15. Hackeando Redes Inalámbricas

Julio Javier Iglesias Pérez

Tipos

- Extensión de una red cableada.
- Access Points múltiples.
- Conexión de Redes Lan-a-Lan
- 3g Hotspot

Estándares

- 802.11a: Hasta 54 Mbps, frecuencia 5 GHz.
- 802.11b: Hasta 11 Mbps, frecuencia 2.5 GHz.
- 802.11g: Hasta 54 Mbps, frecuencia 2.4 GHz.
- 802.11i: WLAN encriptación mejorada para los estándares anteriores.

Estándares

- 802.11n: Múltiples entradas y salidas (MIMO) para darle más velocidad (más de 100 Mbps) y más rango.
- 802.16: Grupo de estándares para Metropolitan Area Networks (MANs).
- Bluetooth: Suporta un pequeño rango (10 metros) y relativamente poco ancho de banda (1-3 Mbps) diseñado para redes de pequeño poder

Service Set Identifier (SSID)

Identificador de una red Wi-Fi. Es una clave secreta, no una clave pública.

Wi-Fi Hotspot Finder

jiwire.com. Es un hotspot que muestra más de 338,271 hotspots gratuitas y pagadas en 144 países.

Otro: WeFi.com

Tipos de antena

- Antena omnidireccional: Provee 360 grados, utilizada pos las estaciones base.
- Antena con rejilla parabólica: Basado en el principio del plato satelital. Puede obtener señales Wi-Fi de 10 millas de distancia o más. Permite

a los atacantes tener mejor señal y más poder para Ataques de capa 1 DoS y MITM.

Tipos de antena

- Antena Yagi: Antena unidireccional comúnmente utilizada en comunicaciones de frecuencia de banda de 10 MHz a VHF y UHF.
- Antena Dipole: Bidireccional, utilizada para soportar conexiones de cliente en vez de aplicaciones site-to-site

Encriptación Wi-Fi

Tipos de encriptación

- WEP: Obsoleto y con poca seguridad, puede ser crackeado fácilmente.
- WPA: Utiliza encriptación 48 bit IV, 32 bit CRC y TKIP.
- WPA2: Utiliza encriptación de datos AES (128 bit) y CCMP.
- WPA2 Enterprise: Integra estándares de encriptación EAP con encriptación WPA.
- TKIP: Protocolo de seguridad utilizado en WPA en remplazo para WEP.

Encriptación Wi-Fi

- LEAP: Autenticación WLAN desarrollada por Cisco.
- RADIUS: Autenticación centralizada y sistema de administración de autorización.
- 801.11i: Es un estándar IEEE qe especifica mecanismos de seguridad para 802.11.
- AES: Encriptación de llave simétrica, utilizada en WPA2 como remplazo de TKIP.
- EAP: Utiliza métodos de autenticación múltiple, como token cards, kerberos, certificados, etc.
- CCMP Utiliza claves de 128 bits con un vector de inicialización (IV) para detección de repetición.

¿Cómo romper la encriptación WEP?

- Iniciar la interfaz wireless en modo monitoreo en el canal específico del AP.
- Probar la capacidad de inyección del dispositivo en el AP.
- Utilizar herramientas como aireplay-ng para falsificar una autenticación con el AP.
- Arrancar la herramienta sniffing como airodump-ng o Cain & Abel con filtro bssid para conectar un IV único.

¿Cómo romper la encriptación WEP?

- Iniciar una herramienta de encriptación de paquetes WI-FI como aireplay-ng en modo ARP request replay para inyectar paquetes.
- Ejecutar una herramienta como Cain & Abel o aircrack-ng para extraer la llave de encriptación del IV.

¿Cómo romper la encriptación WPA/WPA2?

WPA PSK: Utiliza una clave predefinida para inicializar el TKIP. Ataque de diccionario

- Claves WPA por fuerza bruta: Con herramientas como aircrack, aireplay, KisMac para realizar el ataque de fuerza bruta.
- Ataque offline: Estar cerca del AP unos segundos para capturar la autenticación handshake WPA/WPA2, capturando los paquetes correctos, se puede crackear las claves

¿Cómo romper la encriptación WPA/WPA2?

WPA offline.

- Ataque de de-autenticación: Forzar a un cliente conectado a desconectarse, luego capturar la reconexión y paquete de autenticación utilizando herramientas como airplay, luego realizar un ataque de diccionario fuerza bruta al PMK.

¿Cómo defenderse?

- Con contraseñas sumamente complicadas será casi imposible crackear.
- Utilizar encriptación AES/CCMP.
- Seleccionar una passphrase random, con un mínimo de 20 caracteres.
- Utilizar VPN, Remote Access VPN, Extranet VPN, Intranet VPN, etc. Implementar Network Access Control (NAC) o Network Access Protection (NAP).

Amenazas Wireless

- Ataques de Control de Acceso: Los ataques de control de acceso Wireless tienen como objetivo penetrar una red evadiendo los controles de medida de acceso WLAN.
- Ataques de integridad: Los atacantes envían control falsificado, administración o marcos sobre la red wifi para dirigir mal los dispositivos para realizar otro tipo de ataque (Ej: DoS).

Amenazas Wireless

- Ataques de confidencialidad: Estos ataques intentan interceptar información confidencial enviadas sobre las asociaciones wifi.
- Ataques de disponibilidad: Los ataques DoS tienen como objetivo impedir que los usuarios legítimos accedan a sus recursos en la red Wifi.

Amenazas Wireless

- Ataques de autenticación: Tienen como objetivo robar la identidad de los clientes wifi, información personal, credenciales de inicio se sesión, etc. para obtener acceso no autorizado a los recursos de la red.
- Ataque Rogue AP: Son AP puestos dentro de la red 802.11 y pueden ser utilizados para hijackear las conexiones de usuarios legítimos de la red. Cuando un usuario inicia su equipo, estos AP ofrecerán conectarse a la red de la NIC del usuario. Todo el tráfico del usuario pasará por este AP, así habilitara un sniffer.

Amenazas Wireless

- Client mis-association: El atacante configura un AP roque fuera del perímetro de la red y atrae al empleado de la organización a conectarse a él. Una vez asociado, los empleados pueden saltar las políticas de seguridad de la empresa.

Amenazas Wireless

- Ataques de mala configuración AP:
  - SSID Broadcast. Los AP son configurados para difundir SSIDs a los usuarios autorizados.
  - Password débil. Para verificar usuarios autorizados, los administradores de la red incorrectamente utilizan los SSIDs y las contraseñas.
  - Error de configuración. Permite a los intrusos robar el SSID y así engañar al AP que tienen permiso de conectarse.

Amenazas Wireless

- Asociación no autorizada: Los AP software son tarjetas o WLAN radios embebidos en algunos PDSs y laptops que pueden ser utilizados para lanzar inadvertidamente un programa virus. Los atacantes infectan el equipo de la víctima y activan software APs permitiendo tener una conexión no autorizada a la red de la empresa. El atacante se conecta a la red a través de software AP en vez del AP real.

Amenazas Wireless

- Ataque de conexión Ad Hoc: Comunica clientes wifi directamente y no requiere AP. Es inseguro porque no provee autenticación o encriptación seguras. El atacante puede conectarse fácilmente y comprometer el S.O. del cliente.
- Ataques HoneySpot: El atacante atrapa las víctimas utilizando hotspots falsos.
- AP MAC Spoofing: El hacker falsifica la dirección MAC de un cliente WLAN, enmascarándose en un cliente autorizado.

