M-CIB-008
Metodología General De Pruebas De Intrusión A Redes Wireless IEEE 802.11

Responsables

Elaboró:	Especialista Ciberinteligencia
Revisó:	Control de Documentos
Aprobó:	Dirección General

Control de versiones

Versión	Fecha	Descripción del cambio
1	29/09/2022	Emisión Inicial

Clave del formato de manual: F-SGI-004 v3
Comentarios o dudas: sgi@silent4business.com

Contenido

1. Introducción

Silent4Business ha alineado las pruebas técnicas a metodologías mundialmente reconocidas como SEC617del SANS Institute, a WIFU de Offensive Security, OSSTMM e ISSAF PTF. El equipo de Silent4Business utiliza las metodologías mencionadas para realizar las pruebas de penetración a infraestructura Wireless IEEE 802.11.

A continuación, se muestra la metodología empleada para la realización de las pruebas de penetración a infraestructura Wireless IEEE 802.11 en las modalidades de caja negra, que contempla la ejecución de técnicas manuales, técnicas automatizadas y actividades de verificación que nos permiten descubrir riegos antes de que se materialicen.

2. Alcance

Este proceso es de uso del área de ciberinteligencia, es aplicable para servicios ejecutados a clientes externos y/o para Silent4Business.

3. Definiciones

Activo

Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Amenaza

Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Ataque

Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Comprometer

Evasión de controles de seguridad causando posible de pérdida o daño en un activo de cómputo.

Exploit

Código o técnica que es usada por una amenaza para tomar ventaja de una vulnerabilidad.

Impacto

Medición de la consecuencia al materializarse una amenaza.

Mitigación

Acciones para remediar vulnerabilidades identificadas en los activos.

Probabilidad

Es la posibilidad que existe entre una amenaza y las variables de entorno para que una vulnerabilidad sea aprovechada.

