Tecnológico de Monterrey

Instituto Tecnológico de Estudios Superiores de Monterrey
Campus Guadalajara

Aplicación de criptografía y seguridad (Gpo 302)

Reto | Fase 1

Francelio Uriel Rodriguez Garcia	A01352663
Juan Pablo Valenzuela Dorado	A00227321
Juan Pablo Bernal Lafarga	A01742342
Alfredo Murillo Madrigal	A01641791

Teachers:

Dr. Oscar Labrada

Dr. Rajesh Roshan Biswal

26 / Noviembre / 2023

Introducción

A medida que las redes inalámbricas se vuelven omnipresentes en nuestras vidas, las pruebas de penetración inalámbrica se han convertido en una habilidad clave en el repertorio del probador de penetración profesional. La distribución de seguridad de Kali Linux viene con una gran cantidad de herramientas que se utilizan para ataques de red y detección de lagunas de seguridad. Este proyecto presenta pruebas de penetración inalámbrica desde cero, presentando los elementos importantes de las pruebas de penetración con cada nueva tecnología.

Kali Linux es una distribución especializada en seguridad informática y pruebas de penetración, basada en Debian. Optamos por Kali Linux debido a su enfoque específico en herramientas y recursos para evaluaciones de seguridad. Su estabilidad y eficiencia en el rendimiento son fundamentales para entornos de pruebas y auditorías de seguridad. Al ser una distribución de código abierto, Kali Linux permite adaptar y personalizar el sistema según nuestras necesidades, proporcionando flexibilidad en la configuración de entornos de seguridad. Utilizamos VMware Workstation como software de virtualización, aprovechando su capacidad para crear y gestionar máquinas virtuales en un entorno de escritorio. Con esta combinación, podemos ejecutar Kali Linux y otros sistemas operativos simultáneamente, lo que resulta crucial para nuestras actividades de pruebas y desarrollo en el ámbito de seguridad informática.

El enfoque principal de la virtualización es crear entornos de computación virtuales que nos permitan ejecutar diversos sistemas operativos y aplicaciones en una sola computadora, esto resulta en una mejor utilización de la capacidad de procesamiento, memoria y almacenamiento. En otras palabras, al utilizar VMware Workstation para virtualizar y ejecutar Kali Linux, el propósito es crear un entorno de pruebas y desarrollo de seguridad informática de manera eficiente y flexible. Esto permite realizar evaluaciones de seguridad y pruebas de penetración en un entorno controlado y aislado.

Para realizar las evaluaciones de seguridad y pruebas de penetración de nuestra red utilizamos un adaptador USB AWUS1900 de la marca ALFA Network, este adaptador cumple con las características para realizar pruebas de penetración a una red wifi, alguna de ellas consta de que el adaptador debe tener capacidades esenciales, como compatibilidad con el modo monitor y la inyección de paquetes, permitiendo la monitorización y análisis efectivos de redes inalámbricas.

Objetivo

El desafío es obtener la contraseña correcta de su red WiFi doméstica a través de diferentes técnicas aprendidas y también evaluar las debilidades de esta red ya sea que utilicen

WEP, WPA o incluso WPA2, y sugerir cómo proteger las redes de los hackers informáticos. En este desafío, los estudiantes aprenderán diversas metodologías de pruebas inalámbricas hasta la cobertura detallada de métodos y ataques de hackeo.

