CERBERUS SENTINEL

CYBERSECURITY IS A CULTURE,
NOT A PRODUCT®

TRAINING COURSES CATALOG FALL 2021

cerberussentinel.com
sales@cerberussentinel.com

6900 E. Camelback Road, Suite 240
Scottsdale, AZ 85251

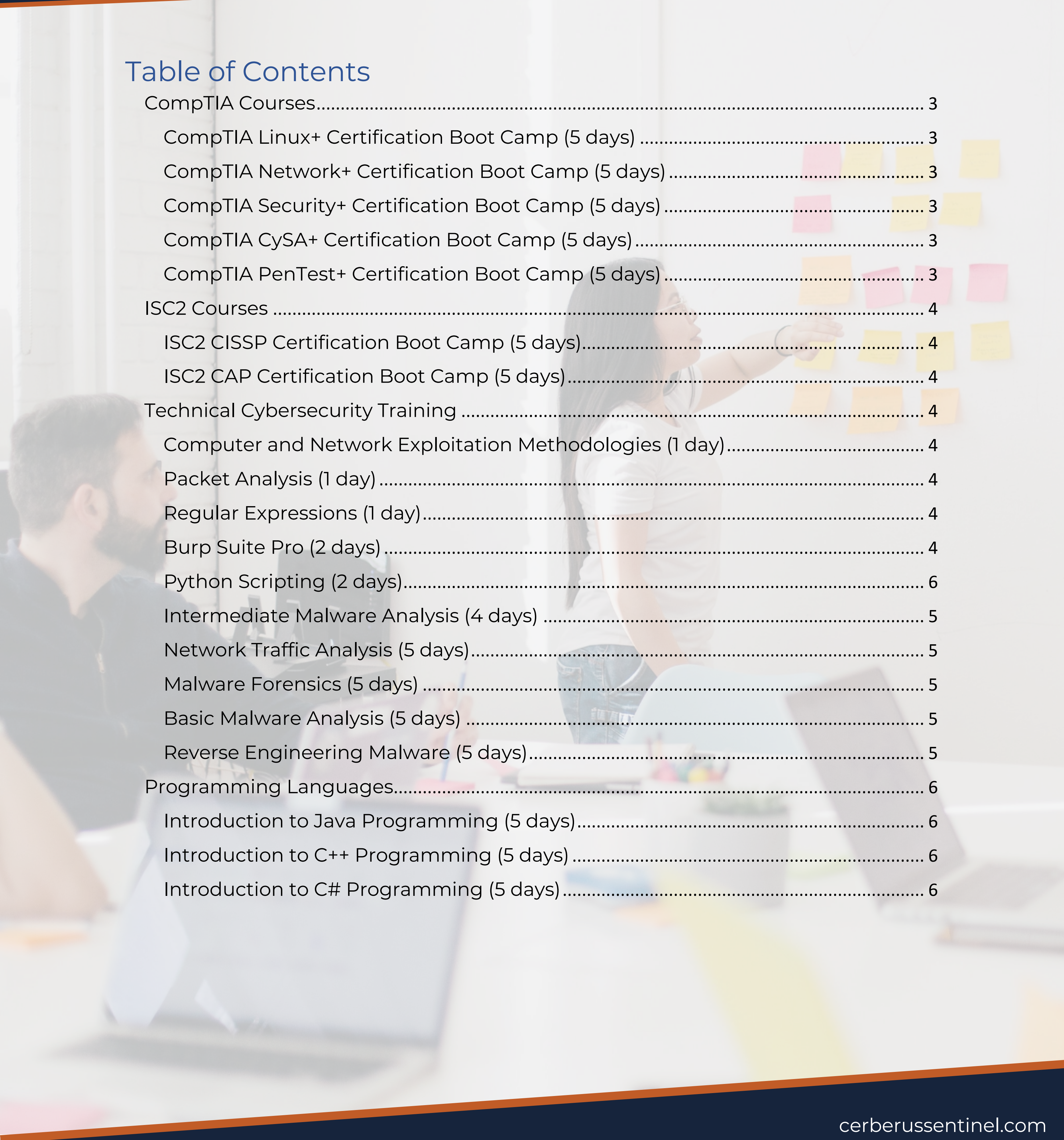


Table of Contents

CompTIA Courses

CompTIA Linux+ Certification Boot Camp (5 days)

This course covers common tasks in major distributions of Linux, including the Linux command line, basic maintenance, installing and configuring workstations, and networking in preparation for the CompTIA Linux+ Certification.

CompTIA Network+ Certification Boot Camp (5 days)

This course is intended for entry-level computer support professionals with a basic knowledge of computer hardware, software, and operating systems who wish to increase their knowledge and understanding of networking concepts and acquire the required skills to prepare for a career in network support or administration with the CompTIA Network+ certification.

CompTIA Security+ Certification Boot Camp (5 days)

This course is targeted toward the IT professional who has networking and administrative skills in Windows®-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks and familiarity with other operating systems, such as Mac OS X®, Unix, or Linux. Ideal for those who wish to further their career in IT by acquiring foundational knowledge of security topics, prepare for the CompTIA Security+ certification examination, or use Security+ as the foundation for advanced security certifications or career roles.

