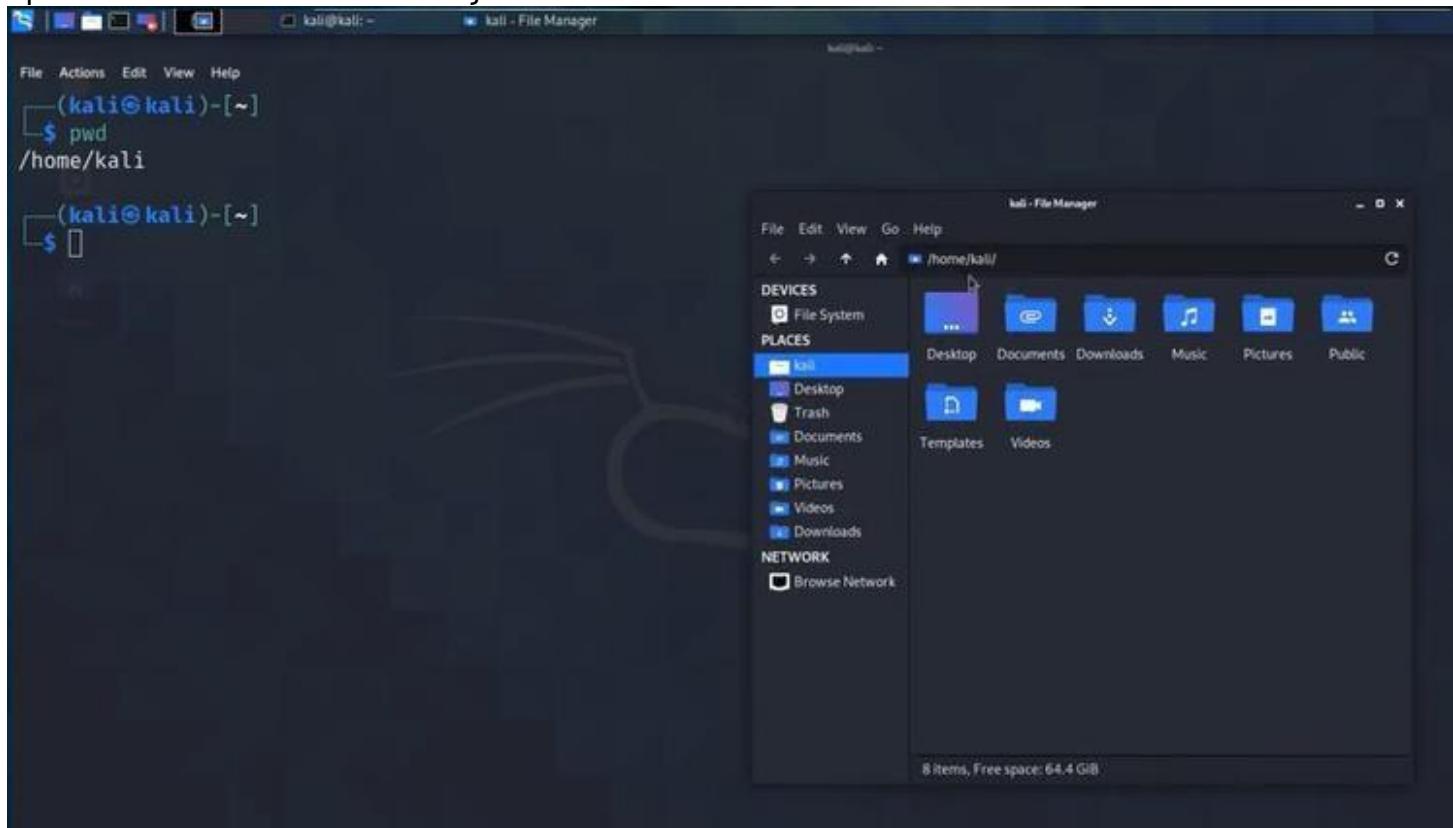
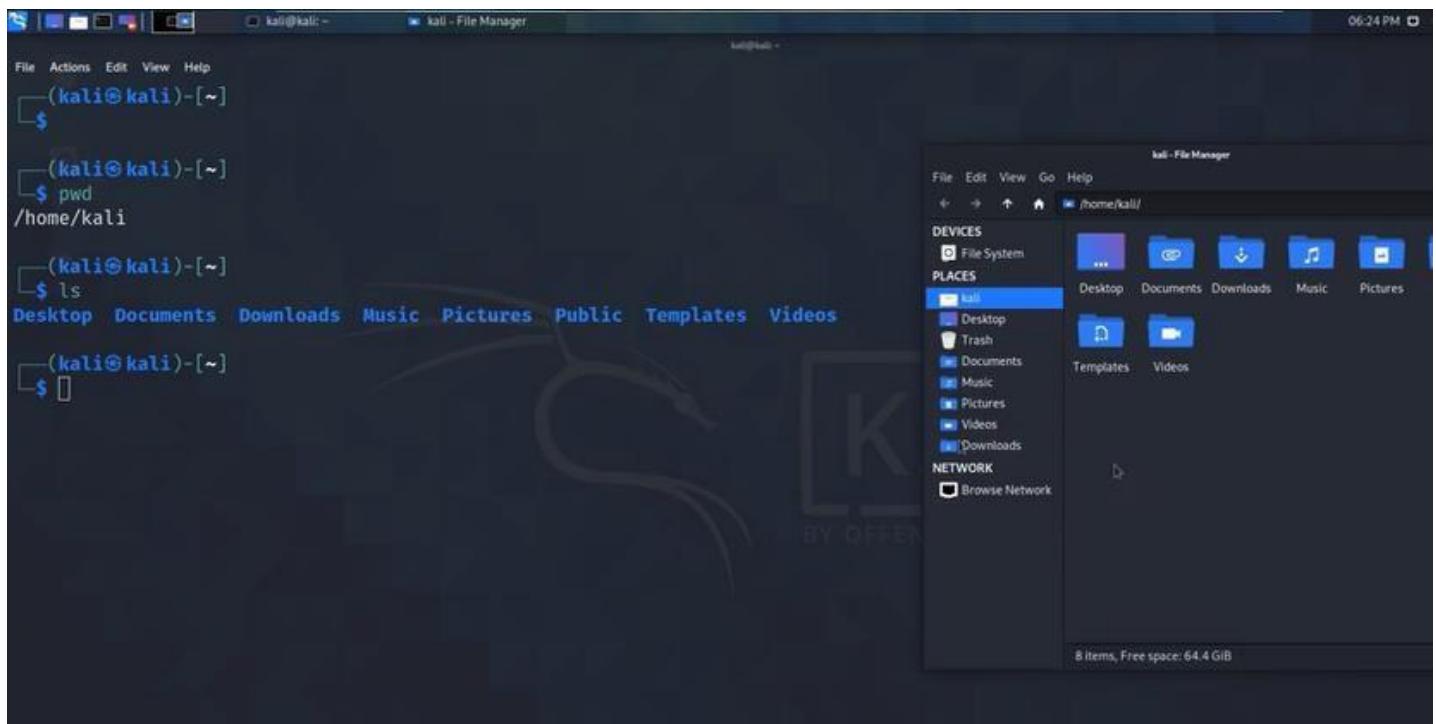


Imprime el directorio actual de trabajo



Como puedo ver lo que tengo en la carpeta





Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

A screenshot of a terminal window on a Kali Linux desktop. The terminal shows a user navigating through their home directory and creating a new folder named 'Desktop'. The desktop environment in the background features a dark theme with a large 'K' logo and the text 'BY OFFEN'.

```
kali@kali: ~/Desktop kali - File Manager
File Actions Edit View Help
(kali㉿kali)-[~]
$ 
(kali㉿kali)-[~]
$ pwd
/home/kali
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(kali㉿kali)-[~]
$ cd Desktop
(kali㉿kali)-[~/Desktop]
$ pwd
/home/kali/Desktop
(kali㉿kali)-[~/Desktop]
$ ls
(kali㉿kali)-[~/Desktop]
$ █
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

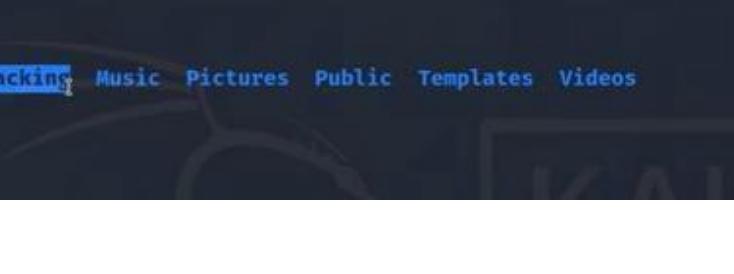
Para regresar



```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ 
(kali㉿kali)-[~]
$ pwd
/home/kali
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(kali㉿kali)-[~]
$ cd Desktop
(kali㉿kali)-[~/Desktop]
$ pwd
/home/kali/Desktop
(kali㉿kali)-[~/Desktop]
$ ls
(kali㉿kali)-[~/Desktop]
$ cd ..
(kali㉿kali)-[~]
$ pwd
/home/kali
(kali㉿kali)-[~]
$ 
$ 
```

Borro la pantalla con clear o Ctrl + L

Crear una nueva carpeta



```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(kali㉿kali)-[~]
$ mkdir Hacking
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Hacking Music Pictures Public Templates Videos
(kali㉿kali)-[~]
$ 
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

Para borrar la carpeta

```
kali㉿kali:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(kali㉿kali)-[~]
$ mkdir Hacking
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Hacking Music Pictures Public Templates Videos
(kali㉿kali)-[~]
$ cd Hacking
(kali㉿kali)-[~/Hacking]
$ ls
(kali㉿kali)-[~/Hacking]
$ cd ..
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Hacking Music Pictures Public Templates Videos
(kali㉿kali)-[~]
$ rmdir Hacking
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
```

Para crear un archivo

```
kali㉿kali:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(kali㉿kali)-[~]
$ touch hacking.txt
(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Hacking.txt Music Pictures Public Templates Videos
(kali㉿kali)-[~]
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

Borrar el archivo

A screenshot of a Kali Linux terminal window titled "kali@kali: ~". The terminal shows the following sequence of commands:

```
File Actions Edit View Help
[(kali㉿kali)-~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
[(kali㉿kali)-~]
$ touch hacking.txt
[(kali㉿kali)-~]
$ ls
Desktop Documents Downloads hacking.txt Music Pictures Public Templates Videos
[(kali㉿kali)-~]
$ rm hacking.txt
[(kali㉿kali)-~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
[(kali㉿kali)-~]
$
```

The terminal background features a watermark of the Kali logo with the text "KALI BY OFFENSIVE SECURITY".



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

Imprimo una palabra o texto o grabar una salida

