INFOSEC Skills
LIVE BOOT CAMPS

Get live, expert instruction from anywhere.

Reverse Engineering Boot Camp

Learn how to reverse engineer and analyze malware! Reverse engineering is a vitally important skill for today's expert security professional. Keep your organization safe by digging into the viruses, Trojans and rootkits being used by cybercriminals.

Course description

Infosec's hands-on Reverse Engineering Boot Camp teaches you the necessary analytical skills to discover the true nature of any Windows binary. You'll learn how to recognize the high-level language constructs (such as branching statements, looping functions and network socket code) critical to performing a thorough and professional reverse engineering analysis of a binary. After learning these important introductory skills, you will advance to the analysis of hostile code and malware, vulnerabilities in binaries, binary obfuscation schemes and more.

You will gain hands-on experience with popular commercial and open-source decompilers and debuggers, as well as learn how to use various hex editors, binary analysis programs and code coverage analyzers. The boot camp also prepares you to pass the Certified Reverse Engineering Analyst (CREA) exam.

Who should attend

- Malware analysts
- Security researchers
- Professionals looking to gain a technical understanding of malware
- Anyone looking to improve their malware analysis and reverse engineering skills

Boot camp at a glance

Hands-on training

- ✓ Build your skills with dozens of hands-on labs
- ✓ Learn about debuggers, disassemblers and other popular tools
- ✓ Analyze malware using anti-reversing techniques and other methods

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 Reverse Engineering training
- Exam Pass Guarantee
- Exam voucher
- Unlimited practice exam attempts
- 100% Satisfaction Guarantee
- 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

- Firm understanding of the Windows Operating System
- Firm understanding of computer architecture concepts
- Grasp of the TCP/IP protocols

If you are unsure if you meet the required prerequisites, contact us for a quick network security training skill check.

Hands-on labs

Learn the methodologies, tools, and manual reversing techniques used in real-world situations in our cloud-hosted reversing engineering lab. You'll learn how to analyze:

- Hostile code and malware, including ransomware, worms, viruses, Trojans, rootkits and bots
- Vulnerabilities in binaries, including format string vulnerabilities, buffer overflow conditions and the identification of flawed cryptographic schemes
- Binary obfuscation schemes used by hackers, Trojan writers and copy protection algorithms
- Additionally, you will learn how to recognize the features of modern optimizing compilers and how to use various hex editors, binary analysis programs and code coverage analyzers

What you'll learn

- Static and dynamic analysis
- Analyzing malware functionality and behavior
- Anti-reversing techniques
- Detecting debuggers
- Advanced reversing topics & CREA exam

Learn from experts

We don't just have great instructors, our instructors have years of industry experience and are recognized as experts. Over the past 15 years, we've helped tens of thousands of students get certified and advance their careers.

Industry-leading exam pass rates

Infosec's courseware materials are always up to date and synchronized with the latest exam objectives. Our industry-leading curriculum and expert instructors have led to the highest pass rates in the industry. More than 93% of Infosec students pass their certification exams on their first attempt.

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

Reverse Engineering 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 reverse engineering (i)	Static and dynamic analysis (i)	Analyzing malware functionality and behavior (i)	Anti-reversing techniques (i)	Advanced reversing topics
Afternoon session	Introduction to reverse engineering (ii)	Static and dynamic analysis (ii)	Analyzing malware functionality and behavior (ii)	Anti-reversing techniques (ii)	CREA exam review CREA 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

Day 1: Introduction to malware analysis and reverse engineering

Day one focuses on the fundamental knowledge required for malware analysis and reverse engineering. This day is designed to build critical skills required to proceed further into deeper discussions on reversing. You will also train on special purpose reversing debuggers and disassemblers. Lab exercises will focus on functionality of various reversing tools and basic static and dynamic analysis process.

- Basic static and dynamic analysis
- Reverse engineering concepts and legality
- Machine code
- Assembly language
- System- and code-level reversing
- Assembly basics (registers, operands, instructions)
- Fundamentals of reverse engineering tools (IDA Pro, Radare2)

Day 2: Static and dynamic analysis

Day two encompasses a deep discussion with hands-on content for reversing Windows binaries. Key concepts include identifying code paths, control functions and developing a general understanding of the code to be analyzed. Debugging concepts are introduced and practiced in hands-on lab exercises.

- Recognizing C Code constructs in assembly
- Windows API
- Windows Registry
- Network APIs
- DLLs
- Processes, threads and services
- Debugging process (stepping, breakpoints, modifying execution)
- Kernel debugging
- Debugging tools

Day 3: Analyzing malware functionality and behavior

Day three includes detailed coverage on reverse engineering malware. Focus is on live malware reversing using examples of viruses, Trojans and rootkits collected from the wild.

- Understanding common malware types and functionality
- Process injection and replacement
- DLL injection
- Direct, hook and APC injection and other malware launching techniques
- Registry persistence
- Svchost.exe
- Trojanized system binaries
- DLL load order hijacking
- Malware network behavior analysis
- Kernel mode rootkits (SSDT hooking, interrupts)
- User mode rootkits

Day 4: Anti-reversing techniques

Day four works with various anti-reversing techniques that software developers and malware writers put in place to make reverse engineering more difficult.

- Basic anti-reversing strategies
- Anti-disassembly
- Detecting debuggers
- Detecting VM presence
- Analyzing packed executables
- Popular packers (UPX, PECompact, ASPack, etc.)
- Simple obfuscation techniques (XOR swap, junk code, etc.)
- Obscuring through data flow and control flow
- Constant unfolding
- Deobfuscation tools
- Base64 and other encoding schemes
- Common ciphers and encoding schemes
- Reversing ransomware

Day 5: Advanced reversing topics & CREA exam

Day five covers advanced reversing topics as well as the CREA exam. The day ends with you taking the CREA exam.

- Recognizing C++ binaries
- Identifying constructors and destructors
- RTTI
- 64-bit architecture
- WoW64
- 64-bit analysis
- CREA exam overview
- CREA exam

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.

©2022 Infosec, Inc. All rights reserved.

INFOSEC