CompTIA CySA+ Certification Boot Camp (5 days)

Cyber threats are increasing at an alarming rate every year and organizations’ ability to defend themselves against full-scale distributed attacks quickly and effectively is becoming more and more difficult. This course is taught by leaders in network defense who work in the computer security industry, this course demonstrates how to defend large scale network infrastructure by building and maintaining intrusion-detection systems, network security auditing, and incident response techniques. You will learn how to isolate and prioritize threats in real-time. This course aids in preparation for the CompTIA CySA certification.

CompTIA PenTest+ Certification Boot Camp (5 days)

This course examines offensive hacking techniques as a step-in understanding Network Defense. This process is explored using a Penetration Testing framework and uses current hacking tools and techniques. During the course, simple but effective countermeasures are offered as steps in improving the Network Defense of the target.

ISC2 Courses

ISC2 CISSP Certification Boot Camp (5 days)

The vendor-neutral CISSP certification is the ideal credential for those with proven deep technical and managerial competence, skills, experience, and credibility to design, engineer, implement, and manage their organization's overall information security program to protect against sophisticated attacks.

ISC2 CAP Certification Boot Camp (5 days)

The vendor-neutral CAP certification course is ideal for IT, information security and information assurance practitioners who work in Governance, Risk and Compliance (GRC) roles and need to understand, apply, and/or implement a risk management program for IT systems within an organization.

Technical Cybersecurity Training

Computer and Network Exploitation Methodologies (1 day)

This introductory course provides an overview of penetration testing, red teaming, vulnerability analysis, and exploitation. This course includes step-by-step labs featuring hands-on exercises.

Packet Analysis (1 day)

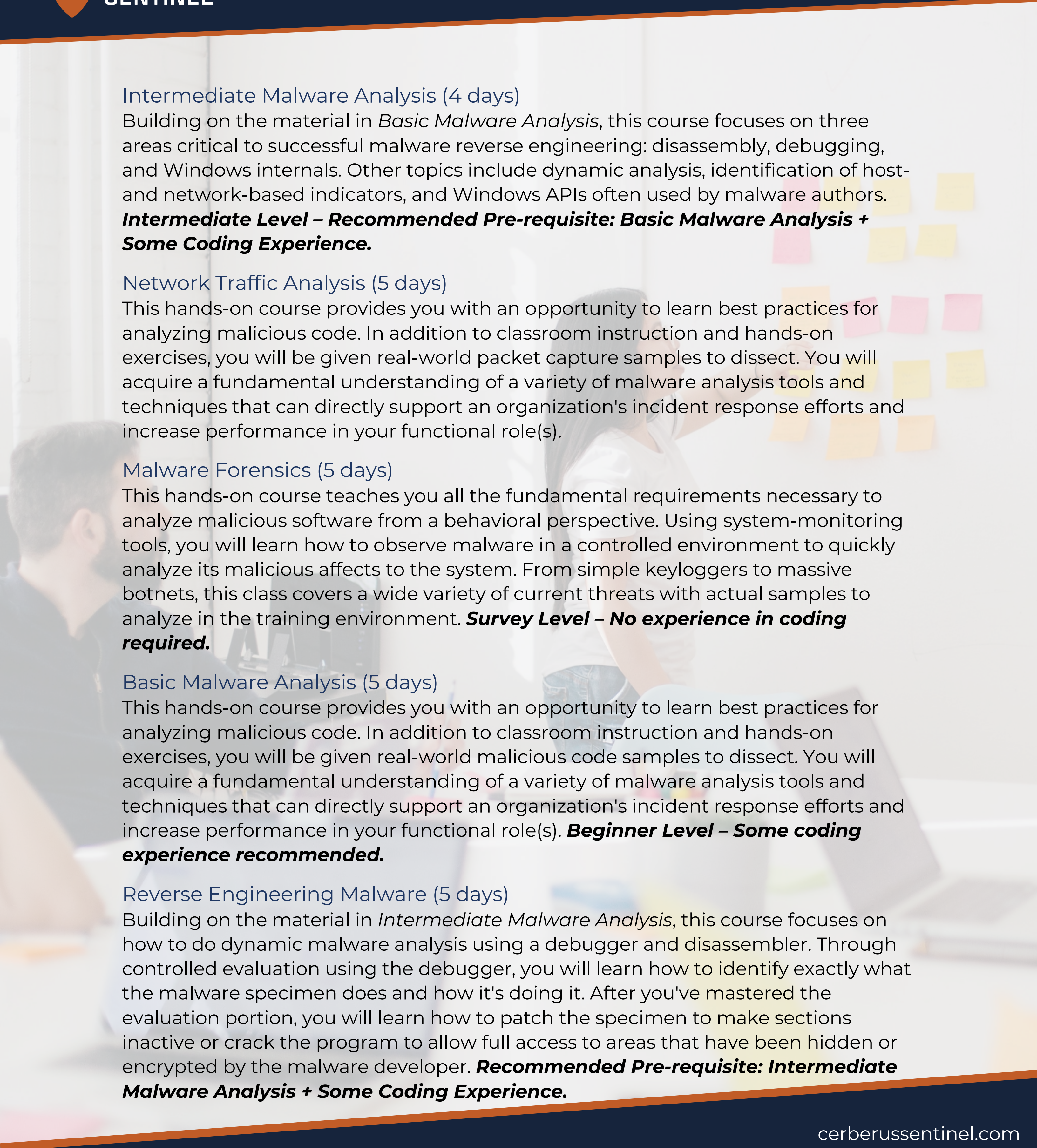
This hands-on course teaches the fundamental concepts, methodologies, and tools necessary to analyze network traffic for the purposes of intrusion and threat detection, network defense, and low-profile offensive operations. The course begins with discussing the role of network packet analysis in computer network operations (CNO) and progresses to a detailed discussion of the TCP/IP protocol suite and ethernet network operations. You will practice using the command line tool tcpdump and a protocol analyzer to capture and analyze self-generated network traffic and learn how to examine actual packet captures, which illustrate various exploits, network reconnaissance techniques, and more advanced network attacks.

