editar Vista Ayuda  
root@machineonruiso:~# sudo apt-get install python3-pip  
Leyendo lista de paquetes ... Hecho  
Creando árbol de dependencias ... Hecho  
Leyendo la información de estado ... Hecho  
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.  
libdap27 libdapclientv5 libdav1d4 libepsilon1 libgdal28 libgpgme1.2-0 libidn11 libnetcdf18 libnftfs-3g83 libomp-11-dev libomp5-11  
libpcre3 libpcre3-b2 libpcre3-dev python3-editor python3-jupyterlab python3-pygments python3-pygments python3-pygments  
utilice «sudo apt autoremove» para eliminarlos.  
Se instalarán los siguientes paquetes adicionales:  
python3-pip python3-wheel  
Se instalarán los siguientes paquetes NUEVOS:  
python3-pip python3-wheel  
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 0 no actualizados.  
Se necesita descargar 2.309 kB de archivos.  
Se utilizarán 3.671 kB de espacio de disco adicional después de esta operación.  
¿Desea continuar? [S/n] S  
0% [Conectando a http://kali.org]  
Des:1 http://kali.download/kali kali-rolling/main amd64 python3-pip-whl all 20.3.4-4 [1.948 kB]  
Des:2 http://kali.download/kali kali-rolling/main amd64 python3-wheel all 0.34.2-1 [24.0 kB]  
Des:3 http://kali.download/kali kali-rolling/main amd64 python3-pip all 20.3.4-4 [337 kB]  
Descargados 2.309 kB en 23s (102 kB/s)  
Seleccionando el paquete python3-pip-whl previamente no seleccionado.  
(Leyendo la base de datos ... 276262 ficheros o directorios instalados actualmente.)  
Preparando para desempaquetar .../python3-pip-whl_20.3.4-4_all.deb ...  
Desempaquetando python3-pip-whl (20.3.4-4) ...  
Seleccionando el paquete python3-wheel previamente no seleccionado.  
Preparando para desempaquetar .../python3-wheel_0.34.2-1_all.deb ...  
Desempaquetando python3-wheel (0.34.2-1) ...  
Seleccionando el paquete python3-pip previamente no seleccionado.  
Preparando para desempaquetar .../python3-pip_20.3.4-4_all.deb ...  
Desempaquetando python3-pip (20.3.4-4) ...  
Configurando python3-wheel (0.34.2-1) ...  
Configurando python3-pip (20.3.4-4) ...  
Procesando disparadores para man-db (2.9.4-2) ...  
Procesando disparadores para kali-menu (2021.4.1) ...  
root@machineonruiso:~#
```

Y como segundo comando utilizaremos: “python3 -m pip install --user --upgrade pip”



```
root@machineonruiso: ~  
Archivo Acciones Editar Vista Ayuda  
root@machineonruiso:~# python3 -m pip install --user --upgrade pip  
Requirement already satisfied: pip in /usr/lib/python3/dist-packages (20.3.4)  
Collecting pip  
  Downloading pip-21.3.1-py3-none-any.whl (1.7 MB)  
    1.7 MB 152 kB/s  
Installing collected packages: pip  
WARNING: The scripts pip, pip3 and pip3.9 are installed in '/root/.local/bin' which is not on PATH.  
Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.  
Successfully installed pip-21.3.1  
root@machineonruiso:~#
```

Ahora instalemos la herramienta con los siguientes comandos:

~ >>> sudo apt-get update && sudo apt-get install nmap

```
(root@machineonruiso)-[~]
# sudo apt-get update && sudo apt-get install nmap
Des:1 http://kali.download/kali kali-rolling InRelease [30,6 kB]
Des:2 http://kali.download/kali kali-rolling/main Sources [14,3 MB]
Des:3 http://kali.download/kali kali-rolling/main amd64 Packages [18,0 MB]
Des:4 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [40,3 MB]
Descargados 72,5 MB en 34s (2.126 kB/s)
Leyendo lista de paquetes... Hecho
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
nmap ya está en su versión más reciente (7.91+dfsg1-1kali1).
fijado nmap como instalado manualmente.
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
 libdap27 libdapclient6v5 libdav1d4 libepsilon1 libgdal28 libgupnp-1.2-0 libidn11 libnetcdf18 libntfs-3g883 libomp-11-dev libomp5-11
 liburcu6 libx265-192 libyara4 python3-editor python3-ipython-genutils python3-pylnk
Utilice «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 3 no actualizados.

(root@machineonruiso)-[~]
#
```

~ >>> git clone <https://github.com/k4m4/kickthemout.git>

```
(root@machineonruiso)-[~]
# git clone https://github.com/k4m4/kickthemout.git
Clonando en 'kickthemout'...
remote: Enumerating objects: 610, done.
remote: Total 610 (delta 0), reused 0 (delta 0), pack-reused 610
Recibiendo objetos: 100% (610/610), 151.14 KiB | 51.00 KiB/s, listo.
Resolviendo deltas: 100% (353/353), listo.

