Advanced Offensive Security and Red Teaming Operations Training Course



16 - 20 Nov 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #CYB1118_89438

Course Introduction / Overview:

This course provides a deep dive into the world of offensive security, focusing on the strategies, tactics, and procedures used in modern red teaming operations. Moving beyond traditional penetration testing, this program is designed to simulate the actions of a real-world Advanced Persistent Threat (APT) to rigorously test an organization's security posture, including its people, processes, and technology. Participants will learn to think like an adversary, mastering the full engagement lifecycle from initial reconnaissance and C2 infrastructure setup to lateral movement, data exfiltration, and defense evasion. The curriculum is heavily influenced by the principles outlined by experts like Joe Vest in works such as "Red Team Development and Operations," emphasizing a structured and objective-driven approach. At BIG BEN Training Center, we have developed a curriculum that not only teaches the use of cutting-edge tools but also instills the critical mindset required to emulate sophisticated attackers. This training course is an immersive, hands-on experience that equips security professionals with the skills to identify and exploit complex vulnerabilities, ultimately providing organizations with invaluable insights to strengthen their defensive capabilities against determined attackers.

Target Audience / This training course is suitable for:

- Penetration Testers seeking to advance into red teaming roles.
- Cybersecurity Analysts and Incident Responders.
- Security Engineers and Architects.
- Network and System Administrators with security responsibilities.
- IT Managers and Team Leads overseeing security operations.
- Blue Team members wanting to understand offensive tactics.
- Cybersecurity consultants and professionals.

Target Sectors and Industries:

- Financial Services and Banking.
- Government and Public Sector Agencies.
- Defense and Military Contractors.
- Technology and Software Development.
- Healthcare and Pharmaceutical.
- Telecommunications and Utilities.
- Critical Infrastructure and Energy.
- E-commerce and Retail.

Target Organizations Departments:

- Information Security and Cybersecurity.
- Information Technology Operations.
- Risk Management and Compliance.
- Internal Audit and Assurance.
- Security Operations Center (SOC).
- Threat Intelligence Teams.
- Application Development and DevOps.

Course Offerings:

By the end of this course, the participants will have able to:

- Plan and execute comprehensive red team engagements from start to finish.
- Conduct advanced open-source intelligence (OSINT) gathering.
- Establish and manage covert command and control (C2) infrastructure.
- Develop and deploy custom payloads for initial access.
- Master techniques for privilege escalation on Windows and Linux systems.
- Execute complex attacks against Active Directory environments.
- Employ sophisticated methods for lateral movement within a network.
- Bypass modern security controls like antivirus (AV) and endpoint detection and response (EDR).
- Emulate the tactics, techniques, and procedures (TTPs) of known threat actors.
- Utilize the MITRE ATT&CK framework for planning and reporting.
- Create professional, actionable reports that drive security improvements.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be deeply immersive and practical, moving beyond theoretical knowledge to build real-world skills. This course is structured around a hands-on, lab-intensive environment where participants spend the majority of their time executing simulated attacks in a secure, virtual corporate network. We employ a blend of interactive lectures, live demonstrations, and individual exercises to introduce new concepts and tools. The core of the learning experience is a series of team-based red team scenarios and Capture-The-Flag (CTF) style challenges that replicate realistic adversary campaigns. These exercises require participants to collaborate, strategize, and adapt their tactics in real-time. Case studies of prominent cyber-attacks are analyzed to provide context and highlight effective TTPs. Continuous feedback is provided by the instructor, and group discussions encourage the sharing of strategies and insights. This approach ensures that participants not only learn the techniques but also understand the strategic mindset of an attacker, preparing them for the complexities of live red team operations.

Course Agenda (Course Units):

Unit One: Red Teaming Fundamentals and Engagement Planning

- Introduction to Offensive Security and Red Teaming.
- Differentiating Red Teaming from Penetration Testing.
- Ethics and Rules of Engagement.
- Understanding the Cyber Kill Chain Methodology.
- Introduction to the MITRE ATT&CK Framework.
- Open-Source Intelligence (OSINT) Gathering Techniques.
- Planning a Red Team Operation and Defining Objectives.
- Setting Up a Covert C2 Infrastructure.

Unit Two: Initial Access and Weaponization

- Advanced Network and Host Discovery.
- Active and Passive Reconnaissance Strategies.
- Social Engineering and Phishing Campaign Development.
- Client-Side Exploitation Techniques.
- Crafting and Delivering Malicious Payloads.
- Weaponizing Documents and Applications.
- Gaining an Initial Foothold in the Target Network.
- Understanding and Bypassing Email Gateways.

Unit Three: Post-Exploitation and Lateral Movement

- Host-Based Enumeration and Situational Awareness.
- Windows and Linux Privilege Escalation Techniques.
- Credential Dumping and Password Cracking (Mimikatz, Hashcat).
- Fundamentals of Active Directory (AD) Security.
- Attacking Active Directory: Kerberoasting and Pass-the-Hash.
- Advanced AD Attacks: Golden and Silver Tickets.
- Pivoting and Lateral Movement Across the Network.
- Establishing Persistence on Compromised Systems.

Unit Four: Defense Evasion and Command & Control

- Understanding Antivirus (AV) and EDR Evasion.
- Techniques for Bypassing Application Whitelisting.
- Customizing Payloads to Avoid Signature-Based Detection.
- Advanced Command & Control (C2) Frameworks and Tactics.
- DNS and HTTP/S Tunneling for Covert Communications.
- Data Staging and Exfiltration Techniques.
- Covering Tracks and Removing Evidence of Intrusion.
- Introduction to Purple Teaming Concepts.

Unit Five: Advanced Operations and Reporting

- Adversary Emulation with ATT&CK Navigator.
- Attacking Cloud Environments (AWS, Azure).
- Introduction to Physical Security Considerations.
- Evading Network-Based Detection Systems (IDS/IPS).
- Consolidating Gains and Achieving Objectives.
- Developing a Professional Red Team Report.
- Presenting Findings to Technical and Executive Audiences.
- Capstone Exercise: Full-Scope Red Team Engagement Simulation.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

Beyond technical vulnerabilities, how does an organization's security culture and human behavior represent the most critical attack surface in a red team engagement?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by focusing on the strategic mindset and operational lifecycle of an adversary, rather than merely teaching a collection of hacking tools. While many courses concentrate on specific exploits, our curriculum emphasizes the art of adversary emulation, teaching participants how to mimic the TTPs of real-world threat actors like APT groups. We dedicate significant time to the crucial, often-overlooked phases of an operation, including meticulous planning, covert infrastructure setup, and sophisticated defense evasion. The program is built around a narrative-driven, hands-on lab environment that simulates a complete corporate network, forcing participants to think critically and adapt their strategies against dynamic defenses. Furthermore, we place a strong emphasis on reporting and communication, ensuring that graduates can translate complex technical findings into actionable business intelligence for stakeholders. The objective is not just to find vulnerabilities but to test an organization's detection and response capabilities in a holistic manner, providing a true measure of its security resilience. This strategic, full-spectrum approach provides a depth of understanding that is essential for executing impactful red team operations.