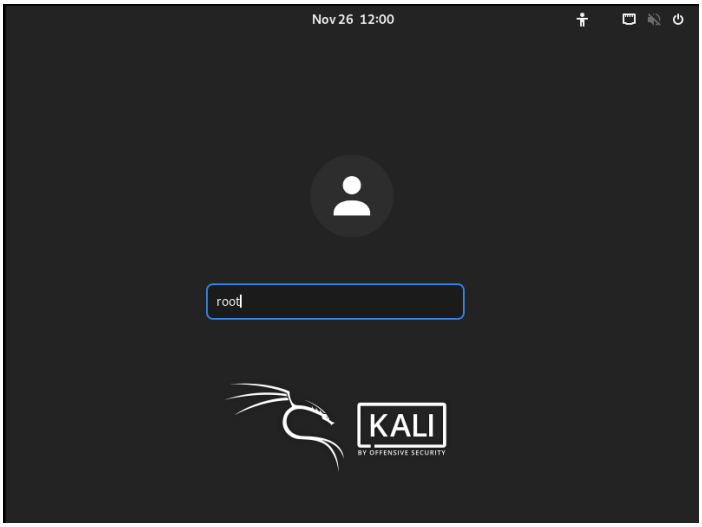
Metodología

El modo administrador (managed mode) es un modo de funcionamiento de una interfaz de red inalámbrica en la que la interfaz se asocia con un punto de acceso específico en una red inalámbrica. De este modo, la interfaz Wi-Fi se utiliza para conectarse y comunicarse con una red Wi-Fi.

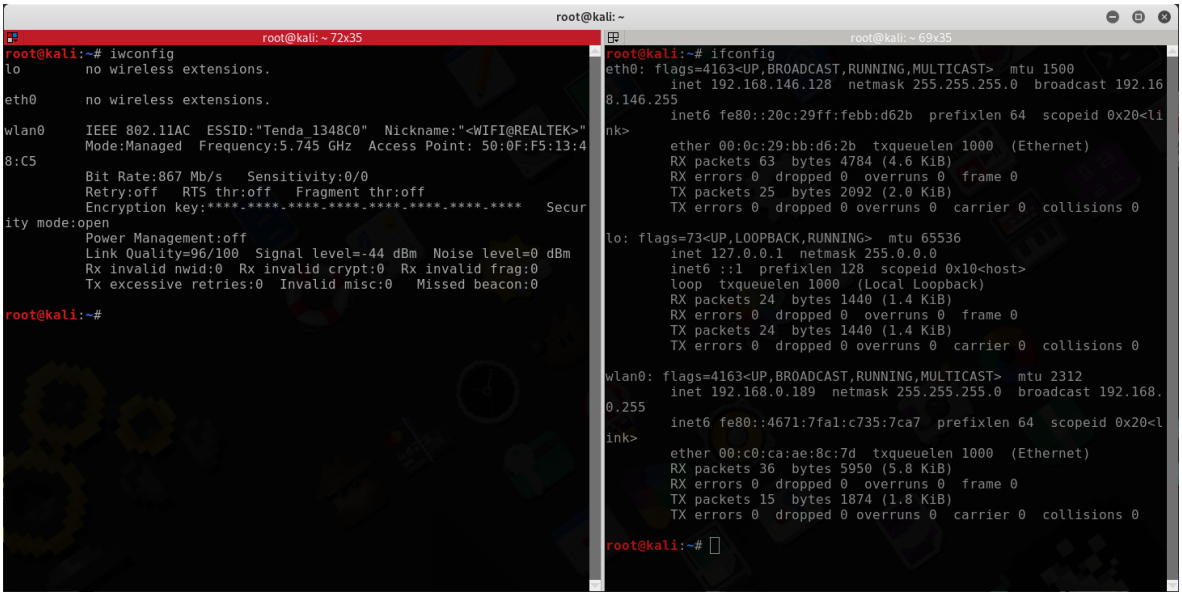
Una de las principales diferencias entre el modo administrador y monitorizado radica en su propósito y la funcionalidad. En el modo administrador, la interfaz Wi-Fi está asociada a un punto de acceso y se utiliza para la comunicación en una red específica.

En cambio, en el modo monitor, la interfaz se configura para capturar y analizar paquetes en el aire sin asociarse a una red específica, lo que es importante para las tareas de auditoría de seguridad y análisis de redes.