(root@machineonruiso)-[~]
#
```

~ >>> cd kickthemout/

```
(root@machineonruiso)-[~]
# cd kickthemout

(root@machineonruiso)-[~/kickthemout]
#
```

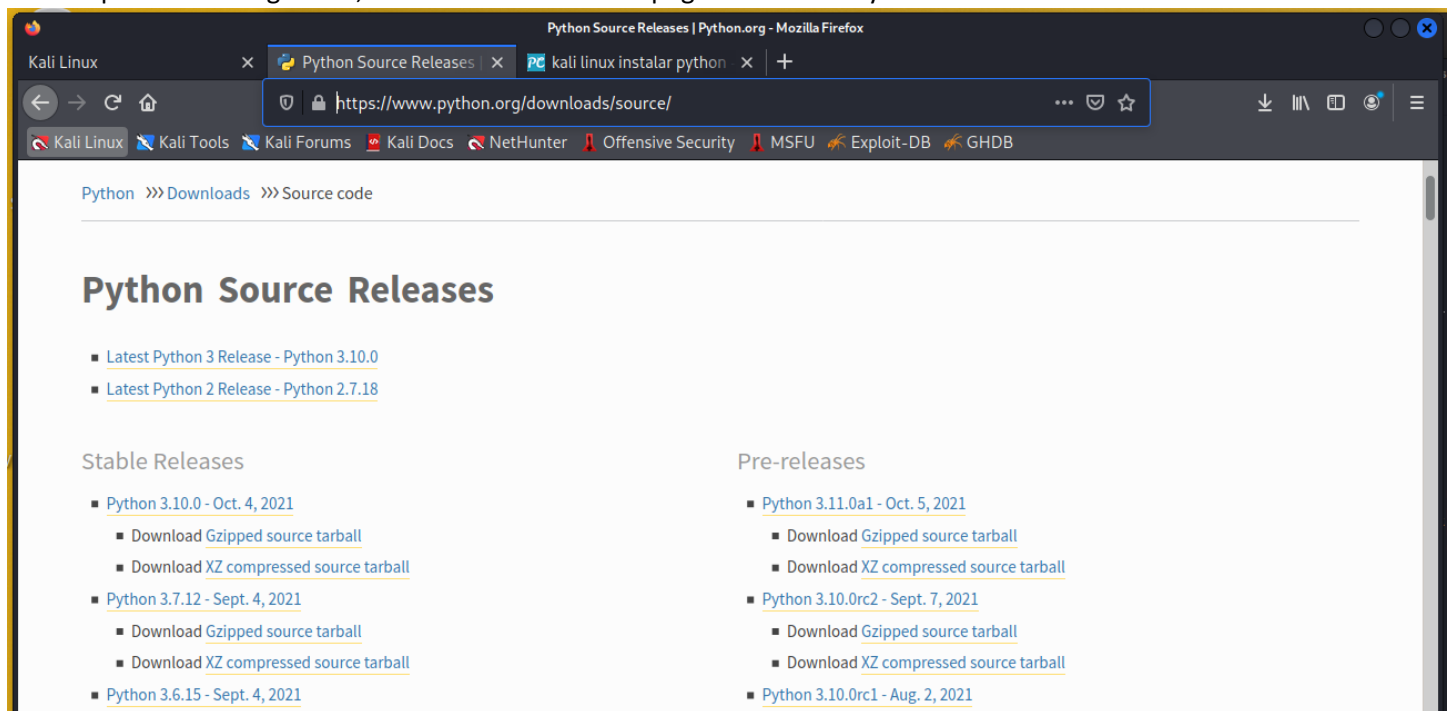
~/kickthemout >>> sudo -H pip3 install -r requirements.txt

```
(root@machineonruiso)-[~/kickthemout]
# sudo -H pip3 install -r requirements.txt
Requirement already satisfied: scapy in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (2.4.4)
Collecting python-nmap
  Downloading python-nmap-0.6.4.tar.gz (43 kB)
    | 43 kB 270 kB/s
  Preparing metadata (setup.py) ... done
Requirement already satisfied: netifaces in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (0.10.9)
Building wheels for collected packages: python-nmap
  Building wheel for python-nmap (setup.py) ... error
  ERROR: Command errored out with exit status 1:
   command: /usr/bin/python3 -u -c 'import io, os, sys, setuptools, tokenize; sys.argv[0] = '''/tmp/pip-install-d8ztj996/python-nmap_5a84b4a3c47b4d08b0c400a0f7413a0d/setup.py'''; __file__ = '''/tmp/pip-install-d8ztj996/python-nmap_5a84b4a3c47b4d08b0c400a0f7413a0d/setup.py'''; f = getattr(tokenize, '''open''', open)(__file__) if os.path.exists(__file__) else io.StringIO(''''from setuptools import setup; setup()'''); code = f.read().replace(''''\\r\\n''', ''''\\n'''); f.close(); exec(compile(code, __file__, ''''exec'''))''' bdist_wheel -d /tmp/pip-wheel-uezahaz3
   cwd: /tmp/pip-install-d8ztj996/python-nmap_5a84b4a3c47b4d08b0c400a0f7413a0d/
  Complete output (2 lines):
  running bdist_wheel
  error: invalid truth value '3'

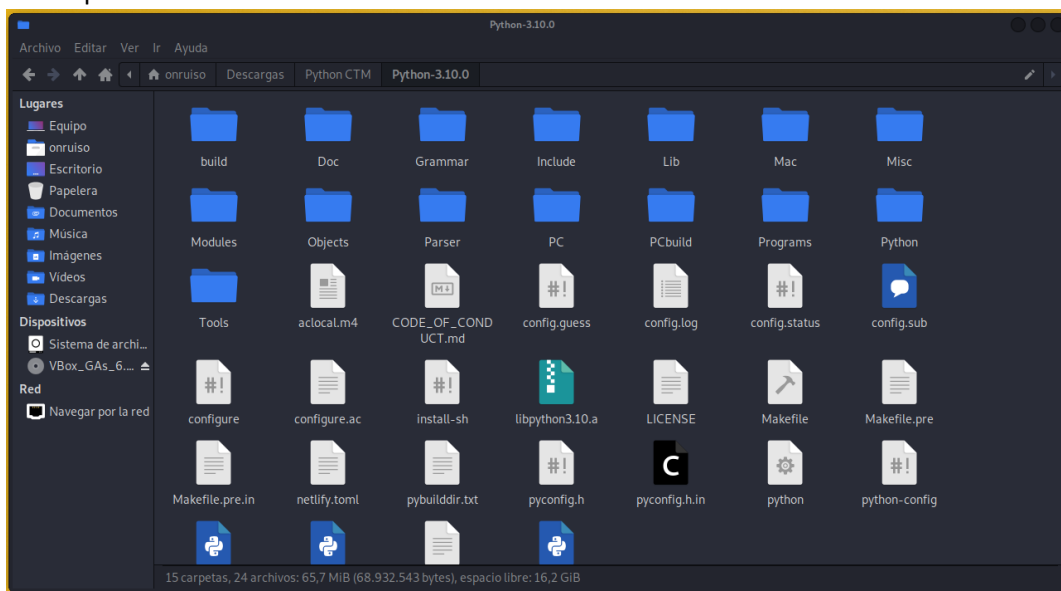
  ERROR: Failed building wheel for python-nmap
  Running setup.py clean for python-nmap
Failed to build python-nmap
Installing collected packages: python-nmap
  Running setup.py install for python-nmap ... done
  DEPRECATION: python-nmap was installed using the legacy 'setup.py install' method, because a wheel could not be built for it. A possible re
  placement is to fix the wheel build issue reported above. Discussion can be found at https://github.com/pyppa/pip/issues/8368
Successfully installed python-nmap-0.6.4
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is rec
ommended to use a virtual environment instead: https://pip.pyppa.io/warnings/venv

