REVERSE ENGINEERING BOOT CAMP

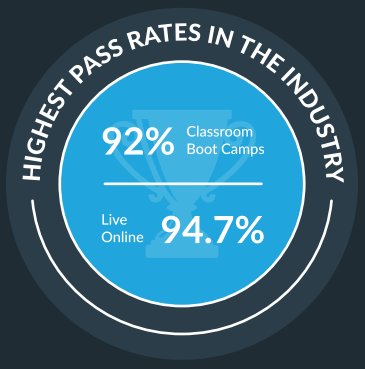
COURSE SYLLABUS

Reverse engineering is a vitally important skill for today's expert security professional. Everything from reverse engineering malware to discovering vulnerabilities in binaries are required in order to properly secure an organization from today's ever evolving threats.

Delivery Methods
Classroom
Live Online
Mentored Online

Duration
5 Days

Certification
Certified Reverse Engineering Analyst



INFOSEC INSTITUTE

866-471-0059

COURSE DESCRIPTION

In this 5 day hands-on course, you gain the necessary binary analysis skills to discover the true nature of any Windows binary. You will 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 & 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

InfoSec Institute will train you on popular commercial and open-source decompilers and debuggers. You will also learn how to use various hex editors, binary analysis programs, and code coverage analyzers.

REVERSE ENGINEERING IS A CRITICAL SKILL

Many incident response situations and computer forensics investigations cannot be completed accurately or thoroughly without understanding the runtime nature of a binary. Hackers increasingly use customized Trojans that are not detected by antivirus which can only be analyzed and traced back to the original attacker via reverse engineering. Additionally, many binary programs contain vulnerabilities, such as buffer overflows and the use of very weak cryptographic algorithms. The only way to discover these critical vulnerabilities for closed-source programs is to reverse engineer them. Reverse engineering is also required in order to understand complex binary obfuscation schemes used by copy protection vendors, as well as obfuscation put in place by commercial software vendors.

LEARN FROM EXPERTS

All of the instructors for InfoSec's Reverse Engineering course actively work in the field of incident response or security research. Our instructors have spoken at high-profile conferences (such as the Black Hat Briefings, the RSA Security Conference, and the Pentagon Security Forum) and industry events.

IDC lists InfoSec Institute as a Major Player in their Security Training Vendor Assessment.

"The quality of its instructors and training materials are viewed as the best of all vendors, as are its options for on-site and self-paced training. In addition, InfoSec Institute is perceived to be the best vendor for certification test preparation, classroom locations, facilities, and practice labs."

IDC
Analyze the Future

CERTIFIED REVERSE ENGINEERING ANALYST

In any hands on reverse engineer training course, it is important to have the opportunity to prove to current or potential employers that you have the skills you say you do. This course prepares you for the top reverse engineering certification in the industry, the CREA. The exam is given on-site, InfoSec Institute has achieved a 93% pass rate for this certification.

HANDS-ON LABS WITH IN-CLASSROOM EQUIPMENT

You will practice Reverse Engineering skills in over 20 separate Hands-On Labs and Capture The Flag (CTF) challenges. Our intuitive virtualized lab environment includes latest Reverse Engineering and Malware Analysis tools. Learn basic and advanced reversing techniques on real malware samples, including ransomware, rootkits, backdoors, and weaponized documents. Perform static and dynamic analysis and practice recognizing malware artifacts and behavior, unpacking, deobfuscation, and then put it all together in a challenging CTF exercise.

HOW YOU BENEFIT

- Gain the in-demand career skills of a reverse engineer. Very few information security professionals, incident response analysts and vulnerability researchers have the ability to reverse binaries efficiently. You will undoubtedly be at the top of your professional field.
- Learn the methodologies, tools, and manual reversing techniques used real world situations in our reversing lab.
- Move beyond automated "input and output" testing of binaries, commonly used by fuzzers and other tools.
- More than interesting theories and lecture, get your hands dirty in our dedicated reversing lab in this security training course.

WHAT'S INCLUDED

- 5 Days of Expert Reverse Engineering Instruction from a instructor with real-world experience and deep knowledge of course content.
- Guaranteed small class size (less than 10-16 Students), you get an intimate learning setting not offered at any of our competitors.
- Infosec Institute's Custom Reversing Tools Enterprise Suite, includes every program covered in the course for at home study. (119 Tools).
- All meals, snacks and refreshments included.
- Certified Reverse Engineering Analyst (CREA) exam fees.
- Lecture, Lab Exercise and Text book

REVERSE ENGINEERING BOOT COURSE DETAILS

Day 1: Introduction to Malware Analysis and Reverse Engineering

Day 1 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)

InfoSec Institute's 100% Satisfaction & Human Capital Guarantee

InfoSec Institute is committed to you having the best possible training experience available. We offer students the opportunity to re-sit a Classroom-based or Live Online course tuition-free for up to one year or until the student obtains certification, whichever comes first. Our Human Capital Guarantee ensures a successful return on investment for employers. If an employer has paid the cost of a class for an employee who leaves within three (3) months of obtaining certification, InfoSec Institute will train an additional employee of the company at no tuition cost to the employer for up to 12 months. Any employer may request their InfoSec Institute graduate re-sit the course tuition-free within three (3) months of the completed training if the employee is not successfully performing a job duty related to the class that was taken.

REVERSE ENGINEERING BOOT COURSE DETAILS (CONTINUED)

- Fundamentals of reverse engineering tools (IDA Pro, Radare2

Day 2: Static and Dynamic Analysis

Day 2 encompasses a deep discussion with hands-on content for reversing Windows binaries. Key concepts such as identifying code paths, control functions and developing a general understanding of the code to be analyzed is covered. 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

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 4 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

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

CREA Exam given on-site in afternoon

LIVE ONLINE TRAINING PLATFORM

Our live-online training program was designed to provide students with a genuine classroom-style boot camp experience without the inconvenience and cost associated with travel. Students can remotely attend any of our live and in-progress sessions from their home or work.

Some key advantages of InfoSec Institute's Live Online Training:

- Exam-Pass Guarantee*
- Real-Time Instructor-Led Training
- Quality Course Materials Shipped To Your Door at No Cost
- Save on Travel and Hotel
- Highest Success Rate
- Hands on Labs with 6 Months Of Extended Access

Live Online Training Platform

CORPORATE ON-SITE DISCOUNTS

Get reverse engineerin training on-site for a fraction of the price of our publicly scheduled boot camps with 10 or more students!

INDUSTRY RECOGNITION

These are just a few of the awards we've received through InfoSec and Intense School in the last few years.

AWARD WINNING TRAINING

- 2016 EC-Council Circle of Excellence
- 2016 TrainingIndustry.com - Top 20 IT Training Company
- 2015 TrainingIndustry.com - Top 20 IT Training Company
- 2014 TrainingIndustry.com - Top 20 IT Training Company
- 2014 Golden Bridge Award - Training and Education Innovation
- 2013 TrainingIndustry.com - Top 20 IT Training Company – WINNER
- 2013 SC Magazine Best Professional Training Program
- 2013 Golden Bridge Award - Training and Education Innovation