Amenazas Wireless

- Ataque DoS: Interrumpe las conexiones wifi difundiendo comandos de-autenticación. Fuerza a los clientes a desconectarse del AP.

Amenazas Wireless

- Ataque Jamming Signal (Bloqueo de señal): Utilizando un amplificador de alto poder, derriba las conexiones, estas señales generadas por estos dispositivos (jamming devices) aparentan ser una transmisión 802.11, pero en realidad es un ataque DoS.
- Ejemplos de dispositivos Jamming:
  - MGT-P6 PGS Jammer
  - MGT-02 Jammer
  - MGT-MP200 Jammer
  - MGT-03 Jammer
  - MGT-P6 WI-FI Jammer
  - MGT-P3x13 Jammer

Metodología Wireless Hacking

Metodología: Su objetivo es comprometer una red Wi-Fi, para obtener acceso no autorizado a los recursos de la red.

- WI-FI Discovery
- GPS Mapping
- Wireless Traffic Analysis
- Launch Wireless Attacks
- Crack Wi-Fi encryption

Encontrar redes Wi-Fi para atacarlas

Revisar redes potenciales que estén en un rango para encontrar la mejor para atacar.

Para descubrir redes Wi-Fi se necesita: Laptop con tarjeta wifi, antena wifi externa, programas de descubrimiento.

Herramientas utilizadas: inSSIDer, NetSurveyor, NetStumbler, Vistumbler, etc.

Footprint la red Wireless.

Los ataques comienzan descubriendo y footprint la red wireless en modo activo o pasivo.

- Método Pasivo: Un atacante puede utilizar el camino pasivo para detectar la existencia de un AP olfateando los paquetes desde las ondas, que revelarán el AP, SSID.
- Método activo: El dispositivo wifi del atacante envía una sondeo con el SSID para ver si el AP responde. Si el dispositivo no tiene el SSID al principio, enviará un sondeo con SSID vacío.

Footprint la red Wireless.

Herramientas: inSSIDer, NetSurveyor, NetStumbler, Vistumbler, WirelessMon, etc.

GPS Mapping

Los atacantes crean un mapeo de redes Wifi descubiertas y crean una base de datos con estadísticas recolectadas por las herramientas de descubrimiento WiFi. Luego se rastrea la locación de las redes WiFi descubiertas y sube las coordenadas a sitios como WIGLE. Los atacantes comparten esta información a la comunidad hacking.

GPS Mapping

Herramienta WIGLE: Consolida locaciones e información sobre redes wifi.

Herramienta: Skyhook: Determina la locación de los WPF (WIFI Positioning System) a una base de datos masiva mundial.

¿Cómo descubrir redes Wifi utilizando Wardriving?

Paso 1. Registrar en Wigle y descargar los mapas de su área.

Paso 2. Conectar la antena, el dispositivo GPS a la laptop vía USB.

Paso 3. Instalar y ejecutar NetStumbler y WIGLE y encender el GPS.

Paso 4. Conducir un auto a 35 mph o menos (a mayores velocidades la antena no podrá detectar WIFI)

¿Cómo descubrir redes Wifi utilizando Wardriving?

Paso 5. Capturar y guardar los logs del NetStumbler que contiene las coordenadas GPS

Paso 6. Subir el log a WIGLE y grafica los puntos en un mapa.

Wireless Traffic Analysis

- Identificar vulnerabilidades. Permite a los atacantes a identificar vulnerabilidades, determinar la estrategia apropiada y de esa manera se puede realizar un ataque sniff y analizar los paquetes de la red.
- Reconocimiento WiFI: Analizan la red para determinar SSID difundidos, presencia de varias AP, posibilidad de recuperar SSIDs, métodos de autenticación utilizados, algoritmos de encriptación WLAN.

Herramientas: Wireshark/Pilot Tool. Omnipeek. CommView. AirMagnet WIFI Analyzer.

Tarjetas y chipsets Wireless

- Determinar los requerimientos wifi.
- Aprender sobre las capacidades de la tarjeta wifi.
- Determinar el chipset de la tarjeta wifi.
- Verificar las capacidades del chipset.
- Determinar los controladores y parches requeridos.

Tarjetas y chipsets Wireless

- WiFI USB Dongle: AirPcap. Captura dados 802.11. Decripta frames. Inyección de tráfico. Trabaja con Wireshark

- Wifi Packet Sniffer: Wi-Fi Pilot. Mide el canal de utilización wireless. Ayuda a identificar las redes wireless rogue. Provee informes profesionales y detallados.

- Wi-Fi Packet Sniffer OmniPeek: Visibilidad y análisis en tiempo real. Actividad de la red wireless. Monitoreo comprensible.

¿Qué es Análisis de espectro?

- Examinan el radio de transmisión WiFi, y mide la amplitud de las señales. Emplea análisis estadístico. Fuentes de interferencia. Detección de ataques.
  AirMagnet Wi-FI

Analyzer, Wi-Spky and Chanalyzer, WifiEagle, etc.

Lanzamiento de ataques Wireless

Aircrack-ng suite: Consiste en un detector, packet sniffer, WEP y WPA/WPA2-PSK cracker y herramienta de análisis para WIFI. Trabaja en Windows y Linux.

La suite consta de:

Lanzamiento de ataques Wireless

- Airbase-ng: Caputara handshare WPA/WPA2, puede actuar como un AP ad-hoc.
- Aireplay-ng: Utilizado para la generación de tráfico, autenticación falsa, packet replay, solicitud de inyección ARP.
- Airmon-ng: Habilita el modo monitor para las interfaces wireless.
- Aircrack-ng: Cracking tool WEP, WPA/WPA2-PSK de facto.

Lanzamiento de ataques Wireless

- Aircrack-ng: Cracking tool WEP, WPA/WPA2-PSK de facto.
- Airgraph-ng: Crea una relación cliente a AP.
- Airtub-ng: Inyecta marcos dentro de una red WPA TKIP.
- Airdecap-ng: Decripta WEP/WPA/WPA2 y puede ser utilizado para despojar los encabezados wireless de los paquetes WiFi.

Lanzamiento de ataques Wireless

- Easside-ng: Permite comunicar vía AP WEP (encriptado) sin saber la clave WEP.
- Airdeclak-ng: Quita el encubrimiento de un archivo pcap.
- Airodump-ng: Utilizado para capturar paquetes de marcos 802.11 y capturar los IVs WEP.
- Packetforge-ng: Utilizado para crear paquetes encriptados que sub consecuentemente pueden ser utilizados para inyección.

Lanzamiento de ataques Wireless

- Airdriver-ng: Provee información del estado de los controladores wireless en su sistema.
- Airlib-ng: Almacena y administra eesid y listas de contraseña utilizadas para crackear WPA/WPA2.
- Tkiptun-ng: Crea una interfaz de túnel virtual para monitorear tráfico encriptado e inyectar tráfico arbitrario dentro de la red.

Lanzamiento de ataques Wireless

- Airdrop-ng: Utilizado para el objetivo, reglas basadas en de-autenticación de usuarios.
- Airserv-ng: Permite múltiples programas utilizar independientemente la tarjeta wifi medíante una conexión TCP cliente servidor.
- Wesside-ng: Incorpora un número de técnicas para obtener claves WEP sin problemas en minutos.

Lanzamiento de ataques Wireless

Paso 1: Ejecutar airmon-ng en modo monitoreo.

Paso 2: Iniciar airdump para descubrir SSIDs en la interface.

