METODOS DE ACCESOMÉTODOS DE ACCESO NO AUTORIZADOS DE WIFI

CÁTEDRA:

SISTEMAS OPERATIVOS DE REDES

CATEDRÁTICO:

ING. MANUEL FLORES VILLATORO

Carnet	Apellidos	Nombres
RG01133698	Reyes García	José Alfredo
SJ01133616	Serpas Jiménez	Edwin Antonio
ZV01133710	Zelaya Villalta	Jerson Ernesto

Introduccion

- Las redes inalámbricas brindan grandes beneficios tanto en lo laboral como en lo domestico, todos en algún momento nos habremos conectado un punto de acceso a internet WIFI, ya sea en nuestras casas o en nuestro trabajo y es en este lugar donde toma un poco más de importancia el tema de seguridad de la red.
- Dichas herramientas pueden ejecutarse en diferentes sistemas operativos (Linux, MacOS, Windows), en la actualidad los sistemas operativos que más se han popularizado son los sistemas Linux dedicados a la auditoria de redes inalámbricas.
- Entre estos tenemos Kali Linux, Wifislax, BackTrack, todas ellas con muchas herramientas para romper los protocolos de seguridad en las redes wifi, entre estas herramientas esta la Suite Aircrack-ng siendo esta la suite más popular y más usada en la auditoria de redes inalámbricas.

Objetivos

- **General**

Conocer y comprender en funcionamientos de diferentes métodos de acceso no autorizados de wifi.

Especificos

Investigar los métodos más usados para obtener acceso no autorizado en una red inalámbrica.

Realizar pruebas con el software utilizado para penetrar las redes inalámbricas.

- **Redes Inalámbricas**
- **Definición de red inalámbrica**
- Es la interconexión de distintos dispositivos con la capacidad de compartir información entre ellos, pero sin un medio físico de transmisión. Estos dispositivos pueden ser de muy variadas formas y tecnologías entre ellos:
- Computadoras de escritorio.
- Teléfonos celulares.
- Asistentes digitales personales (PDA).
- *Access Point* (encargado de permitir a los dispositivos inalámbricos el acceso a la red).
- Computadoras portátiles: *Laptop*, *Netbook* y *Notebook*

