+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 23/02/2024

Sign up

Mandiant Red Team Ethical Hacker training

4 days (28 hours)

Presentation

Our Red Team Ethical Hacker training course will teach you all the techniques and methods of pentesting to become a true Red Team expert. On completion of the course, you'll be able to carry out full-scale attacks to discover and correct vulnerabilities in your organization's infrastructure.

Our program, inspired by leading experts in the field such as OffSec and Mandiant, covers all the skills needed to set up pentesting operations. You'll learn about infrastructure and command control concepts, as well as initial recognition and compromise.

Our training will not only teach you how to carry out attacks on infrastructures, but also how to produce detailed reports that can be used to improve existing cybersecurity strategies and adopt new, more effective ones.

You'll also have the opportunity to test the skills acquired during our training with a practical Capture the Flag workshop.

Objectives

- Identify and compromise a target
- Deploy tactics to maintain access to a compromised target
- Exfiltrate secure data undetected
- Write detailed reports on vulnerabilities in order to correct them

Target audience

- Ethical Hacker
- Cybersecurity Experts

- Pentester

Prerequisites

- Cybersecurity/pentesting experience
- Knowledge of active directory
- Familiarity with PowerShell scripts

Red Team Ethical Hacker training program

INTRODUCTION TO RED TEAMING

- What is Red Teaming?
- Differences from traditional pentesting
- Objectives and benefits
- Rules of engagement and legal aspects
- Presentation of tools and methodology
- The difference between ethical attackers and cybercriminals

INFRASTRUCTURE AND COMMAND & CONTROL (C2)

- Acquisition of domains for operations
- Infrastructure requirements
- Setting up and securing C2 servers
- Domain Fronting
- HTTPS and DNS redirectors

INITIAL RECOGNITION

- Passive recognition: Whois, DNS and social networks
- Active recognition: Network scanning and service discovery
- Google Dorks and data collection
- List e-mails
- Organizational data analysis
- Best practices for keeping a low profile

INITIAL COMPROMISE

- Compromise techniques: Web Shells, SQL injections, Password Spraying
- Preparation and use of social engineering attacks
- Creating malicious payloads
- Distribution via e-mail or cloned websites
- customization of attack vectors
- Simulation of real-life attacks

ESTABLISHING A BRIDGEHEAD

- Obfuscation techniques
- Antivirus evasion
- Use of frameworks such as .NET and PowerShell to execute malicious code
- Executing commands
- Scripts without detection
- Post-operation operation and intelligence gathering
- Strategies to maintain access and avoid detection

ATTACKS AGAINST ACTIVE DIRECTORY AND LATERAL MOVEMENT

- Enumeration and privilege escalation in Active Directory
- Mapping AD relationships
- Lateral movement and propagation in a network
- Importance of opsec
- Attack simulation

GOAL ATTAINMENT AND REPORTING

- Database attack strategies
- Techniques for exfiltrating sensitive data
- Preparation of a detailed vulnerability report
- Retesting and validation of corrective measures
- Analyzing the effectiveness of actions and measuring impact

FRAMEWORKS AND METHODOLOGIES

- Introduction to frameworks such as MITRE ATT&CK™ and Kill Chain
- Understanding and using threat intelligence
- Planning and execution of opponent emulations
- Analysis of indicators of compromise (IoC)
- Technology watch and strategy adaptation

ATTACK INFRASTRUCTURE AND OPERATIONAL SECURITY

- Configuring and managing Red Team tools
- Securing the attack infrastructure
- Setting up redirectors
- Maintaining access and persistence
- Risk management
- Reducing the attack footprint

MALWARE ANALYSIS AND REVERSE ENGINEERING

- Malware analysis tools (Ghidra and IDA Pro)
- Malware reverse engineering
- Executable file formats and internal structure
- Malware tactics
- Importance of malware analysis

CAPTURE THE RED TEAM FLAG

- Organization of a practical Capture The Flag (CTF) exercise
- Simulation of a complete attack on a predefined infrastructure
- Team analysis of strategies used and results obtained
- Importance of collaboration and communication within the Red Team
- Feedback and identification of areas for improvement

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.