Paso 3: De-autenticar (deauth) al cliente para revelar el SSID escondido utilizando aireplay-ng.

Paso 4: Cambiar a airodump para ver el SSID revelado.

Lanzamiento de ataques Wireless

Ataque de fragmentación

- Puede obtener 1500 bytes de PRGA (pseudo random generation algorithm). Este ataque no recupera la clave WEP por si solo. El PRGA puede utilizarse para generar paquetes con packetforge-ng que es utilizado para varios ataques de inyección. Requiere al menos un paquete de dato para ser recibido desde el AP para iniciar el ataque.

Lanzamiento de ataques Wireless

¿Como lanzar un ataque MAC Spoofing?

Para cambiar la dirección MAC en Linux:

```
ifconfig wlan0 down
ifconfig wlan0 hw ether 02:25:ab:4c:2a:bc
ifconfig wlan0 up
```

SMAC para cambiar en Windows, genera MAC de acuerdo al fabricante seleccionado.

Lanzamiento de ataques Wireless

DoS: Ataques de De-autenticación y desasociación

Lanzamiento de ataques Wireless

Ataque MitM utilizando Aircrack-ng

Paso 1: Ejecutar airmon-ng en modo monitoreo.

Paso 2: Ejecutar airodump para descubrir SSIDs en la interfaz.

Paso 3: De-autenticar el cliente utilizando aireplay-ng.

Paso 4: Asocial la tarjeta wireless con el AP que se está accediendo con aireplay-ng.

Lanzamiento de ataques Wireless

Ataque Wireless ARP Poisoning

Lanzamiento de ataques Wireless

Rogue Access Point

- Elegir una localidad apropiada para colocar el rogue AP que permite mayor cobertura desde tu punto de conexión.
- Deshabilitar la difusión SSID (modo silencioso) y las características de administración para impedir detección.
- Colocar el AP detrás del firewall si es posible para impedir scaners de red.

- Implementar el rogue AP por periodos cortos.

Lanzamiento de ataques Wireless

Evil Twin: Es un AP que pretende ser un AP legítimo replicando un nombre de red. El atacante configura el rogue AP fuera del perímetro de la red y atrae al usuario a iniciar sesión con el AP equivocado. una vez asociado, los usuarios pueden saltar la política de seguridad tanto a los atacantes acceso a los datos de la red. Evil Twin puede ser configurado con un SSID residencial común, hotspot SSID, o SSID de la WLAn de la compañía.

Lanzamiento de ataques Wireless

¿Cómo configurar un hotspot falso (Evil Twin)?

1. Se necesita de una laptop con conexión a Internet (3G o conexión con cable) y un mini AP.
2. Habilitar Internet Conexion Sharing en Windows 7 o Internet Sharing en Mac OS X.
3. Difundir la conexión WIFI y ejecutar un programa sniffer para capturar contraseñas.

Crack al cifrado Wifi

¿Cómo crackear WEP utilizando Aircrack?

1: airmon-ng start eth1

2: airodump-ng --ivs --write capture eth1

3: aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1

4: aireplay-ng -3 -b 1e:64:51:eb:ff:3e -h a7:71:fe:8e:d8:25 eth1

5: aircrack-ng -s capture.ivs

Crack al cifrado Wifi

¿Cómo crackear WPA-PSK utilizando aircrack?

Paso 1: Monitorear el tráfico wireless con

airmon-ng

airmon-ng start eth1

Paso 2: Recolectar los datos del tráfico con

airodump-ng

airodump-ng --write capture eth1r

Crack al cifrado Wifi

Paso 3: De-autenticar el cliente utilizando aireplay-ng. El cliente intentará autenticar con AP lo que conducirá a capturar a airodump el paquete de autenticación (WPA handshake).

```
aireplay-ng --deauth 11 -a 02:24:2B:CD:68:EE
```

Paso 4: Ejecutar el archivo de captura a través de aircrack-ng

```
aircrack-ng.exe -a 2 -w capture.cap
```

Crack al cifrado Wifi

- Herramienta de crack WPA: KisMAC
- Se puede realizar ataques de fuerza bruta a las contraseñas WEP y WPA. Trabaja en MAC OS X

Crack al cifrado Wifi

Crackeando WEP utilizando Cain & Abel. Esta herramienta implementa cracking estático y el método PTW cracking para recuperar claves WEP.

Fuerza bruta en WPA utilizando Cain & Abel. Se sniffea la red wireless y crackea las contraseñas WPA-PSK utilizando diccionario y fuerza bruta.

Crack al cifrado Wifi

Herramienta de crack WPA: Elcomsoft Wireless Security Auditor. Permite a los administradores de la red auditar redes wireless accesibles. Viene con un un sniffer de redes wireless (con adaptadores AirPcap). Revisa la fortaleza de las contraseñas WPA/WPA2-PSK que protegen la red.

Crack al cifrado Wifi

WI-FI Sniffer: Kismet. Capa 2 detector de red, sniffer e IDS. Identifica redes colectando paquetes pasivamente. Detecta redes escondidas y la presencia de redes no balizamiento, vía tráfico de datos.

Bluetooth Hacking

Se refiere a la explotación de vulnerabilidades de la pila Bluetooth que comprometen datos sensibles en dispositivos y redes Bluetooth.

Bluetotth Hacking

- Bluemacking: Ataque DoS que hace overflow a dispositivos bluetooth con paquetes aleatorios causando que el dispositivo se bloqueé.
- Blue Snarfning: El robo de la información de un dispositivo wireless a través de una conexión Bluetooth.
- Bluejacking: Arte de enviar mensajes no solicitados a través de dispositivos Bluetooth como PDS o celulares.
- BlueSniff: Prueba de concepto para utilidad wardriving Bluetooth.

Pila Bluetooth

Modos de descubrimiento

1. Discoverable: Envía respuestas de consulta a todas las consultas.
2. Limited discoverable: Visible por un cierto periodo de tiempo.
3. Non-discoverable: Nunca responde a un scan de consulta.

Pila Bluetooth

Modos de emparejamiento

1. Non-pairable mode: Rechaza cada consulta de vinculación.
2. Pairable mode: Se asociará a la petición.

Amenazas Bluetooth

- Fuga de calendarios y libros de direcciones.
- Dispositivos de escucha.
- Envío de mensajes SMS.
- Causa pérdida financiera.
- Control remoto.
- Ingeniería social.
- Código malicioso.
- Vulnerabilidades del protocolo.

¿Como realizar bluejack a una víctima?

Paso 1: Seleccionar un área, café internet, celular, shopping center, etc.. Ir a contactos en tu libro de direcciones.

Paso 2. Crear un nuevo contacto, en el libro. Ingresar el mensaje en el campo nombre, ej: "quis

¿Como realizar bluejack a una víctima?

Paso 3. Guardar el nuevo contacto con el texto del nombre y sin número de teléfono. Elegir enviar vía Bluetooth. Esto buscará cualquier dispositivo Bluetooth en el rango quisieras ir a una cita conmigo?

Paso 4. Elegir un teléfono desde la lista descubierta pro el bluetooth y enviar el contacto. Recibirá un mensaje "tarjeta enviada" y luego podrás escuchar por el tono de mensaje de SMS de la víctima.

Bluejacking es un nuevo término utilizado que define la actividad de enviar mensajes anónimos en dispositivos Bluetooth vía protocolo OBEX.

¿Como realizar bluejack a una víctima?