```
File Actions Edit View Help
└──(kali㉿kali)-[~]
    └──$ ls
        Desktop Documents Downloads Music Pictures Public Templates Videos
└──(kali㉿kali)-[~]
    └──$ touch hacking.txt
└──(kali㉿kali)-[~]
    └──$ ls
        Desktop Documents Downloads hacking.txt Music Pictures Public Templates Videos
└──(kali㉿kali)-[~]
    └──$ rm hacking.txt
└──(kali㉿kali)-[~]
    └──$ ls
        Desktop Documents Downloads Music Pictures Public Templates Videos
└──(kali㉿kali)-[~]
    └──$ echo hola
hola
└──(kali㉿kali)-[~]
    └──$ echo "esto es una prueba"
esto es una prueba
└──(kali㉿kali)-[~]
    └──$ █
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

```
S kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
[(kali㉿kali)-~]
$ touch hacking.txt
[(kali㉿kali)-~]
$ ls
Desktop Documents Downloads hacking.txt Music Pictures Public Templates Videos
[(kali㉿kali)-~]
$ rm hacking.txt
[(kali㉿kali)-~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
[(kali㉿kali)-~]
$ echo hola
hola

[(kali㉿kali)-~]
$ echo "esto es una prueba"
esto es una prueba

[(kali㉿kali)-~]
$ echo "esto es otra prueba" > prueba.txt
[(kali㉿kali)-~]
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

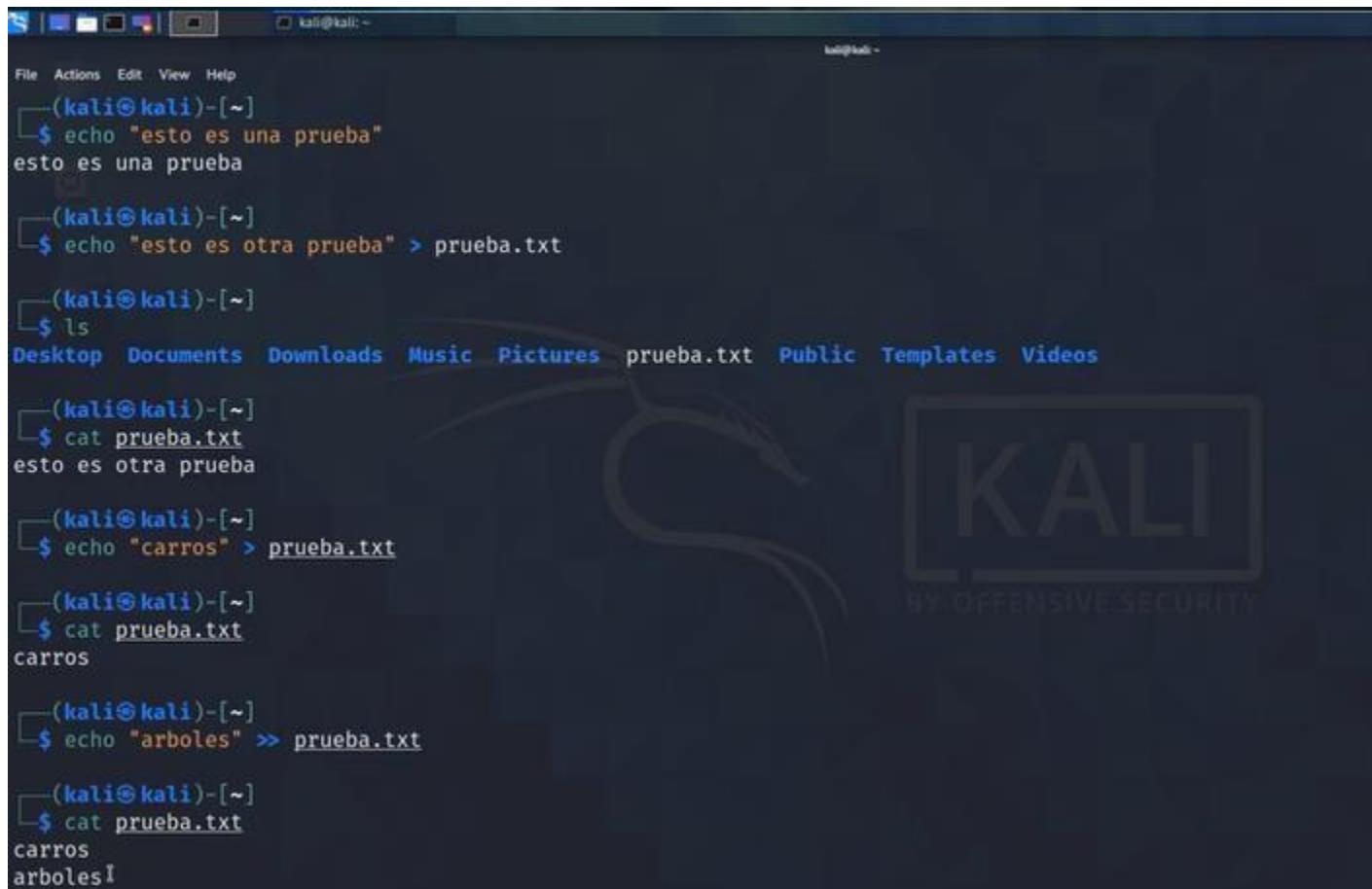
Leo archivos

```
S | kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-~]
└─$ ls
Desktop Documents Downloads hacking.txt Music Pictures Public Templates Videos
[(kali㉿kali)-~]
└─$ rm hacking.txt
[(kali㉿kali)-~]
└─$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
[(kali㉿kali)-~]
└─$ echo hola
hola

[(kali㉿kali)-~]
└─$ echo "esto es una prueba"
esto es una prueba

[(kali㉿kali)-~]
└─$ echo "esto es otra prueba" > prueba.txt
[(kali㉿kali)-~]
└─$ ls
Desktop Documents Downloads Music Pictures prueba.txt Public Templates Videos
[(kali㉿kali)-~]
└─$ cat prueba.txt
esto es otra prueba
```

Imprimir otras opciones



```
(kali㉿kali)-[~]
$ echo "esto es una prueba"
esto es una prueba

(kali㉿kali)-[~]
$ echo "esto es otra prueba" > prueba.txt

(kali㉿kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures prueba.txt Public Templates Videos

(kali㉿kali)-[~]
$ cat prueba.txt
esto es otra prueba

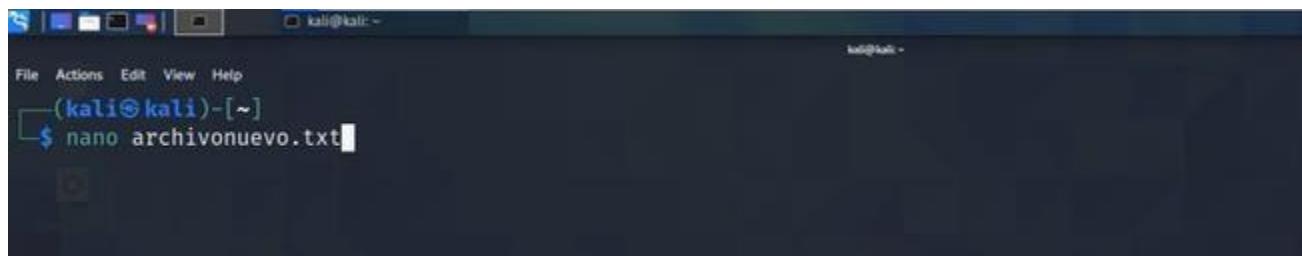
(kali㉿kali)-[~]
$ echo "carros" > prueba.txt

(kali㉿kali)-[~]
$ cat prueba.txt
carros

(kali㉿kali)-[~]
$ echo "arboles" >> prueba.txt

(kali㉿kali)-[~]
$ cat prueba.txt
carros
arboles
```

Permite crear y editar un archivo



```
(kali㉿kali)-[~]
$ nano archivonuevo.txt
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

A screenshot of a terminal window titled 'kali@kali: ~'. The window shows the command 'GNU nano 5.3' at the top. Below it, the file 'archivonuevo.txt' is open, containing the text:

```
probando
1
2
3
4
5
6 I
carros
arboles
```

Guardar con **ctrl + o enter**

Para salir **ctrl + x**

A screenshot of a terminal window titled '(kali㉿kali)-[~]'. The history shows the following commands:

```
$ nano archivonuevo.txt
$ cat archivonuevo.txt
probando
1
2
3
4
5
6
carros
arboles
$ nano archivonuevo.txt
```



```
(kali㉿kali)-[~]
$ nano archivonuevo.txt

(kali㉿kali)-[~]
$ cat archivonuevo.txt
probando
1
2
3
4
5
6
carros
arboles

(kali㉿kali)-[~]
$ nano archivonuevo.txt

(kali㉿kali)-[~]
$ cat archivonuevo.txt
árboles
carros
aviones
trenes

(kali㉿kali)-[~]
$
```

Atributo help, me permite ver información de un comando

```
(kali㉿kali)-[~]
$ ls --help
```



Guía para evaluar de Ciberseguridad

Universidad del Valle

Prof. Claudia Ximena Muñoz Ausecha



```
(kali㉿kali)-[~]
$ ls --help | I
Usage: ls [OPTION]... [FILE]...
List information about the FILEs (the current directory by default).
Sort entries alphabetically if none of -cftuvSUX nor --sort is specified.

Mandatory arguments to long options are mandatory for short options too.
-a, --all           do not ignore entries starting with .
-A, --almost-all   do not list implied . and ..
--author          with -l, print the author of each file
-b, --escape        print C-style escapes for nongraphic characters
--block-size=SIZE   with -l, scale sizes by SIZE when printing them;
                   e.g., '--block-size=M'; see SIZE format below
-B, --ignore-backups do not list implied entries ending with ~
-c                with -lt: sort by, and show, ctime (time of last
                   modification of file status information);
                   with -l: show ctime and sort by name;
                   otherwise: sort by ctime, newest first
-C                list entries by columns
--color[=WHEN]      colorize the output; WHEN can be 'always' (default
                   if omitted), 'auto', or 'never'; more info below
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

El comando -l me lista en formato largo la información, -a para mostrar formatos ocultos o -ls -la o -ls -al

