Hacking Wireless Ofensivo

Teoría, Vectores de Ataque y Práctica Real

El Medio Compartido y la Propagación RF

Naturaleza "Broadcast" del Medio

- A diferencia de una red Switched (Ethernet) donde los paquetes van dirigidos por cable punto a punto, en Wi-Fi el medio es el aire.
- La señal se propaga de forma **omnidireccional** (esférica).
- **Implicación Crítica:** No existe "seguridad física". El perímetro de la red no son las paredes del edificio, sino hasta donde llegue la señal (RSSI detectable).

El Principio de Intercepción Pasiva

- Cualquier radio dentro del radio de cobertura recibe *toda* la información cruda (Raw Frames).
- La tarjeta de red normalmente descarta lo que no es para ella.
- **Modo Monitor:** Al activar este modo, forzamos al driver a pasar *todo* el tráfico al kernel/CPU, eliminando el filtro de hardware. Aquí nace la auditoría.

Topología y Limitaciones de Transmisión

Título: Half-Duplex y Gestión del Espectro

- **Limitación Half-Duplex**
  - Las radios 802.11 **no pueden transmitir (Tx) y recibir (Rx) simultáneamente** en la misma frecuencia. Deben alternar.
  - **Ethernet vs. Wi-Fi:**
    - Ethernet (Full-Duplex): Envía y recibe a la vez (doble carril).
    - Wi-Fi (Half-Duplex): Funciona como un Walkie-Talkie. Solo uno habla a la vez por canal.
- **El "Cuello de Botella" Aéreo**
  - Si un dispositivo transmite, todos los demás en ese canal (incluso los de redes vecinas) deben callar y esperar.
  - Esto explica por qué la velocidad cae drásticamente con muchos usuarios y por qué los ataques de saturación (Jamming) son tan efectivos.

Espectro RF, Bandas y Canalización

Organización del Espectro (Bandas ISM)

- **Bandas No Licenciadas:** Wi-Fi opera principalmente en bandas ISM (Industrial, Scientific and Medical). Son rangos de frecuencia "libres" que no requieren licencia estatal para operar, lo que explica su saturación global.
- **Concepto de "Banda":** No es una frecuencia única, sino un bloque continuo de espectro (ej: de 2.400 GHz a 2.4835 GHz) reservado para estas comunicaciones.

Estructura del Canal (Channelization)

- **Frecuencia Central y Ancho de Banda:** Dentro de una banda, dividimos el espacio en "carriles" llamados canales.
- **El Ancho importa:** Un canal no es una línea fina; tiene un ancho ("grosor") medido en MHz (20, 40, 80 MHz). Por este "ancho" es por donde viajan los datos.
- **Regla Técnica:** A mayor ancho de canal (Channel Bonding), más datos pueden pasar simultáneamente (Throughput), pero mayor es la probabilidad de captar ruido e interferencia.

Física de Ondas: Longitud de Onda (λ) vs. Frecuencia

- **Relación Inversa:** Existe una relación física inmutable entre la frecuencia y la longitud de onda.
- **Menor Frecuencia (ej. 2.4 GHz):** Ondas más largas ("grandes"). Tienen mayor capacidad de difracción (rodear obstáculos) y penetración de materiales sólidos.
- **Mayor Frecuencia (ej. 5 GHz):** Ondas más cortas ("pequeñas"). Transportan más energía y permiten modulaciones más densas (más velocidad), pero son absorbidas fácilmente por paredes y objetos.
- **Contexto para el atacante:** Esto define tu estrategia. ¿Querés atacar desde el estacionamiento (lejos)? Usás 2.4 GHz. ¿Querés crackear una red corporativa rápida? Buscás 5 GHz.

Diferencias Operativas entre Bandas de Frecuencia

Banda 2.4 GHz

Ventajas: Mayor alcance debido a la longitud de onda más larga, mejor penetración a través de obstáculos físicos como paredes y muebles.

Desventajas: Alta saturación del espectro por dispositivos como microondas, Bluetooth y otras redes Wi-Fi. Solo 3 canales no solapados disponibles (1, 6, 11).

Caso de uso: Ideal para cobertura amplia en espacios con múltiples barreras físicas.

Banda 5 GHz

Ventajas: Velocidades superiores, hasta 23 canales no solapados, menor interferencia ambiental, mejor para aplicaciones de alto ancho de banda.

Desventajas: Menor alcance efectivo, mayor absorción por materiales densos, requiere más puntos de acceso para cobertura equivalente.

Caso de uso: Entornos de alta densidad que requieren throughput elevado.

Canales y Solapamiento

En 2.4 GHz, cada canal ocupa 22 MHz pero están espaciados solo 5 MHz, causando interferencia. El solapamiento se evita usando canales 1, 6 y 11.

Ancho de Banda

20 MHz (legado), 40 MHz (802.11n), 80 MHz y 160 MHz (802.11ac/ax). Mayor ancho = mayor velocidad pero menor cantidad de canales disponibles.

Modos de Operación de Tarjeta de Red

Modo Managed

Modo estándar de cliente. La tarjeta se asocia a un AP específico y solo procesa tramas dirigidas a su dirección MAC. Funcionalidad normal de conexión a redes.