Regular Expressions (1 day)

This course will instruct you on the use of regular expressions in a variety of programming languages and applications.

Burp Suite Pro (2 days)

This training provides you with both a theoretical and practical understanding of how to use the popular vulnerability scanning tool, Burp Suite Pro, which enables you to easily find vulnerabilities in your web applications.



Intermediate Malware Analysis (4 days)

Building on the material in *Basic Malware Analysis*, this course focuses on three areas critical to successful malware reverse engineering: disassembly, debugging, and Windows internals. Other topics include dynamic analysis, identification of host- and network-based indicators, and Windows APIs often used by malware authors. ***Intermediate Level – Recommended Pre-requisite: Basic Malware Analysis + Some Coding Experience.***

Network Traffic Analysis (5 days)

This hands-on course provides you with an opportunity to learn best practices for analyzing malicious code. In addition to classroom instruction and hands-on exercises, you will be given real-world packet capture samples to dissect. You will acquire a fundamental understanding of a variety of malware analysis tools and techniques that can directly support an organization's incident response efforts and increase performance in your functional role(s).

Malware Forensics (5 days)

This hands-on course teaches you all the fundamental requirements necessary to analyze malicious software from a behavioral perspective. Using system-monitoring tools, you will learn how to observe malware in a controlled environment to quickly analyze its malicious affects to the system. From simple keyloggers to massive botnets, this class covers a wide variety of current threats with actual samples to analyze in the training environment. ***Survey Level – No experience in coding required.***

Basic Malware Analysis (5 days)

This hands-on course provides you with an opportunity to learn best practices for analyzing malicious code. In addition to classroom instruction and hands-on exercises, you will be given real-world malicious code samples to dissect. You will acquire a fundamental understanding of a variety of malware analysis tools and techniques that can directly support an organization's incident response efforts and increase performance in your functional role(s). ***Beginner Level – Some coding experience recommended.***

Reverse Engineering Malware (5 days)

Building on the material in *Intermediate Malware Analysis*, this course focuses on how to do dynamic malware analysis using a debugger and disassembler. Through controlled evaluation using the debugger, you will learn how to identify exactly what the malware specimen does and how it's doing it. After you've mastered the evaluation portion, you will learn how to patch the specimen to make sections inactive or crack the program to allow full access to areas that have been hidden or encrypted by the malware developer. ***Recommended Pre-requisite: Intermediate Malware Analysis + Some Coding Experience.***

Programming & Scripting Languages

This course introduces you to the software development problem-solving methodologies utilizing current software design and development tools and techniques. This is useful in malware analysis and reverse engineering. Topics include data structures, program design, language control structures, procedures and functions, error handling, object-oriented design using classes and inheritance. Assignments are developed in Java using a current integrated development environment (IDE).

Introduction to C++ Programming (5 days)

This course introduces you to the software development problem-solving methodologies utilizing current software design and development tools and techniques. This is useful in malware analysis and reverse engineering. Topics include data structures, program design, language control structures, procedures and functions, error handling, object-oriented design using classes and inheritance. Assignments are developed in C++ using a current integrated development environment (IDE).

Introduction to C# Programming (5 days)

This course introduces you to the software development problem-solving methodologies utilizing current software design and development tools and techniques. This is useful in malware analysis and reverse engineering. Topics include data structures, program design, language control structures, procedures and functions, error handling, object-oriented design using classes and inheritance. Assignments are developed in C# using a current integrated development environment (IDE).

Introduction to Python Scripting (2 days)

This course introduces you to python scripting, a popular language used in cybersecurity. You will perform practical exercises to learn the aspects of scripting in the language. Topics include: data types, operators, collections, external modules, functions, error handling, and analyzing data files. ***No previous experience with programming languages is required.***