

# kali-linux

## ¿Qué es kali-linux? ¿para que sirve?

---

Kali Linux es la versión mejorada y renovada de la distribución BackTrack, creada por Offensive Security. La distro se basa en Debian, mientras que Backtrack se fijó en Ubuntu para la creación de su programación.

Su principal objetivo es poner a disposición del usuario, las mejores herramientas para trabajar la auditoría en internet y contar con un potente sistema de seguridad informática ante los peligros que puedan existir.

## ¿En qué sistema operativo está basado?

---

distribución Linux y como antes mencionado versión mejorada y renovada de la distribución BackTrack

## ¿Qué herramientas incluyen?

AIRCRAK-NG

THC HYDRA

JOHN THE RIPPER

---

METASPLOIT FRAMEWORK

NETCAT

NMAP (“NETWORK MAPPER”)

NESSUS

WIRESHARK

SNORT

KISMET WIRELESS

FERN WIFI CRACKER

GNU MAC CHANGER

WIFITE2

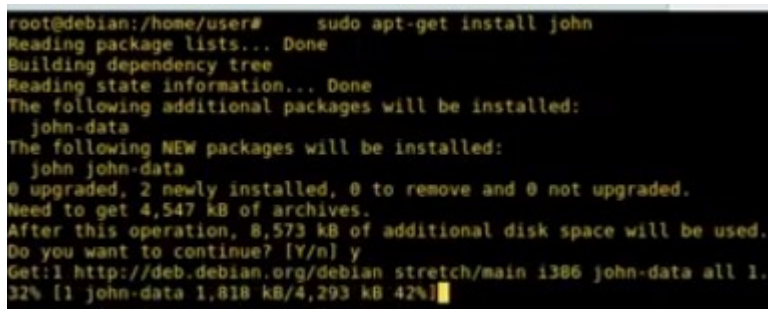
## Investiga al menos dos herramientas y documenta cómo emplearlas.

---

### JOHN THE RIPPER

John the Ripper es una herramienta popular de cracking utilizada en la comunidad de pruebas de penetración (y hacking). Inicialmente fue desarrollado para sistemas Unix, pero ha crecido para estar disponible en más de 10 distros.

Cuenta con un cracker personalizable, detección de hash de contraseña automática, ataque de fuerza bruta y ataque de diccionario (entre otros modos de cracking).



```
root@debian:/home/user# sudo apt-get install john
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  john-data
The following NEW packages will be installed:
  john john-data
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 4,547 kB of archives.
After this operation, 8,573 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian stretch/main i386 john-data all 1.
32% [1 john-data 1,818 kB/4,293 kB 42%]
```

A continuación veremos como descifrar la clave de un usuario

```
root@kali:~# useradd maria
root@kali:~# passwd maria
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
root@kali:~#
```

```
root@kali:~# unshadow /etc/passwd /etc/shadow > ataque
.txt
```

esto guarda la información y a continuación utilizamos john para crakear la contraseña

