

Simulación de hacking inalámbrico usando recursos de red y software libre

MANUAL TÉCNICO

Administración de servicios de red bajo Linux

Integrantes:

Córdova Balón Alex Alberto

Alcívar Peña Kevin Eduardo

Cevallos Salas Carlos Xavier

espol

Facultad de Ingeniería en
Electricidad y Computación

Resumen Ejecutivo

El siguiente proyecto basado en Hacking ético está conformado por estudiantes de la materia de Administración de Servicios de Red bajo Linux dictada en la carrera de Ingeniería en Telemática.

Mediante el uso de recursos de red y de software libre se busca vulnerar el protocolo de seguridad inalámbrica WPA con el fin de obtener las credenciales usadas para acceder a la red inalámbrica; además se pretende prohibir el acceso de determinados equipos a dicha red por medio de un software analizador de paquetes utilizada en el sistema operativo Kali Linux.

Descripción del problema

Las redes wifi han sido la masificación durante los últimos años, permitiendo la transferencia de una gran cantidad de información que puede ser vulnerable, esto nos obliga a entender cómo funcionan estos tipos de sistemas y como protegerlos de personas que harían un mal uso.

En la actualidad existen dos tipos de cifrado para la transferencia y protección de la información, cada uno con distintas características que incluyen seguridad. Características que deben ser tomadas en cuenta al momento de la instalación de una red inalámbrica.

WEP, es el primer sistema implementado para redes inalámbricas y aprobado como un estándar en 1999, que se disponía a entregar el mismo nivel de seguridad que las redes cableadas, sin embargo, este conllevó a un sin número de problemas, lo que permitía romperlo fácilmente, además de ser difícil de configurar.

WPA, usado como una mejora temporal de seguridad frente a los problemas presentados por WEP durante un año previo a que este fuera oficialmente descartado, WPA fue adoptado.

El nivel de vulnerabilidad de las redes wifi es el problema presentado, dado que esto depende de los distintos protocolos de seguridad inalámbricos que han ido apareciendo en los últimos años, además de los múltiples recursos que son usados para fracturar este tipo de barreras de encriptación.

Objetivos específicos

- ❖ Utilizar la tarjeta de red en modo monitoreo en Kali Linux como recurso para vulnerar una red inalámbrica y conseguir las credenciales de acceso a dicha red.
- ❖ Usar comandos pertenecientes al software libre Aircrack-ng para prohibir acceso de dispositivos específicos a la red.

Funcionamiento

Se realizará una simulación de hacking inalámbrico con una red configurada en base a la encriptación WAP en la clave de acceso, haciendo uso de una distro Linux, Kali y un software libre Aircrack-ng, que viene preinstalado en el Sistema Operativo. Todo realizado con recursos Open Source.

Recursos de Hardware y Software

Software

- ❖ La distribución Kali Linux, basada en Debian GNU/Linux, usada principalmente para auditorías y seguridad informática en general.
- ❖ Aircrack-ng, software diseñado para seguridad informática, con el fin de analizar paquetes en las redes y poder recuperar las contraseñas de los distintos modos de cifrado.
- ❖ GNS3 o Packet Tracer, son softwares que utilizaremos para realizar la topología de la red de ejemplo.

Hardware

Dado que usaremos una distro Linux, los requerimientos mínimos del pc (portátil) para esta práctica son:

- ❖ Espacio de almacenamiento en disco duro: 10 [GB] (sugerido 20 [GB])
- ❖ Memoria RAM: 1 [GB] (sugerido 3 [GB])
- ❖ Una tarjeta de red que pueda cambiarse de modo.
- ❖ Con respecto al procesador, soporta las distintas arquitecturas.
- ❖ Un módem o router para realizar la simulación de una red inalámbrica.