Dentro del contexto de pruebas de penetración y seguridad informática, el modo monitor es fundamental ya que le permite a los encargados de seguridad analizar el tráfico inalámbrico y realizar pruebas de seguridad sin la limitación de estar asociado a una red específica. Esto facilita la detección de posibles vulnerabilidades y la evaluación de la seguridad de las redes Wi-Fi.



Máquina Virtual Kali | Modo root

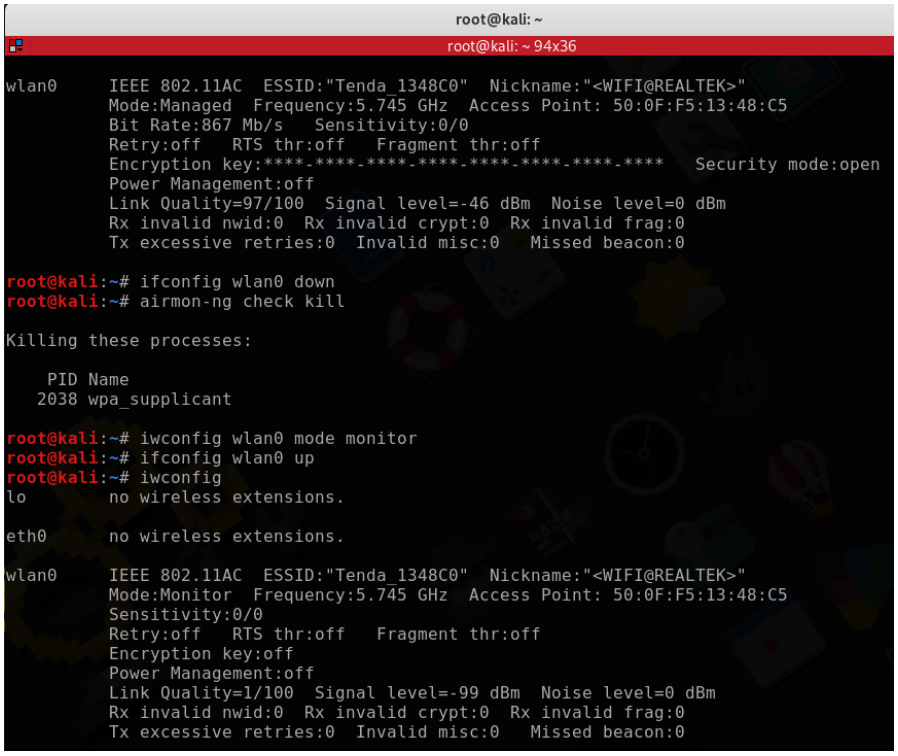


Configuración de la interfaz de red.

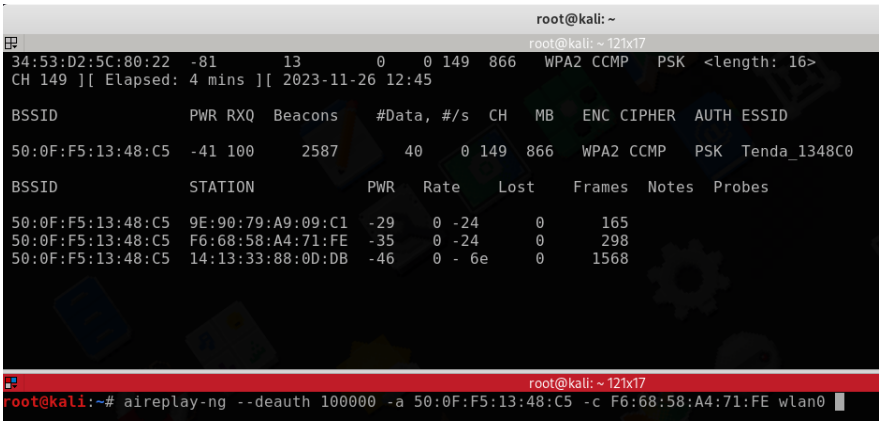
- ¿Qué diferencia observa con iwconfig e ifconfig en la máquina kali? ¿Qué información obtenemos de cada comando?

