

# WXS

## Wireless eXploitation Specialist

Manual del curso



# Índice

|                                                                                      |    |
|--------------------------------------------------------------------------------------|----|
| Módulo 0 — Aviso legal y propiedad intelectual.....                                  | 7  |
| 0. Copyright y condiciones de uso del material.....                                  | 7  |
| Titularidad y derechos.....                                                          | 7  |
| Restricciones de uso y prohibición de distribución .....                             | 7  |
| Uso permitido.....                                                                   | 7  |
| Uso responsable y marco de autorización.....                                         | 7  |
| Particularidades legales de las redes inalámbricas .....                             | 8  |
| Protección de datos personales .....                                                 | 8  |
| Confidencialidad y protección del entorno de aprendizaje.....                        | 8  |
| Incumplimiento .....                                                                 | 8  |
| Módulo 1 — Introducción al curso.....                                                | 9  |
| 1.1. Introducción.....                                                               | 9  |
| 1.2. Qué es una auditoría WiFi y qué partes incluye .....                            | 9  |
| 1.3. Cómo se trabaja en WXS: reconocer, plantear hipótesis, validar y reportar ..... | 10 |
| 1.4. Qué es evidencia reproducible en WiFi.....                                      | 11 |
| 1.5. Entregables que construiremos durante el curso.....                             | 12 |
| 1.6. Marco ético y alcance de uso responsable .....                                  | 13 |
| Módulo 2 — Fundamentos de RF y redes WiFi.....                                       | 14 |
| 2.1. El espectro radioeléctrico y las bandas 2.4 / 5 / 6 GHz.....                    | 14 |
| 2.2. Canales, solapamiento y ancho de canal.....                                     | 15 |
| 2.3. El estándar IEEE 802.11 (de WiFi 4 a WiFi 7).....                               | 15 |
| 2.4. Arquitectura de una red WiFi: STA, AP, BSS, ESS, IBSS y DS .....                | 16 |
| 2.5. Identificadores: SSID, BSSID y ESSID .....                                      | 17 |
| 2.6. Tipos de redes por cifrado.....                                                 | 18 |
| 2.7. Conceptos clave de seguridad: WPS, PMF y roaming.....                           | 19 |
| 2.8. Resumen del módulo .....                                                        | 19 |
| Módulo 3 — Tramas 802.11 y protocolos desde la perspectiva del auditor .....         | 21 |
| 3.1. La trama 802.11 como unidad de evidencia .....                                  | 21 |
| 3.2. Tramas de gestión: beacon, probe, autenticación y asociación .....              | 22 |
| 3.3. Tramas de control y de datos: qué información filtran .....                     | 23 |
| 3.4. El proceso de conexión: descubrimiento, autenticación y asociación.....         | 23 |
| 3.5. EAPOL y el 4-way handshake .....                                                | 24 |
| 3.6. Información que filtra una red aun protegida.....                               | 25 |
| 3.7. Aleatorización de MAC del cliente.....                                          | 26 |
| 3.8. Resumen del módulo .....                                                        | 27 |
| Módulo 4 — Entorno y herramientas: el workflow de auditoría WiFi .....               | 28 |