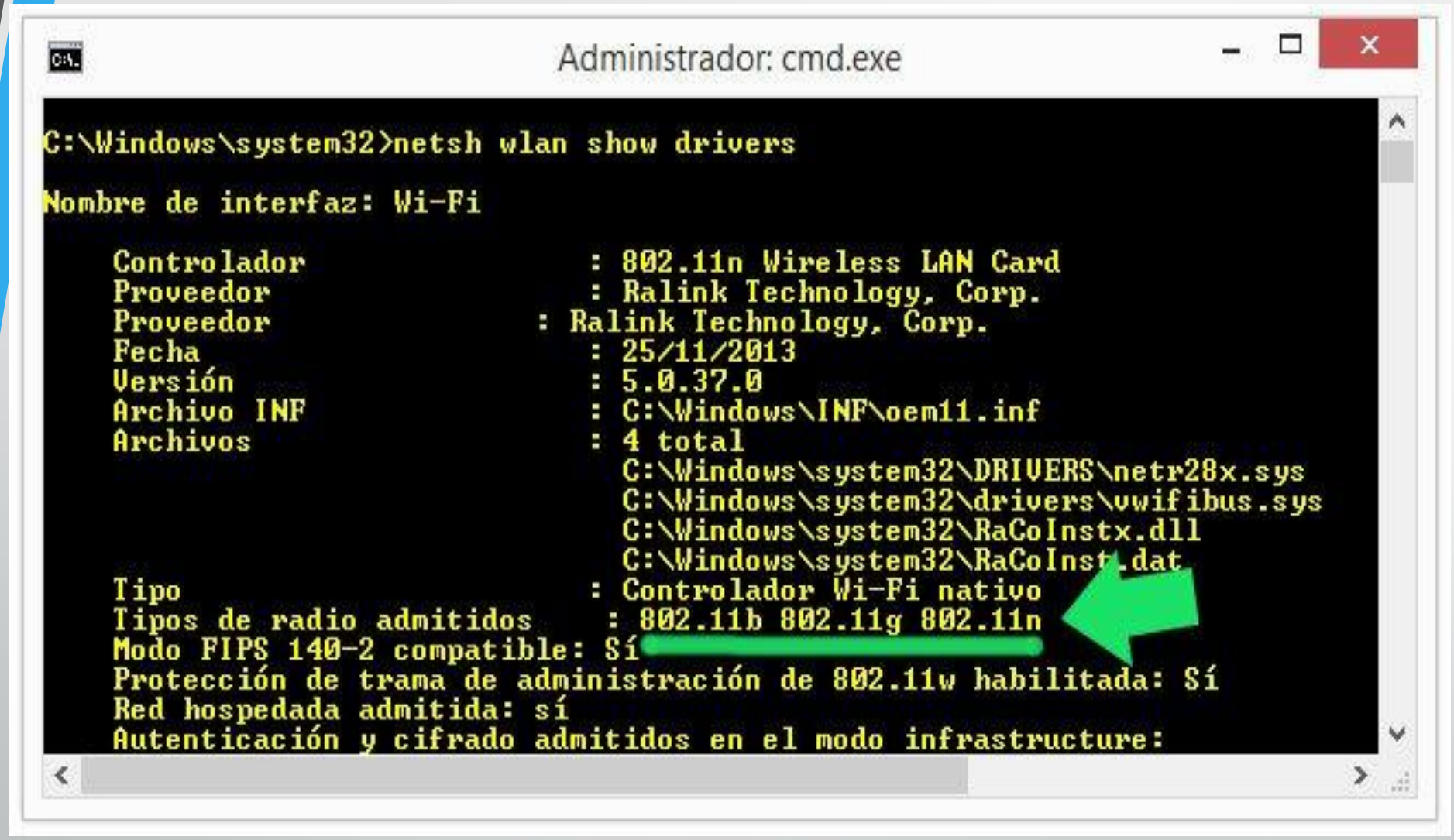

Interconexión inalámbrica
Laptop
PC
Acces
Point
Celular
PDA

Nombre	Tecnología	Velocidad de Transmisión	Características
Wireless B	IEEE 802.11b	11 Mbps (Megabits por segundo)	Trabaja en la banda de frecuencia de 2.4 GHz solamente, compatible con velocidades menores.
Wireless G	IEEE 802.11g	11 / 22 / 54 Mbps	Trabaja en la banda de frecuencia de 2.4 GHz solamente.
Wireless N	IEEE 802.11n	300 Mbps	Utiliza una tecnología denominada MIMO (que por medio de múltiples antenas trabaja en 2 canales), frecuencia 2.4 GHz y 5 GHz simultáneamente.
Nombre	Tecnología	Velocidad de Transmisión	Características
Wireless AC	IEEE 802.11ac	433 Mbps / 1.3 Gbps	Trabaja sobre la banda de los 2.5 Ghz a 5 Ghz (MIMO) de 3 canales, múltiples antenas, tambien llamada Wi-Fi 5/5G

- El estándar 802.11ah o Wi-Fi HaLow, características y ventajas
- IEEE 802.11ah es un nuevo protocolo de redes inalámbricas que comienza a implementarse en el 2016.
- Surge a causa de los constantes requerimientos de la tecnología, la información y el mercado.
- Se diferencia de los anteriores por usar frecuencias inferiores a 1 GHz y permite aumentar el rango de alcance de estas redes, hasta alrededor de 1000 metros.
- Esto facilita en la práctica su distribución en áreas rurales, usando torres de telefonía con sensores para compartir la señal.

- **Información de un dispositivo Wi-Fi usando el comando NETSH**

- Otra de las formas de obtener información de cualquier dispositivo, es con el comando NETSH en Windows.
- Haz lo siguiente:
- Abre una ventana de la consola de CMD o Símbolo del sistema.
- Para eso abre la herramienta Ejecutar mediante las teclas Windows + R, escribe CMD y presiona Enter.
- Escribe en la ventana de la consola lo siguiente y presiona la tecla Enter. netsh wlan show drivers
- Se mostrará toda la información disponible del adaptador inalámbrico.
- Busca la línea: "Tipos de radio admitidos" como se muestra en la siguiente imagen.