(root@machineonruiso)-[~/kickthemout]
#
```

Reintentemos instalar manualmente python para ver si se soluciona el problema que nos ha ocurrido con el archivo “setup.py”. Este paso es extra pero no estrictamente necesario, pues como podemos ver en el mensaje de Warning, la herramienta si se instaló. Bajaremos la última versión ESTABLE de Python para nuestra distribución o en su defecto la versión para Linux en general, esta se encuentra en la página oficial de Python.



Al bajar nuestro archivo comprimido de formato “tgz”, debemos descomprimirlo y acceder a la ruta de la carpeta, esta la podemos ver por el explorador de archivos de nuestro Kali Linux.



Para acceder a nuestra carpeta por la terminal podemos hacer un juego entre el comando “cd” y la descripción de carpetas que genera el comando “dir”.


```

(root@machineonruiso)~[~]
# cd ..

(root@machineonruiso)~[/]
# dir
bin dev home initrd.img.old lib32 libx32 media opt root sbin sys usr vmlinuz
boot etc initrd.img lib lib64 lost+found mnt proc run srv tmp var vmlinuz.old

(root@machineonruiso)~[/]
# cd home

(root@machineonruiso)~[/home]
# dir
onruiso

(root@machineonruiso)~[/home]
# cd onruiso

(root@machineonruiso)~[/home/onruiso]
# dir
Descargas Documentos Escritorio Imágenes Música Plantillas Público Videos

(root@machineonruiso)~[/home/onruiso]
# cd Descargas

(root@machineonruiso)~[/home/onruiso/Descargas]
# dir
pexels-aleksandar-pasaric-3280211.jpg pexels-cottonbro-8720593.jpg Python\ CTM Python-3.10.0.tgz

(root@machineonruiso)~[/home/onruiso/Descargas]
# cd Python\ CTM

(root@machineonruiso)~[/home/onruiso/Descargas/Python CTM]
# dir
Python-3.10.0

(root@machineonruiso)~[/home/onruiso/Descargas/Python CTM]
# cd Python-3.10.0

(root@machineonruiso)~[/home/onruiso/Descargas/Python CTM/Python-3.10.0]
# dir
aclocal.m4 config.sub Doc install-sh Mac Modules Parser Programs README.rst
CODE_OF_CONDUCT.md configure Grammar Lib Makefile.pre.in netlify.toml PC pyconfig.h.in setup.py
config.guess configure.ac Include LICENSE Misc Objects PCbuild Python Tools

```

Ahora que estamos dentro del directorio, podemos acceder a el archivo de configuración de Python.

```

(root@machineonruiso)~[/home/onruiso/Descargas/Python CTM/Python-3.10.0]
# ./configure --prefix=/usr/local/python-3.10.0
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking for python3.10... no
checking for python3... python3
checking for --enable-universalsdk... no
checking for --with-universal-archs... no
checking MACHDEP... "linux"
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
...
config.status: creating Modules/ld_so_aix
config.status: creating pyconfig.h
creating Modules/Setup.local
creating Makefile

If you want a release build with all stable optimizations active (PGO, etc),
please run ./configure --enable-optimizations

(root@machineonruiso)~[/home/onruiso/Descargas/Python CTM/Python-3.10.0]
#

```

Ahora procedemos a compilar.

```
(root@machineonruiso)-[/home/onruiso/Descargas/Python CTM/Python-3.10.0]
# make
gcc -pthread -c -Wno-unused-result -Wsign-compare -DNDEBUG -g -fwrapv -O3 -Wall -std=c99 -Wextra -Wno-unused-result -Wno-unused-parameter -Wno-missing-field-initializers -Werror=implicit-function-declaration -fvisibility=hidden -I./Include/internal -I. -I./Include -DPy_BUILD_CORE -o Programs/python.o ./Programs/python.c
gcc -pthread -c -Wno-unused-result -Wsign-compare -DNDEBUG -g -fwrapv -O3 -Wall -std=c99 -Wextra -Wno-unused-result -Wno-unused-parameter -Wno-missing-field-initializers -Werror=implicit-function-declaration -fvisibility=hidden -I./Include/internal -I. -I./Include -DPy_BUILD_CORE -o Parser/token.o Parser/token.c
gcc -pthread -c -Wno-unused-result -Wsign-compare -DNDEBUG -g -fwrapv -O3 -Wall -std=c99 -Wextra -Wno-unused-result -Wno-unused-parameter -Wno-missing-field-initializers -Werror=implicit-function-declaration -fvisibility=hidden -I./Include/internal -I. -I./Include -DPy_BUILD_CORE -o Parser/pegen.o Parser/pegen.c
gcc -pthread -c -Wno-unused-result -Wsign-compare -DNDEBUG -g -fwrapv -O3 -Wall -std=c99 -Wextra -Wno-unused-result -Wno-unused-parameter -Wno-missing-field-initializers -Werror=implicit-function-declaration -fvisibility=hidden -I./Include/internal -I. -I./Include -DPy_BUILD_CORE -o Programs/_testembed.o ./Programs/_testembed.c
gcc -pthread -Xlinker -export-dynamic -o Programs/_testembed Programs/_testembed.o libpython3.10.a -lcrypt -lpthread -ldl -lutil -lm -lm
sed -e "s,@EXENAME@,/usr/local/python-3.10.0/bin/python3.10," < ./Misc/python-config.in >python-config.py
LC_ALL=C sed -e "s,${\[[A-Za-z0-9_]*\)}\,${\{1\},g" < Misc/python-config.sh >python-config

...