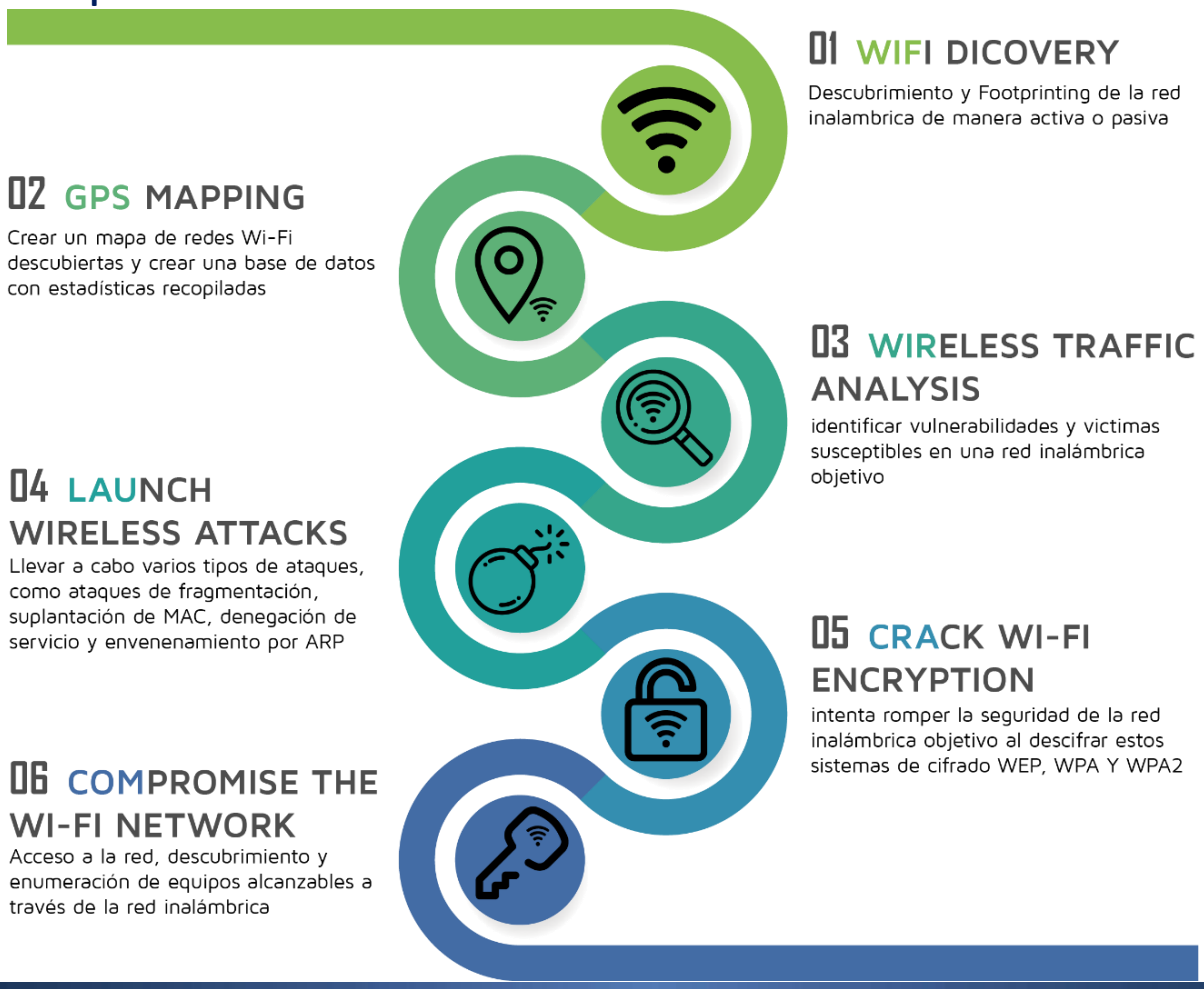
Riesgo

Es la probabilidad de que una amenaza explote una vulnerabilidad con su correspondiente impacto al negocio.

Vulnerabilidad

Son debilidades que influyen negativamente en un activo y que posibilita la materialización de una amenaza.

4. Descripción del manual



A. Técnicas de ataque por fase de la metodología

Por cada fase de la metodología, el equipo de SILENT4BUSINESS está capacitado para realizar técnicas de ataques específicos a redes Wireless IEEE 802.11. A continuación, se detallan algunas técnicas de ataque:

1. Wi-Fi Discovery

- Passive Footprinting
  - Detectar la existencia de APs por medio de sniffing a los paquetes de las ondas aéreas
- Active Footprinting
  - Envió de solicitudes de sonda con el SSID para identificar la respuesta de los APs

2. GPS Mapping

Creación de un mapa de redes Wi-Fi descubiertas y crear una base de datos con estadísticas recopiladas por Wi-Fi.

3. Wireless Traffic Analysis

- Identificación de vulnerabilidades y víctimas susceptibles en la red inalámbrica objetivo
- Determinar la estrategia apropiada para un ataque exitoso
- Analizar la red inalámbrica para determinar el SSID transmitido, la presencia de múltiples puntos de acceso, la posibilidad de recuperar SSIDs, el método de autenticación utilizado, los algoritmos de encriptación WLAN.
- Captura y análisis del tráfico de la red inalámbrica objetivo.

4. Launch Wireless Attacks

- Ataques de fragmentación
- Ataques de suplantación de MAC
- Ataques de denegación de servicio
- Ataques de envenenamiento por ARP.

5. Crack Wi-Fi Encryption

- WEP
  - Creación de autenticación falsa con el punto de acceso
  - Recolección de IVs únicos
  - Inyección de paquetes
  - Craqueo de clave de cifrado de los IV
- WPA/WPA2
  - Recopilar datos de tráfico inalámbrico
  - Des-autenticación (deauth) de cliente

- Captura de paquete de autenticación (WPA handshake).
- Craqueo de WPA Key

6. Compromise the Wi-Fi Network

- Descubrimiento de equipos alcanzables desde la red Wi-Fi
- Enumeración de los servicios activos de los equipos alcanzables desde la red Wi-Fi

B. Herramientas por fases de la metodología

A continuación, se listan las herramientas que usa el equipo de SILENT4BUSINESS durante las diferentes fases de la metodología.

Fase de la Metodología	Herramienta	Descripción
Wi-Fi Discovery	**Kismet**	Kismet es un detector de red inalámbrica 802.11 de capa 2, sniffer y sistema de detección de intrusos. Funcionará con cualquier tarjeta inalámbrica que admita el modo de monitoreo sin formato (rfmon) y puede detectar el tráfico 802.11a / b / g / n.
	Aircrack	Conjunto completo de herramientas para evaluar la seguridad de redes Wi-Fi. Se enfoca en diferentes áreas de seguridad Wi-Fi: Monitoreo: captura de paquetes y exportación de datos a archivos de texto para su posterior procesamiento por herramientas de terceros Ataque: ataques de repetición, autenticación, puntos de acceso falsos y otros mediante inyección de paquetes Pruebas: comprobación de tarjetas Wi-Fi y capacidades de controladores (captura e inyección) Cracking: WEP y WPA PSK (WPA 1 y 2)
GPS Mapping	**WiGLE**	WiGLE consolida la ubicación y la información de redes inalámbricas en todo el mundo en una base de datos central, y proporciona aplicaciones Java, Windows y web fáciles de usar que pueden mapear, consultar y actualizar la base de datos a través de la web. Puede agregar una red inalámbrica a WiGLE desde un archivo de tropiezo o manualmente y agregar comentarios a una red existente.