Limitación: No permite escuchar tráfico de otros dispositivos ni inyectar paquetes arbitrarios.

Modo Monitor

Modo pasivo que captura todas las tramas 802.11 en el canal especificado sin asociarse a ningún AP. Esencial para auditorías de seguridad.

Capacidades: Captura de handshakes, análisis de tráfico, inyección de paquetes, detección de redes ocultas.

Modo Promiscuo

Opera en capa Ethernet. Captura todo el tráfico que llega a la interfaz física, pero solo funciona con tráfico ya desencapsulado (después de la asociación 802.11).

Diferencia clave: No captura frames de management ni control, solo datos ya procesados.

Requisito técnico: El chipset de la tarjeta debe soportar modo monitor nativamente. Chipsets recomendados: Atheros AR9271, Ralink RT3070, Realtek RTL8812AU.

Anatomía del Frame 802.11

Los frames 802.11 se dividen en tres categorías funcionales, cada una con propósitos específicos en la comunicación inalámbrica.

Management Frames

Beacon: Anuncios periódicos del AP con SSID, capacidades y parámetros de red.

Probe Request/Response: Búsqueda activa/respuesta de redes disponibles.

Authentication/Association: Proceso de conexión cliente-AP.

Deauthentication: Desconexión forzada (explotable en ataques).

Control Frames

RTS/CTS: Request to Send / Clear to Send para evitar colisiones en medios compartidos.

ACK: Confirmación de recepción exitosa de frames.

Block ACK: Confirmación agregada para múltiples frames.

Data Frames

Transportan la carga útil de la comunicación. Pueden estar cifrados (WPA2/WPA3) pero el header 802.11 permanece en claro.

Información siempre visible: MACs origen/destino, BSSID, secuencia, tipo de frame.

El header no cifrado de los frames es la base del análisis pasivo. Incluso en redes cifradas, podemos extraer metadatos críticos: direcciones MAC, potencia de señal, canales, y patrones de tráfico.

Preparación del Entorno de Ataque

Gestión de Procesos Conflictivos

Antes de activar el modo monitor, es fundamental eliminar procesos que interfieren con la manipulación de la tarjeta inalámbrica. Estos servicios intentan mantener la conectividad normal y previenen el cambio de modo.

Comando esencial

```
airmon-ng check kill
```

Este comando identifica y termina automáticamente procesos problemáticos. Los servicios más comunes que causan conflictos incluyen:

- **NetworkManager:** Gestor de red de entornos de escritorio Linux
- **wpa_supplicant:** Daemon de autenticación WPA/WPA2
- **dhclient:** Cliente DHCP que solicita configuración de red
- **avahi-daemon:** Servicio de descubrimiento de red

Advertencia: Ejecutar airmon-ng check kill desconectará todas las interfaces de red activas. Asegúrate de tener acceso físico o una conexión alternativa antes de proceder.

01

Verificar interfaz disponible

iwconfig o airmon-ng para listar interfaces wireless

02

Eliminar procesos conflictivos

airmon-ng check kill

03

Activar modo monitor

airmon-ng start wlan0

04

Confirmar nuevo interface

Normalmente wlan0mon o similar

Airodump-ng: Interpretación de Métricas RF

Airodump-ng es la herramienta fundamental para el reconocimiento pasivo de redes inalámbricas. Su interfaz presenta métricas técnicas críticas que requieren interpretación correcta para targeting efectivo.

PWR (Power) - Medido en dBm

Indica la potencia de señal recibida. Valores típicos: -30 dBm (excelente, muy cerca) a -90 dBm (débil, límite de conectividad). Cada -3 dBm representa aproximadamente la mitad de potencia.

Uso táctico: Targets con PWR > -70 dBm tienen mayor probabilidad de captura exitosa de handshake.

Beacons - Frames de Anuncio

Cantidad de frames Beacon capturados. Los APs transmiten beacons cada 100ms típicamente. Un conteo bajo puede indicar distancia, obstáculos o potencia de transmisión reducida.

Anomalía: Beacons = 0 pero Data > 0 sugiere SSID oculto.

Data Packets - Tráfico Real

Cantidad de frames de datos capturados. Tráfico activo indica clientes conectados generando comunicación. Fundamental para determinar el momento óptimo de ataque de deautenticación.

Estrategia: Redes con Data > 1000 tienen mayor actividad y probabilidad de recaptura rápida de handshake.

BSSID vs ESSID

BSSID: Dirección MAC física del punto de acceso (identificador único de hardware, inmutable en hardware pero modificable por software).

ESSID: Nombre de red configurado (identificador lógico, múltiples APs pueden compartir el mismo ESSID en redes enterprise).

Información Adicional

CH (Channel): Canal de operación (1-14 en 2.4GHz, 36-165 en 5GHz).

ENC: Tipo de cifrado (WEP, WPA, WPA2, WPA3, OPN para redes abiertas).

CIPHER: Algoritmo específico (TKIP, CCMP, GCMP).

Targeting y Filtrado Preciso

Importancia del Bloqueo de Canal

Por defecto, airodump-ng realiza "channel hopping", rotando entre todos los canales disponibles cada 2-3 segundos. Este comportamiento es útil para reconocimiento inicial pero contraproducente durante ataques activos.

