INFOSEC Skills
LIVE BOOT CAMPS

Get live, expert instruction from anywhere.

Red Team Operations Boot Camp

Do good by being bad in this exclusive Red Team Operations training designed to teach you to think like a cybercriminal, help you better defend your organization, and prepare you for the Certified Red Team Operations Professional exam.

Course description

"Know your enemy, and know yourself." Sun Tzu's most famous advice from The Art of War still applies in the 21st century, and on the digital battlefield, knowing your enemy is more important than ever. So put on your black hat and get ready for Infosec's groundbreaking Red Team Operations Boot Camp!

In our exclusive Red Team Operations Boot Camp, you'll learn to defend against hacking and fraud attacks on your organization — from network vulnerabilities to social-engineering tactics. And you'll learn from the attacking side! Our experienced instructors will lead you through the basics of multiple cybercrime assaults and show you how you can use these techniques to improve security at your own organization.

Who should attend

- Red team members and offensive security specialists
- Penetration testers, security researchers and ethical hackers
- Incident responders
- CISOs and security managers
- Security and networks architects, engineers and administrators
- Any professionals whose responsibilities include physical and information security

Boot camp at a glance

Hands-on training

- ✓ Find and exploit network vulnerabilities
- ✓ Learn how to bypass physical controls
- ✓ Hone your social engineering skills with a phishing campaign

Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite

Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 5-day boot camp
- ✓ 90-day extended access to all boot camp materials

The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

700+ IT and security courses

Earn CPEs and build new skills with 100s of additional training courses.

What's included

- Five days of expert, live Red Team Operations training
- Exam Pass Guarantee
- Exam voucher
- 100% Satisfaction Guarantee
- Unlimited practice exam attempts
- Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- 90-day extended access to all boot camp video replays and materials
- Onsite proctoring of exam
- Pre-study learning path
- Knowledge Transfer Guarantee

Prerequisites

- Understanding of fundamental information security concepts
- Professional exposure to penetration testing methodologies and tools
- Basic understanding of networking concepts
- Firm understanding of the Windows Operating System
- Exposure to the Linux Operating System or other Unix-based OS
- Desire to learn about pentesting and red teaming, stay ethical and get great security training!

Hands-on labs

Our practical exercises are designed to make you feel like a part of a real red team operation. Find and exploit network vulnerabilities in our intuitive virtualized environment configured with popular hacking tools. Learn how to bypass physical controls with a professional-grade lockpick demonstration. Hone your social engineering skills by crafting convincing phishing emails and running a real phishing campaign against your classmates, friends or family members using an industry-leading phishing simulator.

What you'll learn

After completing the course you will gain sufficient knowledge and skills to be able to:

- Thoroughly understand and apply a variety of passive and active intelligence-gathering techniques
- Discover and leverage vulnerabilities in physical and network infrastructure
- Select and effectively use social engineering techniques, from phishing to phone to face-to-face
- Gain entry into a target location using various covert and overt methods
- Test and evade all types of security control types: logical, physical and administrative
- Perform a comprehensive red team operation penetration test, from reconnaissance to establishing a foothold and maintaining a covert presence

Certification details

The Certified Red Team Operations (CRTOP) body of knowledge consists of seven domains covering the responsibilities of a red team member. The certification exam is a 50-question, traditional multiple-choice test. Questions are randomly pulled from a master list and must be completed in two hours. The seven CRTOP domains are:

- Red team roles and responsibilities
- Red team assessment methodology
- Physical reconnaissance tools and techniques
- Digital reconnaissance tools and techniques
- Vulnerability identification and mapping
- Social engineering
- Red team assessment reporting

Skill up and get certified, guaranteed

Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.

100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

What our students are saying

I really appreciate that our instructor was extremely knowledgeable and was able to provide the information in a way that it could be understood. He also provided valuable test-taking strategies that I know not only helped me with this exam, but will help in all exams I take in the future.

Michelle Jemmott
Pentagon

Excellent! Our instructor had a vast background and related the materials to real life. Much better than just teaching the materials to pass an exam … but he did that as well. He went out of his way in class. The extra materials really benefited us when we returned to our real jobs! Great experience!