Administrador: cmd.exe
C:\Windows\system32>netsh wlan show drivers
Nombre de interfaz: Wi-Fi
Controlador : 802.11n Wireless LAN Card
Proveedor : Ralink Technology, Corp.
Proveedor : Ralink Technology, Corp.
Fecha : 25/11/2013
Versión : 5.0.37.0
Archivo INF : C:\Windows\INF\oem11.inf
Archivos : 4 total
C:\Windows\system32\DRIVERS\netr28x.sys
C:\Windows\system32\drivers\vwifibus.sys
C:\Windows\system32\RaCoInstx.dll
C:\Windows\system32\RaCoInst.dat
Tipo : Controlador Wi-Fi nativo
Tipos de radio admitidos : 802.11b 802.11g 802.11n
Modo FIPS 140-2 compatible: Sí
Protección de trama de administración de 802.11w habilitada: Sí
Red hospedada admitida: sí
Autenticación y cifrado admitidos en el modo infrastructure:

Modos de conexiones Wi-Fi

- Existen dos tipos de conexiones Wi-Fi: el modo "infraestructura" y el modo "ad hoc".
- El primero de ellos es la conexión que se efectúa entre un equipo o dispositivo y un punto de acceso inalámbrico (AP) ya sea un router o un punto público.
- Existen redes abiertas y protegidas. Algunas son públicas y otras privadas.
- El segundo, el modo ad-hoc es la conexión que se establece entre dos equipos o dispositivos de forma independiente. Esta conexion solo permite algunos metros de alcance.

¿Que son las redes ad hoc?

- Con Wi-Fi podemos crear una conexión entre dos computadoras o entre una computadora y un dispositivo portable, sin mediar un punto de acceso inalámbrico.
- Incluso de esa forma podemos compartir una conexión de internet, funcionando uno de los equipos como un router, AP o HotSpot.
- Este tipo de red virtual es llamada "red ad hoc".

¿Qué es Wi-Fi Direct?

- Wi-Fi Direct es la tecnología que permite crear una conexión entre dos dispositivos por Wi-Fi, de forma similar a una red ad hoc.
- Los dispositivos que la admiten ya traen integrado un pequeño punto de acceso, por lo que no es necesario depender de una computadora para crear la red y todo se hace más sencillo y seguro.

Alcance de las redes Wi-Fi

- El alcance de las redes Wi-Fi es limitado.
- Un punto de acceso usando 802.11b puede llegar hasta los 100 metros (exterior).
- Usando 802.11n se puede llegar hasta los 200 metros.
- El alcance puede extenderse hasta algunos kilómetros, usando antenas direccionales.
- Las redes que usan la banda de 5 GHz (802.11ac) poseen un menor alcance, aunque menos interferencia.

Vulnerabilidades de WEP, WPA, y WPA2

- **WEP**
- El lanzamiento del estándar IEEE 802.11 para conexiones inalámbricas que se ratificó en 1997 incluyó un apartado para la seguridad de esas conexiones: el llamado Wired Equivalent Privacy (WEP) —curioso que el acrónimo haga uso de la palabra "Wired" y no "Wireless", por cierto— planteaba un algoritmo de seguridad para proteger la confidencialidad de los datos de forma similar a la que se proporcionaba a redes de cable.
- El protocolo WEP hacía uso del cifrado RC4 y del mecanismo CRC-32 para la integridad, y el sistema estándar de 64 bits hacía uso de una clave de 40 bits que se concatenaba con un vector de inicialización (IV) de 24 bits para conformar la clave RC4. A cualquiera que haya usado este protocolo le resultarán familiares esas clave WEP de 64 bits, pero en formato hexadecimal, que hacían que al conectarnos a una red WiFi con esa seguridad tuviésemos que introducir esos diez caracteres hexadecimales (números del 0 al 9, letras de la A a la F).

WPA

- Aquellos enormes fallos al concebir un protocolo de seguridad para las comunicaciones inalámbricas trataron de corregirse con el desarrollo del estándar IEEE 802.11i, que no llegaría hasta un año después. La urgencia de la situación hizo que la Wi-Fi Alliance sacara una versión preliminar de ese estándar, y es así como en 2003 apareció en escena el protocolo Wi-Fi Protected Access (WPA).

Cifrados inseguros para nuestra red Wi-Fi

- **Sin cifrado o red Wi-Fi abierta**
- Las redes sin cifrado, o abiertas, son aquellas que no tienen ninguna contraseña y que permiten a cualquier usuario conectarse a ellas sin necesidad de nada más. Estas redes son totalmente inseguras ya que, además de permitir a cualquiera conectarse al router, la conexión no cuenta con ningún tipo de cifrado, por lo que cualquier usuario podría capturar los paquetes que enviamos y obtener así toda nuestra información.
- Este sistema es, sin duda, el menor recomendable.