```
(kali㉿kali)-[~]
(kali㉿kali)-[~]
└─$ ls -a -l
total 140
drwxr-xr-x 15 kali kali 4096 Jan 16 18:47 .
drwxr-xr-x  3 root root 4096 Nov 17 07:31 ..
-rw-r--r--  1 kali kali   30 Jan 16 18:47 archivonuevo.txt
-rw-r--r--  1 kali kali   1 Nov 17 09:49 .bash_history
-rw-r--r--  1 kali kali  220 Nov 17 07:31 .bash_logout
-rw-r--r--  1 kali kali 4503 Nov 17 07:31 .bashrc
-rw-r--r--  1 kali kali 3526 Nov 17 07:31 .bashrc.original
drwxr-xr-x  5 kali kali 4096 Jan 16 18:10 .cache
drwx----- 9 kali kali 4096 Jan 16 17:02 .config
drwxr-xr-x  2 kali kali 4096 Nov 17 07:33 Desktop
-rw-r--r--  1 kali kali   55 Nov 17 09:06 .dmrc
drwxr-xr-x  2 kali kali 4096 Nov 17 07:33 Documents
drwxr-xr-x  2 kali kali 4096 Nov 17 07:33 Downloads
-rw-r--r--  1 kali kali 11759 Nov 17 07:31 .face
lrwxrwxrwx  1 kali kali     5 Nov 17 07:31 .face.icon → .face
drwx----- 3 kali kali 4096 Jan 16 17:01 .gnupg
-rw-----  1 kali kali     0 Nov 17 07:33 .ICEauthority
drwxr-xr-x  3 kali kali 4096 Nov 17 07:33 .local
drwxr-xr-x  2 kali kali 4096 Nov 17 07:33 Music
drwxr-xr-x  2 kali kali 4096 Nov 17 07:33 Pictures
-rw-r--r--  1 kali kali   807 Nov 17 07:31 .profile
drwxr-xr-x  2 kali kali 4096 Jan 16 18:33 Prueba
drwxr-xr-x  2 kali kali 4096 Nov 17 07:33 Public
drwxr-xr-x  2 kali kali 4096 Nov 17 07:33 Templates
drwxr-xr-x  2 kali kali 4096 Nov 17 07:33 Videos
-rw-----  1 kali kali    49 Jan 16 18:10 .Xauthority
-rw-----  1 kali kali 10051 Jan 16 18:23 .xsession-errors
```

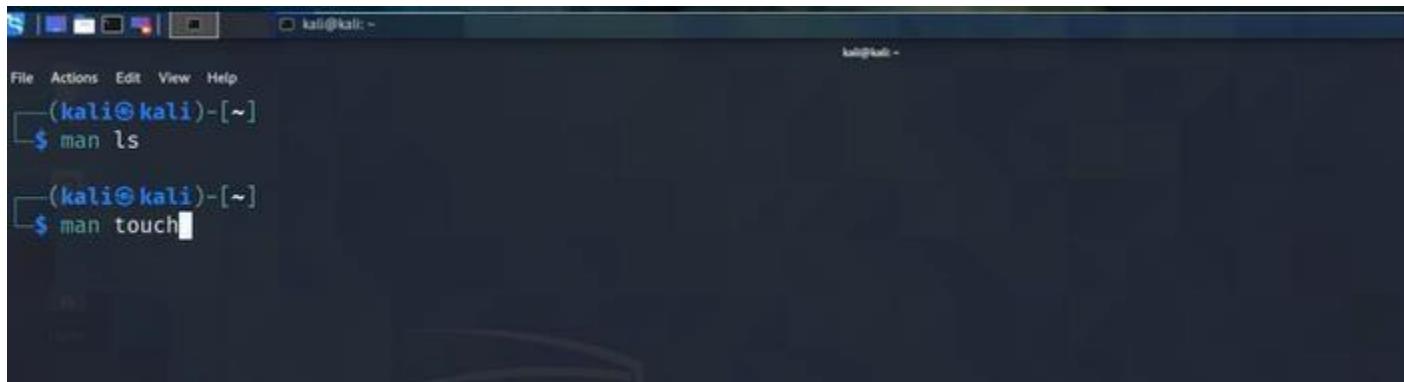
Ver de manera intuitivo y organizado el comando ls enter y para salir utilizo la tecla Q

```
(kali㉿kali)-[~]
(kali㉿kali)-[~]
└─$ man ls
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

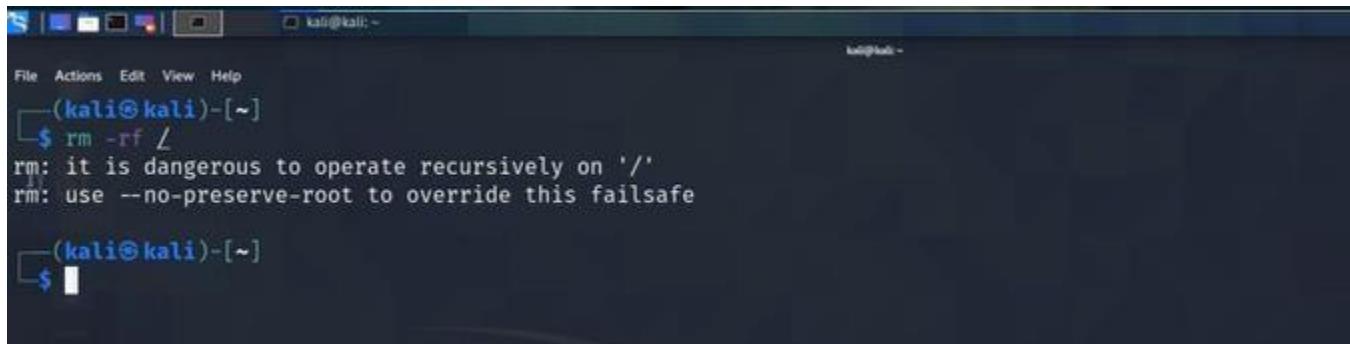
Muestra los atributos del comando touch



```
(kali㉿kali)-[~]
$ man ls

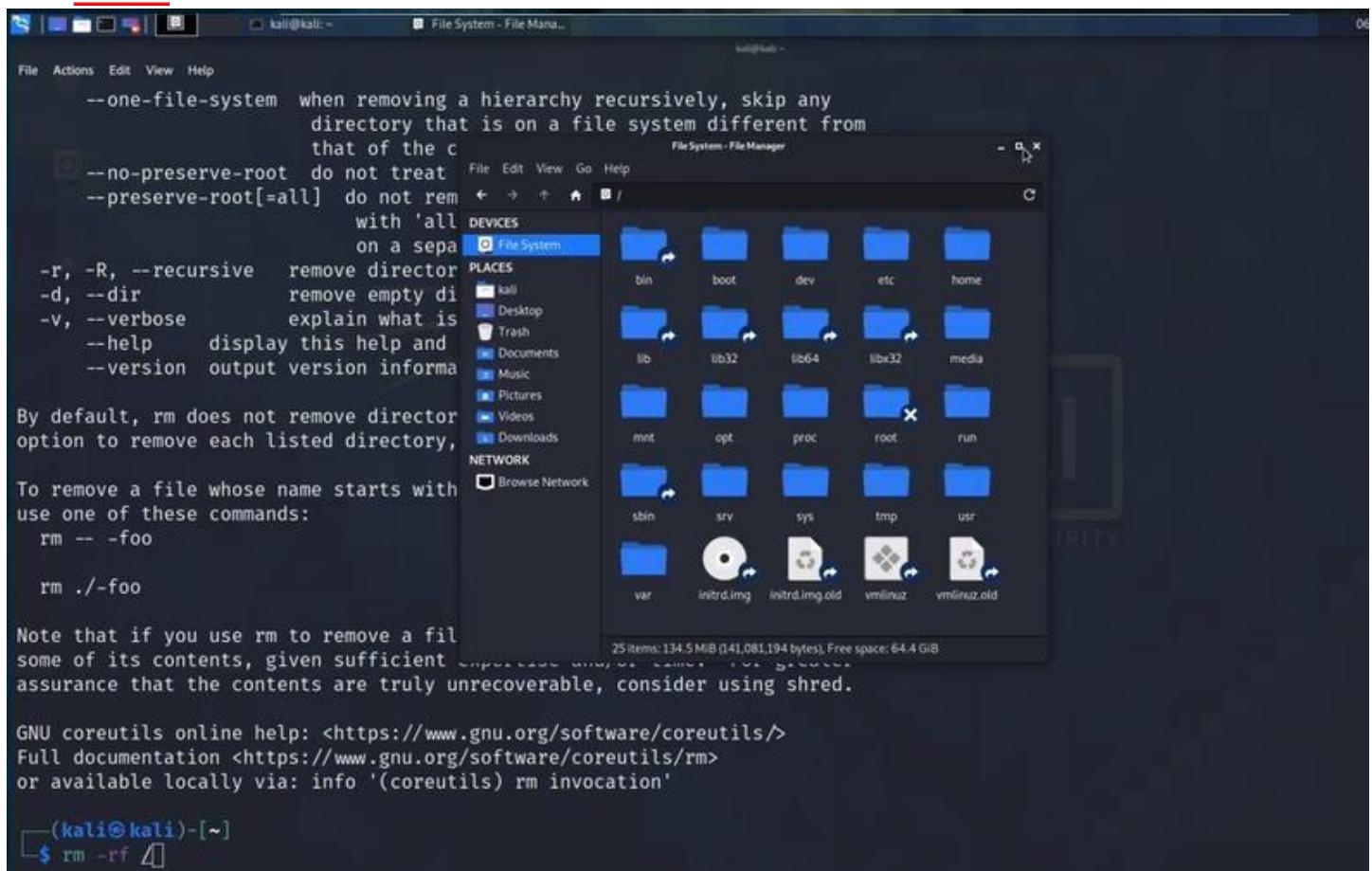
(kali㉿kali)-[~]
$ man touch
```

Borra de forma recursiva y forzada todo lo que haya en el directorio raíz, recomiendo que sea por usuario y no por admin EVITAR



```
(kali㉿kali)-[~]
$ rm -rf /
rm: it is dangerous to operate recursively on '/'
rm: use --no-preserve-root to override this failsafe

(kali㉿kali)-[~]
$
```