Problema crítico: Si el handshake ocurre mientras la tarjeta está escuchando otro canal, los frames EAPOL se perderán y la captura será inútil.

Sintaxis de bloqueo

```
airodump-ng -c 6 --bssid XX:XX:XX:XX:XX:XX -w capture wlan0mon
```

El parámetro **-c** fija el canal específico, y **--bssid** filtra solo el tráfico del AP objetivo, reduciendo ruido y tamaño de archivo de captura.

Tip profesional: Utiliza la opción -w para guardar todas las capturas con prefijo de nombre. Airodump generará automáticamente archivos .cap, .csv y .kismet para análisis posterior.

Reconocimiento General

Escaneo sin filtros para mapear todas las redes disponibles y sus características

1

Selección de Target

2

Identificar AP objetivo basado en PWR, cifrado, y actividad de clientes

Bloqueo y Enfoque

3

Fijar canal y BSSID para captura dedicada sin pérdida de frames

Ataque Activo

4

Deauth o espera pasiva hasta capturar handshake completo

Mapeo de Clientes y Relación AP-Station

La sección inferior de airodump-ng muestra las "Stations" o dispositivos cliente. Esta información es crucial para entender la topología de red, identificar targets específicos, y planificar ataques de deautenticación selectivos.

Relación AP-Cliente

La columna BSSID en la sección de stations muestra a qué AP está asociado cada cliente. "(not associated)" indica dispositivos buscando redes pero sin conexión activa.

Identificación por OUI

Los primeros 3 octetos de la MAC identifican al fabricante del dispositivo (Organizationally Unique Identifier). Útil para profiling: Apple, Samsung, Intel, etc.

Probe Requests

Solicitudes de clientes buscando redes conocidas. Revela el historial de conexiones del dispositivo y puede exponer información sensible de ubicaciones previas.

Métricas de Station

- **PWR:** Potencia de señal del cliente (diferente al PWR del AP)
- **Rate:** Velocidad de transmisión negociada
- **Lost:** Paquetes perdidos (indicador de calidad de conexión)
- **Frames:** Cantidad de frames capturados del cliente
- **Probes:** SSIDs que el dispositivo ha buscado activamente

Estrategia de Deauth Selectivo

En lugar de desautenticar todo el AP (ruidoso, detectabl), se puede targetear un cliente específico enviando deauth dirigido a su MAC. Esto fuerza solo ese dispositivo a reconectar, minimizando la huella del ataque.

```
aireplay-ng -0 5 -a [AP_MAC] -c [CLIENT_MAC] wlan0mon
```

Técnicas para Redes Ocultas (Hidden SSID)

Las redes con SSID oculto no incluyen el nombre de red en los Beacon frames, transmitiendo un ESSID de longitud cero. Esta técnica de "seguridad por oscuridad" es fácilmente derrotable con conocimiento técnico apropiado.

Detección de Red Oculta

En airodump-ng aparece como "<length: 0>" o campo ESSID vacío. Indicadores: Beacons presentes pero sin nombre visible, clientes asociados al BSSID.

Espera Pasiva de Probe Response

Cuando un cliente se conecta, transmite un Probe Request con el SSID en claro. El AP responde con Probe Response o Association Request conteniendo el nombre real.

Deautenticación Forzada

Enviar deauth frames a clientes conectados para forzar reconexión inmediata. Durante el proceso de reassociación, el SSID se transmite en texto plano.

Captura y Revelación

Airodump actualizará automáticamente el ESSID cuando capture el frame apropiado. El nombre queda expuesto y registrado en el archivo de captura.

Realidad técnica: Ocultar el SSID no proporciona seguridad real. Herramientas básicas de análisis revelan el nombre en minutos. La medida correcta de seguridad es WPA3 con contraseña robusta, no oscuridad del SSID.

OpSec y Técnicas de Evasión

MAC Spoofing con Macchanger

La dirección MAC de tu tarjeta inalámbrica es visible en todos los frames transmitidos. Cambiarla antes de un análisis reduce la trazabilidad forense.

Uso de macchanger

```
ifconfig wlan0 down
macchanger -r wlan0
ifconfig wlan0 up
```

-r: MAC aleatoria completa

-a: Aleatoriza solo los octetos de dispositivo, mantiene OUI válido

-p: Restaura MAC original

Consideración: Algunas redes filtran por MAC whitelist. Un OUI de fabricante reconocido (-a) puede ser más efectivo que aleatorización total.

Control de Potencia de Transmisión

Reducir la potencia Tx disminuye el radio de detección física de tus frames de ataque.

```
iwconfig wlan0mon txpower 10
```

Valores típicos: 0-20 dBm. Menor potencia = menor alcance pero también menor detección por IDS/WIPS.

Timing y Patrones

Evita patrones predecibles de escaneo. Introduce delays aleatorios entre acciones, varía duración de capturas, no operes en horarios fijos.

Posicionamiento Físico

La triangulación RF puede localizar emisores. Mantén movilidad, evita transmitir desde ubicaciones fijas, considera ángulos de radiación de antena.