Cifrado WEP

- El cifrado WEP fue uno de los primeros cifrados utilizados para proteger las redes inalámbricas. Este cifrado es débil y vulnerable y, aunque en el pasado podía servir más o menos, actualmente con la potencia de los sistemas informáticos domésticos y las aplicaciones desarrolladas para explotar este tipo de cifrado, finalmente se considera un cifrado "inseguro" y es posible obtener su clave en tan solo unos minutos capturando paquetes mediante falsas solicitudes de acceso. El cifrado WEP ofrece una protección insuficiente, por lo que no es recomendable su uso.

Cifrados seguros para nuestra red Wi-Fi

- **Cifrado WPA**
- El cifrado WPA nació a partir de la necesidad de solucionar los problemas del cifrado WEP. Este sistema de cifrado ofrece una serie de variantes según la finalidad que se le vaya a dar:
- WPA-Personal: Utiliza un sistema de claves PSK o claves precompartidas donde el administrador especifica su propia contraseña y todos los usuarios se conectan a la red con ella, de manera que sea más fácil recordarla.
- RADIUS: Enfocado a empresas, este sistema de seguridad se basa en un servidor en el que los usuarios deben autenticarse con un usuario y una contraseña diferente para cada uno en vez de conectarse todos con una contraseña global.

Cifrado WPA2

- El cifrado WPA2 es la actualización del cifrado WPA y mejora tanto la seguridad como el rendimiento de este. Este sistema también cuenta con las variantes de claves personales PSK y sistemas RADIUS para la gestión de redes, aunque el cifrado es muy superior al de WPA.

- **Tipo de cifrado (TKIP / AES) en WPA / WPA2**

- Las contraseñas WPA y WPA2 pueden utilizar dos tipos de cifrado diferente: TKIP y AES. Los usuarios que buscan compatibilidad con dispositivos antiguos (por ejemplo, una Nintendo DS) deben utilizar WPA con cifrado TKIP, sin embargo, recientemente se han detectado varias vulnerabilidades en este cifrado, por lo que, salvo en casos de extrema necesidad, no es recomendable utilizarlo.

Principales herramientas usadas para encontrar vulnerabilidades en una red WIFI

- **El Aircrack** es una de las herramientas más populares para romper cifrado WEP/WPA/WPA2. La suite de Aircrack-ng contiene herramientas para capturar paquetes y apretones de manos para autenticar a clientes conexión generando tráfico y herramientas para realizar ataques de fuerza bruta y diccionario. El Aicrack-ng es un todo-en-uno que cuenta con las siguientes herramientas (entre otros):
  - Aircrack-ng para agrietarse de la contraseña;
  - Aireplay-ng para generar tráfico y autenticación de cliente;
  - Airodump-ng para capturar paquetes;
  - airbase-ng para configurar puntos de acceso falsos.

- **Reaver**
- Realiza ataques de fuerza bruta contra los pernos de la configuración protegida WiFi (WPS) para recuperar la contraseña WPA/WPA2. Puesto que muchos fabricantes de routers y liguam de ISPs el WPS por defecto, muchos routers son vulnerables a este tipo de ataques.
- para utilizar reaver, se necesita una buena señal para el router inalámbrico y también la configuración correcta. En promedio de 4 a 10 horas, raver puede recuperar contraseñas de router vulnerables, dependiendo de la intensidad de la señal de punto de acceso y el PIN propio. Estadísticamente, tienes 50% de probabilidades de romper un PIN de WPS en mitad del tiempo.

- **PixieWPS**
- PixieWPS está escrito en C y se utiliza para fuerza bruta en WPS pines sin conexión, explorar la baja o ninguna entropía de los puntos vulnerables de acceso. Este ataque es conocido como polvo de pixie (polvo de duende o hada). Los PixieWPS requiere una versión modificada del Get o Wifite para trabajar eficazmente.

- **Wireshark**
- Es una de las mejores herramientas de protocolo de red de análisis disponibles si no el mejor. Con Wireshark, puede analizar una red con mayor detalle para ver lo que está sucediendo. Wireshark puede ser utilizado para la captura de paquete vivo, inspección profunda de cientos de protocolos, búsqueda y filtro de paquetes y es multiplataforma.

