

WXS

Wireless eXploitation Specialist Course Manual



Table of Contents

Module 0 — Legal Notice and Intellectual Property	7
0. Copyright and Terms of Use of the Material	7
Ownership and Rights	7
Restrictions on Use and Prohibition of Distribution	7
Permitted Use	7
Responsible Use and Authorization Framework	7
Legal Particularities of Wireless Networks	8
Protection of Personal Data	8
Confidentiality and Protection of the Learning Environment	8
Non-Compliance	8
Module 1 — Course Introduction	9
1.1. Introduction	9
1.2. What Is a WiFi Audit and What Does It Include?	9
1.3. How We Work in WXS: Reconnaissance, Hypothesis, Validation, and Reporting	10
1.4. What Is Reproducible Evidence in WiFi?	11
1.5. Deliverables We Will Build During the Course	12
1.6. Ethical Framework and Scope of Responsible Use	13
Module 2 — RF and WiFi Network Fundamentals	14
2.1. The Radio Spectrum and the 2.4 / 5 / 6 GHz Bands	14
2.2. Channels, Overlap, and Channel Width	14
2.3. The IEEE 802.11 Standard (from WiFi 4 to WiFi 7)	15
2.4. WiFi Network Architecture: STA, AP, BSS, ESS, IBSS, and DS	16
2.5. Identifiers: SSID, BSSID, and ESSID	17
2.6. Network Types by Encryption	18
2.7. Key Security Concepts: WPS, PMF, and Roaming	19
2.8. Module Summary	20
Module 3 — 802.11 Frames and Protocols from the Auditor's Perspective	21
3.1. The 802.11 Frame as a Unit of Evidence	21
3.2. Management Frames: Beacon, Probe, Authentication, and Association	22
3.3. Control and Data Frames: What Information They Leak	23
3.4. The Connection Process: Discovery, Authentication, and Association	23
3.5. EAPOL and the 4-Way Handshake	24
3.6. Information Leaked Even by a Protected Network	25
3.7. Client MAC Randomization	26
3.8. Module Summary	27

Module 4 — Environment and Tools: the WiFi Audit Workflow.....	28
4.1. Hardware: Which Adapter You Need and Why	28
4.2. Antennas: Omnidirectional Versus Directional	28
4.3. Operating System: Kali or Parrot, on Physical or Virtual Hardware.....	29
4.4. Verifying the Adapter	29
4.5. Monitor Mode and Injection	30
4.6. The Workbench: airodump-ng, Wireshark, and hcxtools.....	31
4.7. Evidence: What to Save and How to Present It.....	32
4.8. Labs: the Course Practice Environment.....	32
4.9. Dedicated Audit Hardware.....	33
4.10. Building Your Own Practice Access Point with hostapd	33
4.11. Troubleshooting Common Problems	34
Module 5 — Offensive WiFi Reconnaissance.....	36
5.1. Passive and Active Reconnaissance: Applying the Method to Recon	36
5.2. airodump-ng in Depth.....	36
5.3. Reading Encryption: the ENC, CIPHER, and AUTH Columns.....	37
5.4. Manufacturer Identification by OUI and Client Enumeration.....	38
5.5. Kismet and wifi_db: Advanced Reconnaissance and Persistence	39
5.6. Hidden Networks: Revealing the ESSID.....	40
5.7. Probe Requests and the Client's Preferred Network List.....	41
5.8. Reconnaissance in the Presence of MAC Randomization	41
5.9. Wardriving: Geolocating Networks	42
5.10. Module Summary and Recommended Reconnaissance Order.....	43
Module 6 — Open Networks, OWE, and WEP	44
6.1. Open Networks: Risks and MAC Spoofing.....	44
6.2. Captive Portals: Operation and Basic Bypasses.....	45
6.3. OWE (Enhanced Open): What Changes Compared with an Open Network.....	45
6.4. WEP: Why It Was Broken from the Start.....	45
6.5. Attacks Against WEP.....	46
6.6. Recovering the Key with aircrack-ng.....	47
6.7. Module Summary and Checklist.....	48
Module 7 — WPA/WPA2-PSK: Handshake and PMKID.....	50
7.1. 4-Way Handshake Theory	50
7.2. Capturing the Handshake with airodump-ng.....	51
7.3. Forcing Reconnection: Directed and Broadcast Deauthentication.....	52
7.4. Verifying That the Handshake Is Valid	53
7.5. The PMKID Attack: Capture Without Clients	54
7.6. Converting to the Cracking Format.....	55
7.7. Module Summary and Recommended Test Order	56