John Peck
EPA

Very impressed with Infosec. My instructor did a great job delivering the information strategically and in a way for all to understand. I would definitely take another class/certification prep course.

Sylvia Swinson
Texeltek

The instructor was able to take material that prior to the class had made no sense, and explained it in real world scenarios that were able to be understood.

Erik Heiss
United States Air Force

The course was extremely helpful and provided exactly what we needed to know in order to successfully navigate the exam. Without this I am not confident I would have passed.

Robert Caldwell
Salient Federal Solutions

Red Team Operations Boot Camp details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

	Day 1	Day 2	Day 3	Day 4	Day 5
Morning session	Introduction to Red Team Operations Setting objectives	Reconnaissance (cont.)	Gaining access	Establishing foothold and maintaining presence (cont.)	Reporting Additional Red Team Operations resources
Afternoon session	Reconnaissance	Target identification	Establishing foothold and maintaining presence	Completing objectives	CRTOP exam review and prep Take the CRTOP exam
Evening session	Optional group & individual study	Optional group & individual study	Optional group & individual study	Optional group & individual study	

Schedule may vary from class to class

Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

During your boot camp

Module 1: Introduction to Red Team Operations

- Course introduction
- Types of Security Assessments
- What is Red Teaming?
- Role of Red Team in Organizational Security Programs
- Red Team vs. Blue Team
- Red Team Assessment Phases
- Red Teaming Methodology
- Planning Red Team Operations

Module 2: Red team assessment phases: Setting objectives

- Defining Assessment Methodology and Objectives
- Identifying Points of Contact
- Analyzing Initial Information
- Gathering Team and Equipment

Module 3: Red team assessment phases: Reconnaissance

- Passive Intelligence Gathering and OSINT
- Physical Recon
- Getting Started with Social Engineering
- Social Engineering Tactics
- Pretexting
- Phishing, Vishing, SMiShing
- Physical and Digital Surveillance
- Wireless Recon
- DNS and SNMP Recon
- Identifying Possible Attack Vectors

Module 4: Red team assessment phases: Target identification

- Identifying Physical Controls and Vulnerabilities
- Passive Network Discovery and Scanning
- TCP Scanning
- Scanning through Firewalls
- Stealthy Scanning Techniques
- Idle Scanning
- Avoiding IDS/IPS Detection
- Proper Identification of Services
- Vulnerability Identification
- Types of Network and Application Vulnerabilities

Module 5: Red team assessment phases: Gaining access

- Covert and Overt Entry
- Evading Surveillance and Physical IDS
- Lock Picking
- RFID Cloning
- Using Social Engineering to Gain Entry
- Vulnerability Mapping
- Types of Exploits
- Client-Side Exploits
- Password Attacks
- Exploiting Flaws in Encryption
- Attacking Web Application
- Wireless Hacking

Module 6: Red team assessment phases: Establishing foothold and maintaining presence

- Avoiding Anti-Virus Detection
- Use of Trojans
- Hardware and Software Keyloggers
- Installing Rogue Access Points and Network Taps
- Port Redirection and Other Anti-Firewall Techniques
- IDS Operations and Avoidance
- Internal Recon and Pivoting
- Encrypting Your Communications
- Protocol Abuse for Covert Communications
- Creating Custom Encryption Tunneling Applications

Module 7: Red team assessment phases: Completing objectives

- Identifying and Extracting Target Data
- SQL Data Extraction
- Sniffing Network Traffic
- Exploiting Targets of Opportunity
- Anti-Forensics
- Log Modification/Deletion
- Rootkits
- Communication and Evidence Management

Module 8: Red team assessment phases: Reporting

- Report Structure and Content
- Reporting for Compliance
- Providing Recommendations
- Presenting Your Findings

Module 9: Red team assessment phases: Target identification

- Red Team Operations Best Practices
- Commercial and Open-Source Tools
- The Future of Red Team Operations

After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.

INFOSEC