Firma Digital

Herramientas como Kismet, AirMagnet pueden fingerprint tarjetas por timing de frames, secuencias, implementación de driver. Actualiza firmware y varía herramientas.

Consideración legal: El análisis de redes inalámbricas sin autorización explícita puede constituir delito en muchas jurisdicciones. Estas técnicas deben aplicarse únicamente en entornos controlados, con consentimiento documentado, o en equipos de propiedad personal para fines educativos.

Fase de Explotación: Captura y Handshake en Redes WPA2

Una guía técnica avanzada sobre los mecanismos de captura y cracking de redes inalámbricas protegidas con WPA2, explorando desde la teoría del 4-Way Handshake hasta las técnicas modernas de explotación y defensa.

FUNDAMENTOS CRIPTOGRÁFICOS

Teoría del 4-Way Handshake en WPA2

Concepto Crítico del Handshake

WPA2 no transmite la contraseña en texto plano en ningún momento. Lo que realmente buscamos capturar es el "apretón de manos" criptográfico (4-Way Handshake) que valida que un cliente posee la clave correcta. Este proceso es el punto débil fundamental que permite los ataques offline posteriores.

El handshake es un intercambio de cuatro mensajes EAPOL (Extensible Authentication Protocol over LAN) entre el Access Point (AP) y el cliente. Durante este proceso, ambas partes demuestran que conocen la contraseña sin revelarla directamente, utilizando nonces (números aleatorios) y códigos de integridad de mensaje.

El Objetivo del Atacante

Forzar este proceso de autenticación. Normalmente, el 4-Way Handshake solo ocurre cuando un usuario se conecta inicialmente a la red. Como atacantes, no queremos esperar horas o días; debemos provocar este evento de manera artificial mediante técnicas de desautenticación.

1

ANonce

Número aleatorio generado por el Access Point (Authenticator Nonce)

SNonce

Número aleatorio generado por el cliente (Supplicant Nonce)

MIC

Message Integrity Code - firma que valida la integridad del intercambio

Crítico: Si logramos capturar los 4 paquetes EAPOL (o al menos M1/M2), podemos atacar la contraseña offline sin necesidad de mantener conexión con la red objetivo.

TÉCNICA OFENSIVA

Ataque de Desautenticación (Deauth Attack)

Mecánica Detallada del Ataque

El ataque de desautenticación explota una vulnerabilidad fundamental en el estándar 802.11: las tramas de gestión (Management Frames) no están autenticadas en WPA2. Un atacante puede inyectar tramas de Management falsificadas (Subtype 12 - Deauthentication) suplantando la dirección MAC del Access Point hacia el cliente, o viceversa.

Esto instruye al dispositivo objetivo a desconectarse inmediatamente de la red. El sistema operativo del cliente (Windows, Android, iOS, Linux) detecta la desconexión y, por diseño, intentará reconectarse automáticamente de forma inmediata, generando precisamente el 4-Way Handshake que nuestra interfaz en modo monitor está esperando capturar.

01

Preparación del Entorno

Interfaz en modo monitor activa, airodump-ng capturando tráfico del AP objetivo, identificación de clientes conectados

02

Inyección de Tramas Deauth

Uso de aireplay-ng para enviar paquetes de desautenticación falsificados hacia el cliente objetivo

03

Desconexión Forzada

El cliente recibe la trama y procede a desconectarse, creyendo que proviene del AP legítimo

04

Reconexión Automática

El dispositivo inicia automáticamente el proceso de reconexión, generando el 4-Way Handshake

05

Captura del Handshake

Airodump-ng captura los paquetes EAPOL del intercambio y los almacena en el archivo .cap

Sintaxis Práctica con Aireplay-ng

```
aireplay-ng -0 [N] -a [BSSID] -c [STATION] wlan0mon

Parámetros:
-0       : Modo Deauthentication
[N]      : Cantidad de paquetes (Recomendado: 5-10, no infinito)
-a [BSSID]: MAC del Access Point objetivo
-c [STATION]: MAC del cliente a desautenticar (opcional)
wlan0mon  : Interfaz en modo monitor
```

Nota Operacional: Evitar enviar deauths infinitos (-0 0). Esto genera ruido excesivo, puede ser detectado por sistemas WIPS, y algunos clientes modernos implementan protecciones contra desautenticaciones masivas.

Estrategias de Ejecución: Targeted vs Broadcast

Ataque Dirigido (Targeted)

Implementación:

- Especificar el parámetro -c [MAC_CLIENTE]
- Desconecta únicamente al dispositivo seleccionado
- Requiere reconocimiento previo de clientes activos

Ventajas Tácticas:

- **Sigiloso:** Menor huella en logs del router
- **Precisión:** No afecta a otros usuarios
- **Profesional:** Reduce el impacto en operaciones legítimas
- **Evasión:** Menos probable de activar alarmas en sistemas IDS/WIPS

Caso de Uso: Auditorías de seguridad en entornos corporativos donde se requiere minimizar la interrupción del servicio.