Renaming build/scripts-3.10/pydoc3 to build/scripts-3.10/pydoc3.10
renaming build/scripts-3.10/idle3 to build/scripts-3.10/idle3.10
renaming build/scripts-3.10/2to3 to build/scripts-3.10/2to3-3.10
/usr/bin/install -c -m 644 ./Tools/gdb/libpython.py python-gdb.py
gcc -pthread -c -Wno-unused-result -Wsign-compare -DNDEBUG -g -fwrapv -O3 -Wall -std=c99 -Wextra -Wno-unused-result -Wno-unused-parameter -Wno-missing-field-initializers -Werror=implicit-function-declaration -fvisibility=hidden -I./Include/internal -I. -I./Include -DPy_BUILD_CORE -o Programs/_testembed.o ./Programs/_testembed.c
gcc -pthread -Xlinker -export-dynamic -o Programs/_testembed Programs/_testembed.o libpython3.10.a -lcrypt -lpthread -ldl -lutil -lm -lm
sed -e "s,@EXENAME@,/usr/local/python-3.10.0/bin/python3.10," < ./Misc/python-config.in >python-config.py
LC_ALL=C sed -e "s,${\[[A-Za-z0-9_]*\)}\,${\{1\},g" < Misc/python-config.sh >python-config

(root@machineonruiso)-[/home/onruiso/Descargas/Python CTM/Python-3.10.0]
#
```

Ahora instalemos la compilación.

```
(root@machineonruiso)-[/home/onruiso/Descargas/Python CTM/Python-3.10.0]
# make install
Creating directory /usr/local/python-3.10.0/bin
Creating directory /usr/local/python-3.10.0/lib
if test "no-framework" = "no-framework" ; then \
    /usr/bin/install -c python /usr/local/python-3.10.0/bin/python3.10; \
else \
    /usr/bin/install -c -s Mac/pythonw /usr/local/python-3.10.0/bin/python3.10; \
fi
if test "3.10" != "3.10"; then \
    if test -f /usr/local/python-3.10.0/bin/python3.10 -o -h /usr/local/python-3.10.0/bin/python3.10; \
    then rm -f /usr/local/python-3.10.0/bin/python3.10; \
    fi; \
    (cd /usr/local/python-3.10.0/bin; ln python3.10 python3.10); \
fi
if test "x" != "x" ; then \
    rm -f /usr/local/python-3.10.0/binpython3.10-32; \
    lipo \
        -output /usr/local/python-3.10.0/bin/python3.10-32 \
        /usr/local/python-3.10.0/bin/python3.10; \
fi

...

WARNING: Value for scheme.headers does not match. Please report this to <https://github.com/pypa/pip/issues/10151>
distutils: /usr/local/python-3.10.0/include/python3.10/UNKNOWN
sysconfig: /home/onruiso/Descargas/Python CTM/Python-3.10.0/Include/UNKNOWN
WARNING: Additional context:
user = False
home = None
root = '/'
prefix = None
Looking in links: /tmp/tmpm92gk_cv
Processing /tmp/tmpm92gk_cv/setuptools-57.4.0-py3-none-any.whl
Processing /tmp/tmpm92gk_cv/pip-21.2.3-py3-none-any.whl
Installing collected packages: setuptools, pip
WARNING: Value for scheme.headers does not match. Please report this to <https://github.com/pypa/pip/issues/10151>
distutils: /usr/local/python-3.10.0/include/python3.10/UNKNOWN
sysconfig: /home/onruiso/Descargas/Python CTM/Python-3.10.0/Include/setuptools
WARNING: Value for scheme.headers does not match. Please report this to <https://github.com/pypa/pip/issues/10151>
distutils: /usr/local/python-3.10.0/include/python3.10/pip
sysconfig: /home/onruiso/Descargas/Python CTM/Python-3.10.0/Include/pip
WARNING: The scripts pip3 and pip3.10 are installed in '/usr/local/python-3.10.0/bin' which is not on PATH.
Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
Successfully installed pip-21.2.3 setuptools-57.4.0
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv

(root@machineonruiso)-[/home/onruiso/Descargas/Python CTM/Python-3.10.0]
#
```

Con Python nuevamente instalado, podemos volver a probar la instalación de la herramienta.

```
(root@machineonruiso)-[~]
# cd kickthemout

(root@machineonruiso)-[~/kickthemout]
# sudo -H pip3 install -r requirements.txt
Requirement already satisfied: scrapy in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (2.4.4)
Requirement already satisfied: python-nmap in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (0.6.4)
Requirement already satisfied: netifaces in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (0.10.9)
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv

(root@machineonruiso)-[~/kickthemout]
#
```

Una vez instalada la herramienta de Kickthemout exitosamente, podemos ponerla en ejecución con el comando “sudo python3 kickthemout.py”, pero antes de ejecutarla debemos tener en cuenta la dirección IP y MAC de nuestro equipo, siendo esta nuestra maquina virtual Kali Linux, el comando utilizado es “ifconfig”.

```
(root@machineonruiso)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.21.103.140 netmask 255.255.255.0 broadcast 172.21.103.255
    inet6 fe80::a00:27ff:fe07:df8 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:07:0d:f8 txqueuelen 1000 (Ethernet)
    RX packets 10514 bytes 1030471 (1006.3 KiB)
    RX errors 0 dropped 993 overruns 0 frame 0
    TX packets 38 bytes 4186 (4.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@machineonruiso)-[~]
#
```

Ejecutando la herramienta tendríamos lo siguiente en la terminal:

```
(root@machineonruiso)-[~/kickthemout]
# sudo python3 kickthemout.py

ERROR: Gateway IP could not be obtained. Please enter IP manually.

kickthemout> Enter Gateway IP (e.g. 192.168.1.1):
```

Como podemos observar en nuestra consola, nos esta pidiendo un Gateway IP, esto hace referencia a nuestra dirección MAC, debemos escribirla a continuación.