Herramienta hacking bluetooth: Super Bluetooth Hack

Es un troyano bluetooth, que controla y lee información desde el celular de la víctima. Utiliza comandos at bluetooth para acceder/hackear teléfonos bluetooth. Una vez infectado, habilita a los atacantes a leer mensajes y contactos, cambiar perfil, manipular ringtones, reiniciar el celular, opciones de fábrica, etc.

¿Como realizar bluejack a una víctima?

- Herramienta hacking bluetooth: Phonesnoop: Es un spyware BlackBerry que habilita al atacante a activar remotamente el micrófono del BlackBerry y escuchar sonidos cerca de él.

- Otra herramienta: BlueScanner: Es una herramienta de valoración para Windows. Descubre tipos de dispositivo (teléfono, computadora, teclado, pda, etc.) y los servicios publicados por los dispositivos. Guarda toda la información que puede ser adquirida por el dispositivo, sin intento de autenticar con el dispositivo remoto.

Contramedidas

¿Cómo defenderse contra Bluetooth Hacking?

- Utilizar patrones no regulares como PIN keys.
- Habilitar encriptación.
- Revisar todos los dispositivos vinculados.
- Mantener el BT en estado deshabilitado.
- Mantener el BT en modo no descubrimiento (oculto).
- No aceptar solicitudes inesperadas.

¿Cómo detectar y bloquear Rogue AP?

Detectando

- RF sensores son enchufados en toda la red cableada.
- AP Scanning, AP que tienen la funcionalidad de detectar APs vecinos operando cerca.
- Utilizando wired side inputs: Software que detecta dispositivos en la WAN incluyendo Telnet, SNMP, CDP (Cisco Discovery Protocol) utilizando protocolos múltiples.

¿Cómo detectar y bloquear Rogue AP?

Bloqueando

- Denegando servicio wireless a nuevos clientes lanzando ataques DoS en un Rogue AP. Bloqueando el puerto del switch que esta conectado o manualmente localizar el AP y sacarlo físicamente de la red LAN.

Capas de seguridad Wireless

- Seguridad de la señal Wireless: Wireless IDS Seguridad de espectro RF.
- Seguridad del dispositivo: Vulnerabilidades y parches.
- Protección de la red: Autenticación fuerte.
- Protección al usuario final: Sateful Firewalls por el usuario.
- Protección de datos: WPA2 y AES.
- Conexión segura: Autenticación pre-empaquetada, encriptación centralizada.

¿Cómo defenderse contra ataques en contra la Wireless?

- Cambiar el SSID por defecto luego de la configuración WLAN.
- - Configurar la contraseña de acceso al router y habilitar protección firewall.
- - Deshabilitar difusión SSID.
- - Deshabilitar inicio de sesión de router remota y administración wireless.
- - Habilitar el filtrado de direcciones MAC en el AP o router.
- - Habilitar la encriptación y AP y cambiar también la passphrase.

Mejores prácticas de opciones SSID

- Utilizar encubrimiento SSID para mantener ciertos mensajes wireless por defecto desde la difusión del ID a todos.
- No utilizar tu SSID, nombre de compañía, de red o cualquier otra cadena fácil de adivinar en las passphrases.
- Colocar firewall o filtrar paquetes entre el AP y la Intranet corporativa.

Mejores prácticas de opciones SSID

- Limitar la fortaleza de la red wireless de manera que no pueda ser detectada fuera de los límites de la organización.
- Revisar los dispositivos wireless para problemas de configuración.
- Implementar distintas técnicas para cifrar el tráfico, como IPSec sobre Wireless.

Mejores prácticas para la autenticación WiFi.

- Elegir WPA en vez de WEP.
- Implementar WPA2 Enterprise si es posible.
- Deshabilitar la red cuando no se la necesite.
- Colocar los AP en una locación segura.
- Mantener los controladores del equipo wireless actualizados.
- Utilizar servidor centralizado para autenticación.

Herramientas de Seguridad Wireless

Sistemas de prevención de intrusión Wireless: Protege a las redes wireless de amenazas, permite a los administradores detectar y prevenir varios ataques a la red.

Herramientas de Seguridad Wireless

Herramienta de auditoría de seguridad Wireless: Airmagnet Wifi Analyzer. Audita y busca problemas. Detecta amenazas de seguridad. Detecta ataques WiFi. Puede localizar dispositivos no autorizados (rogue).

Herramientas de Seguridad Wireless

Airdefense. Monitorea el wireless, protege de intrusos. Detecta rogues. Sensores distribuidos para monitorear tráfico 802.11. Amenazas existentes y de día zero. Investigación forense.

Herramientas de Seguridad Wireless

Adaptive Wireless IPS. Provee detección de amenazas y mitigación contra ataques maliciosos. Detecta, analiza e identifica amenazas wireless.

Herramientas de Seguridad Wireless

Aruba RFProtect WIPS. Detección de intrusos, mitigación contra amenazas automáticas para la evaluación forense. Reporte de complimiento automático.