Ataque Broadcast

Implementación:

- No especificar cliente o usar FF:FF:FF:FF:FF:FF
- Envía deauths a todos los dispositivos conectados
- No requiere identificar clientes específicos

Efecto y Riesgos:

- **DoS Masivo:** Genera Denegación de Servicio total en la red
- **Alta Detección:** Extremadamente ruidoso y visible en logs
- **Múltiples Handshakes:** Captura de varios dispositivos simultáneamente
- **Implicaciones Legales:** Puede constituir un ataque DoS ilegal

Consideración: Reservar solo para escenarios controlados o situaciones de desesperación. Algunos sistemas enterprise registran estos eventos y disparan alertas automáticas.

Consideraciones de Hardware y Protecciones Modernas

Algunos clientes modernos (especialmente dispositivos iOS recientes y sistemas con 802.11w/Management Frame Protection) implementan protecciones contra desautenticaciones excesivas. Pueden ignorar múltiples tramas deauth en períodos cortos o requerir autenticación de las tramas de gestión. La clave en estos casos es la precisión y el timing, no el volumen masivo de paquetes.

Además, routers enterprise con sistemas WIPS (Wireless Intrusion Prevention System) pueden detectar patrones de deauth y bloquear la MAC del atacante, cambiar el canal del AP, o enviar alertas al equipo de seguridad. Por ello, la estrategia targeted es siempre preferible en entornos profesionales.

VALIDACIÓN

Validación y Limpieza de Captura (.cap)

Captura Inicial

Archivo .cap crudo generado por airodump-ng con todo el tráfico

Confirmación Visual

Verificar que el handshake fue capturado correctamente

Sanitización

Eliminar datos innecesarios y extraer solo EAPOL

Análisis Profundo

Validar integridad del handshake con Wireshark

Confirmación Visual en Airodump-ng

Durante la captura activa, observar la esquina superior derecha de la interfaz de airodump-ng. Debe aparecer el mensaje:

```
[ WPA Handshake: AA:BB:CC:DD:EE:FF ]
```

Donde la dirección MAC corresponde al BSSID del Access Point objetivo. Si este mensaje no aparece después de ejecutar el ataque deauth, la captura no contiene un handshake válido y no servirá para el cracking posterior.

Tip Práctico: Mantener airodump-ng ejecutándose durante al menos 30-60 segundos después de ver la notificación del handshake. Esto asegura que se capturen los 4 mensajes completos.

Sanitización con wpaclean

Los archivos .cap crudos contienen megabytes de información innecesaria: beacons, tramas de datos, ACKs, tráfico de otros dispositivos. Para el cracking solo necesitamos los paquetes EAPOL del handshake.

```
wpaclean clean.cap original.cap

Resultado:
- Archivo de entrada: 45 MB
- Archivo limpio: 2 KB
- Solo contiene los 4 mensajes EAPOL necesarios
```

Esta limpieza acelera significativamente el procesamiento posterior y reduce el tamaño de archivo, facilitando la transferencia y el análisis.

Análisis Detallado con Wireshark

Para un análisis forense profundo, abrir el archivo .cap en Wireshark y aplicar el filtro:

```
eapol
```

Verificar que existan exactamente 4 paquetes etiquetados como "Message 1 of 4", "Message 2 of 4", "Message 3 of 4", y "Message 4 of 4". Un handshake corrupto (con nonces faltantes o MIC incorrecto) generará falsos negativos durante el proceso de cracking, desperdiciando tiempo de procesamiento GPU.

Buscar específicamente los campos ANonce y SNonce en los paquetes. Si estos valores están presentes y son diferentes de cero, el handshake tiene alta probabilidad de ser válido.

TÉCNICA MODERNA

Vector Moderno: Ataque PMKID (Client-less)

Limitación del Deauth Tradicional

El ataque de desautenticación tiene una debilidad fundamental: **requiere que exista al menos un cliente conectado** a la red objetivo. En escenarios donde la red está activa pero sin usuarios (por ejemplo, durante la noche en una oficina, o en redes recién configuradas), el método tradicional falla completamente.

La Solución: Vulnerabilidad PMKID

El ataque PMKID explota una vulnerabilidad descubierta en 2018 en el RSN IE (Robust Security Network Information Element) de muchos routers modernos. Esta técnica revolucionaria permite recuperar el hash de autenticación **directamente del Access Point**, sin necesidad de interactuar con ningún usuario legítimo ni esperar conexiones.

El PMKID (Pairwise Master Key Identifier) es un valor opcional que algunos APs incluyen en el primer mensaje del 4-Way Handshake. Este identificador se calcula usando HMAC-SHA1 sobre la PMK, y contiene suficiente información criptográfica para realizar un ataque de diccionario offline.

Fórmula Criptográfica

```
PMKID = HMAC-SHA1-128(PMK, "PMK Name" | MAC_AP | MAC_STA)
```

Donde PMK es derivado de la contraseña mediante PBKDF2, permitiendo así el cracking sin necesidad del handshake completo.