```
(root@machineonruiso) ~/kickthemout
# sudo python3 kickthemout.py

ERROR: Gateway IP could not be obtained. Please enter IP manually.

kickthemout> Enter Gateway IP (e.g. 192.168.1.1): 172.21.103.140
Scanning your Network, hang on...
ERROR: Default Gateway MAC Address could not be obtained. Please enter MAC manually.

kickthemout> Enter your gateway's MAC Address (MM:MM:MM:SS:SS:SS): 172.21.103.140

      KICK THEM OUT

      Kick Devices Off Your LAN (KickThemOut)
      Made With <3 by: Nikolaos Kamarinakis (k4m4) & David Schütz (xdavidhu)
                        Version: 2.0

Using interface 'eth0' with MAC address '08:00:27:07:0d:f8'.
Gateway IP: '172.21.103.140' → 147 hosts are up.

Choose an option from the menu:

    [1] Kick ONE Off
    [2] Kick SOME Off
    [3] Kick ALL Off

    [E] Exit KickThemOut

kickthemout> 
```

Aquí lo que queremos hacer, es desconectar una IP en específico de la red, para ello seleccionamos la opción DOS denominada KICK SOME OFF, la cual desplegará una lista de los equipos que están conectados a nuestra red. Para desconectar un dispositivo bastaría solo con escribir el número que le corresponde en la lista que tenemos.

```
kickSOMEOff selected ...

Online IPs:
[0] 172.21.103.1      70:EA:1A:28:D9:CD      Cisco Systems, Inc (N/A)
[1] 172.21.103.16    0C:2F:80:E3:40:88      Samsung Electronics Co.,L (N/A)
[2] 172.21.103.24    00:02:D1:87:12:84      Vivotek, Inc. (N/A)
[3] 172.21.103.30    20:47:47:FF:D0:72      Dell Inc. (N/A)
[4] 172.21.103.32    F4:8E:38:DD:05:D0      Dell Inc. (N/A)
[5] 172.21.103.33    F4:8E:38:DE:0B:31      Dell Inc. (N/A)
[6] 172.21.103.34    F4:8E:38:DD:06:29      Dell Inc. (N/A)
[7] 172.21.103.41    00:17:C8:7D:1D:D6      KYOCERA Document Solution (N/A)

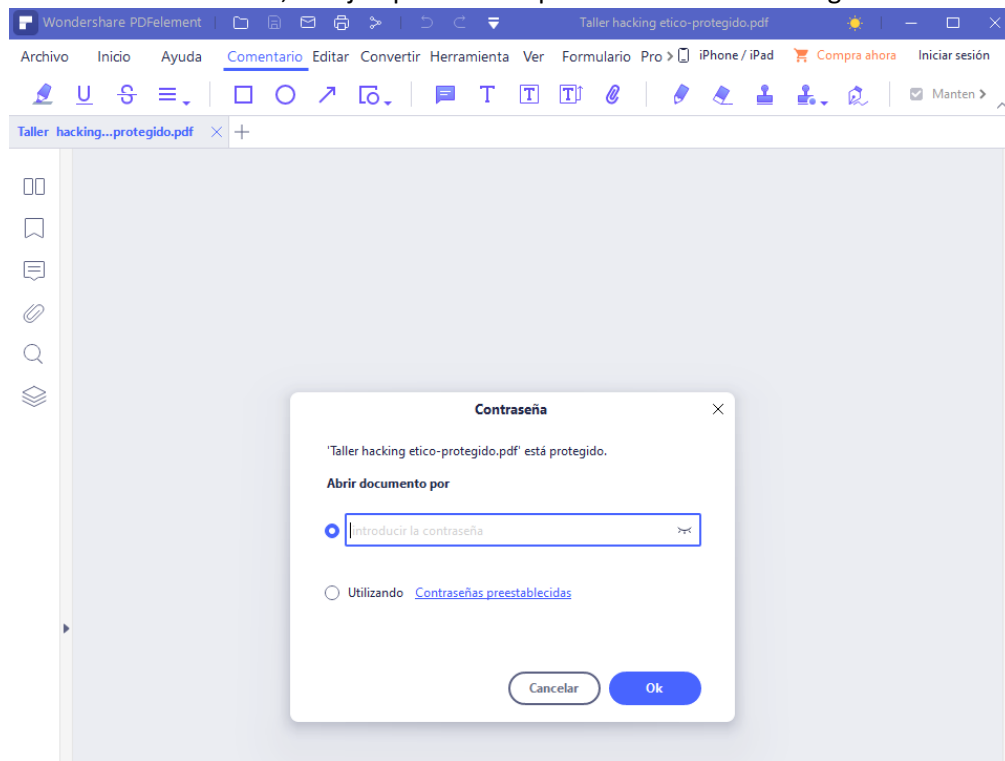
...