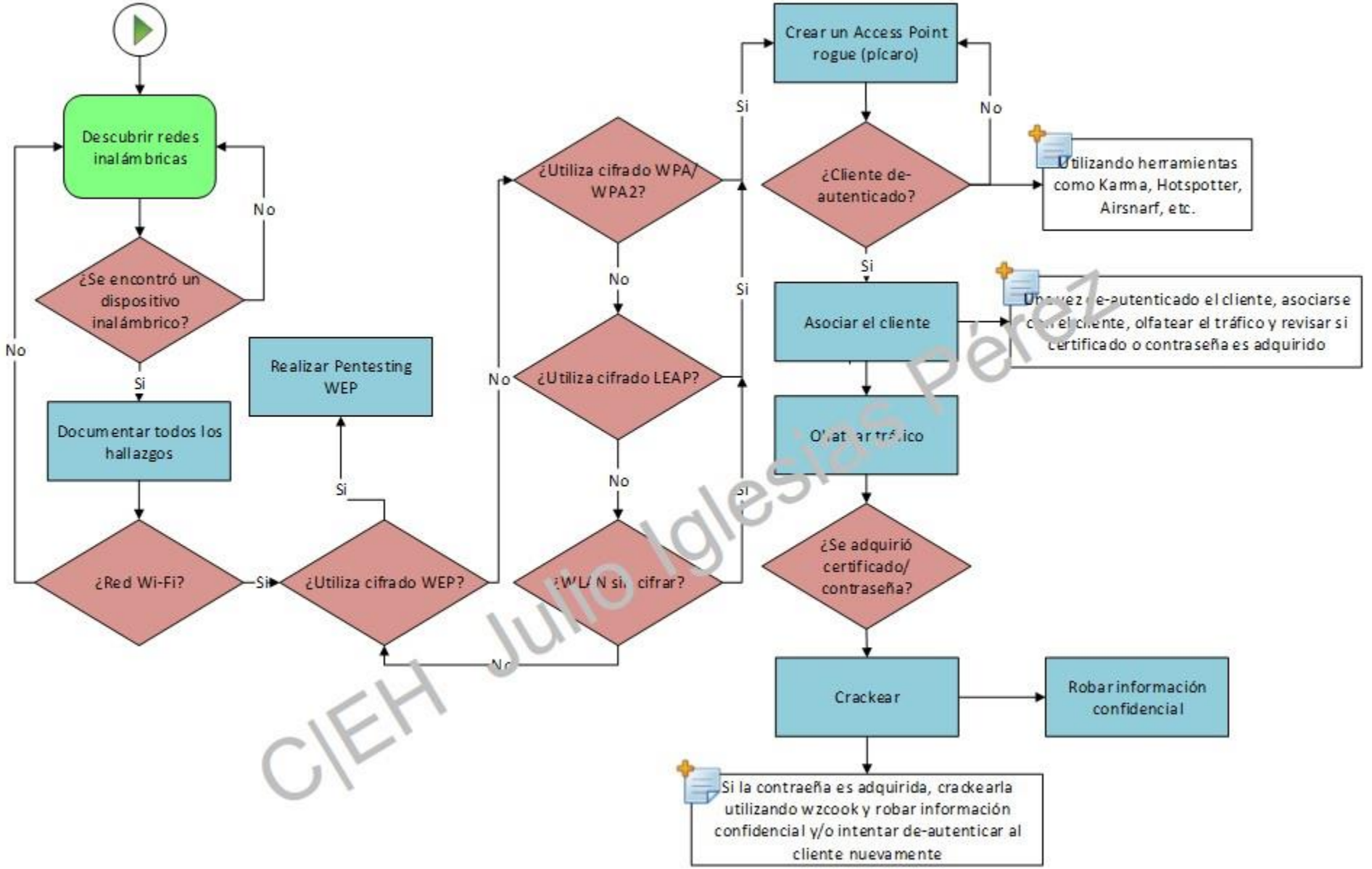
Test de Intrusión a Redes Inalámbricas

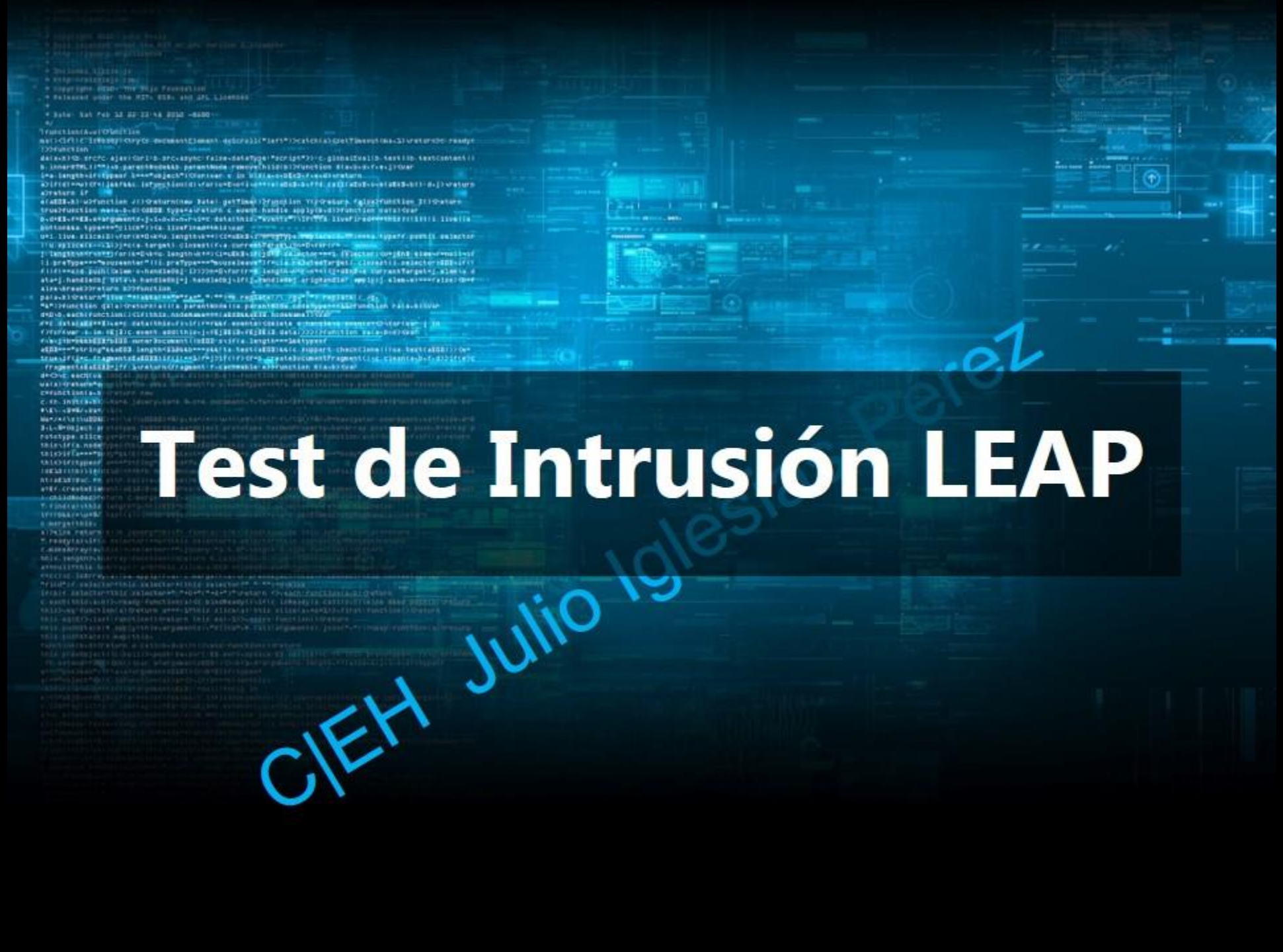
Proceso de evaluar activamente información sobre medidas de seguridad implementadas en una red wifi y analizar debilidades de diseño, fallas técnicas y vulnerabilidades.

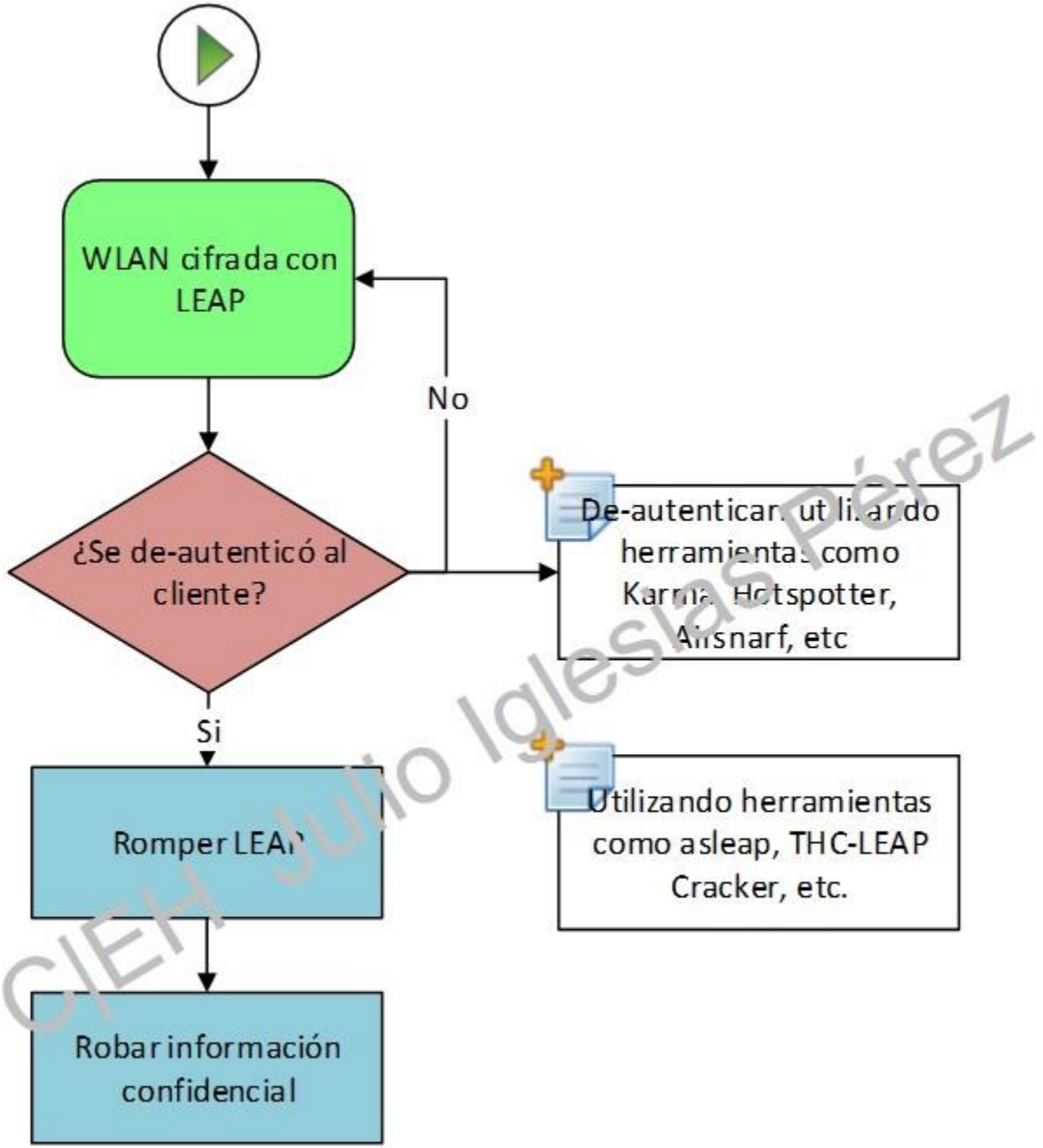
- Evaluaciones de amenazas. Identificar las amenazas de wireless.
- Actualizando infraestructura. Cambiar o actualizar la infraestructura existente del software, hardware o diseño de red.