Ventajas Operacionales

- **Sin clientes requeridos:** Ataque directo al AP
- **Totalmente pasivo:** No genera tráfico deauth detectable
- **Más sigiloso:** No interrumpe el servicio
- **Rápido:** Captura en segundos
- **Efectivo 24/7:** No depende de actividad de usuarios

Herramienta Principal: hcxdumptool

```
hcxdumptool -i wlan0mon -o capture.pcapng --
enable_status=1

Parámetros clave:
-i       : Interfaz en modo monitor
-o       : Archivo de salida
--enable_status: Mostrar estado en tiempo real
--filterlist: Lista de MACs objetivo (opcional)
--filtermode: 2 (solo APs de la lista)
```

La herramienta envía solicitudes de asociación legítimas a los APs, provocando que respondan con el PMKID sin necesidad de completar la autenticación.

Tasa de Éxito: Aproximadamente 60-70% de routers domésticos y 30-40% de APs enterprise son vulnerables a este ataque. Los routers más modernos (post-2019) han comenzado a parchear esta vulnerabilidad.

Conversión y Procesamiento

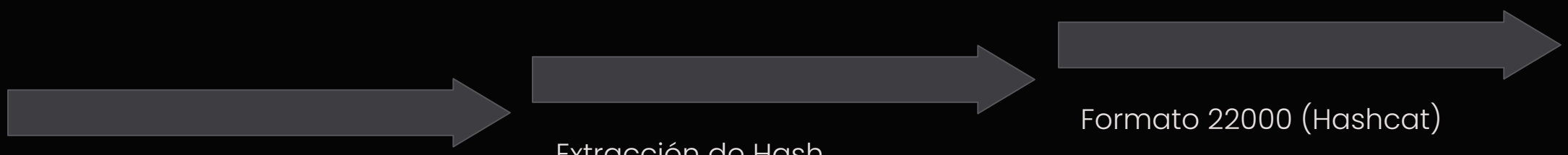
Una vez capturado el PMKID, se debe convertir a formato compatible con Hashcat:

```
hcxpcapngtool -o pmkid.hc22000 capture.pcapng
```

El formato resultante (22000) es idéntico al usado para handshakes WPA2 completos, permitiendo usar exactamente las mismas técnicas de cracking que se describirán en las siguientes secciones.

POST-EXPLOTACIÓN

Preparación del Hash para Cracking



Archivo Capturado (.cap/.pcapng)

Formato crudo de tcpdump/wireshark con todos los paquetes de red capturados durante el ataque

Extracción de Hash

Conversión a formato estandarizado compatible con herramientas de cracking GPU-accelerated

Formato 22000 (Hashcat)

Hash optimizado listo para procesamiento paralelo masivo en tarjetas gráficas

Formatos de Archivo y Compatibilidad

Las herramientas profesionales de cracking como **Hashcat** no procesan archivos .cap nativamente de forma eficiente. Los archivos de captura contienen metadatos, timestamps, y estructuras de paquetes completas que no son necesarias para el proceso de derivación de claves.

El formato **22000** es el estándar moderno para WPA-PBKDF2-PMKID+EAPOL. Este formato contiene únicamente:

- El SSID de la red (actúa como salt)
- La MAC del Access Point
- La MAC del cliente (Station)
- Los nonces (ANonce y SNonce)
- El MIC (Message Integrity Code)
- Los datos EAPOL necesarios

Esta estructura compacta permite a Hashcat cargar millones de hashes en memoria GPU sin desperdiciar recursos en datos irrelevantes.

Herramienta: hcxpcapngtool

Parte de la suite hcxtools, esta utilidad moderna reemplaza a las antiguas herramientas de conversión como cap2hccapx.

```
hcxpcapngtool -o hash.hc22000 captura.cap

Opciones adicionales útiles:
-E       : Extraer también PMKIDs
-o       : Archivo de salida en formato 22000
--eapoltimeout: Timeout para paquetes EAPOL
--nonce-error-corrections: Corregir errores en nonces
```

El archivo resultante (.hc22000) es un archivo de texto plano que contiene una línea por cada handshake/PMKID capturado, con todos los campos separados por asteriscos (*).

Ejemplo de Hash 22000

```
WPA*02*4d4fe7aac3a2cecab195321ceb99a7d0*64bc0c...
  |  |  |                       |
  |  |  |                     MAC_AP
  |  |  MIC (Message Integrity Code)
  |  Tipo (02 = EAPOL)
  Protocolo (WPA)
```

Verificación: Usar `wc -l hash.hc22000` para contar cuántos hashes válidos se extrajeron. Un archivo con 0 líneas indica que la captura no contenía handshakes válidos.

Teoría del Cracking WPA2: PBKDF2 y el Rol del SSID

Algoritmo PBKDF2

Password-Based Key Derivation Function 2 con 4096 iteraciones de HMAC-SHA1

SSID como Salt

El nombre de la red actúa como sal criptográfica única

Complejidad Computacional

Cada hash requiere procesamiento intensivo individualizado

El Algoritmo Criptográfico

WPA2 utiliza PBKDF2 (Password-Based Key Derivation Function 2), específicamente con 4096 iteraciones de HMAC-SHA1, para derivar la Pairwise Master Key (PMK) de 256 bits a partir de la contraseña y el SSID.