Software

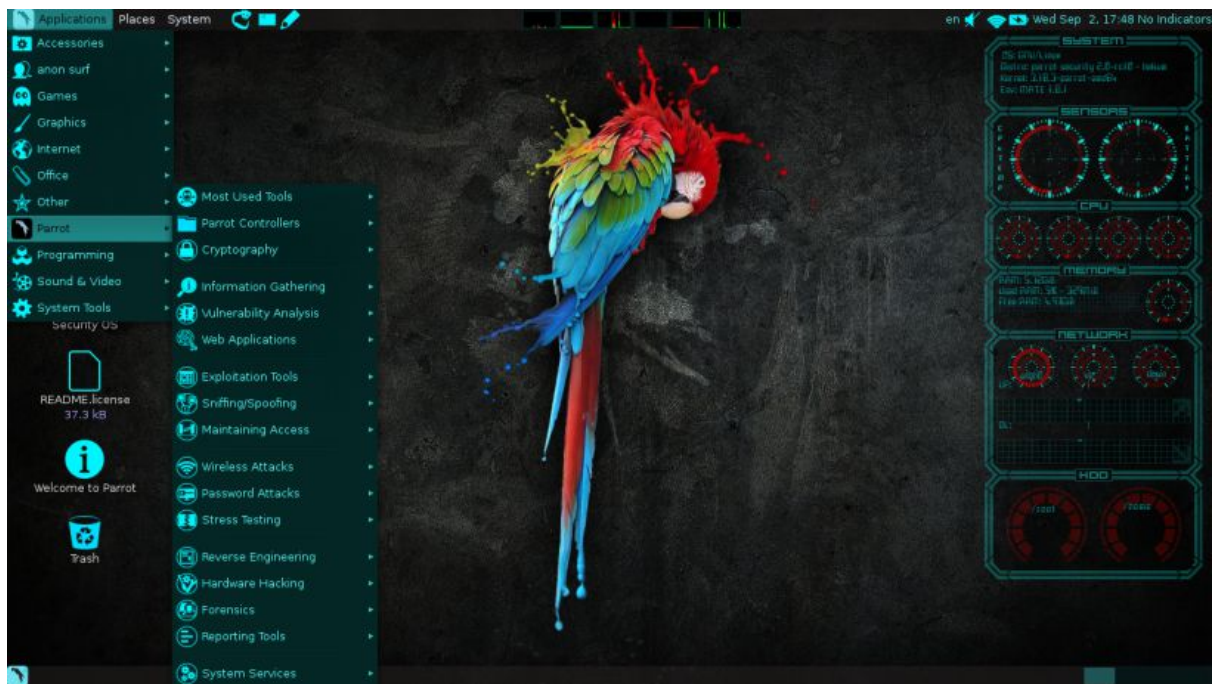



Ilustración 1 Interfaz de Linux

Programas similares a Aircrack-ng


Potente herramienta para descifrar claves WEP y WPA que te permitirá auditar tus redes WIFI



Xiaopan OS 6.4.1

Una aplicación que revela las claves de acceso de diferentes modelos de routers y tarjetas WiFi


Gratuito En Español



Wifiway 3.4

LiveCD con aplicaciones para auditoría de seguridad y análisis de redes WiFi, Bluetooth y RFID

Gratis (GPL) En Español



Wireless Network Watcher 2.21

Si estás harto de que tu vecino te robe wifi, instala esta aplicación para ver quién se conecta a tu red y mantenerlo a raya

Gratuito En Inglés

Ilustración 2 Programas Similares a Aircrack-ng

Status	<input type="radio"/> Disable Security
Quick Setup	
WPS	
Network	
Wireless	
- Wireless Settings	
- Wireless Security	
- Wireless MAC Filtering	
- Wireless Advanced	
- Wireless Statistics	
DHCP	
Forwarding	
Security	
Parental Control	
Access Control	
Advanced Routing	
Bandwidth Control	
IP & MAC Binding	
Dynamic DNS	
System Tools	

☒ **WPA/WPA2 - Personal(Recommended)**

Version:

Encryption:

Wireless Password:

(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: Seconds (Keep it default if you are not sure, minimum is 30, 0 means no update)

☐ **WPA/WPA2 - Enterprise**

Version:

Encryption:

Radius Server IP:

Radius Port: (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: (in second, minimum is 30, 0 means no update)

☐ **WEP**

Type:

WEP Key Format:

Key Selected	Key Type
WEP Key	

Wireless Security Help

You can select one of the following security options:

- **Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect this device without encryption. It is recommended strongly that you choose one of following options to enable security.
- **WEP** - Select 802.11 WEP security.
- **WPA/WPA2 - Personal** - Select WPA based on pre-shared passphrase.
- **WPA/WPA2 - Enterprise** - Select WPA based on Radius Server.