File Actions Edit View Help

```
--one-file-system    when removing a hierarchy recursively, skip any
                     directory that is on a file system different from
                     that of the c
--no-preserve-root   do not treat      File Edit View Go Help
--preserve-root[=all] do not rem      ← → + ⌂ / C
                     with 'all
                     on a sepa
-r, -R, --recursive  remove director
-d, --dir            remove empty di
-v, --verbose         explain what is
--help               display this help and
--version            output version informa
```

By default, rm does not remove director option to remove each listed directory,

To remove a file whose name starts with use one of these commands:

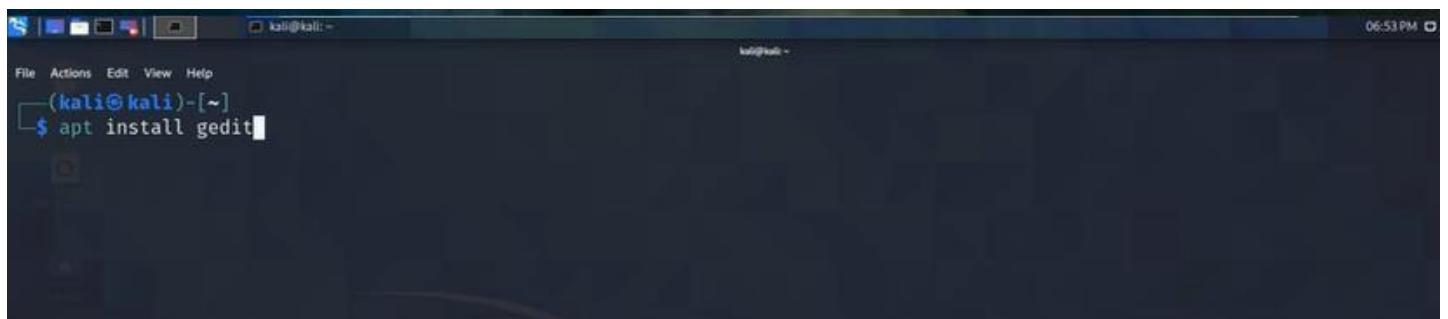
```
rm -- -foo
rm ./-foo
```

Note that if you use rm to remove a fil some of its contents, given sufficient assurance that the contents are truly unrecoverable, consider using shred.

GNU coreutils online help: <<https://www.gnu.org/software/coreutils/>>
Full documentation <<https://www.gnu.org/software/coreutils/rm>>
or available locally via: info '(coreutils) rm invocation'

```
(kali㉿kali)-[~]
$ rm -rf [ ]
```

Comando para borrar aplicaciones EVITAR HACERLO



```
File Actions Edit View Help
(kali㉿kali)-[~]
$ apt install gedit
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

Leer archivos y trabajar de manera rápida, con flechas hacia arriba

```
(kali㉿kali)-[~]
└─$ man touch

(kali㉿kali)-[~]
└─$ ls
archivonuevo.txt Desktop Documents Downloads Music Pictures Prueba Public Templates Videos

(kali㉿kali)-[~]
└─$ cat archivonuevo.txt
```

```
(kali㉿kali)-[~]
└─$ ls
archivonuevo.txt Desktop Documents Downloads Music Pictures Prueba Public Templates Videos

(kali㉿kali)-[~]
└─$ pwd
/home/kali

(kali㉿kali)-[~]
└─$ cd ..
(kali㉿kali)-[/home]
└─$ pwd
/home

(kali㉿kali)-[/home]
└─$ cd ..
(kali㉿kali)-[/]
└─$ pwd
/
(kali㉿kali)-[/]
└─$ ls
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

(kali㉿kali)-[/]
└─$ cd ..
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ cd ..
(kali㉿kali)-[~]
$ pwd
/
(kali㉿kali)-[~]
$ ls
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
(kali㉿kali)-[~]
$ cd root
cd: permission denied: root
(kali㉿kali)-[~]
$ pwd
/
(kali㉿kali)-[~]
$ cd home
(kali㉿kali)-[~/home]
$ cd kali
(kali㉿kali)-[~]
$ cd /home/kali/Desktop
(kali㉿kali)-[~/Desktop]
$ █
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

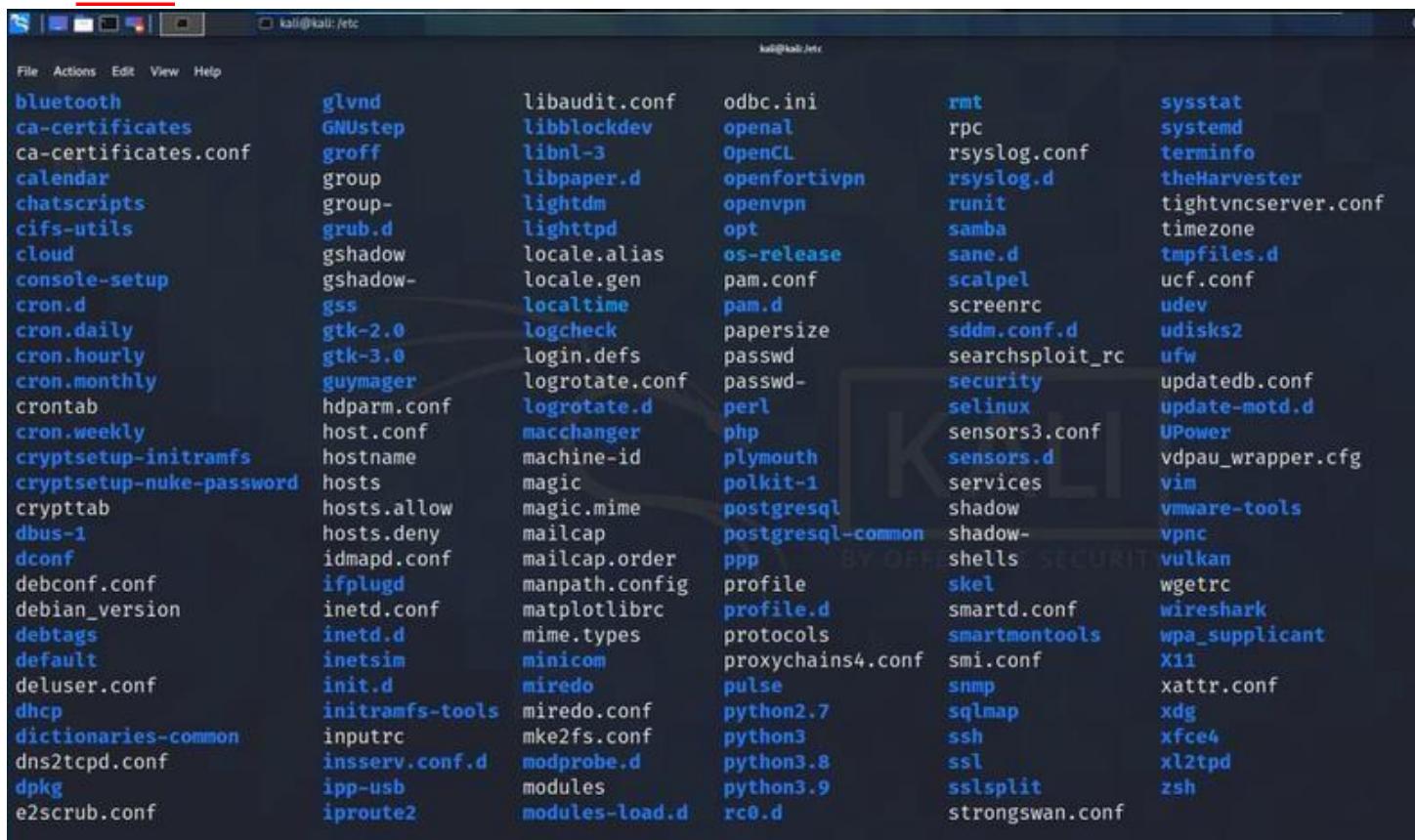


A terminal window showing a Kali Linux desktop environment. The terminal history is as follows:

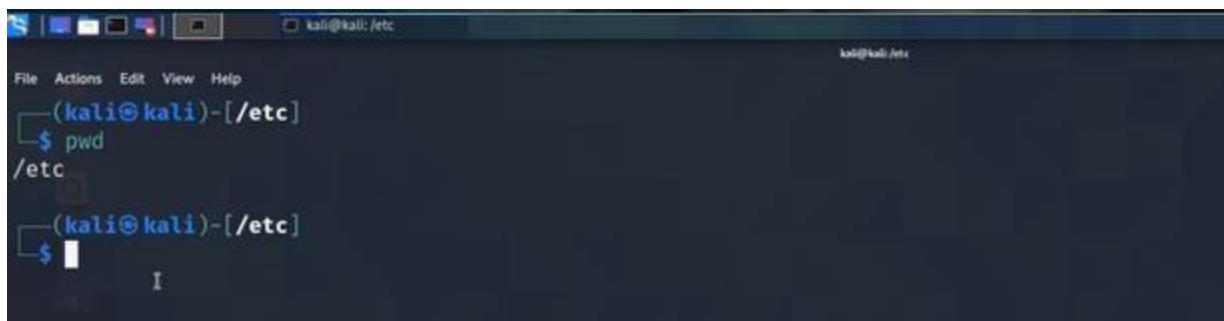
```
(kali㉿kali)-[~]
$ pwd
/
(kali㉿kali)-[~]
$ ls
bin dev home initrd.img.old lib32 libx32 media opt root sbin sys usr vmlinuz
boot etc initrd.img lib lib64 lost+found mnt proc run srv tmp var vmlinuz.old

(kali㉿kali)-[~]
$ cd root
cd: permission denied: root

(kali㉿kali)-[~]
$ pwd
/
(kali㉿kali)-[~]
$ cd home
(kali㉿kali)-[/home]
$ cd kali
(kali㉿kali)-[~/]
$ cd /home/kali/Desktop
(kali㉿kali)-[~/Desktop]
$ ls
(kali㉿kali)-[~/Desktop]
$ cd /etc
```