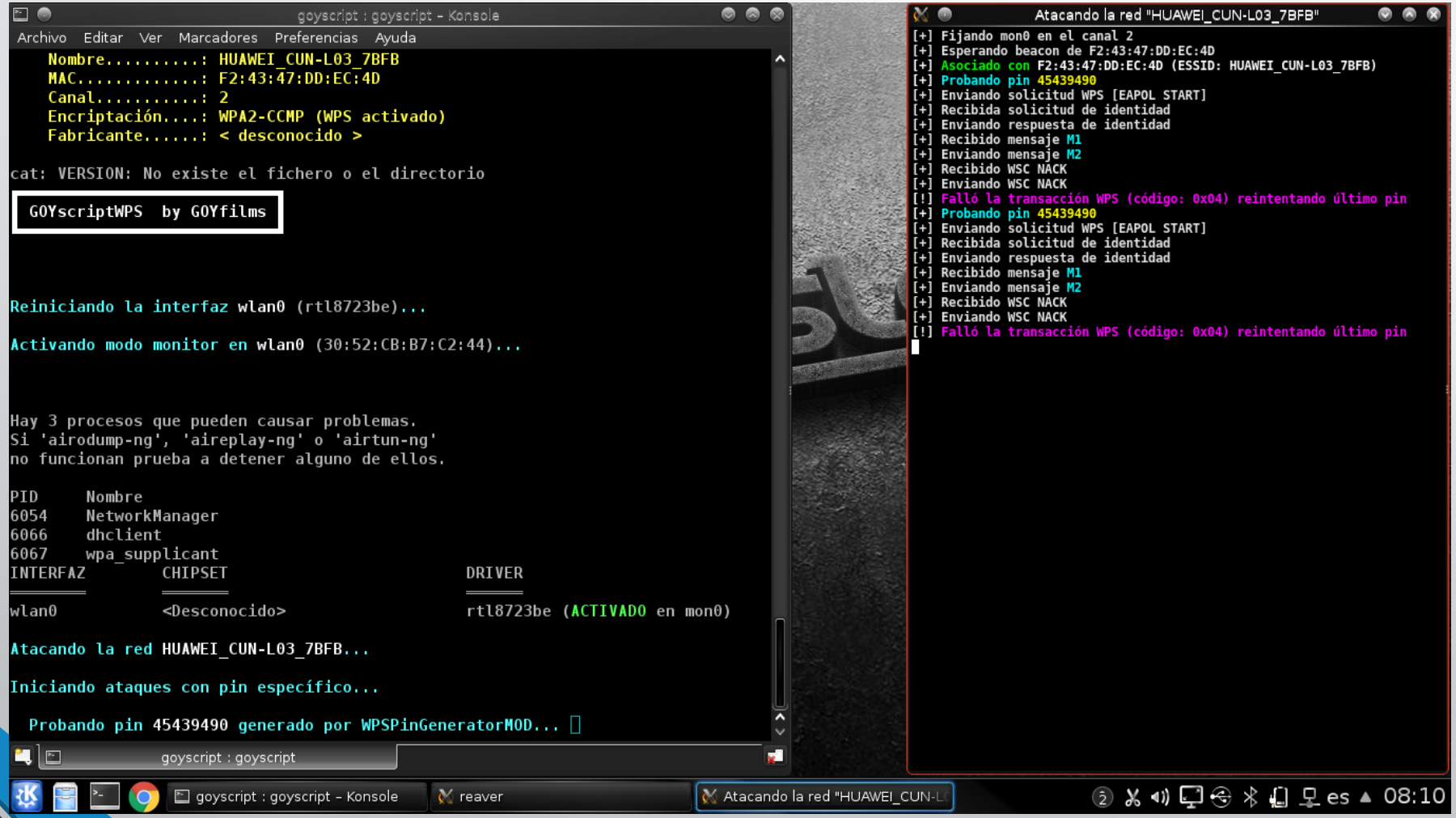
Las contraseñas WiFi, talón de Aquiles de WPA (y WPA2)

- A este protocolo le fallaba otra pata: la de las contraseñas. Aunque los fabricantes de equipos de comunicaciones (routers, puntos de acceso) establecían contraseñas relativamente fuertes por defecto para proteger las redes WiFi predefinidas en sus equipos, los usuarios acababan renombrando sus redes y cambiándoles las contraseñas por otras fáciles de recordar.