[137] 172.21.103.234 C8:1F:66:B6:D3:A2      Dell Inc. (N/A)
[138] 172.21.103.235 18:1D:EA:23:77:74      Intel Corporate (N/A)
[139] 172.21.103.236 B4:00:16:87:6F:21      INGENICO TERMINALS SAS (N/A)
[140] 172.21.103.238 C8:1F:66:B6:D7:51      Dell Inc. (N/A)
[141] 172.21.103.240 C8:1F:66:B6:CB:43      Dell Inc. (N/A)
[142] 172.21.103.242 48:F1:7F:8A:06:CE      Intel Corporate (N/A)
[143] 172.21.103.245 48:F1:7F:37:2D:0F      Intel Corporate (N/A)
[144] 172.21.103.248 18:1D:EA:22:0B:C8      Intel Corporate (N/A)
[145] 172.21.103.250 18:1D:EA:22:1B:54      Intel Corporate (N/A)
[146] 172.21.103.251 18:1D:EA:22:0A:6F      Intel Corporate (N/A)

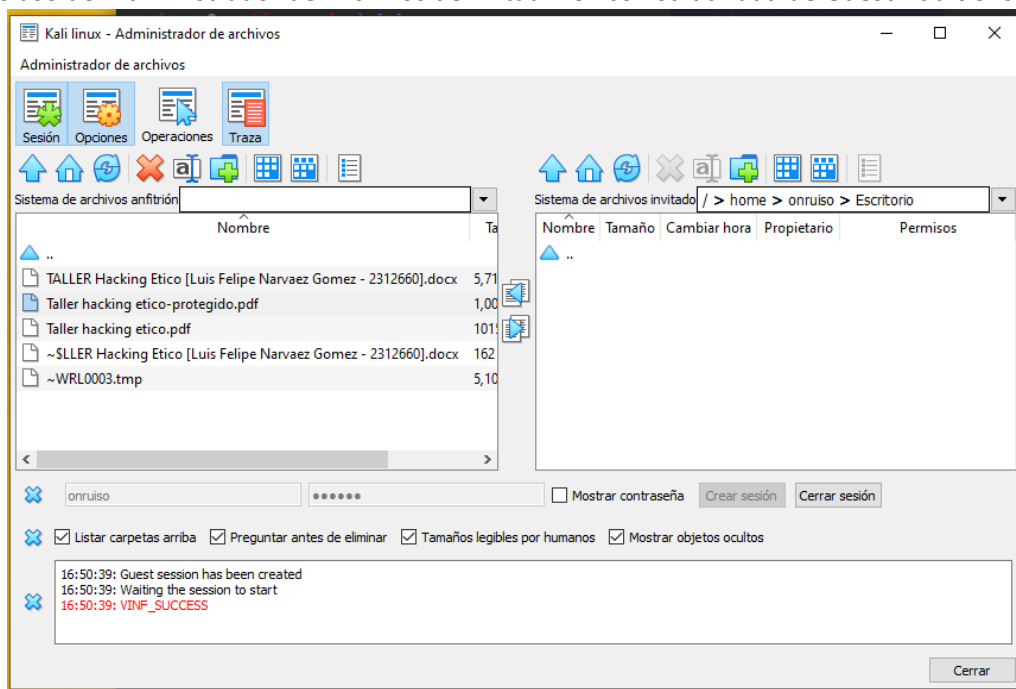
Choose devices to target (comma-separated): 
```


ABRIR UN PDF A FUERZA BRUTA

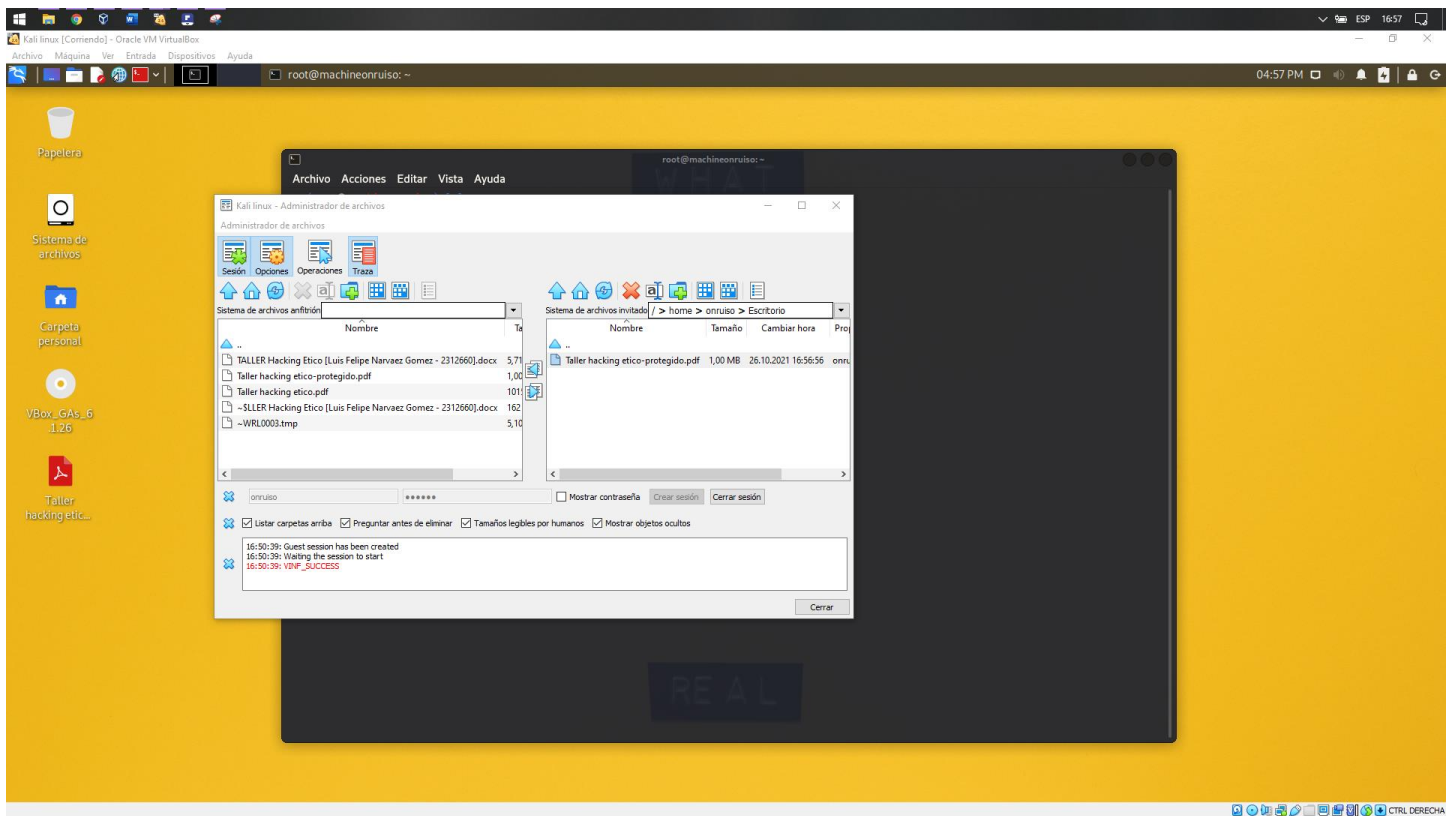
Lo que primero debemos tener para esta practica es un archivo en formato PDF que este protegido frente a lectura y escritura mediante el suso de contraseña, un ejemplo seria el que se muestra en la imagen.



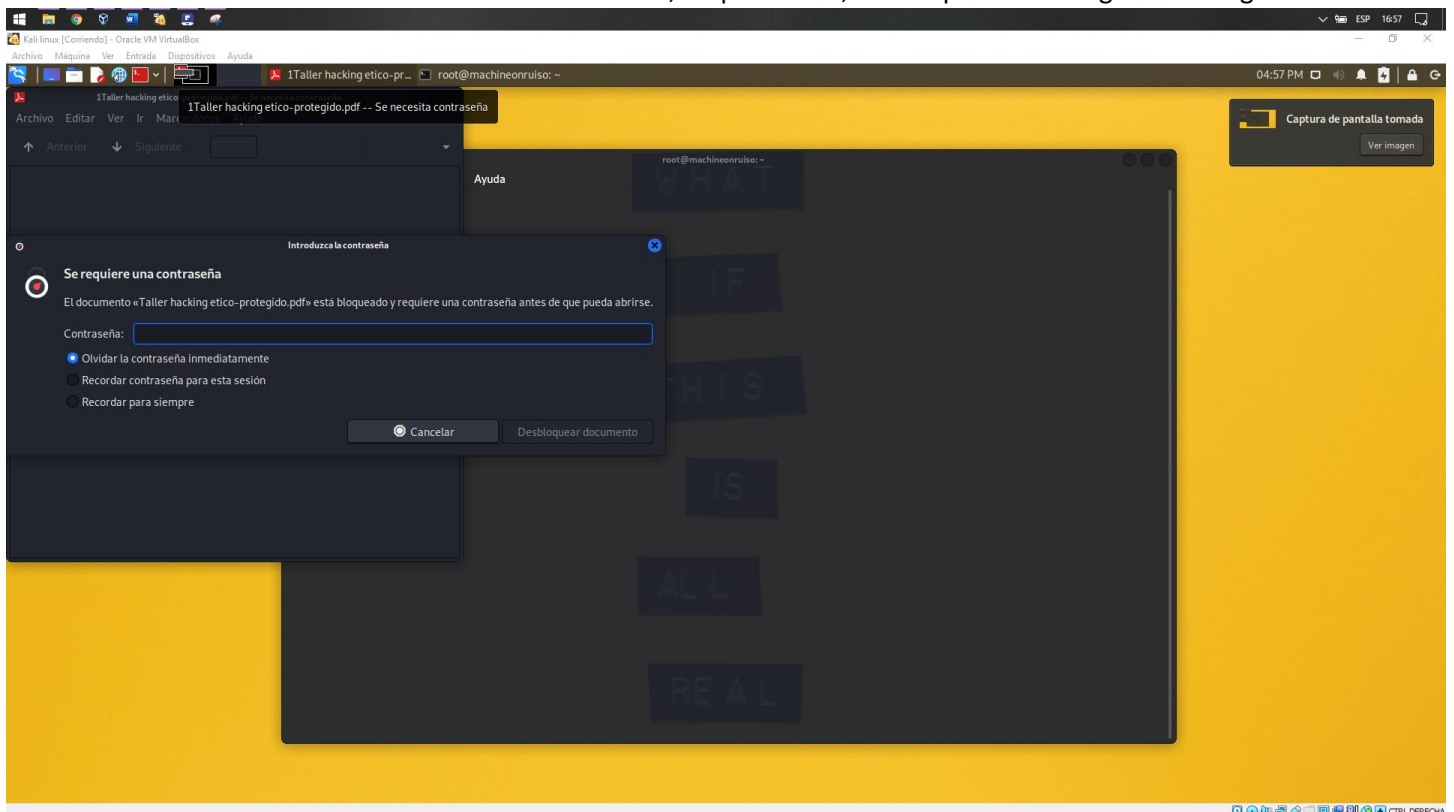
Este archivo se encuentra en la Maquina Anfitrión Windows 10 y debemos pasarlo a nuestra maquina virtual Kali Linux, para eso haremos uso del Administrador de Archivos de Virtual Box con su utilidad de Guest Additions.



Para que funcione nuestra transacción entre maquinas debemos tener en cuenta que hay que crear la sección en el Administrador de archivos de nuestra maquina virtualizada. Para ello ingresaremos las credenciales normales de ingreso en la parte inferior de la ventana, seguido de esto ubicaremos en ambos espacios tanto el archivo que queremos pasar como la ruta a donde que queremos pasarlo. Para pasarlo solo debemos seleccionar el archivo de origen e indicar con las flechas centrales el sentido en que se moverá (lo copiará en el destino) a su nuevo destino.



Si intentamos abrirlo sin la contraseña aun en Kali Linux, no podremos, como aparece en la siguiente imagen.



Ahora bien, hay varios métodos para poder obtener las credenciales o abrir sin ellas un PDF protegido por contraseña, la herramienta que utilizaremos es PDFCRACK, la cual, mediante el uso de fuerza bruta, probar una lista de caracteres u contraseñas cíclicamente hasta abrir el documento, lograr abrir el archivo que queremos. Lo primero será instalar la herramienta PDFCRACK con el comando “sudo apt-cache search pdfcrack” seguido del comando “sudo apt-get install pdfcrack”.