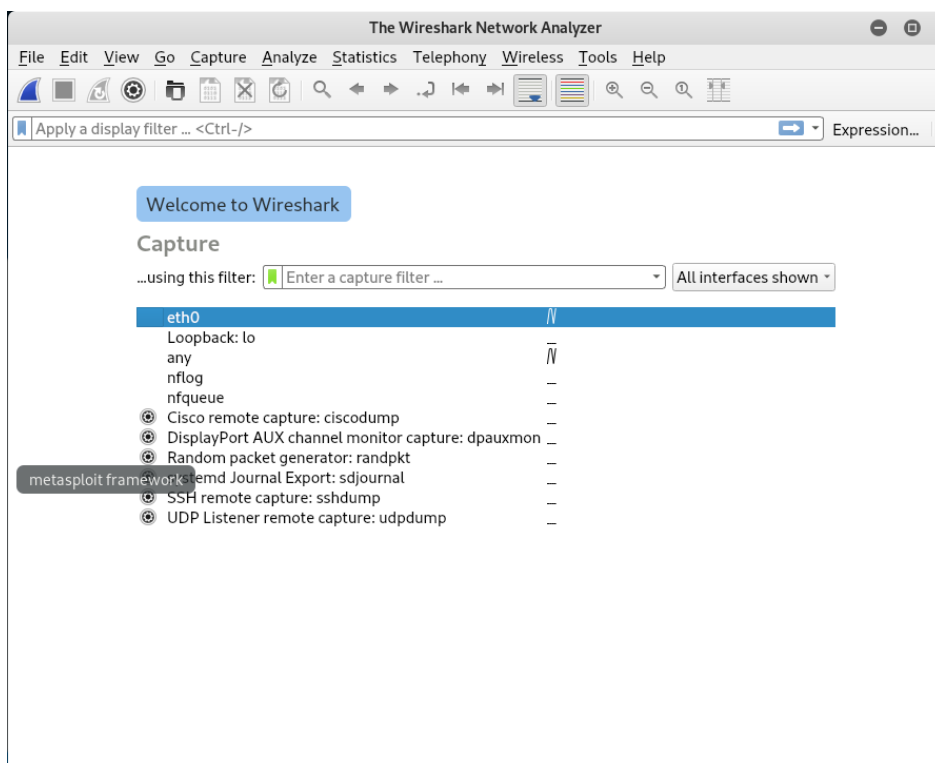
```
root@kali:~# john --format=sha512crypt ataque.txt
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Remaining 1 password hash
Press 'q' or Ctrl-C to abort, almost any other key for status
123 (maria)
lg 0:00:00:01 DONE 2/3 (2018-12-12 14:19) 0.7299g/s 65
5.4p/s 655.4c/s 655.4C/s 123456..green
Use the "--show" option to display all of the cracked
passwords reliably
Session completed
```