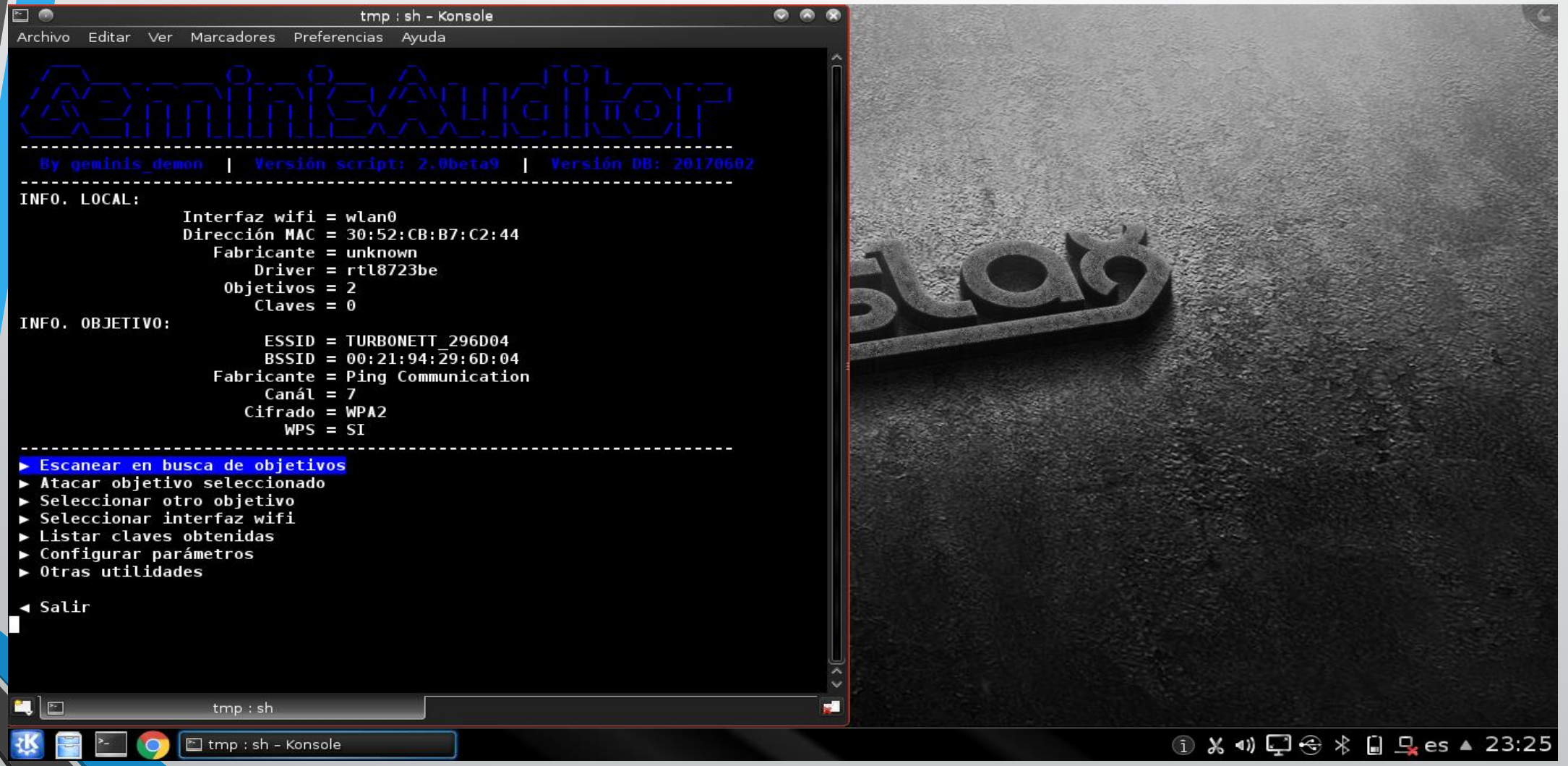
HERRAMIETAS

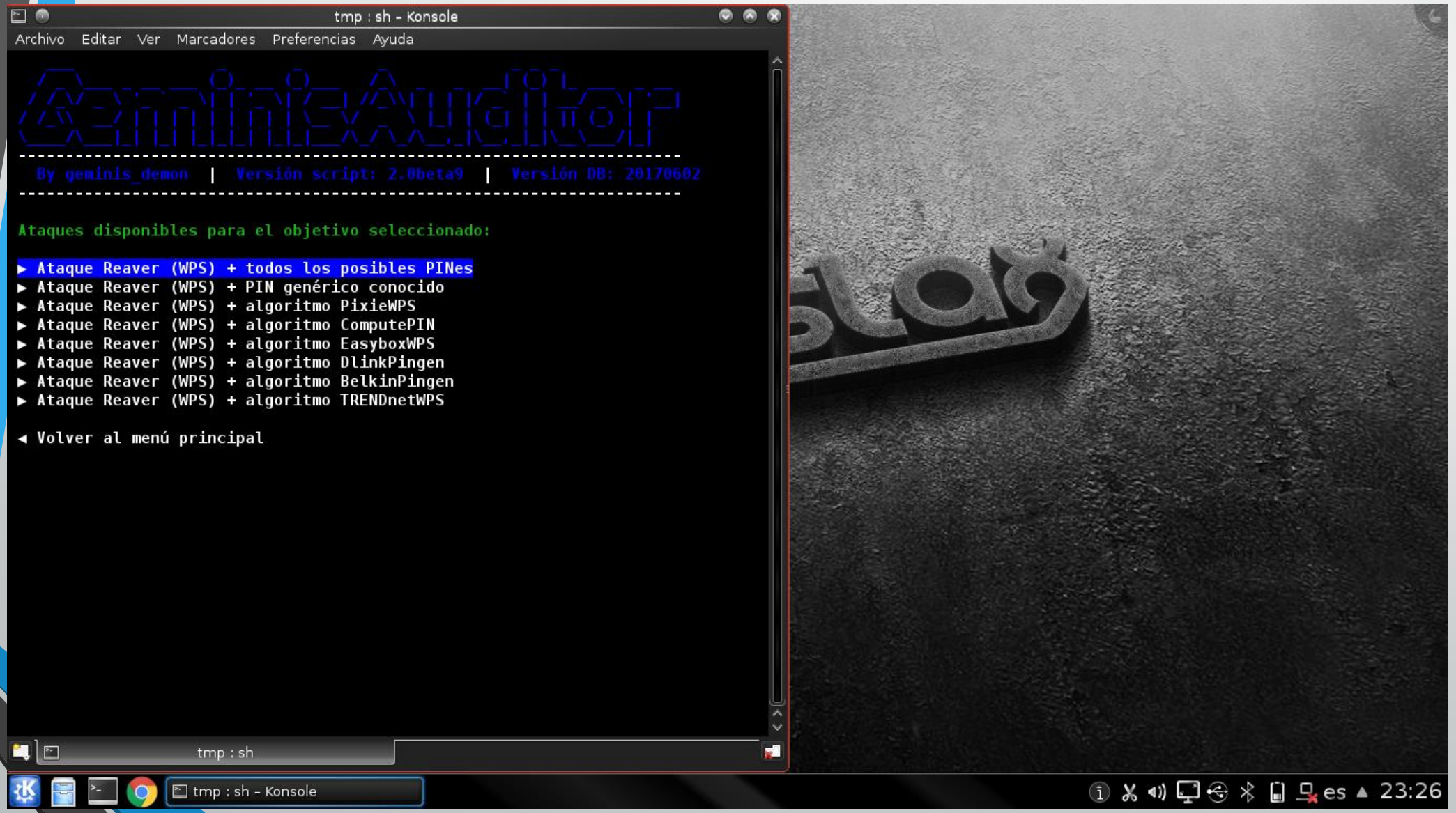
Equipos utilizados para las pruebas		
Equipo #1		
Marca y modelo	Características	
ASUS. X453S.	Procesador	Intel Celeron 3050. 2,16 GHz
	Memoria RAM	4 GB
	Disco duro	500 GB
	Tarjeta inalámbrica	Realtek rtl8723be
	GPU	Gráficos HD Intel® para el procesador Intel® Celeron® serie N3000
	S.O	Wifislax LIVE 64bits
Equipo # 2		
Marca y modelo	Características	
ACER ASPIRE ES1-411	Procesador	Intel Celeron N2840 2,58 GHz
	Memoria RAM	2 GB
	Disco duro	500 GB
	Tarjeta inalámbrica	Broadcom bcm94313hmgb
	GPU	Gráficos HD Intel® para procesadores Intel Atom® serie Z3700