La fórmula de derivación es:

```
PMK = PBKDF2(HMAC-SHA1, passphrase, SSID, 4096, 256)
```

Cada iteración aplica HMAC-SHA1 sobre el resultado de la iteración anterior, creando una función deliberadamente lenta que dificulta los ataques de fuerza bruta. Las 4096 iteraciones fueron escogidas en el diseño del estándar 802.11i como balance entre seguridad y rendimiento en hardware de consumo.

Implicaciones de Seguridad

Esta función de derivación tiene varias propiedades importantes:

- **Resistencia a fuerza bruta:** 4096 iteraciones ralentizan significativamente cada intento
- **Determinística:** Misma contraseña + mismo SSID = mismo PMK
- **Avalanche effect:** Cambio mínimo en input produce output completamente diferente

El Rol Crítico del SSID como Salt

El nombre de la red (SSID) no es simplemente un identificador; actúa como **salt criptográfico** en el proceso de derivación. Esto tiene consecuencias fundamentales:

No Existen Rainbow Tables Universales

A diferencia de hashes como MD5 o SHA1, **no se pueden pre-computar tablas para WPA2**. Una tabla calculada para la red "Linksys" es completamente inútil para la red "Linksys_5G" o "CasaJuan".

Cada Hash es Único

Dos redes con la misma contraseña "password123" pero diferentes SSIDs generarán PMKs completamente distintos. Esto obliga a crackear cada captura desde cero.

Impacto en Tiempo de Cracking

No hay atajos. Cada contraseña candidata debe ser procesada a través de las 4096 iteraciones de PBKDF2 usando el SSID específico de la red capturada.

Excepción: Algunas organizaciones pre-computan PMKs para sus propios SSIDs con diccionarios comunes. Por ejemplo, un auditor podría tener tablas pre-calculadas para el SSID corporativo específico que audita regularmente.

Matemática del Cracking

Para validar una contraseña candidata, el atacante debe:

1. Derivar PMK = PBKDF2(contraseña_candidata, SSID, 4096)
2. Derivar PTK usando PMK + Nonces + MACs
3. Calcular MIC esperado usando el PTK
4. Comparar MIC calculado con MIC capturado

Si los MICs coinciden, la contraseña es correcta. Este proceso debe repetirse para cada contraseña en el diccionario o cada combinación en fuerza bruta.

Ataques de Diccionario, Reglas y Hardware Accelerado

Ataques de Diccionario (Wordlists)

El método más eficiente para crackear WPA2 se basa en listas de contraseñas conocidas o filtradas. La premisa fundamental es que **los humanos son predecibles** y tienden a usar contraseñas débiles o comunes.

Wordlists Populares:

- **rockyou.txt:** 14 millones de contraseñas reales filtradas (133 MB)
- **SecLists:** Colección curada de múltiples diccionarios especializados
- **CrackStation:** 15 GB de contraseñas combinadas
- **Específicas de región:** Diccionarios en español, contraseñas comunes de LATAM

Comando básico de Hashcat con diccionario:

```
hashcat -m 22000 hash.hc22000 rockyou.txt
```

Ataques Basados en Reglas (Rule-based)

Las reglas potencian exponencialmente un diccionario pequeño aplicando mutaciones automáticas en tiempo real. Esto transforma cada palabra base en decenas o cientos de variantes probables.

Ejemplo de Transformaciones:

- Palabra base: "verano"
- Regla aplica: Mayúscula inicial → "Verano"
- Agregar año → "Verano2024"
- Agregar símbolo → "Verano2024!"
- Leet speak → "V3r4n02024!"

```
hashcat -m 22000 hash.hc22000 wordlist.txt -r rules/best64.rule

Reglas populares incluidas en Hashcat:
- best64.rule: 64 reglas más efectivas
- dive.rule: 114,000 reglas exhaustivas
- rockyou-30000.rule: Optimizada para rockyou.txt
```

Hardware: CPU vs GPU

5K

Aircrack-ng (CPU)

~5,000 claves/segundo en CPU moderna. Inviable para contraseñas complejas o diccionarios grandes.

500K

Hashcat GPU Media

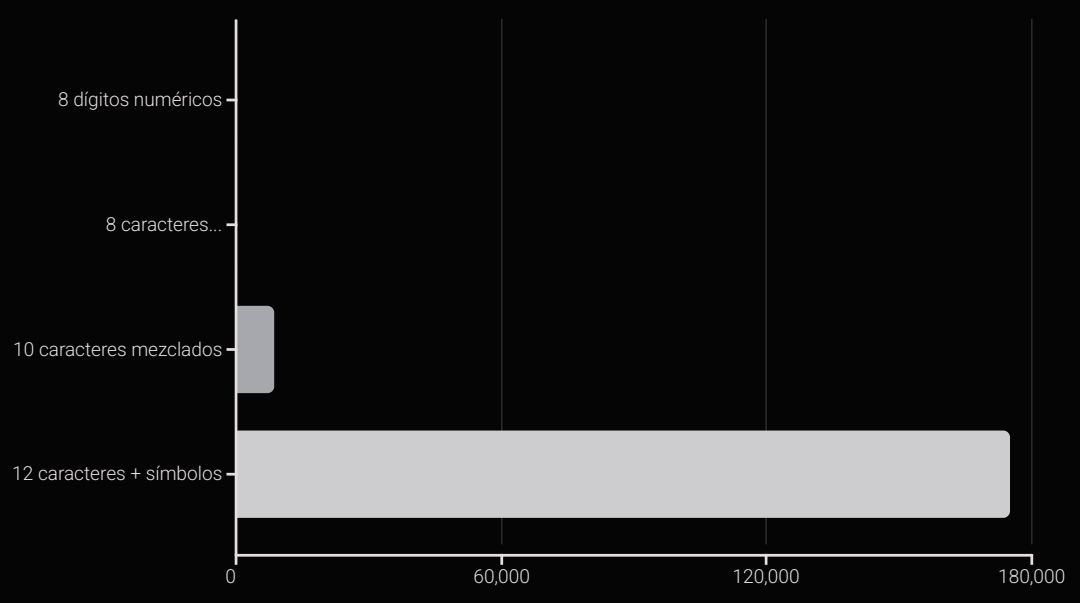
~500,000 claves/segundo en RTX 3060/4060. Reducción de 99% en tiempo de cracking.