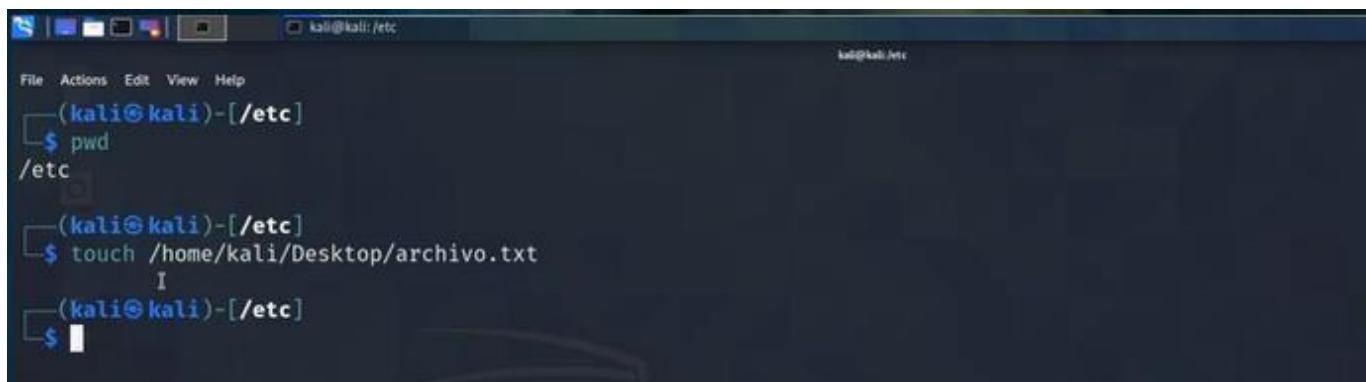


```
kali@kali:~$ cd /etc
kali@kali:/etc$ ls
bluetooth      glvnd      libaudit.conf    odbc.ini      rmt          sysstat
ca-certificates   GNUstep    libblockdev     openal        rpc           systemd
ca-certificates.conf  groff      libnl-3         OpenCL       rsyslog.conf  terminfo
calendar        group      libpaper.d      openfortivpn  rsyslog.d    theHarvester
chatscripts      group-     lightdm        openvpn       runit         tightvncserver.conf
cifs-utils       grub.d     lighttpd       opt           samba         timezone
cloud           gshadow    locale.alias    os-release   sane.d       tmpfiles.d
console-setup    gshadow-   locale.gen     pam.conf     scalpel       ucf.conf
cron.d          gss        localtime    pam.d        screenrc     udev
cron.daily       gtk-2.0    logcheck      pamsize     sddm.conf.d  udisks2
cron.hourly      gtk-3.0    login.defs    passwd      searchsploit_rc ufw
cron.monthly     guymager   logrotate.conf  passwd-     security      updatedb.conf
crontab         hdparm.conf logrotate.d    perl        selinux       update-motd.d
cron.weekly      host.conf  macchanger   php         sensors3.conf UPower
cryptsetup-initramfs  hostname  machine-id   Plymouth    sensors.d    vdpau_wrapper.cfg
cryptsetup-nuke-password  hosts    magic        polkit-1    services      vim
crypttab        hosts.allow  hosts.deny    mailcap     postgresql   vmware-tools
dbus-1          hosts.deny  idmapd.conf   mailcap.order  postgresql-common  vpnc
dconf           ifplugd    inetd.conf    manpath.config profile     sensors.d
debconf.conf    init.d     inetd.d       mime.types   protocols    smartd.conf
debian_version  initramfs-tools  inputrc     minicom     proxychains4.conf smartmontools
dictionaries-common  inserv.conf.d  modprobe.d  miredo      pulse        smi.conf
dns2tcpd.conf   ipp-usb    modules     miredo.conf  python2.7    snmp
dpkg            iproute2   modules-load.d  mke2fs.conf  python3     sqlmap
e2scrub.conf    iproute2   rc0.d       modprobe.d  python3.8   ssh
                         iproute2   modules     modules-load.d  python3.9   ssl
                         iproute2   rc0.d       rc0.d       sslsplit    xfce4
                         iproute2   rc0.d       rc0.d       strongswan.conf xl2tpd
                         iproute2   rc0.d       rc0.d       zsh
                         iproute2   rc0.d       rc0.d       xattr.conf  xdg
                         iproute2   rc0.d       rc0.d       xattr.conf  xfce4
                         iproute2   rc0.d       rc0.d       xattr.conf  xl2tpd
                         iproute2   rc0.d       rc0.d       xattr.conf  zsh
```



```
(kali㉿kali)-[~/Desktop]
$ pwd
/etc

(kali㉿kali)-[~/Desktop]
```



```
(kali㉿kali)-[~/Desktop]
$ touch /home/kali/Desktop/archivo.txt
I

(kali㉿kali)-[~/Desktop]
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

```
(kali㉿kali)-[~/Desktop]
$ touch archivo.txt
(kali㉿kali)-[~/Desktop]
$ ls
archivo.txt
(kali㉿kali)-[~/Desktop]
$
```

Comandos de red ifconfig

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.196.129 netmask 255.255.255.0 broadcast 192.168.196.255
        inet6 fe80::20c:29ff:fee4:2bec prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:e4:2b:ec txqueuelen 1000 (Ethernet)
                RX packets 1080805 bytes 1581680503 (1.4 GiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 518501 bytes 31354156 (29.9 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 84 bytes 17305 (16.8 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 84 bytes 17305 (16.8 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
$
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

Ip a

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:e4:2b:ec brd ff:ff:ff:ff:ff:ff
    inet 192.168.196.129/24 brd 192.168.196.255 scope global dynamic noprefixroute eth0
        valid_lft 1415sec preferred_lft 1415sec
        inet6 fe80::20c:29ff:fee4:2bec/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

El comando ping

```
kali@kali: ~
File Actions Edit View Help
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:e4:2b:ec brd ff:ff:ff:ff:ff:ff
        inet 192.168.196.129/24 brd 192.168.196.255 scope global dynamic noprefixroute eth0
            valid_lft 1415sec preferred_lft 1415sec
        inet6 fe80::20c:29ff:fe4:2bec/64 scope link noprefixroute
            valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$ ping 192.168.196.1
PING 192.168.196.1 (192.168.196.1) 56(84) bytes of data.
64 bytes from 192.168.196.1: icmp_seq=1 ttl=128 time=0.442 ms
64 bytes from 192.168.196.1: icmp_seq=2 ttl=128 time=0.352 ms
64 bytes from 192.168.196.1: icmp_seq=3 ttl=128 time=0.793 ms
64 bytes from 192.168.196.1: icmp_seq=4 ttl=128 time=0.367 ms
64 bytes from 192.168.196.1: icmp_seq=5 ttl=128 time=0.451 ms
64 bytes from 192.168.196.1: icmp_seq=6 ttl=128 time=0.279 ms
64 bytes from 192.168.196.1: icmp_seq=7 ttl=128 time=0.406 ms
64 bytes from 192.168.196.1: icmp_seq=8 ttl=128 time=0.281 ms
64 bytes from 192.168.196.1: icmp_seq=9 ttl=128 time=1.43 ms
64 bytes from 192.168.196.1: icmp_seq=10 ttl=128 time=0.348 ms
64 bytes from 192.168.196.1: icmp_seq=11 ttl=128 time=1.03 ms
^C
--- 192.168.196.1 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10155ms
rtt min/avg/max/mdev = 0.279/0.561/1.431/0.351 ms
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

```
$ kali@kali: ~
File Actions Edit View Help
PING 192.168.196.3 (192.168.196.3) 56(84) bytes of data.
From 192.168.196.129 icmp_seq=1 Destination Host Unreachable
From 192.168.196.129 icmp_seq=2 Destination Host Unreachable
From 192.168.196.129 icmp_seq=3 Destination Host Unreachable
From 192.168.196.129 icmp_seq=4 Destination Host Unreachable
From 192.168.196.129 icmp_seq=5 Destination Host Unreachable
From 192.168.196.129 icmp_seq=6 Destination Host Unreachable
From 192.168.196.129 icmp_seq=7 Destination Host Unreachable
From 192.168.196.129 icmp_seq=8 Destination Host Unreachable
From 192.168.196.129 icmp_seq=9 Destination Host Unreachable
^C
--- 192.168.196.3 ping statistics ---
10 packets transmitted, 0 received, +9 errors, 100% packet loss, time 9223ms
pipe 4

--(kali㉿kali)-[~]
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=19.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=20.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=21.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=19.0 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=22.5 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4010ms
rtt min/avg/max/mdev = 19.037/20.593/22.455/1.362 ms
```