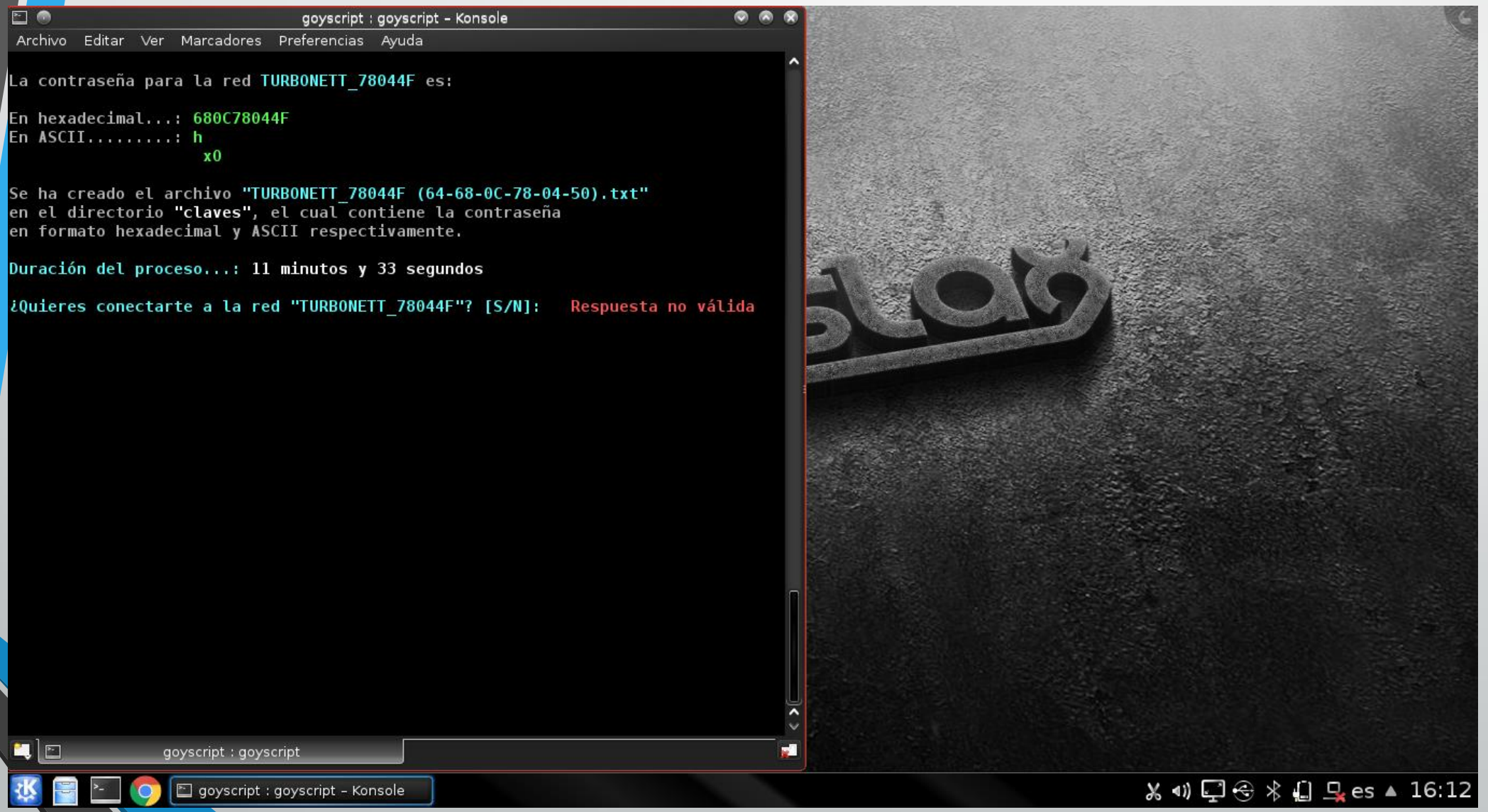
Prueba con Goyscript



Pruebas con Geminis Auditor




tmp : sh – Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
By geminis_demon | Versión script: 2.0beta9 | Versión DB: 20170602
Ataques disponibles para el objetivo seleccionado:
▶ Ataque Reaver (WPS) + todos los posibles PINes
▶ Ataque Reaver (WPS) + PIN genérico conocido
▶ Ataque Reaver (WPS) + algoritmo PixieWPS
▶ Ataque Reaver (WPS) + algoritmo ComputePIN
▶ Ataque Reaver (WPS) + algoritmo EasyboxWPS
▶ Ataque Reaver (WPS) + algoritmo DlinkPingen
▶ Ataque Reaver (WPS) + algoritmo BelkinPingen
▶ Ataque Reaver (WPS) + algoritmo TRENDnetWPS
◀ Volver al menú principal
tmp : sh
tmp : sh – Konsole
es
23:26


goyscript : goyscript – Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
La contraseña para la red TURBONETT_78044F es:
En hexadecimal...: 680C78044F
En ASCII.....: h
x0
Se ha creado el archivo "TURBONETT_78044F (64-68-0C-78-04-50).txt"
en el directorio "claves", el cual contiene la contraseña
en formato hexadecimal y ASCII respectivamente.
Duración del proceso...: 11 minutos y 33 segundos
¿Quieres conectarte a la red "TURBONETT_78044F"? [S/N]: Respuesta no válida
goyscript : goyscript
goyscript : goyscript – Konsole
es
16:12