Each security option has its own settings as described follows,

WEP

Type - You can select one of following types,

- **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
- **Shared Key** - Select 802.11

Ilustración 3 Configuración del Router

Diagramas de diseño del proyecto

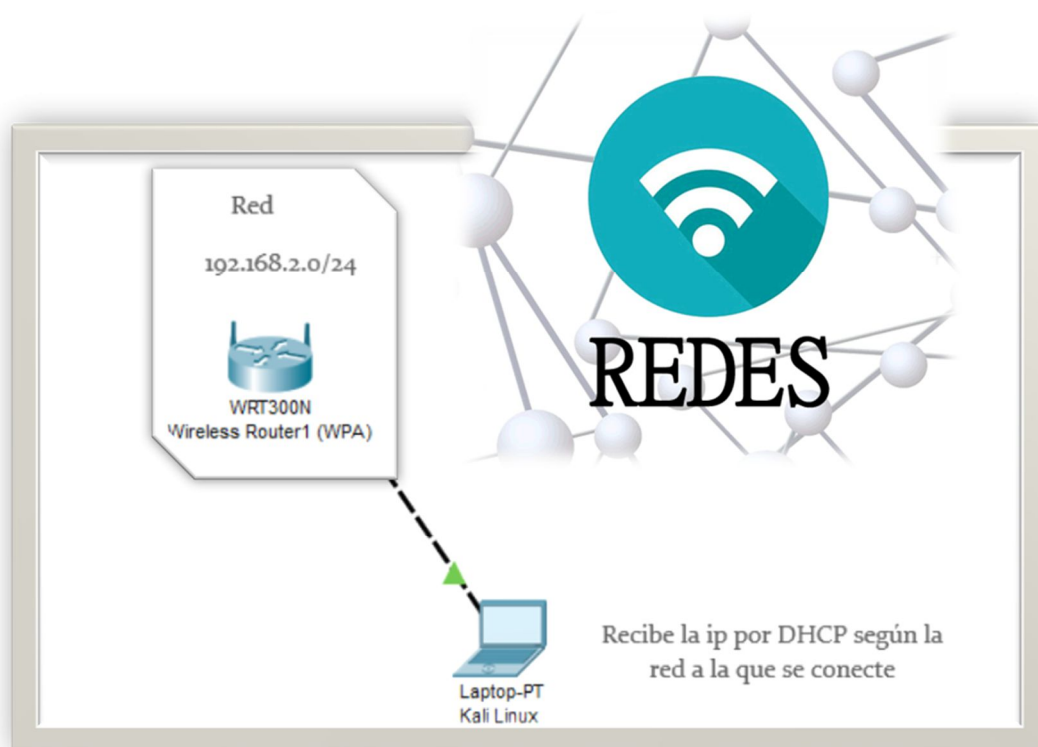


Ilustración 4 Diagrama

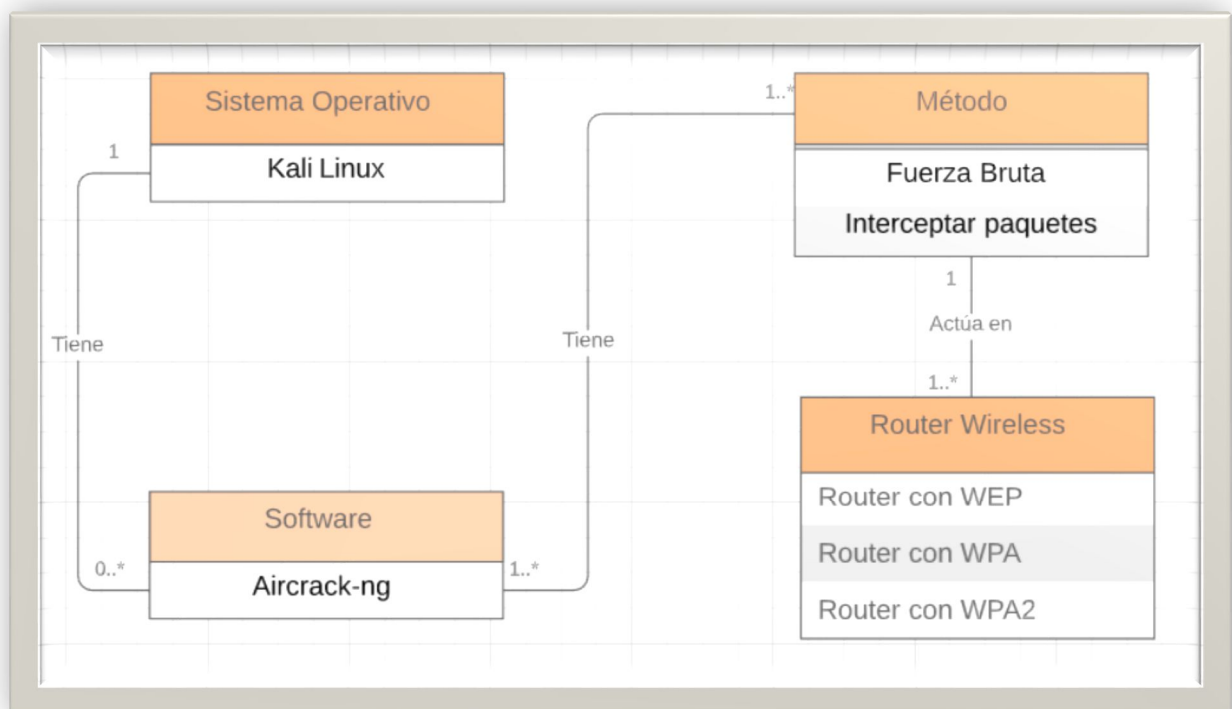


Ilustración 5 Modelo entidad/relación

Explicación del proyecto

Primero se necesita instalar el Sistema Operativo, con el cual vamos a realizar las pruebas de Pentesting.

En nuestro caso utilizamos la distro de Linux, Kali que cuenta con varios paquetes de herramientas de Pentesting.

Se procede a identificar cual herramienta es la mejor opción para el objetivo de este proyecto.

En este caso se utilizará la aplicación Aircrack-ng. Que es una aplicación que realiza un ataque de fuerza bruta para poder descifrar la contraseña de una red Wifi, por medio de un ataque de diccionario.

Descripción de comandos

- **airmon-ng check kill:** Este comando se encarga de analizar los procesos que se están ejecutando y detecta a los que podrían causar conflictos.
- **airmon-ng start wlan0:** Para poder obtener la contraseña descifrada, se necesita que la tarjeta de red se encuentre en modo monitor, para poder obtener varios valores e información necesaria para los siguientes procedimientos.
