Reverse Engineering Malware Training Boot Camp

Reverse engineering is a vitally important skill for today's expert security professional. Everything from reverse engineering malware to discovering vulnerabilities in binaries is required in order to properly secure an organization from today's ever evolving threats. In this five day hands-on course, you will 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: Worms, viruses, trojans, rootkits and bots .
- Vulnerabilities in Binaries, including: Format string vulnerabilities, buffer overflow conditions, and the identification of flawed cryptographic schemes
- Business Intelligence, used by: Hackers, trojan writers and copy protection algorithms

- Gain the in-demand career skills of a reverse engineer.
- 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 analysis tools.
- More than interesting theories and lecture, get your hands dirty in our dedicated reversing lab in this security training course.

Learn from Advanced Reversing Experts: All of the instructors for Cyber Security Institute'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.

What You'll DO

- Thwart anti-debugger code
- Learn about memory management
- Debug multi-threaded programs
- Work with recursive traversal disassemblers
- Reverse .NET bytecode
- CREA review
- Learn about legal issues and the DMCA
- Understand conditional branching statements
- Learn about Win32 executable formats and image sections
- Use virtual machines and bytecode
- Learn the fundamentals of IDA Pro
- Learn system vs. code Level reversing
- Identify variables
- Learn advanced uses of IDA Pro with hostile code
- Use Ollydbg for runtime analysis of malware
- Use Kernel mode debugging with SoftICE
- Dump executables from memory with Dumpbin
- Learn about compilers and branch prediction
- Locate undocumented APIs
- Reverse ntdll.dll
- Lear obfuscation of file formats

What You'll LEARN

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.

- Understanding hashing functions
- Working with encrypted binaries
- Reversing UPX and other compression types
- Discovering stack overflows
- Discovering heap overflows
- Creating a sandbox to isolate malware
- Unpacking malware
- Monitoring registry changes
- Identifying malware communication channels
- Understanding Digital Rights Management (DRM) implementations