Module 8 — Key Cracking (aircrack-ng / hashcat)	57
8.1. Dictionary Cracking with aircrack-ng.....	57
8.2. hashcat and Mode 22000	57
8.3. hashcat Attack Modes.....	58
8.4. Dictionaries and Targeted Generation	59
8.5. Rules and Masks for Real Passwords.....	59
8.6. Optimization, Benchmarking, and Distributed Cracking.....	60
8.7. Decrypting Captured Traffic with the Recovered Key	61
8.8. Module Summary and Checklist.....	62
Module 9 — WPS: Reaver, Bully, and Pixie Dust.....	64
9.1. What WPS Is and Where It Fails.....	64
9.2. Detecting WPS with wash	64
9.3. Attacking the PIN: reaver and bully.....	65
9.4. Pixie Dust: the Offline Attack.....	66
9.5. Null PINs, Lockout, and How to Handle Them	67
9.6. Module Summary and Checklist.....	68
Module 10 — WPA-Enterprise / 802.1X (MGT)	69
10.1. Enterprise Network Architecture: Supplicant, Authenticator, and RADIUS Server	69
10.2. EAP Methods.....	69
10.3. The Weak Point: Server-Certificate Validation	70
10.4. Enterprise Evil Twin with hostapd-wpe	70
10.5. eaphammer: Credential Capture	71
10.6. Cracking the MSCHAPv2 Challenge.....	71
10.7. Module Summary and Recommended Test Order.....	72
Module 11 — Evil Twin, Rogue AP, and MITM.....	73
11.1. What an Evil Twin Is and When It Is Used	73
11.2. Creating the Twin Access Point	73
11.3. Phishing Captive Portal with wifiphisher.....	74
11.4. Karma, MANA, and Known Beacons	75
11.5. Attracting the Client: Deauthentication, Signal Strength, and PNL Exploitation	76
11.6. Man-in-the-Middle After the Client Connects	77
11.7. Downgrade Attacks and Transition Mode.....	78
11.8. Module Summary and Checklist.....	78
Module 12 — WPA3, SAE, and Dragonblood	79
12.1. What WPA3 Solves Compared with WPA2	79
12.2. The SAE Handshake.....	79
12.3. Mandatory PMF and Its Impact on Classic Attacks.....	80
12.4. Dragonblood: Side Channels and Downgrade	81
12.5. The Achilles' Heel: Transition Mode	81

12.6. WPA3-Enterprise and 192-Bit Mode.....	83
12.7. SSID Confusion (CVE-2023-52424)	83
12.8. Current State of WPA3 Attacks and Practical Limits	84
12.9. Module Summary.....	84
Module 13 — DoS, Deauthentication, and PMF (802.11w)	85
13.1. Deauthentication and Disassociation as Denial of Service.....	85
13.2. Beacon and Authentication Flooding with mdk4.....	85
13.3. PMF (802.11w): How It Stops Deauthentication Attacks	86
13.4. Detecting PMF and What to Do When It Is Active.....	87
13.5. Legal Warning About Jamming.....	88
13.6. Module Summary.....	89
Module 14 — Post-Exploitation and Pivoting	90
14.1. Inside the Network: Discovery and Scanning.....	90
14.2. ARP Spoofing and Man-in-the-Middle on the Internal Network.....	91
14.3. Client Isolation and Its Bypass	92
14.4. Pivoting to the Corporate Network.....	92
14.5. Module Summary.....	93
Module 15 — Automation: airgeddon and wifite2.....	94
15.1. airgeddon: the Interactive Orchestrator	94
15.2. wifite2: Automated Attack from Start to Finish.....	95
15.3. When to Automate and When to Work Manually	95
Module 16 - Professional Reporting	97
16.1. Report structure and intended audience.....	97
16.2. The finding template and reproducible evidence	97
16.3. Impact, risk, and prioritization	98
16.4. Verifiable recommendations and remediation plan	99
16.5. Appendices: inventory and encryption matrix	99
16.6. Presentation, report defense, and retesting.....	100
Module 17 - The WiFi Security Model in Depth and Landmark CVEs.....	101
17.1. The key hierarchy in detail.....	101
17.2. Inside SAE	102
17.3. Inside PMF	102
17.4. Roaming: 802.11r, 802.11k, and 802.11v	103
17.5. 6 GHz, WiFi 7, and DFS channels.....	103
17.6. Landmark WiFi attacks and CVEs.....	103
17.7. Interpreting modern protections correctly in a report	104
Module 18 - Preparing for the WXS Exam.....	106
18.1. What the WXS exam assesses	106
18.2. Time management and strategy.....	106

18.3. Common mistakes to avoid	107
18.4. Mental models for finding issues faster	107
18.5. Pre-exam checklist	108