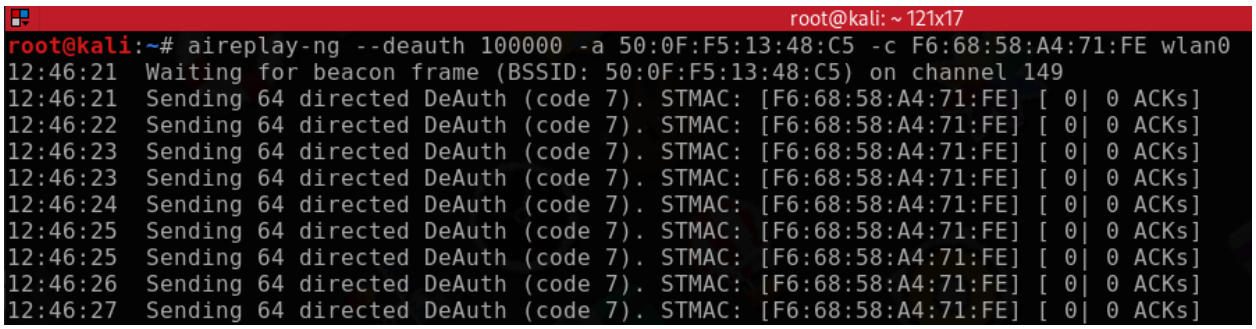
Comando	Función	Información proporcionada
iwconfig	Se utiliza para configurar y mostrar información **específica** sobre **interfaces** de redes inalámbricas	- Estado de la interfaz inalámbrica - ESSID al que está conectada la interfaz. - Poder de transmisión. - Frecuencia de transmisión. - Modo de Operación - Calidad y fuerza de la señal.
ifconfig	Se utiliza para configurar y mostrar **información** sobre **todas** las **interfaces** de red en el sistema, tanto inalámbricas como con cable Ethernet	- Dirección IP de la interfaz - Máscara de red. - Dirección MAC. - Estadística de tráfico. - Estado de la interfaz.

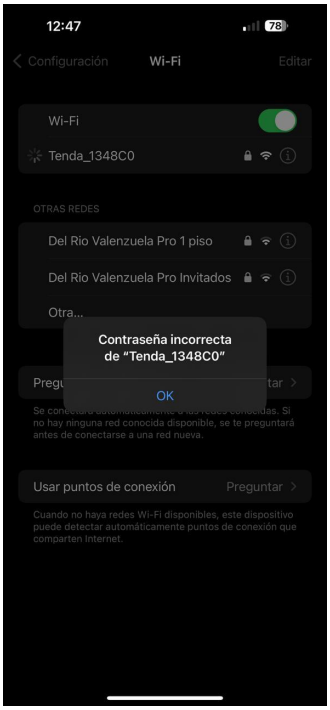
- Localice su adaptador inalámbrico y cámbielo al modo monitor (Captura la pantalla)