```
(root@machineonruiso)-[~]
# sudo apt-cache search pdfrack
forensics-extra - Forensics Environment - extra console components (metapackage)
pdfrack - PDF files password cracker

(root@machineonruiso)-[~]
#
```

```
(root@machineonruiso)-[~]
# sudo apt-get install pdfrack
Leyendo lista de paquetes ... Hecho
Creando árbol de dependencias ... Hecho
Leyendo la información de estado ... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
 libdap27 libdapclient6v5 libdav1d4 libepsilon1 libgdal28 libgupnp-1.2-0 libidn11 libnetcdf18 libntfs-3g883 libomp-11-dev libomp5-11 liburcu6
 libx265-192 libyara4 python3-editor python3-ipython-genutils python3-pylnk
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes NUEVOS:
 pdfrack
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
Se necesita descargar 36,0 kB de archivos.
Se utilizarán 93,2 kB de espacio de disco adicional después de esta operación.
Des:1 http://kali.download/kali kali-rolling/main amd64 pdfrack amd64 0.19-2 [36,0 kB]
Descargados 36,0 kB en 2s (21,4 kB/s)
Seleccionando el paquete pdfrack previamente no seleccionado.
(Leyendo la base de datos ... 276556 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../pdfrack_0.19-2_amd64.deb ...
Desempaquetando pdfrack (0.19-2) ...
Configurando pdfrack (0.19-2) ...
Procesando disparadores para man-db (2.9.4-2) ...
Procesando disparadores para kali-menu (2021.4.1) ...

(root@machineonruiso)-[~]
#
```

Ahora podemos hacer uso de la herramienta, hay varias formas de hacerlo, incluso poder acelerar la búsqueda, orientarla a trabajar con solo con números, limitar el numero de caracteres a probar, trabajar con un diccionario de claves, etc.

- Algunos ejemplos serian:
- Con diccionario de claves: "pdfrack -f "Old is gOld.pdf" -w /usr/share/wordlists/rockyou.txt"
- Aceleracion dando opciones de caracteres que puede llegar a tener: "pdfrack -f file.pdf -c abcdef123"
- Especificar que trabaje con números y con un limite de 11 digitos: "sudo pdfrack -f Extracto_Protección_S.A._202003_518113930.pdf -c 1234567890 -n 11"

```
(root@machineonruiso)-[/home/onruiso/Escritorio]
# pdfrack -f Taller\hacking\etico-protegido.pdf -c abcdefghijklmñopqrstuvwxyz1234567890
PDF version 1.6
Security Handler: Standard
V: 2
R: 3
P: -4
Length: 128
Encrypted Metadata: True
FileID: 2d29941b2042232da05bd2609eda61bf
U: 8e38aab93dfb96daf1b1cd7bda3d4d5028bf4e5e4e758a4164004e56fffa0108
O: e386b59a977eb504bef944276d6041a59f5b9590bc9a0df9da4f4a398f1f6612
Average Speed: 46990.4 w/s. Current Word: '33do'
Average Speed: 43035.5 w/s. Current Word: 'c624'
Average Speed: 46755.5 w/s. Current Word: 'ip4ka'
Average Speed: 46399.4 w/s. Current Word: '9d1za'
Average Speed: 46263.1 w/s. Current Word: '95ugb'
Average Speed: 46500.4 w/s. Current Word: '57svb'
Average Speed: 46596.4 w/s. Current Word: 'llscc'
Average Speed: 46191.7 w/s. Current Word: 'yc0rc'
Average Speed: 46511.2 w/s. Current Word: 'kkm9c'
Average Speed: 46550.2 w/s. Current Word: 'al0d'
Average Speed: 45917.5 w/s. Current Word: 'r0a5d'
Average Speed: 45561.2 w/s. Current Word: 'cbwke'
Average Speed: 46166.6 w/s. Current Word: 'kppze'
Average Speed: 46382.8 w/s. Current Word: 'j6ngf'
Average Speed: 46256.0 w/s. Current Word: 'rsivf'
Average Speed: 46015.7 w/s. Current Word: 'k60bg'
Average Speed: 45452.0 w/s. Current Word: 'ñtgq'
Average Speed: 44548.4 w/s. Current Word: '7037g'
Average Speed: 43921.8 w/s. Current Word: 'x13mh'
Average Speed: 44745.3 w/s. Current Word: '5qe2h'
Average Speed: 44464.8 w/s. Current Word: 'nmhi'
Average Speed: 44646.6 w/s. Current Word: 'uzuvi'
Average Speed: 45215.9 w/s. Current Word: 'o0ccj'
Average Speed: 45753.8 w/s. Current Word: 'y1qj'
Average Speed: 45148.2 w/s. Current Word: 'vai8j'
Average Speed: 44960.4 w/s. Current Word: '0zunk'
Average Speed: 44674.2 w/s. Current Word: 'yq62k'
Average Speed: 44629.8 w/s. Current Word: 'dwfil'
Average Speed: 45333.7 w/s. Current Word: '8rxwl'
Average Speed: 44681.5 w/s. Current Word: 'r9cm'
Average Speed: 45094.9 w/s. Current Word: 'y90rm'
Average Speed: 45235.2 w/s. Current Word: 'yq68m'
```

```
Average Speed: 45490.2 w/s. Current Word: '6sp0n'
Average Speed: 45369.5 w/s. Current Word: 't803n'
Average Speed: 44451.4 w/s. Current Word: 'cvhj0'
Average Speed: 44774.9 w/s. Current Word: '31rx0'
Average Speed: 45223.0 w/s. Current Word: '0eae0'
Average Speed: 45067.9 w/s. Current Word: 'nmos0'
Average Speed: 45811.4 w/s. Current Word: 'w4e0'
Average Speed: 45121.2 w/s. Current Word: 'w2t0'
found user-password: '578so'
```

```
root@machineonruiso:~/home/onruiso/Escritorio
```

Listo, hemos averiguado la contraseña, ahora a utilizarla y ver lo que contiene el archivo.

