Advanced Wireless Operations Course

The Advanced Wireless Operations Course (AWOC) introduces students to operational planning, tactics, and techniques around the exploitation of 802.11 (WiFi).

The program begins with classroom based exercises designed to guide students through operational testing and configuration of their equipment prior to executing the exercises.

During the classroom based block, we teach students how to scan through 802.11 frequencies, identify and locate WiFi emitters, bypass encryption, understand and analyze collected WiFi and network data, and exploit the connected network.

Days 2-5 consist of various scenario based exercises that require concept of operations planning, movement to target Area of Operations, Target Identification, WiFi Encryption Bypassing, Network Sniffing, Network Exploitation, and Data Exfiltration.

The AWOC curriculum is uniquely designed and taught by members of BlackHorse's Special Activities Division to provide students with cutting edge best practices that have proven successful in facilitating operations focused on Force Protection, Penetration Testing, SIGINT/CYBER Collection, Counter Surveillance, Surveillance, and Precise Geo-Location.

We have supported and provided this training to operational units within the Department of Defense (DoD), Law Enforcement Agencies, and Intelligence Community (IC) partners.

AWOC FRAMEWORK

The AWOC course utilizes hands-on practical scenarios and instruction on various methods, techniques and trade craft where learning new skills is the focus, as opposed to the technology or tool.

AWOC teaches students a comprehensive offensive wireless methodology that can be applied with the use of various tools and applications to protect and exploit both professional and operational networks and devices. Students graduate the course with the skills to effectively monitor or exploit all types of wireless network implementations.

THE AWOC DIFFERENCE

Tool Agnostic – The course is focused primarily on the Kali Linux Operating System, but alternative tools are worked with for most modules. Government off the shelf programs can be used for the final exercise.

No Fluff – This class doesn't contain history lessons; it is designed to teach actionable tools, techniques, and procedures.

BLACK HORSE

SECURITY FOR THE NEW INDUSTRIAL REVOLUTION

WHAT STUDENTS WILL NEED

- A basic familiarity with Linux Command Line
- WiFi Theory | Experience with Basic Operations (Scanning, identifying access points and devices)
- Operational Laptop w/ 3 Wireless Interface Cards with External Antennas (Bi-Directional and Omni-Directional), USB GPS Adapter,

Course Schedule (Days 1-5)

1 DAY ONE

- Admin/Introduction
- Linux Command Line Familiarization
- WiFi Gear Operational Testing
- Classroom Based Exercises

2 DAY TWO

- Target Acquisition (MAC Grabbing) - Mobile Devices and Laptops
- Find/Fix Operations
- Encryption Bypassing

3 DAY THREE

- Denial of Services
- Evil Twin/ MiTM Attacks
- Basic Penetration Testing

4 DAY FOUR

- Network Scanning
- Network Exploitation
- Network Sniffing
- Data Exfiltration

5 DAY FIVE

- Full Mission Profile Exercise
- Protecting Devices from Exploitation
- After Action Review

tognc@blackhorsesolutions.com | (910) 286 - 1743 | www.blackhorsesolutions.com