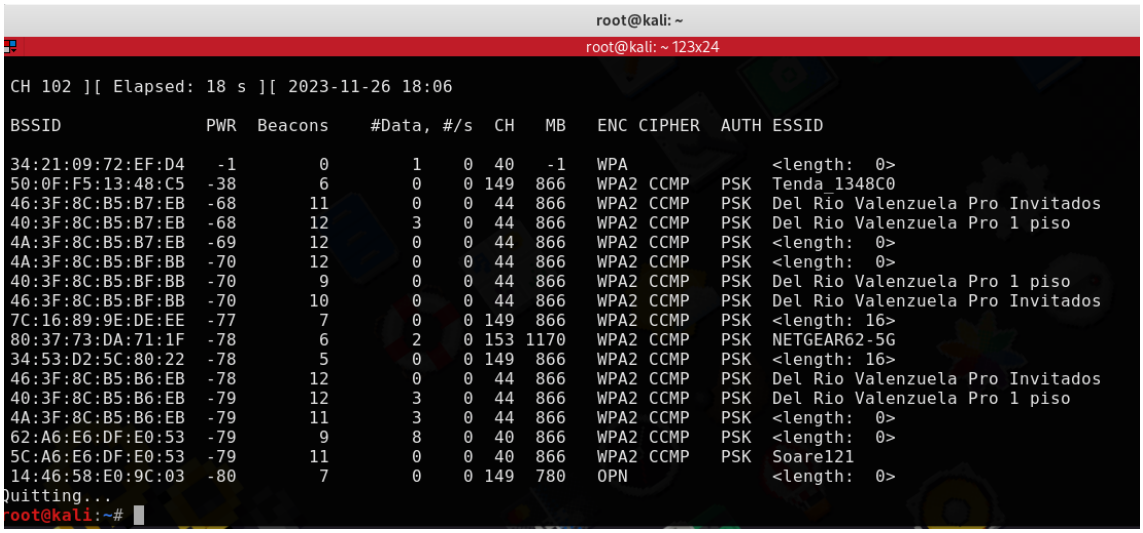
- Haz un “fake authentificacion” para conectar a la red. (Captura la pantalla)

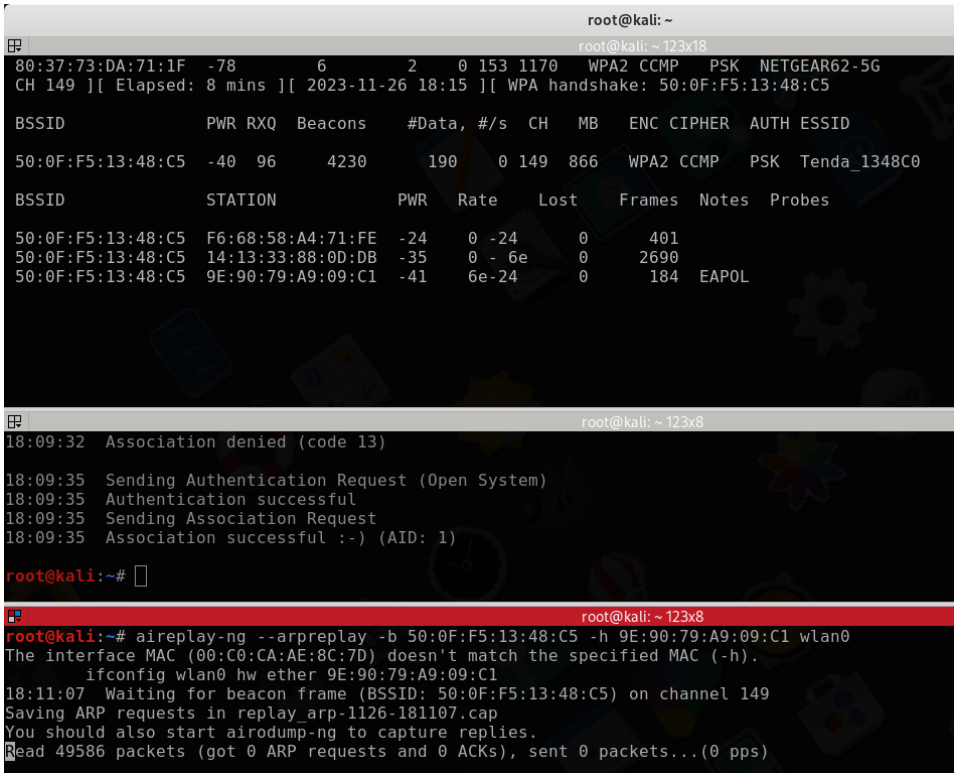






- Haz un ARP request para la red (Captura la pantalla)