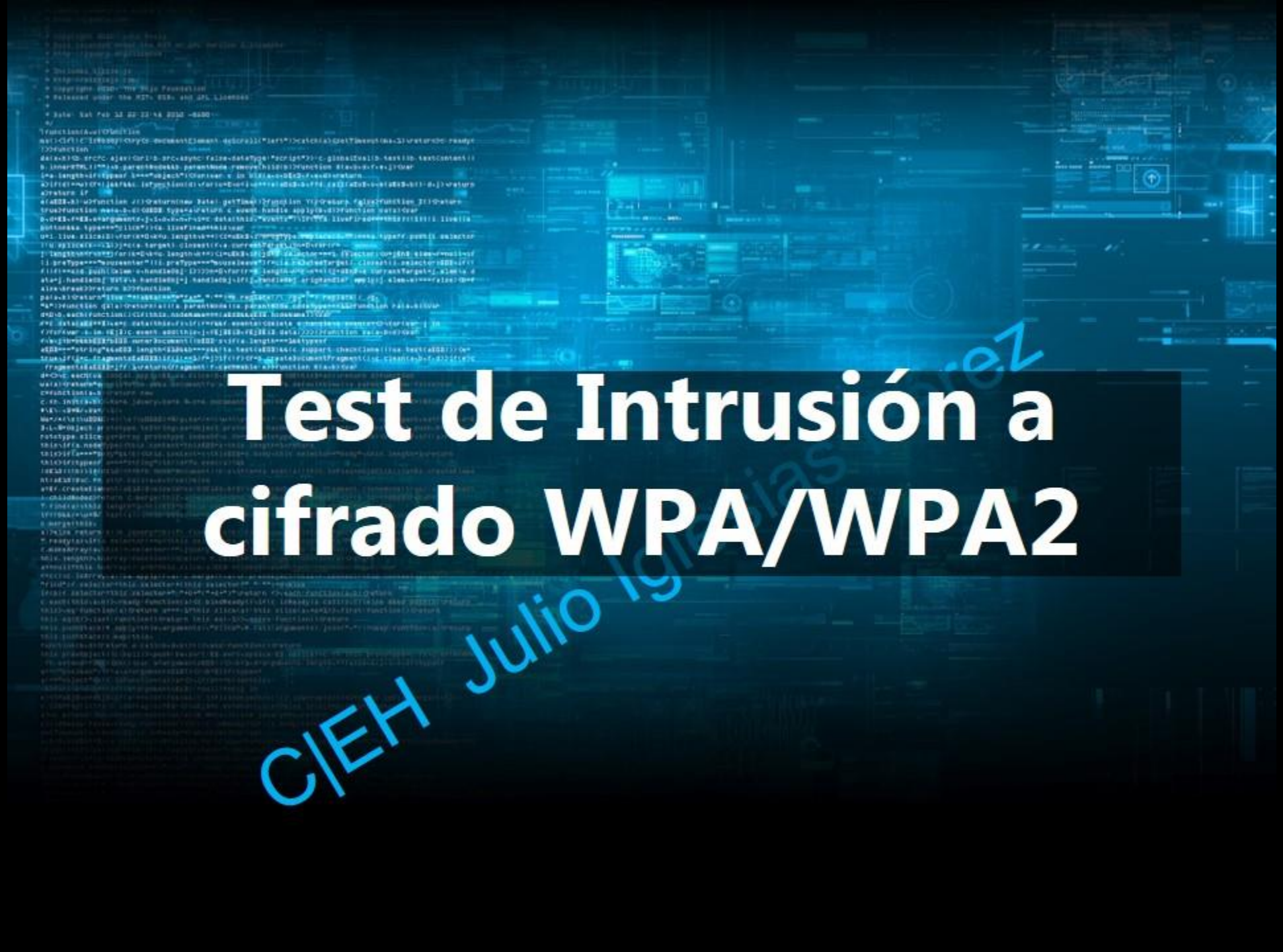
Test de Intrusión a Redes Inalámbricas

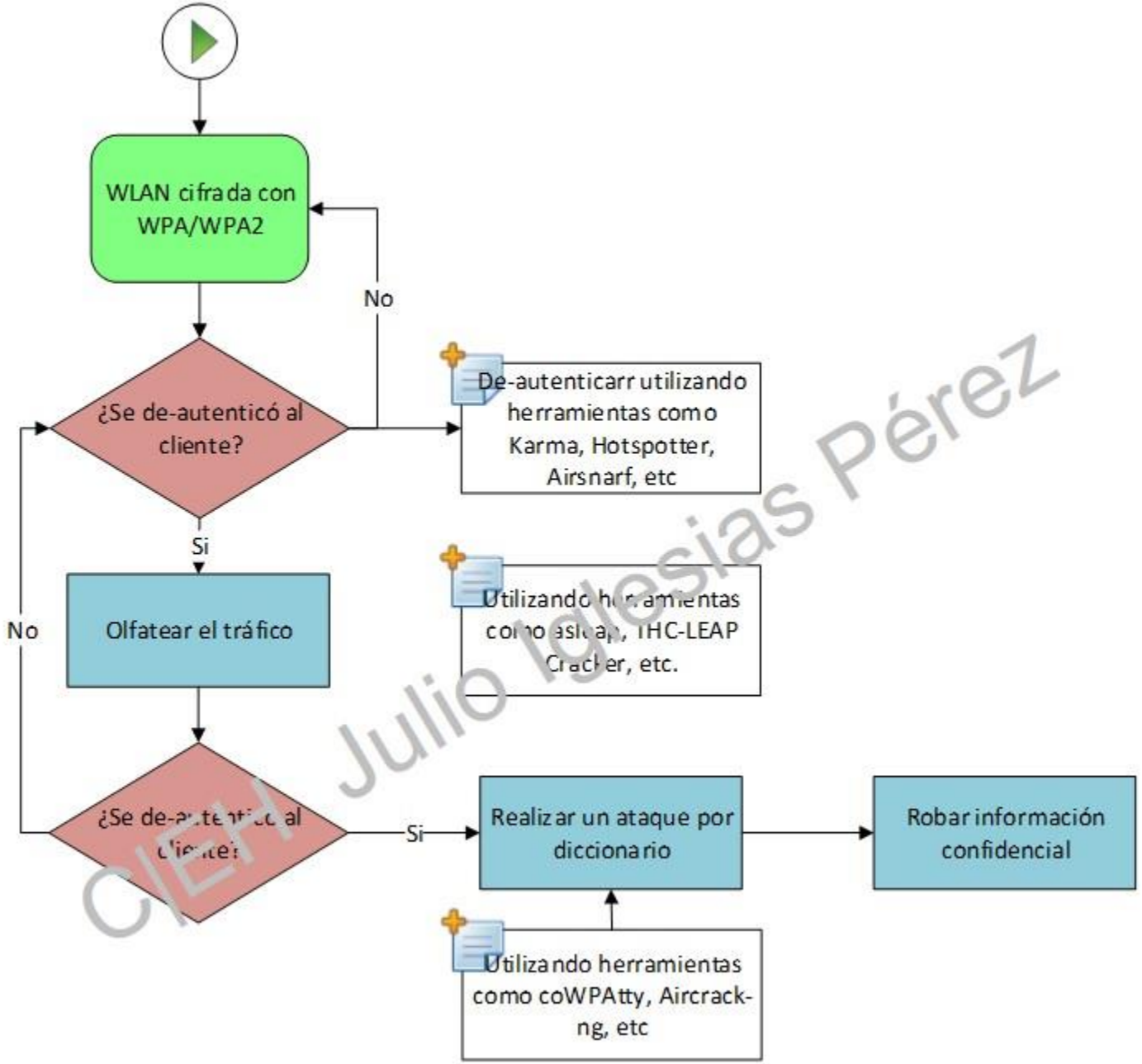
- Prevención de Riesgo y respuesta. provee un acercamiento comprensivo de los pasos de preparación que pueden ser tomados para prevenir explotaciones venideras.
- Auditoría de Control de Seguridad. Para probar y validar la protección y controles de seguridad wireless.
- Detección de robo de datos. Encontrar corrientes de datos sensibles olfateando el tráfico.
- Administración de información del sistema. Recolectar información en los protocolos de seguridad, fortaleza de la red y dispositivos conectados.