2M

GPU High-End

~2,000,000+ claves/segundo en RTX 4090. Capacidad de procesar diccionarios masivos en horas.

Benchmarks Prácticos



Tiempos expresados en horas para fuerza bruta completa en RTX 3060.

Conclusión Crítica: La seguridad de WPA2 depende ENTERAMENTE de la complejidad de la contraseña. Una contraseña de 16+ caracteres aleatorios es matemáticamente inviable de crackear con tecnología actual.

Comando Completo Optimizado

```
hashcat -m 22000 -a 0 hash.hc22000 rockyou.txt \
 -r rules/best64.rule \
 --force \
 -O \
 -w 3

Parámetros:
-m 22000: Modo WPA2
-a 0: Ataque de diccionario
-r: Archivo de reglas
--force: Ignorar advertencias
-O: Optimizar kernels (usa más RAM, más rápido)
-w 3: Workload intensivo (máximo rendimiento)
```

DEFENSA Y MITIGACIÓN

Estrategias de Defensa y Resumen de Kill Chain

Mitigaciones Reales y Efectivas

1

Contraseñas Robustas

Mínimo recomendado: 16 caracteres con mezcla de mayúsculas, minúsculas, números y símbolos. Mejor aún: passphrases de 20+ caracteres generadas aleatoriamente.

Matemáticamente inviables de crackear por fuerza bruta con tecnología actual. Una contraseña aleatoria de 16 caracteres tomaría millones de años en hardware convencional.

2

Migración a WPA3

WPA3 introduce **SAE (Simultaneous Authentication of Equals)**, que reemplaza el PSK y elimina la vulnerabilidad fundamental de los ataques de diccionario offline.

SAE utiliza el protocolo Dragonfly, que proporciona forward secrecy y protección contra ataques de diccionario incluso si se captura el handshake completo.

Limitación: Aún vulnerable a ataques de downgrade si el AP soporta modo de transición WPA2/WPA3.

3

802.11w: Management Frame Protection

Protege las tramas de gestión (incluyendo deauth/disassociation) mediante criptografía, evitando ataques de desautenticación.

Disponible en WPA2 enterprise y mandatorio en WPA3. Requiere soporte tanto en AP como en clientes.

4

Segmentación de Red (VLANs)

Separar el tráfico de invitados del corporativo mediante VLANs, limitando el impacto de una posible compromisión de la red Wi-Fi.

Red de invitados aislada con acceso únicamente a Internet, sin visibilidad de recursos internos.

5

Detección y Monitoreo (WIPS)

Sistemas de Prevención de Intrusiones Inalámbricas que detectan ataques de deauth, handshake captures, y rogue APs en tiempo real.

Herramientas: Cisco ISE, Aruba WIPS, Ruckus SmartZone.

Resumen de la Kill Chain Completa

1. Reconocimiento
   Airodump-ng para identificar redes objetivo, canales, encriptación y clientes conectados
2. Targeting
   Selección de AP objetivo basado en señal, número de clientes y probabilidad de éxito
3. Desautenticación
   Aireplay-ng para forzar desconexión de clientes y provocar reconexión
4. Captura
   Intercepción del 4-Way Handshake o PMKID mediante airodump-ng/hcxdumptool
5. Validación
   Verificación de captura con Wireshark y limpieza con wpaclean
6. Conversión
   Extracción de hash a formato 22000 con hcxpcapngtool
7. Cracking
   Ataque de diccionario + reglas con Hashcat en GPU hasta obtener contraseña

Tiempo Total: En condiciones óptimas (red vulnerable, buena señal, diccionario efectivo, GPU potente), el proceso completo puede tomar entre 30 minutos y 2 horas.

Consideraciones Éticas y Legales

Todos los ataques descritos en esta presentación deben realizarse ÚNICAMENTE en entornos controlados, con autorización explícita por escrito, o en redes propias para fines educativos. La ejecución de estos ataques contra redes sin permiso constituye acceso no autorizado a sistemas informáticos, penado por ley en la mayoría de jurisdicciones.

Como profesionales de seguridad, nuestra responsabilidad es comprender estas técnicas para defender sistemas, no para comprometer infraestructuras ajenas.