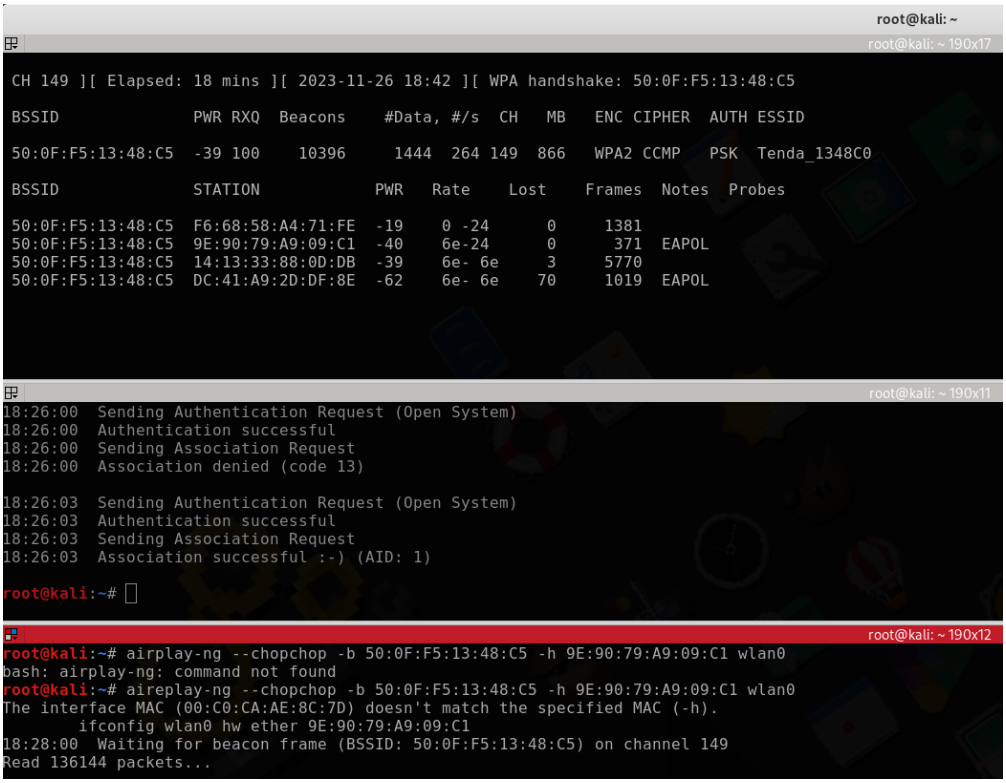
Tiempo de ejecución de comandos más de 30 min

Para hacer un ARP request es necesario que la red tenga una seguridad WEP y que la red no esté segmentada, lamentablemente esta técnica hoy en día es obsoleto en la mayoría de los routers ya que tienen configurado por defecto una seguridad WPA o WPA2, donde inclusive en algunos casos la compañía proveedora de servicios no permite el cambio de protocolo de seguridad. Y por si no fuera suficiente, con la implementación de puntos de acceso en los módems por parte de las compañías proveedoras de internet, las redes ahora están segmentadas, impidiendo así que se efectúe la técnica de ARP request.

- Cual es la diferencia entre el ataque chop chop y ataque de fragmentación.

  Un ataque chop chop y un ataque de fragmentación son dos formas de romper el cifrado WEP de las redes inalámbricas. El primero consiste en modificar y enviar paquetes cifrados para obtener la clave WEP, mientras que el segundo consiste en crear y enviar paquetes cifrados para acceder a la red sin la clave WEP. Ambos ataques son muy rápidos y peligrosos, por lo que se recomienda usar protocolos más seguros como WPA o WPA2.