|                                                                           |    |
|---------------------------------------------------------------------------|----|
| 4.1. Hardware: qué adaptador necesitas y por qué .....                    | 28 |
| 4.2. Antenas: omnidireccionales frente a direccionales .....              | 28 |
| 4.3. Sistema operativo: Kali o Parrot, en máquina física o virtual .....  | 29 |
| 4.4. Verificación del adaptador .....                                     | 29 |
| 4.5. Modo monitor e inyección .....                                       | 30 |
| 4.6. El centro de trabajo: airodump-ng, Wireshark y hcxtools .....        | 31 |
| 4.7. Evidencias: qué guardar y cómo presentarlo .....                     | 32 |
| 4.8. Labs: el entorno de prácticas del curso .....                        | 32 |
| 4.9. Hardware dedicado de auditoría .....                                 | 33 |
| 4.10. Montar tu propio punto de acceso de prácticas con hostapd .....     | 34 |
| 4.11. Resolución de problemas habituales .....                            | 35 |
| Módulo 5 — Reconocimiento WiFi ofensivo .....                             | 36 |
| 5.1. Reconocimiento pasivo y activo: el método aplicado al recon .....    | 36 |
| 5.2. airodump-ng a fondo .....                                            | 36 |
| 5.3. Lectura del cifrado: las columnas ENC, CIPHER y AUTH .....           | 37 |
| 5.4. Identificación de fabricante por OUI y enumeración de clientes ..... | 38 |
| 5.5. Kismet y wifi_db: reconocimiento avanzado y persistencia .....       | 39 |
| 5.6. Redes ocultas: revelar el ESSID .....                                | 40 |
| 5.7. Probe requests y la lista de redes preferidas del cliente .....      | 41 |
| 5.8. Reconocimiento frente a la aleatorización de MAC .....               | 42 |
| 5.9. WarDriving: geolocalización de redes .....                           | 42 |
| 5.10. Resumen del módulo y orden de reconocimiento recomendado .....      | 43 |
| Módulo 6 — Redes abiertas, OWE y WEP .....                                | 45 |
| 6.1. Redes abiertas: riesgos y suplantación de MAC .....                  | 45 |
| 6.2. Portales cautivos: funcionamiento y evasiones básicas .....          | 46 |
| 6.3. OWE (Enhanced Open): qué cambia frente a una red abierta .....       | 46 |
| 6.4. WEP: por qué nació roto .....                                        | 47 |
| 6.5. Ataques contra WEP .....                                             | 47 |
| 6.6. Recuperar la clave con aircrack-ng .....                             | 48 |
| 6.7. Resumen del módulo y checklist .....                                 | 49 |
| Módulo 7 — WPA/WPA2-PSK: handshake y PMKID .....                          | 51 |
| 7.1. Teoría del 4-way handshake .....                                     | 51 |
| 7.2. Captura del handshake con airodump-ng .....                          | 52 |
| 7.3. Forzar la reconexión: desautenticación dirigida y por difusión ..... | 53 |
| 7.4. Verificar que el handshake es válido .....                           | 54 |
| 7.5. El ataque PMKID: captura sin clientes .....                          | 55 |
| 7.6. Conversión al formato de cracking .....                              | 57 |
| 7.7. Resumen del módulo y orden de pruebas recomendado .....              | 57 |
| Módulo 8 — Cracking de claves (aircrack-ng / hashcat) .....               | 59 |

|                                                                                            |    |
|--------------------------------------------------------------------------------------------|----|
| 8.1. Cracking por diccionario con aircrack-ng .....                                        | 59 |
| 8.2. hashcat y el modo 22000 .....                                                         | 59 |
| 8.3. Los modos de ataque de hashcat .....                                                  | 60 |
| 8.4. Diccionarios y generación dirigida .....                                              | 61 |
| 8.5. Reglas y máscaras para contraseñas reales .....                                       | 62 |
| 8.6. Optimización, benchmark y cracking distribuido.....                                   | 63 |
| 8.7. Descifrar el tráfico capturado con la clave obtenida .....                            | 64 |
| 8.8. Resumen del módulo y checklist.....                                                   | 65 |
| Módulo 9 — WPS: Reaver, Bully y Pixie Dust .....                                           | 66 |
| 9.1. Qué es WPS y dónde está su fallo.....                                                 | 66 |
| 9.2. Detección de WPS con wash .....                                                       | 67 |
| 9.3. Ataque al PIN: reaver y bully .....                                                   | 67 |
| 9.4. Pixie Dust: el ataque offline.....                                                    | 68 |
| 9.5. PIN nulo, bloqueo y cómo manejarlo .....                                              | 69 |
| 9.6. Resumen del módulo y checklist.....                                                   | 70 |
| Módulo 10 — WPA-Enterprise / 802.1X (MGT) .....                                            | 71 |
| 10.1. Arquitectura de una red Enterprise: suplicante, autenticador y servidor RADIUS ..... | 71 |
| 10.2. Los métodos EAP .....                                                                | 72 |
| 10.3. El punto débil: la validación del certificado del servidor.....                      | 72 |
| 10.4. Evil Twin contra Enterprise con hostapd-wpe.....                                     | 73 |
| 10.5. eaphammer: captura de credenciales .....                                             | 73 |
| 10.6. Crackear el reto MSCHAPv2 .....                                                      | 74 |
| 10.7. Resumen del módulo y orden de pruebas recomendado .....                              | 74 |
| Módulo 11 — Evil Twin, Rogue AP y MITM.....                                                | 76 |
| 11.1. Qué es un Evil Twin y cuándo se usa .....                                            | 76 |
| 11.2. Levantar el punto de acceso gemelo .....                                             | 76 |
| 11.3. Portal cautivo de phishing con wifiphisher .....                                     | 77 |
| 11.4. Karma, MANA y known beacons .....                                                    | 78 |
| 11.5. Atraer al cliente: desautenticación, señal y explotación de la PNL.....              | 79 |
| 11.6. Intermediario una vez conectado el cliente.....                                      | 80 |
| 11.7. Ataques de degradación y transition mode .....                                       | 81 |
| 11.8. Resumen del módulo y checklist.....                                                  | 81 |
| Módulo 12 — WPA3, SAE y Dragonblood .....                                                  | 82 |
| 12.1. Qué resuelve WPA3 frente a WPA2 .....                                                | 82 |
| 12.2. El handshake SAE .....                                                               | 82 |
| 12.3. PMF obligatorio y su impacto en los ataques clásicos.....                            | 83 |
| 12.4. Dragonblood: canales laterales y degradación.....                                    | 84 |
| 12.5. El talón de Aquiles: el modo de transición .....                                     | 84 |
| 12.6. WPA3-Enterprise y el modo de 192 bits.....                                           | 86 |