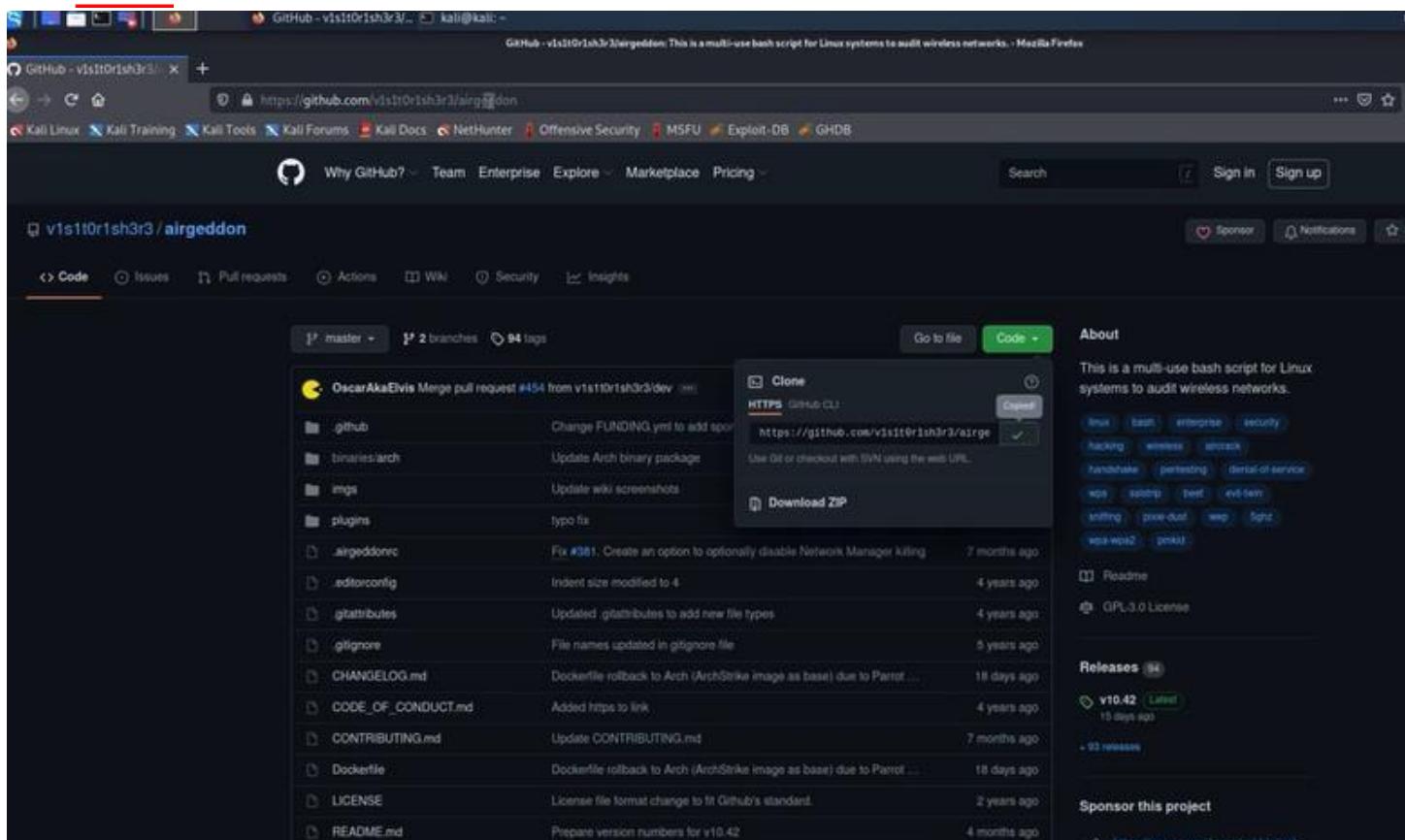


Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

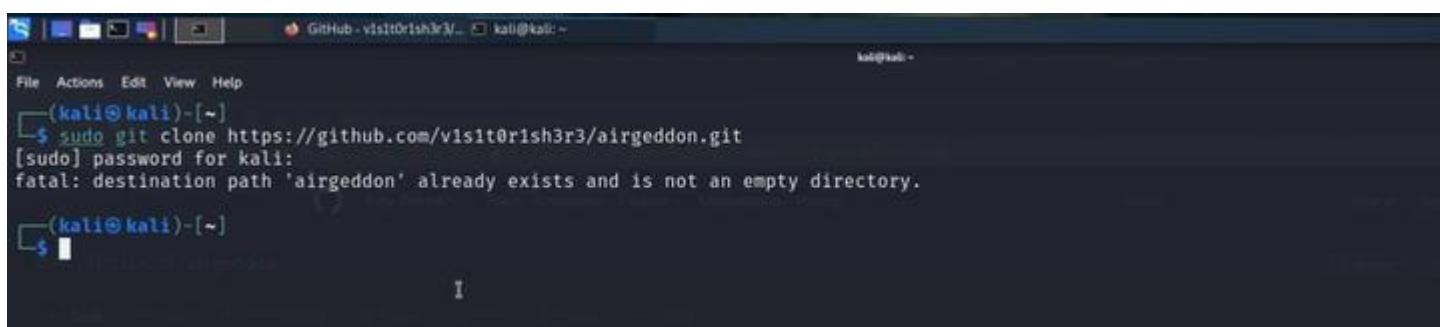
The screenshot shows a Mozilla Firefox browser window with the title bar "Google - Mozilla Firefox" and the address bar "https://www.google.com/gws_rd=ssl". The main content is the Google search homepage with the "Google" logo, a search bar, and links for "Buscar con Google" and "Me siento con suerte". At the bottom, it shows "Ofrecido por Google en: English". The browser interface includes tabs for "Kali Linux", "Kali Training", "Kali Tools", "Kali Docs", "Kali Forums", "NetHunter", "Offensive Security", "Exploit-DB", "GHDB", and "MSFU". The status bar at the bottom indicates "Ecuador".

Herramienta airgeddon, ingreso a Firefox y digito la url

<https://github.com/v1s1t0r1sh3r3/airgeddon>



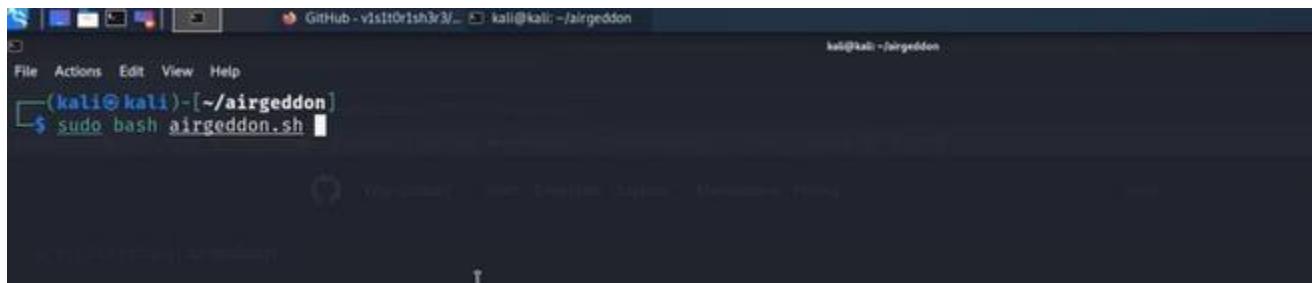
The screenshot shows the GitHub repository page for 'v1s10r1sh3r3/airgeddon'. The repository has 94 tags and 2 branches. The master branch is selected. The repository description states: 'This is a multi-use bash script for Linux systems to audit wireless networks.' It includes a 'Clone' button with the HTTPS URL: https://github.com/v1s10r1sh3r3/airge... and a 'Download ZIP' button. The repository has 93 releases, with the latest being v10.42. The 'About' section lists various tags such as 'blue', 'black', 'enterprise', 'security', 'hacking', 'wireless', 'attack', 'handshake', 'pentesting', 'denial-of-service', 'kali', 'airdrop', 'test', 'evil-twin', 'sniffing', 'poke-dust', 'wep', 'light', 'kali-wireless', 'pk3cr', 'Readme', and 'GPL-3.0 License'.



```
(kali㉿kali)-[~]
$ sudo git clone https://github.com/v1s10r1sh3r3/airgeddon.git
[sudo] password for kali:
fatal: destination path 'airgeddon' already exists and is not an empty directory.

(kali㉿kali)-[~]
$
```

Ejecutamos



```
(kali㉿kali)-[~/airgeddon]
$ sudo bash airgeddon.sh
```

Éxitos



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

```
GitHub - visit0rsh3r3/... kali@kali: ~/airgeddon
File Actions Edit View Help
***** Welcome *****
Welcome to airgeddon script v10.42

[Stylized logo composed of brackets and braces]

Developed by visit0r

*   *   *
. (   )   .
*   *
```

```
GitHub - visit0rsh3r3/... kali@kali: ~/airgeddon
File Actions Edit View Help
raspbian" "Red Hat" "SuSE" "Ubuntu" "Kifislax"

Detecting system ...
Kali Linux

Let's check if you have installed what script needs
Press [Enter] key to continue...

Essential tools: checking ...
iw .... ok
awk .... ok
airmon-ng .... ok
airodump-ng .... ok
aircrack-ng .... ok
xterm .... ok
ip .... ok
lspci .... ok
ps .... ok

Optional tools: checking ...
bettercap .... ok
ettercap .... ok
dnsmasq .... ok
hostapd-wpe .... ok
iptables .... ok
beef-xss .... ok
aireplay-ng .... ok
bully .... ok
pixiewps .... ok
dhcpcd .... ok
asleep.... ok
packetforge-ng .... ok
hashcat .... ok
wpaclean .... ok
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

Enter para continuar

```
GitHub - visit0r1sh3r3/... kali@kali: ~/airgeddon
File Actions Edit View Help
***** Interface selection *****
Select an interface to work with:
1. eth0 // Chipset: Intel Corporation 82545EM
2. eth1 // Chipset: Intel Corporation 82545EM
3. wlan0 // 2.4Ghz // Chipset: Ralink Technology, Corp. RT2870/RT3070
*Hint* If you have any doubt or problem, you can check Wiki FAQ section (https://github.com/visit0r1sh3r3/airgeddon/wiki/FAQ%20&%20Troubleshooting)
our Discord channel: https://discord.gg/sQ9dgt9
> [ ]
```

Colocamos una opción ejemplo 3

```
GitHub - visit0r1sh3r3/... kali@kali: ~/airgeddon
File Actions Edit View Help
***** airgeddon v10.42 main menu *****
Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz
Select an option from menu:
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. DoS attacks menu
5. Handshake/PMKID tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
11. About & Credits
12. Options and language menu
*Hint* We are looking for translators to other languages. If you want to see airgeddon in your native language and you also know english, please contribute at: https://github.com/visit0r1sh3r3/airgeddon/wiki/Contributing
> [ ]
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

Luego la opción 12

```
File Actions Edit View Help
***** Options and language menu *****
Automatic updates: Enabled
Skip intro: Disabled
Basic colorization: Enabled
Extended colorization: Enabled
Startup language autodetection: Disabled
Silent checks: Disabled
Print hints: Enabled
5Ghz: Enabled
Network Manager force stop: Enabled
Current windows handling: xterm
Selected mdk version: mdk4
Plugins system: Enabled

Select an option from menu:
0. Return to main menu
1. Change language
2. Disable automatic updates permanently
3. Enable skip intro permanently
4. Disable basic colorization permanently
5. Disable extended colorization permanently
6. Enable startup language autodetection permanently
7. Enable silent checks permanently
8. Disable print hints permanently
9. Disable 5Ghz permanently
10. Change windows handling method to tmux
11. Set mdk version to mdk3
12. Disable plugins system permanently
13. Disable Network Manager force stop permanently
14. Set permanently airgeddon's language to the current one

*Hint* Since airgeddon 9.20 version, tmux is supported and it can be used instead of xterm as windows handler. Script can run without a graphical X window system. It is recommended only for advanced users. Like any other option, it can be configured in airgeddonrc options file or launched using AIRGEDDON WINDOWS HANDLING "flag" in the command line. More information about
```

Cambiamos el lenguaje con la opción 2, enter

```
File Actions Edit View Help
***** Change language *****
Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz

Select a language:
0. Return to options menu
1. English
2. Spanish
3. French
4. Catalan
5. Portuguese
6. Russian
7. Greek
8. Italian
9. Polish
10. German
11. Turkish
12. Arabic

*Hint* If you see any bad translation or just want [PoT] marks to disappear, write me to visit0r.is.h3r3@gmail.com to collaborate with tra
> |
```