Fase de la Metodología	Herramienta	Descripción
	Skyhook	El Sistema de posicionamiento de Wi-Fi (WPS) de Skyhook determina la ubicación en función de la base de datos masiva mundial de Skyhook de puntos de acceso de Wi-Fi conocidos. Utiliza una combinación de rastreo GPS y un sistema de posicionamiento Wi-Fi para determinar la ubicación de una red inalámbrica en interiores y en áreas urbanas. Incluso descubre la posición del dispositivo móvil entre 10 y 20 metros con la ayuda de la dirección MAC de los AP inalámbricos cercanos y algoritmos patentados.
Wireless Traffic Analysis	**Wireshark**	Wireshark tiene un conjunto de características que incluye lo siguiente: Inspección profunda de cientos de protocolos, y se agregan más todo el tiempo Captura en vivo y análisis fuera de línea Soporte de descifrado para muchos protocolos, incluidos IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP y WPA / WPA2
	Aircrack	Conjunto completo de herramientas para evaluar la seguridad de redes Wi-Fi. Se enfoca en diferentes áreas de seguridad Wi-Fi: Monitoreo: captura de paquetes y exportación de datos a archivos de texto para su posterior procesamiento por herramientas de terceros Ataque: ataques de repetición, autenticación, puntos de acceso falsos y otros mediante inyección de paquetes Pruebas: comprobación de tarjetas Wi-Fi y capacidades de controladores (captura e inyección) Cracking: WEP y WPA PSK (WPA 1 y 2)
Launch Wireless Attacks	**MAC Address Changer**	MAC Address Changer permite cambiar (falsificar) la dirección de control de acceso a medios (MAC) de sus adaptadores de red.

Fase de la Metodología	Herramienta	Descripción
	Aircrack	Conjunto completo de herramientas para evaluar la seguridad de redes Wi-Fi. Se enfoca en diferentes áreas de seguridad Wi-Fi: Monitoreo: captura de paquetes y exportación de datos a archivos de texto para su posterior procesamiento por herramientas de terceros Ataque: ataques de repetición, autenticación, puntos de acceso falsos y otros mediante inyección de paquetes Pruebas: comprobación de tarjetas Wi-Fi y capacidades de controladores (captura e inyección) Cracking: WEP y WPA PSK (WPA 1 y 2)
Crack Wi-Fi Encryption	**Cain & Abel**	Cain & Abel es una herramienta de recuperación de contraseñas para Microsoft Windows. Puede recuperar muchos tipos de contraseñas utilizando métodos como el sniffing de paquetes de red, también puede crackear varios hashes de contraseñas utilizando métodos maliciosos como ataques de diccionario, de fuerza bruta y ataques basados en "criptoanálisis".
	Aircrack	Conjunto completo de herramientas para evaluar la seguridad de redes Wi-Fi. Se enfoca en diferentes áreas de seguridad Wi-Fi: Monitoreo: captura de paquetes y exportación de datos a archivos de texto para su posterior procesamiento por herramientas de terceros Ataque: ataques de repetición, autenticación, puntos de acceso falsos y otros mediante inyección de paquetes Pruebas: comprobación de tarjetas Wi-Fi y capacidades de controladores (captura e inyección) Cracking: WEP y WPA PSK (WPA 1 y 2)
	Pyrit	Pyrit es un programa con muchas funcionalidades enfocadas principalmente a descifrar mediante fuerza bruta o diccionarios por tablas, claves como las de los AP (Puntos de Acceso) WPA.

Fase de la Metodología	Herramienta	Descripción
	coWPAtty	coWPAtty es una herramienta basada en C para ejecutar un ataque de diccionario de fuerza bruta contra WPA-PSK y auditar claves WPA precompartidas.
Compromise the Wi-Fi Network	**Nmap**	Nmap es una utilidad para el descubrimiento de redes y la auditoría de seguridad. Nmap utiliza paquetes IP sin procesar de formas novedosas para determinar qué hosts están disponibles en la red, qué servicios (nombre y versión de la aplicación) están ofreciendo, qué sistemas operativos (y versiones de SO) están ejecutando, qué tipo de paquetes de filtros / firewalls están en uso, y docenas de otras características. Fue diseñado para escanear rápidamente redes grandes, pero funciona bien con hosts únicos.

5. Anexos

NA