como se ve en la linea que empieza por 123 la contraseña crakeada es la de maria

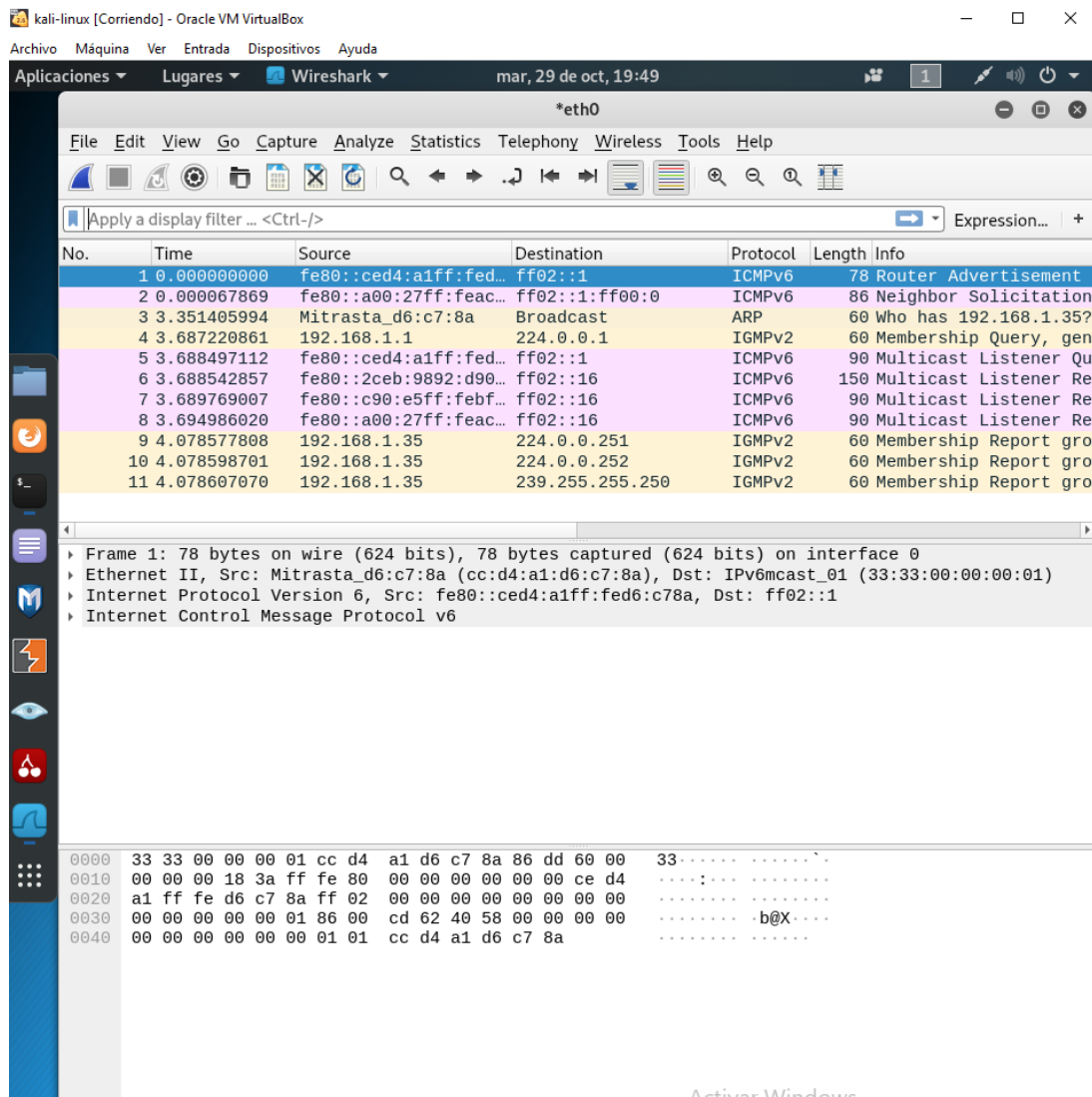
## WIRESHARK

Wireshark es un analizador de paquetes de fuente abierta que puedes usar sin cargo. Con él, puedes ver las actividades en una red desde un nivel microscópico junto con acceso a archivos pcap, informes personalizables, activadores avanzados, alertas, etc.

Se informa que es el analizador de protocolo de red más utilizado en el mundo para Linux.



Seleccionamos la tarjeta de red para proceder a trabajar con el programa



ahora podemos proceder al filtrado de paquetes arp por ejemplo

kali-linux [Corriendo] - Oracle VM VirtualBox

ArchivoMáquinaVerEntradaDispositivosAyuda

AplicacionesLugaresWiresharkmar, 29 de oct, 19:53

\*eth0

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

arp

Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
3	3.264527267	Mitrasta_d6:c7:8a	Broadcast	ARP	60	Who has 192.168.1.35?
17	13.859842817	HuaweiTe_6c:8b:48	Broadcast	ARP	60	Who has 192.168.1.1?
34	21.262004134	PcsCompu_ac:25:9f	Broadcast	ARP	42	Who has 192.168.1.1?
35	21.265875829	Mitrasta_d6:c7:8a	PcsCompu_ac:25:9f	ARP	60	192.168.1.1 is at cc:
151	26.284975660	Mitrasta_d6:c7:8a	Broadcast	ARP	60	Who has 192.168.1.39?
152	26.284988108	PcsCompu_ac:25:9f	Mitrasta_d6:c7:8a	ARP	42	192.168.1.39 is at 08
390	31.180859771	Mitrasta_d6:c7:8a	Broadcast	ARP	60	Who has 192.168.1.35?

Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

Ethernet II, Src: Mitrasta\_d6:c7:8a (cc:d4:a1:d6:c7:8a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

Wireshark

0000	ff ff ff ff ff ff cc d4 a1 d6 c7 8a 08 06 00 01	.....
0010	08 00 06 04 00 01 cc d4 a1 d6 c7 8a c0 a8 01 01	.....
0020	00 00 00 00 00 00 c0 a8 01 23 00 00 00 00 00 00	.....#.....
0030	00 00 00 00 00 00 00 00 00 00 00 00	.....

Activar Windows

Ve a Configuración para activar Windows.