- **airodump-ng wlan0mon** Escanea todas las redes wifi que se encuentren alrededor y se puede observar a los clientes conectados a la red wifi con sus respectivas direcciones MAC's.
- **airodump-ng -c canal -w archivo.cap --bssid macDelRouter wlan0mon:** Esta aplicación esta a la espera de obtener el archivo en donde se encuentra cifrada la contraseña de la red Wifi (WPA-Handshake), el cual se obtiene al momento en que un cliente se autentique en la red.
- **aireplay-ng -0 5 -a macDelRouter -c macDeAlgunCliente wlan0mon:** Para evitar la espera de que un cliente se conecte, es necesario que exista algún cliente conectado y se procede a des autentificarlo de la red para obtener el WPA-Handshake.
- **crunch 8 8 -t %%%%%%%%%% 1234567890 | aircrack-ng -w - archivo.cap -e nombreDelRouter:** La aplicación Crunch se encarga de generar las posibles combinaciones y se las envía por medio de un Pipe al programa Aircrack-ng, el cual realiza los testeos de estas combinaciones

Conclusiones

- El estudiante tiene el conocimiento suficiente de cómo proteger los enrutadores de los piratas informáticos y cómo eliminar los errores.
- Los estudiantes podrán romper el cifrado WPA y WPA2, así como la autenticación de PIN de forma ética.

Bibliografía

- [1] «Udemy,» [En línea]. Available: <https://www.udemy.com/course/ethical-hacking-of-wifi-wpa-and-wpa2-encryption/>. [Último acceso: 31 1 2020].