Éxitos



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

Volvemos a la opción inicial con opción 0

The screenshot shows a terminal window titled 'GitHub - v1s1t0r1sh3r3/... kali㉿kali: ~/airgeddon'. The window displays the configuration menu for Airgeddon. The menu lists various options and their current status, such as 'Actualizaciones automáticas: Activadas' (Automatic updates: Enabled) and 'Colorización básica: Activada' (Basic coloring: Enabled). It also shows the current window manager ('Manejo de ventanas actual: xterm') and selected mdk version ('Versión mdk seleccionada: mdk4'). The menu includes a section for selecting an option from a numbered list, ranging from 0 to 14, which corresponds to different configuration items. At the bottom, there is a note about repository installations.

```
***** Menú de opciones e idioma *****
Actualizaciones automáticas: Activadas
Saltarse la intro: Desactivado
Colorización básica: Activada
colorización extendida: Activada
Autodetección de idioma al inicio: Desactivada
Chequeos silenciosos: Desactivados
Mostrar consejos: Activado
5Ghz: Activado
Forzado de parada de Network Manager: Activado
Manejo de ventanas actual: xterm
Versión mdk seleccionada: mdk4
Sistema de plugins: Activado

Selección una opción del menú:
0. Volver al menú principal
1. Cambiar idioma
2. Deshabilitar permanentemente la actualización automática
3. Habilitar permanentemente saltarse la intro
4. Deshabilitar permanentemente la colorización básica
5. Deshabilitar permanentemente la colorización extendida
6. Habilitar permanentemente la autodetección de idioma al inicio
7. Habilitar permanentemente chequeos silenciosos
8. Deshabilitar mostrar consejos permanentemente
9. Deshabilitar 5Ghz permanentemente
10. Cambiar el método de manejo de ventanas a tmux
11. Cambiar versión mdk a mdk3
12. Deshabilitar sistema de plugins permanentemente
13. Deshabilitar forzado de parada de Network Manager permanentemente
14. Cambiar permanentemente el idioma de airgeddon al actual

*Consejo* Si instalaste airgeddon desde un repositorio, no deberías activar la actualización automática. airgeddon se act
on en el repositorio
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

```
GitHub - visit0r1sh3r3/... kali@kali: ~/airgeddon
kali@kali: ~/airgeddon

File Actions Edit View Help
Saltarse la intro: Desactivado
Colorización básica: Activada
Colorización extendida: Activada
Autodetección de idioma al inicio: Desactivada
Chequeos silenciosos: Desactivados
Mostrar consejos: Activado
5Ghz: Activado
Forzado de parada de Network Manager: Activado
Manejo de ventanas actual: xterm
Versión mdk seleccionada: mdk4
Sistema de plugins: Activado

Selección una opción del menú:
0. Volver al menú principal
1. Cambiar idioma
2. Deshabilitar permanentemente la actualización automática
3. Habilitar permanentemente saltarse la intro
4. Deshabilitar permanentemente la colorización básica
5. Deshabilitar permanentemente la colorización extendida
6. Habilitar permanentemente la autodetección de idioma al inicio
7. Habilitar permanentemente chequeos silenciosos
8. Deshabilitar mostrar consejos permanentemente
9. Deshabilitar 5Ghz permanentemente
10. Cambiar el método de manejo de ventanas a tmux
11. Cambiar versión mdk a mdk3
12. Deshabilitar sistema de plugins permanentemente
13. Deshabilitar forzado de parada de Network Manager permanentemente
14. Cambiar permanentemente el idioma de airgeddon al actual

*Consejo* Si instalaste airgeddon desde un repositorio, no deberías activar la actualización automática. airgeddon se ejecuta en el repositorio
> 14

se va a cambiar permanentemente el idioma al actual para que al siguiente inicio de airgeddon este sea el idioma en el
continuar? [Y/n]
> Y
```



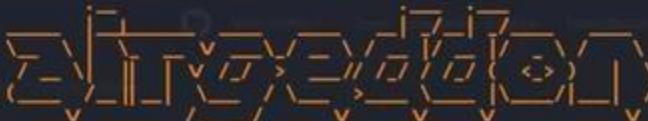
Guía para evaluar de Ciberseguridad

Universidad del Valle

Prof. Claudia Ximena Muñoz Ausecha

Iniciamos nuevamente el script

A screenshot of a terminal window titled "GitHub - visit0rsh3r3/... kali@kali: ~/airgeddon". The window displays the following text:

```
***** Bienvenido *****  
Bienvenido a airgeddon script v10.42  
  
Programado por visit0r  

```

The terminal has a dark background with light-colored text and icons.

Seleccionamos la interfaz

```
S GitHub - visit0r1sh3r3/... kali@kali: ~/airgeddon
File Actions Edit View Help
***** Menú principal airgeddon v10.42 *****
Interfaz wlan0 seleccionada. Modo: Managed. Bandas soportadas: 2.4Ghz

Selecciona una opción del menú:

0. Salir del script
1. Selecciona otra interfaz de red
2. Poner la interfaz en modo monitor
3. Poner la interfaz en modo managed

4. Menú de ataques DoS
5. Menú de herramientas Handshake/PMKID
6. Menú de descifrado WPA/WPA2 offline
7. Menú de ataques Evil Twin
8. Menú de ataques WPS
9. Menú de ataques WEP
10. Menú de ataques Enterprise

11. Acerca de & Créditos
12. Menú de opciones e idioma

*Consejo: Si tienes cualquier duda o problema, puedes consultar la sección FAQ del Wiki (https://github.com/visit0r1sh3r3/airgeddon/wiki) o preguntar en nuestro canal de Discord. Enlace de invitación: https://discord.gg/sQ9dgt9
> [ ]
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

Ahora veremos los distintos ataques que tiene airgeddon

Selecciono la interfaz

```
kali@kali: ~/airgeddon
File Actions Edit View Help
***** Selección de interfaz *****
Selecciona una interfaz para trabajar con ella:
1. eth0 // Chipset: Intel Corporation 82545EM
2. eth1 // Chipset: Intel Corporation 82545EM
3. wlan0 // 2.4GHz // Chipset: Ralink Technology, Corp. RT2870/RT3070
*Consejo* Cada vez que veas un texto con el prefijo [PoT] acrónimo de "Pending of Translation", significa que su traducción ha sido generada automáticamente
> 1
```

```
kali@kali: ~/airgeddon
File Actions Edit View Help
***** Menú principal airgeddon v10.42 *****
Interfaz wlan0 seleccionada. Modo: Managed. Bandas soportadas: 2.4GHz

Selecciona una opción del menú:
0. Salir del script
1. Selecciona otra interfaz de red
2. Poner la interfaz en modo monitor
3. Poner la interfaz en modo managed
4. Menú de ataques DoS
5. Menú de herramientas Handshake/PMKID
6. Menú de descifrado WPA/WPA2 offline
7. Menú de ataques Evil Twin
8. Menú de ataques WPS
9. Menú de ataques WEP
10. Menú de ataques Enterprise
11. Acerca de & Créditos
12. Menú de opciones e idioma
*Consejo* Selecciona una interfaz wifi para poder realizar más acciones que con una interfaz ethernet
> 2
Poniendo la interfaz en modo monitor...
Esta interfaz ha cambiado su nombre al ponerla en modo monitor. Se ha seleccionado automáticamente
Se ha puesto el modo monitor en wlan0mon
Pulsa la tecla [Enter] para continuar...]
```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

Denegación de servicio con opción 4

```
kali㉿kali: ~/airgeddon
File Actions Edit View Help
***** Menú ataques DoS *****
Interfaz wlan0mon seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz
Selecciona una opción del menú:
0. Volver al menú principal
1. Selecciona otra interfaz de red
2. Poner la interfaz en modo monitor
3. Poner la interfaz en modo managed
4. Explorar para buscar objetivos (modo monitor requerido)
    (modo monitor requerido en ataques)
5. Ataque Deauth / Disassoc amok mdk4
6. Ataque Deauth aireplay
7. Ataque WIDS / WIPS / WDS Confusion
    (antiguos ataques "obsoletos/no muy efectivos")
8. Ataque Beacon flood
9. Ataque Auth DoS
10. Ataque Michael shutdown exploitation (TKIP)

*Consejo* Si seleccionas una red objetivo con el ESSID oculto, no podrás usarlo, pero puedes hacer ataques basados en BSSID sobre esa red
> |
```

Ahora modo ataque

```
kali㉿kali: ~/airgeddon
File Actions Edit View Help
***** Menú ataques DoS *****
Interfaz wlan0mon seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz
Selecciona una opción del menú:
0. Volver al menú principal
1. Selecciona otra interfaz de red
2. Poner la interfaz en modo monitor
3. Poner la interfaz en modo managed
4. Explorar para buscar objetivos (modo monitor requerido)
    (modo monitor requerido en ataques)
5. Ataque Deauth / Disassoc amok mdk4
6. Ataque Deauth aireplay
7. Ataque WIDS / WIPS / WDS Confusion
    (antiguos ataques "obsoletos/no muy efectivos")
8. Ataque Beacon flood
9. Ataque Auth DoS
10. Ataque Michael shutdown exploitation (TKIP)

*Consejo* Si seleccionas una red objetivo con el ESSID oculto, no podrás usarlo, pero puedes hacer ataques basados en BSSID sobre esa red
> |
```

Enter , aparecen las redes

```

Exploring for targets  kali@kali:~/airgeddon
File Actions Edit View Help
***** Menú ataques DoS *****
Interfaz wlan0mon seleccionada. Modo: Monitor. Bandas soportadas: 2.4ghz
Selecciona una opción del menú:
0. Volver al menú principal
1. Selecciona otra interfaz de red
2. Poner la interfaz en modo monitor
3. Poner la interfaz en modo managed
4. Explorar para buscar objetivos (modo monitor requerido)
    (modo monitor requerido en ataques)
5. Ataque Deauth / Disassoc mdk4
6. Ataque Deauth aireplay
7. Ataque WIDS / WIPS / WDS Confusion
    (antiguos ataques "obsoletos/no muy efectivos")
8. Ataque Beacon flood
9. Ataque Auth DoS
10. Ataque Michael shutdown exploitation (TKIP)

*Consejo* Si seleccionas una red objetivo con el ESSID oculto, no podrás usarlo, pero puedes hacer ataques
> 4

***** Explorar para buscar objetivos *****
Elegida opción de exploración para buscar objetivos (modo monitor requerido)

La interfaz seleccionada wlan0mon está en modo monitor. La exploración se puede realizar
No hay filtros activados en el escaneo. Una vez comenzado, pulse [Ctrl+C] para pararlo...
Pulsa la tecla [Enter] para continuar...