- Packet injection (chop chop) (capturar la pantalla en cada paso)
    - Captura un paquete y determina el flujo de llaves(key stream)
    - Forjar un nuevo paquete
    - Inyectar el paquete forjado a la red para generar nuevo IV y decriptar

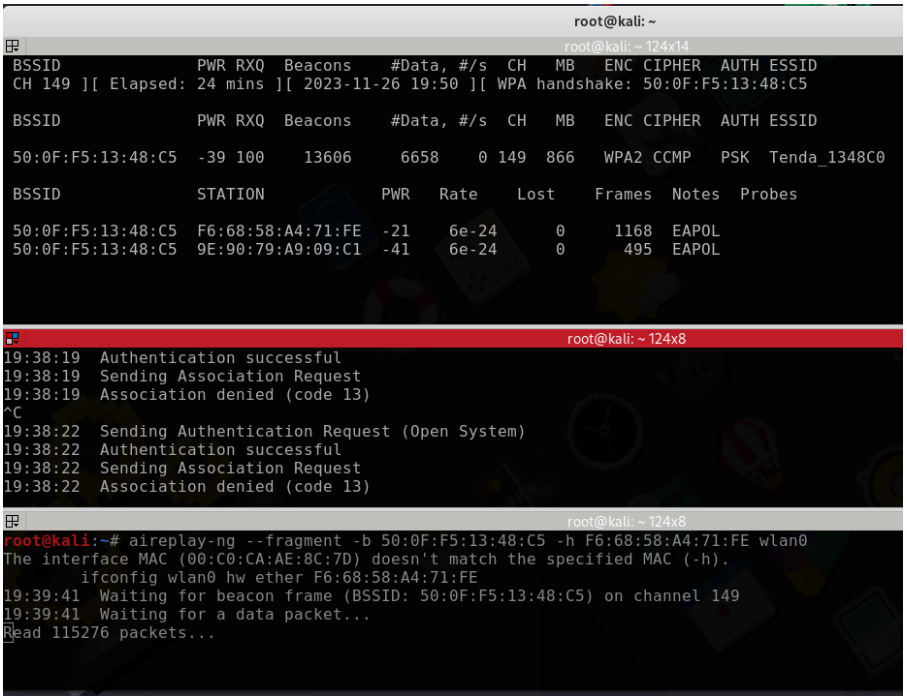


Tiempo de ejecución de comandos más de 20 min.

El objetivo de capturar e inyectar paquetes para generar IV, es determinar la encriptación y así romperla, obteniendo la clave de los paquetes inyectados y usandola con ciertos paquetes de la red.

Es importante aclarar que una red WPA2 utiliza una encriptación más fuerte en comparación con WEP. WEP ha demostrado ser vulnerable a varios ataques, incluidos los basados en la inyección de paquetes. WPA2, por otro lado, utiliza algoritmos de cifrado más robustos como AES que son considerablemente más seguros, es por ello que el tiempo de ejecución de los comandos para la inyección son más largo y difíciles de acceder en una red WPA2 que en una red WEP.

- Packet injection (fragmentation) (capturar la pantalla en cada paso)
    - Obtener PRGA (pseudo random generation algorithm)
    - Forjar un nuevo paquete
    - Inyectar el paquete forjado a la red para generar nuevo IV y decriptar



Tiempo de ejecución de comandos más de 20 min.

Cómo mencionamos antes, una red WEP utiliza un cifrado más débil y ha demostrado ser vulnerable a este tipo de ataques, basados en la inyección de paquetes. Esto se debe en parte al uso de claves estáticas y al algoritmo RC4 para generar la secuencia de claves.
WPA2, por otro lado, utiliza un cifrado más robusto, como AES, que es considerablemente más seguro que el algoritmo utilizado por WEP. Además, WPA2 utiliza un protocolo de autenticación más robusto que WEP, lo que hace que sea más difícil comprometer la seguridad de la red.
Basándonos en lo anterior, nuestra red doméstica está protegido por WPA2, es por ello que difícilmente se pudo acceder a la red, debido a la alta seguridad de la red, sin embargo si nuestra red fuera una red WEP, fácilmente pudiéramos realizar el ataque exitosamente.

