Masterclass: Red Team Tradecraft and Operations

Cursusduur: 3 Dagen **Cursuscode: RTO** **Trainingsmethode: Virtual Learning**

Beschrijving:

Red Team Tradecraft and Operations is an intensive 3-day, 21-hour course focused on the professional execution and management of Red Team engagements. Unlike traditional penetration testing courses that focus primarily on how to hack, this course focuses on how to operate, covering strategic planning, infrastructure execution, operational security, collaboration, and reporting throughout the full lifecycle of a Red Team engagement.
Participants will learn how to build and maintain resilient, secure, and automated Red Team infrastructure, define Rules of Engagement, select and configure Command & Control (C2) frameworks, apply operational security (OPSEC), translate threat intelligence into adversary emulation plans, coordinate multi-operator engagements, and produce high-value reports that communicate technical findings in terms of business impact.

Updated Auguts 2026

Virtueel en Klassikaal™

Virtueel en Klassikaal™ is een eenvoudig leerconcept en biedt een flexibele oplossing voor het volgen van een klassikale training. Met Virtueel en Klassikaal™ kunt u zelf beslissen of u een klassikale training virtueel (vanuit huis of kantoor)of fysiek op locatie wilt volgen. De keuze is aan u! Cursisten die virtueel deelnemen aan de training ontvangen voor aanvang van de training alle benodigde informatie om de training te kunnen volgen.

Doelgroep:

This course is designed for:
- Red Team Leads
- Senior Penetration Testers transitioning to Red Teaming
- Adversary Emulation Specialists
- C2 Infrastructure Engineers
- Security Managers overseeing offensive operations
- Penetration Testers
- Security Analysts
- IT Administrators
- Cybersecurity Professionals
- IT professionals with a technical background who want to develop their skills in cybersecurity penetration testing

Doelstelling:

- **By the end of the course, participants will be able to:**
- Manage the end-to-end lifecycle of a Red Team operation, including scoping, deconfliction, and legal boundaries.
- Define effective Rules of Engagement (RoE) and identify critical assets or “Crown Jewels.”
- Translate Cyber Threat Intelligence (CTI) into actionable adversary emulation and simulation plans using MITRE ATT&CK.
- Design resilient, tiered Red Team infrastructure, including Team Servers, Redirectors, and Payload Servers.
- Deploy disposable Red Team infrastructure using Infrastructure as Code (IaC) and automation.
- Configure and manage Command & Control (C2) infrastructure and profiles.
- Configure redirectors and use techniques to mask the origin of attacks and blend traffic into normal organizational network traffic.
- Implement effective OPSEC workflows and secure team communication.
- Maintain accurate logging to support reconstruction of operational events.
- Coordinate multi-operator Red Team engagements.
- Translate technical findings into business-impact narratives and executive-level reporting.

Vereiste kennis en vaardigheden:

- Technical background in IT or cybersecurity
- Basic knowledge of penetration testing and cybersecurity concepts

Examens en certificering

Participants receive a **CQURE lifelong certification** upon successful completion of the course.

Vervolgcursussen:

None

Cursusinhoud:

18 expert-level modules delivered over

3 intensive days, combining strategic planning, infrastructure engineering, operational tradecraft, and reporting methodologies.

This training focuses on the professional execution of Red Team engagements. Students will learn how to design resilient command-and-control infrastructure, manage operational security, translate threat intelligence into adversary emulation plans, coordinate multi-operator engagements, and deliver executive-level reporting that demonstrates real business impact.

Day 1: Engagement Strategy ; Infrastructure Engineering

- Module 1: The Red Team Framework: Red Teaming vs. Penetration Testing. Defining “Objectives Based” vs. “Scope Based” assessments.
- Module 2: Scoping, RoE ; Legal: The art of the kick-off meeting. Defining Rules of Engagement (RoE), “Crown Jewels” identification, White Cards, and legal protections.
- Module 3: Threat Intelligence (CTI) ; Emulation: Translating CTI reports into actionable Adversary Emulation/Simulation Plans using MITRE ATT;CK.
- Module 4: Infrastructure Architecture: Designing the Tiered Infrastructure Model (Team Servers, Redirectors, Payload Servers) for non-attribution.
- Module 5: Automation (DevSecOps): Hands-on automated deployment of disposable infrastructure. Automating SMTP relays, phishing servers, C2 nodes etc..
- Module 6: Traffic Management: Configuring Redirectors (Nginx/Socat) and utilizing CDNs/Domain Fronting to mask the origin of attacks. Using ExternalC2 to blend into the common organization network traffic.

Day 2: Comand, Control ; Operational Tradecraft

- Module 7: C2 Framework Selection: Comparative analysis of modern frameworks and selection strategy based on operation goals.
- Module 8: Traffic Engineering: Customizing traffic signatures (Malleable C2/Profiles) to blend with legitimate network traffic (jitter, sleep, user-agent spoofing). Using application-related external C2 channels.
- Module 9: Communication Channels: Deep dive into HTTP/S, DNS, and SMB piping. Understanding “Beaconing” heuristics and detection logic.
- Module 10: Team Collaboration: Managing shared sessions, operator logs, and deconfliction servers to avoid “Red-on-Red” issues.
- Module 11: Initial Access Strategy: Planning the delivery vector (Physical vs. Phishing vs. Assumed Breach). Tracking payload execution rates and landing success.
- Module 12: OPSEC ; “Silence”: Managing “Time on Target” and noise levels. Decision-making matrices for when to use active scanning vs. passive enumeration.

Day 3: Execution Management, Analysis ; Reporting

- Module 13: Persistence Strategy: Long-term access management. Differentiating between “Interactive Access” (high noise) and “Sleepy Agents” (low noise).
- Module 14: The “Assume Breach” Execution: Methodologies for internal-only engagements and lateral movement discipline (avoiding event log spikes).
- Module 15: Logging ; Reconstruction: Aggregating operator logs (ELK/Splunk). Correlating Red Team actions with Blue Team alerts for the debrief.
- Module 16: The Red Team Report: Structuring the strategic report. Writing Executive Summaries, visualizing Attack Graphs, and defining Business Impact.
- Module 17: Purple Teaming ; Remediation: Transitioning from attack to defense. Delivering constructive feedback and verifying fixes.
- Module 18: Capstone Workshop: Students design a complete Operation Plan for a fictional client, including Infrastructure design, CTI selection, RoE drafting, and Reporting structure.

Nadere informatie:

Neem voor nadere informatie of boekingen contact op met onze Customer Service Desk 030 - 60 89 444

info@globalknowledge.nl

www.globalknowledge.com/nl-nl/

Iepenhoeve 5, 3438 MR Nieuwegein