|                                                                               |     |
|-------------------------------------------------------------------------------|-----|
| 12.7. SSID Confusion (CVE-2023-52424) .....                                   | 86  |
| 12.8. Estado actual de los ataques a WPA3 y límites prácticos .....           | 87  |
| 12.9. Resumen del módulo.....                                                 | 88  |
| Módulo 13 — DoS, deauth y PMF (802.11w).....                                  | 89  |
| 13.1. Desautenticación y desasociación como denegación de servicio .....      | 89  |
| 13.2. Inundación de beacons y de autenticación con mdk4 .....                 | 89  |
| 13.3. PMF (802.11w): cómo cierra los ataques de desautenticación.....         | 90  |
| 13.4. Detectar PMF y qué hacer cuando está activo .....                       | 91  |
| 13.5. Advertencia legal sobre el jamming.....                                 | 92  |
| 13.6. Resumen del módulo.....                                                 | 93  |
| Módulo 14 — Post-explotación y pivoting.....                                  | 94  |
| 14.1. Ya dentro: descubrimiento y escaneo de la red .....                     | 94  |
| 14.2. ARP spoofing e intermediario en la red interna .....                    | 95  |
| 14.3. El aislamiento de clientes y su evasión.....                            | 96  |
| 14.4. Pivoting hacia la red corporativa .....                                 | 96  |
| 14.5. Resumen del módulo.....                                                 | 97  |
| Módulo 15 — Automatización: airgeddon y wifite2 .....                         | 98  |
| 15.1. airgeddon: el orquestador interactivo.....                              | 98  |
| 15.2. wifite2: ataque automatizado de principio a fin .....                   | 99  |
| 15.3. Cuándo automatizar y cuándo hacerlo a mano .....                        | 99  |
| Módulo 16 — Informe profesional.....                                          | 101 |
| 16.1. Estructura del informe y a quién va dirigido .....                      | 101 |
| 16.2. La plantilla de hallazgo y la evidencia reproducible .....              | 101 |
| 16.3. Impacto, riesgo y priorización.....                                     | 102 |
| 16.4. Recomendaciones verificables y plan de remediación .....                | 103 |
| 16.5. Los anexos: inventario y matriz de cifrados.....                        | 103 |
| 16.6. Presentación, defensa del informe y retest.....                         | 104 |
| Módulo 17 — Modelo de seguridad WiFi en profundidad + CVEs emblemáticos ..... | 105 |
| 17.1. La jerarquía de claves en detalle .....                                 | 105 |
| 17.2. El interior de SAE.....                                                 | 106 |
| 17.3. PMF por dentro.....                                                     | 106 |
| 17.4. Roaming: 802.11r, 802.11k y 802.11v.....                                | 107 |
| 17.5. 6 GHz, WiFi 7 y canales DFS .....                                       | 107 |
| 17.6. Ataques emblemáticos y CVEs de WiFi.....                                | 108 |
| 17.7. Leer correctamente las protecciones modernas en un informe .....        | 109 |
| Módulo 18 — Preparación para el examen WXS.....                               | 110 |
| 18.1. Qué evalúa el examen WXS.....                                           | 110 |
| 18.2. Gestión del tiempo y estrategia .....                                   | 110 |
| 18.3. Errores comunes que debes evitar.....                                   | 111 |

---

|                                                                  |     |
|------------------------------------------------------------------|-----|
| 18.4. Modelos mentales para encontrar hallazgos más rápido ..... | 111 |
| 18.5. Checklist pre examen .....                                 | 112 |