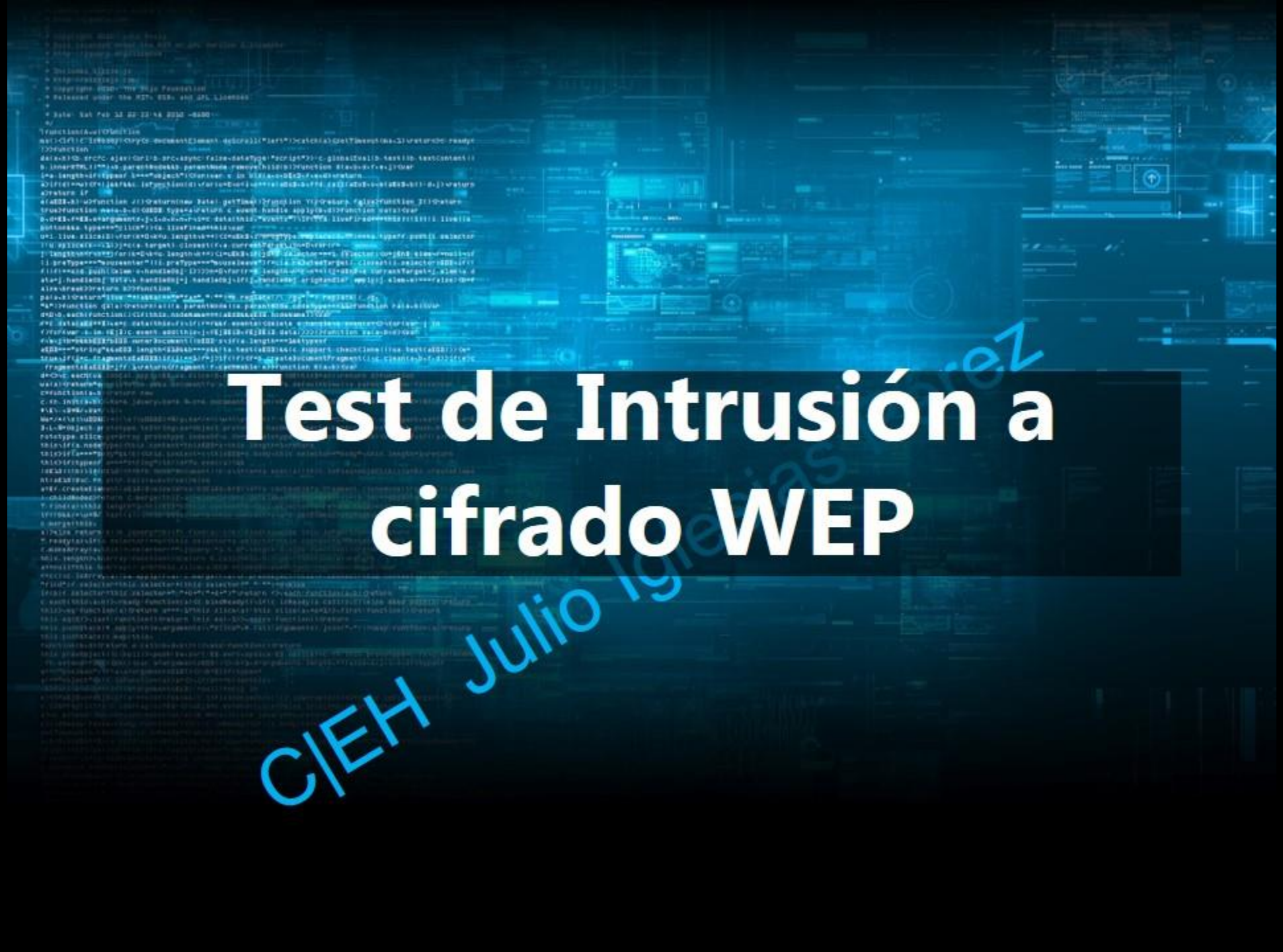


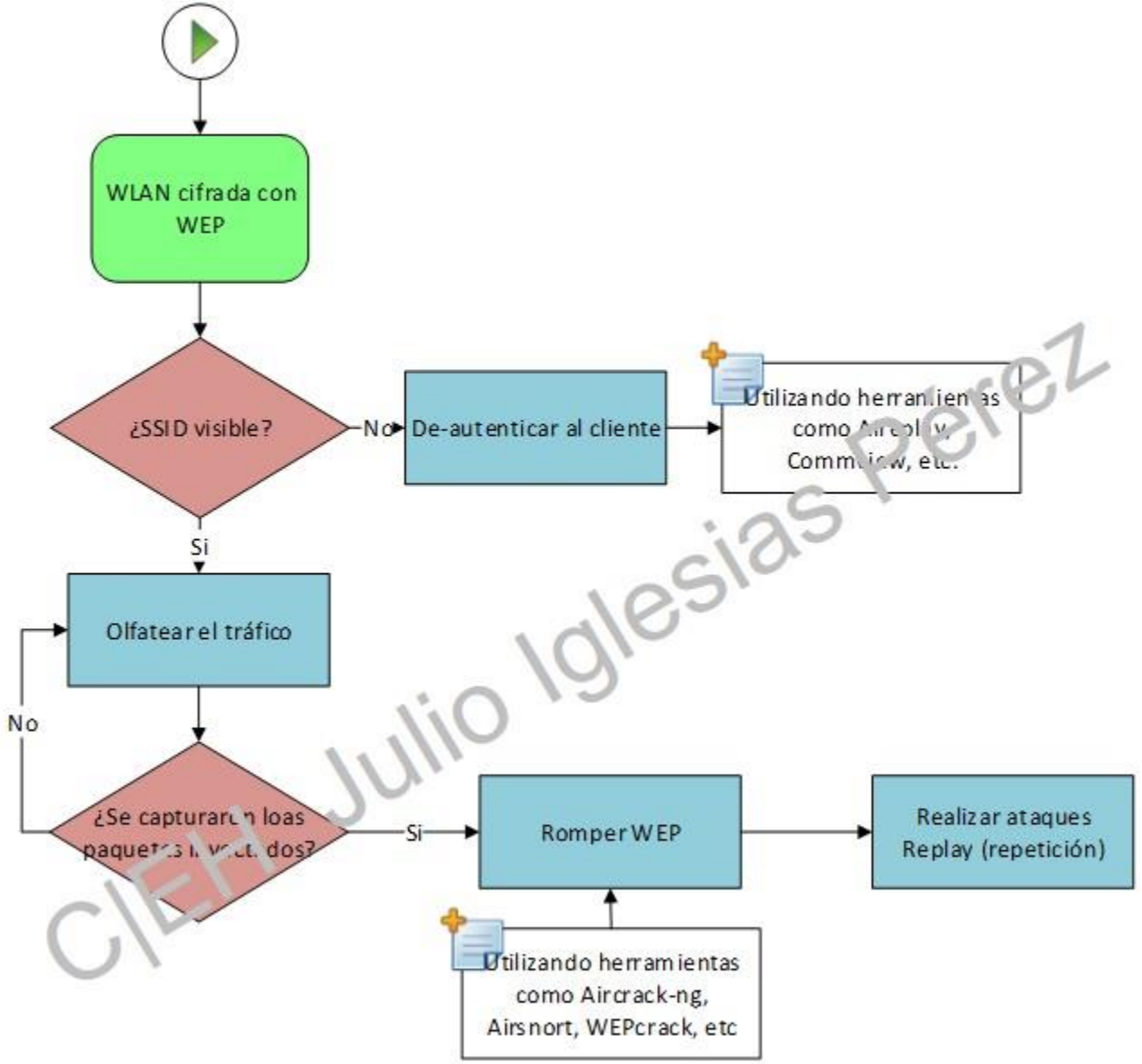

Test de Intrusión LEAP
C|EH Julio Iglesias Perez



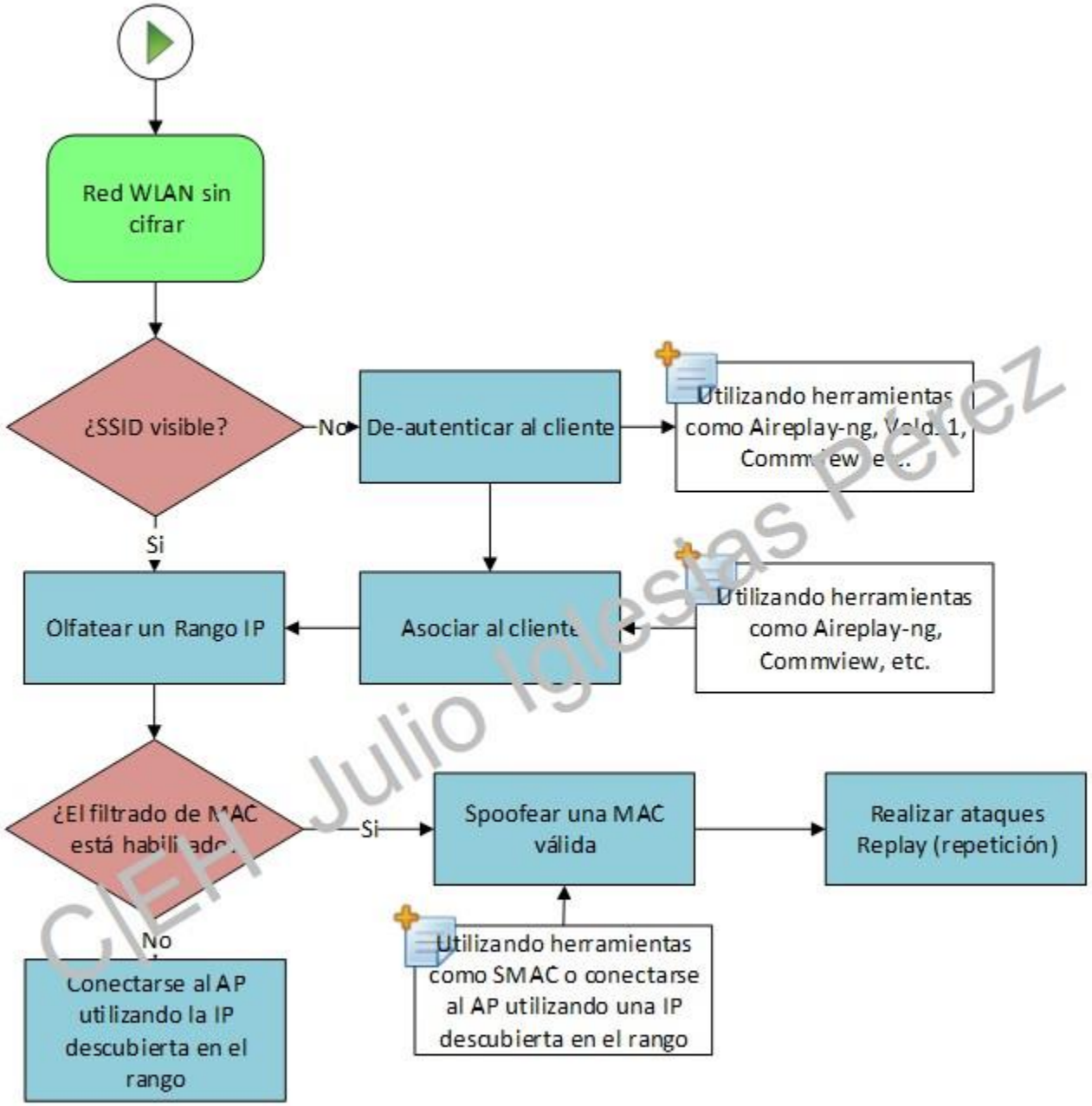

Test de Intrusión a cifrado WPA/WPA2
C|EH Julio Iglesias Pérez




Test de Intrusión a cifrado WEP
C|EH Julio Iglesias Suárez




Test de Intrusión a red WLAN sin cifrar
C|EH Julio Iglesias Pérez




¡Muchas Gracias!
C|EH Julio Iglesias Perez