```

BSSID	PWR	Beacons	#Data	%	OK	NOK	ENC	CODNR	RTH	ESSID
HE:0C:13:92:9d:F0:00	-71	2	0	0	3	05	WPA2	PSK	Length:	00
00:14:00:00:31:47	-47	3	44	0	2	279	WPA2	PSK	HACKER MENTOR PRINCIPAL	
04:70:02:99:80:16	-93	4	0	0	1	139	WPA2	PSK	HACKER MENTOR SECUNDARIO	
04:51:00:73:99:44	-71	2	0	0	1	139	WPA2	PSK	CELESTY_INES_EXT	
00:0F:D7:06:0B:5A	-79	2	0	0	1	139	WPA2	PSK	NETLIFE-DON SUCO EXT	

Ctrl + c

```

Exploring for targets  kali@kali:~/airgeddon
File Actions Edit View Help
***** Seleccionar objetivo *****
N.      BSSID          CANAL  PWR   ENC   ESSID
1)  E4:C3:2A:7D:80:4D  1     25%  WPA2  CELESTY_INES_EXT
2)  D2:14:3D:6A:31:47  10    37%  WPA2  DIRECT-QP-BRAVIA
3)  78:57:73:69:48:60  11    40%  WPA2  HACKER MENTOR ESTUDIO
4)* A0:F3:C1:52:37:C2  7     53%  WPA2  HACKER MENTOR PRINCIPAL
5)  64:70:02:99:80:16  1     83%  WPA2  HACKER MENTOR SECUNDARIO
6)  C8:1F:B0:F6:4D:F4  10    0%   (Hidden Network)
7)  FA:8F:CA:96:F6:CC  11    26%  OPN   (Hidden Network)
8)  AE:AE:19:BA:F0:BD  3     29%  WPA2  (Hidden Network)
9)* 60:32:B1:32:FF:C8  6     33%  WPA2  MAURICIO_1_EXT
10) 28:C6:8E:BB:AF:8C  6     32%  WPA2  MAURICIO_1
11) 68:FF:7B:6E:8D:18  10    28%  WPA2  NETLIFE-DON SUCO EXT
12) C8:1F:B0:E4:A4:DC  2     29%  WPA2  NETLIFE-Fmla.TecaSuarez
13) 58:60:5F:2F:A0:50  5     31%  WPA2  NETLIFE-VASCO

(*) Red con clientes

Selecciona la red objetivo:
> 1

```



Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

Aquí se ven las redes de alrededor

```
kali㉿kali:~/airgeddon
File Actions Edit View Help
*****
Interfaz wlan0mon seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz
BSSID seleccionado: 64:70:02:99:80:16
Canal seleccionado: 3
ESSID seleccionado: HACKER MENTOR SECUNDARIO
Tipo de encriptado: WPA2

Selecciona una opción del menú:
0. Volver al menú principal
1. Selecciona otra interfaz de red
2. Poner la interfaz en modo monitor
3. Poner la interfaz en modo managed
4. Explorar para buscar objetivos (modo monitor requerido)
   (modo monitor requerido en ataques)
5. Ataque Deauth / Disassoc amok mdk4
6. Ataque Deauth aireplay
7. Ataque WIDS / WIPS / WDS Confusion
   (antiguos ataques "obsoletos/no muy efectivos")
8. Ataque Beacon flood
9. Ataque Auth DoS
10. Ataque Michael shutdown exploitation (TKIP)

*Consejo: No todos los ataques afectan a todos los puntos de acceso. Si un ataque no funciona contra un punto de acceso, elige otro :)*
> |
```



Guía para evaluar de Ciberseguridad

Universidad del Valle

Prof. Claudia Ximena Muñoz Ausecha

Lanzamos el ataque

```
[root@kali ~]# ./mdk4 amok attack
[*] mdk4 amok attack
[*] kati@kali: ~/airgeddon
[*] [!] Verificando la conexión de red...
[*] [!] mdk4 amok attack
[*] [!] mdk4 amok attack
[*] [!] kati@kali: ~/airgeddon

[*] Consejo: No todos los ataques afectan a todos los puntos de acceso. Si un ataque no funciona contra un punto de acceso, elige otro :)
> 5

***** Parámetros mdk4 amok *****
Elegido ataque de Desautenticación / Desasociación mdk4 (modo monitor requerido)

La interfaz seleccionada wlan0mon está en modo monitor. El ataque se puede realizar

BSSID elegido 64:70:02:99:80:16

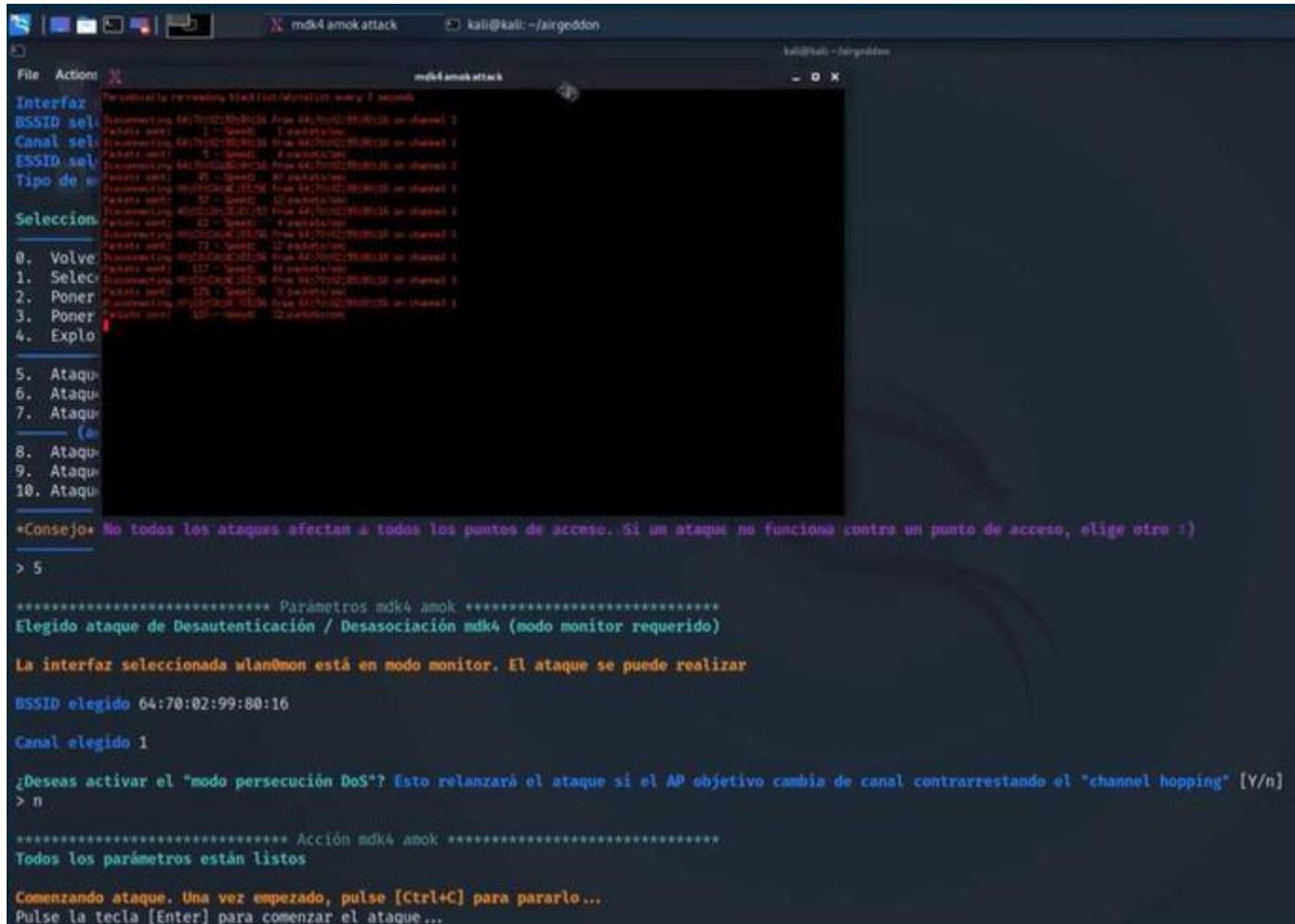
Canal elegido 1

¿Deseas activar el "modo persecución DoS"? Esto relanzará el ataque si el AP objetivo cambia de canal contrarrestando el "channel hopping" [Y/n]
> n

***** Acción mdk4 amok *****
Todos los parámetros están listos

Comenzando ataque. Una vez comenzado, pulse [Ctrl+C] para pararlo ...
Pulse la tecla [Enter] para comenzar el ataque ...
```

Envía paquetes de autenticación a la víctima



```

Guía para evaluar de Ciberseguridad
Universidad del Valle
Prof. Claudia Ximena Muñoz Ausecha

Envía paquetes de autenticación a la víctima

[Terminal]
File Actions mdk4 amok attack kali@kali: ~/airgeddon
Interfaz: wlan0mon
BSSID selecciónado: 64:70:02:99:80:16
Canal seleccionado: 1
ESSID seleccionado: 44:70:02:99:80:16
Tipo de ataque: Desautentificación / Desasociación
Selección: 1. Seleccionar canal
0. Volver
1. Seleccionar canal
2. Poner
3. Poner
4. Explorar
5. Ataque
6. Ataque
7. Ataque
8. Ataque
9. Ataque
10. Ataque

Consejo: No todos los ataques afectan a todos los puntos de acceso. Si un ataque no funciona contra un punto de acceso, elige otro :)
> 5

***** Parámetros mdk4 amok *****
Elegido ataque de Desautentificación / Desasociación mdk4 (modo monitor requerido)

La interfaz seleccionada wlan0mon está en modo monitor. El ataque se puede realizar

BSSID elegido 64:70:02:99:80:16
Canal elegido 1

¿Deseas activar el "modo persecución DoS"? Esto relanzará el ataque si el AP objetivo cambia de canal contrarrestando el "channel hopping" [Y/n]
> n

***** Acción mdk4 amok *****
Todos los parámetros están listos

Comenzando ataque. Una vez comenzado, pulse [Ctrl+C] para pararlo...
Pulse la tecla [Enter] para comenzar el ataque...

```

RUBRICA

1. Inicio de máquina virtual y arranque de Sistema operativo Kali Linux	1.0
2. Sigue los pasos de la guía y realizas una nueva guía con tus datos que arroje el sistema justificando cada pantallazo	2.0
3. Con sus propias palabras justifique el proceso para el cual se utilizó el hackeando de una wireless	2.0