- Explica cómo se puede hackear explotando WPS

Para acceder a una red Wi-Fi protegida con WEP, podemos usar la técnica de fake authentication, que consiste en asociarse con el punto de acceso usando credenciales falsas o modificadas, pero que el router acepta como válidas. De esta forma, podemos enviar y recibir paquetes de datos sin conocer la contraseña de la red.

Una vez conectados al router, podemos usar reaver, una herramienta que explota una vulnerabilidad en el protocolo WPS (Wi-Fi Protected Setup), que permite conectar dispositivos sin introducir una contraseña, solo un PIN de 8 dígitos. Reaver realiza un ataque de fuerza bruta

sobre el PIN de WPS, probando diferentes combinaciones hasta acertar el correcto. Luego, usa el PIN para calcular la contraseña de la red y mostrarla al usuario.

Así, podemos hackear una red Wi-Fi usando fake authentication y reaver, sin necesidad de capturar ningún paquete cifrado ni realizar ningún análisis de tráfico. Sin embargo, este método solo funciona con redes que usan WEP y WPS, que son protocolos inseguros y obsoletos. Para redes que usan WPA o WPA2, que son protocolos más seguros y actuales, se requieren otros métodos más complejos y lentos.

Conclusión:

El proyecto realizado se enfoca en la aplicación de criptografía y seguridad, específicamente en pruebas de penetración inalámbrica. Utilizando la distribución especializada en seguridad informática Kali Linux y el software de virtualización VMware Workstation, creamos un entorno de pruebas eficiente y flexible.

El objetivo del proyecto es realizar pruebas de penetración inalámbrica, centrándonos en la obtención de contraseñas de redes WiFi domésticas y evaluando las debilidades de estas redes, ya sea utilizando WEP, WPA o WPA2. La metodología incluye el uso de un adaptador USB AWUS1900 de ALFA Network con capacidades esenciales, como modo monitor y inyección de paquetes, para realizar evaluaciones de seguridad de manera efectiva.

Estudiamos diferentes técnicas, como el cambio al modo monitor, la autenticación falsa, ARP requests, ataques chop chop y de fragmentación, y explotamos vulnerabilidades en el protocolo WPS. También destacamos la importancia del modo monitor en las pruebas de penetración, permitiendo el análisis del tráfico inalámbrico sin estar asociados a una red específica.

Además, de señalar la obsolescencia de ciertas técnicas, como ARP requests en redes con seguridad WPA/WPA2 y la segmentación de redes que impide su aplicación.Sería factible para futuros proyectos trabajar con redes con seguridad WEP para que la práctica resulte exitosa.

En resumen, el proyecto demuestra la aplicación práctica de conocimientos en seguridad informática y pruebas de penetración inalámbrica, utilizando herramientas especializadas y técnicas avanzadas para evaluar la seguridad de las redes WiFi.

Referencias

Altube, R. (2023). *Kali Linux: Qué es y características principales*. OpenWebinars.net. https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/

Asia, S. de la información, & Seguridad de la información AsiaInformation Security Asia es el sitio web de referencia para conocer las últimas noticias sobre tecnología y ciberseguridad en varios sectores. Nuestros redactores expertos brindan información y análisis en los que puede co. (2023). *¿Qué es WPA (acceso protegido wi-fi)?*. Information Security Asia. https://informationsecurityasia.com/es/what-is-wpa/

Carloslopezjurado. (2023). *Qué son los ataques por fragmentación*. CCM. https://es.ccm.net/aplicaciones-e-internet/museo-de-internet/enciclopedia/11064-que-es-un-ataque-por-fragmentacion/

Cybolt. (2022). *Las 10 mejores herramientas para Pruebas de Penetración*. https://cybolt.com/blog/las-10-mejores-herramientas-para-pruebas-de-penetracion/

Pruebas de Penetración Para Principiantes: 5 Herramientas Para Empezar. Inicio. (n.d.). https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar