CYBERSTRONGER COURSE CATALOG

Comtech | 275 West Street, Annapolis, MD 21401 | cyberstronger.com | comtech.com

TABLE OF CONTENTS

COMTECH™

CYBERSTRONGER…. TRAINING CYBER PROFESSIONALS OF TOMORROW.

Comtech Cyberstronger is committed to educating cyber security professionals in incident response, malware analysis, computer, media and mobile device exploitation, penetration testing and vulnerability assessment, reverse engineering, information assurance and cyber forensics. We believe learning is best by doing, and our students train on the latest cyber security practices and methodologies, whether in a classroom, workplace or at home. Our courses are mapped directly to specific learning objectives from governing institutions and cyber security communities of practice.

OUR MISSION:

With over 30 courses and 600 labs, we provide entry level through seasoned cyber professionals with world-class education to build knowledge, skills and abilities in the latest cyber security techniques, skills, and best practices.

OUR EDUCATORS:

We employ cyber security professionals with the practical experience and skills needed to defend an enterprise, and demand that instructors remain current with the latest cyber security certifications and methods to ensure our curriculum remains current and relevant.

Our core team comes from diverse backgrounds, including the Department of Defense, defensive cyber organizations and commercial enterprises. All of our educators possess hands-on practical experience and skills beyond what can be learned solely from a book. More than that, our educators share the intellectual curiosity to constantly ask the why's and how's, and have the drive and discipline to discover the answers to those questions.

COMTECH™

WHY THE COMTECH CYBERSTRONGER ACADEMY?

Hands-on, Performance-Based Education Tied to Clearly-Defined and Accurate Performance Outcomes

» Comtech Cyberstronger has defined student expectations and assessment criteria used to grade performance. We match specific job role competencies to knowledge areas, achieving maximum understanding and retention of the material

Education Developed from the Job Outward

» We continually analyze industry job role competencies to precisely identify course exercises and materials needed to deliver students the most necessary and critical information

Practice and Immediate Feedback Provided

» Comtech Cyberstronger immerses students in real-world exercises as a means of learning and knowledge demonstration, with these exercises designed to provide immediate feedback to students and instructors.

Tasks Replicated through Real-World Scenarios

» We design exercises to mirror real-world job role competencies in a classroom environment, with instructors using course materials that demonstrate and represent major situations students are likely to encounter

Focus on Essentials

» The Comtech Cyberstronger curriculum strips non-essential information from course work and materials to focus solely on efficient performance-based training. Beyond developing a general knowledge of the material, our curriculum aims to equip students with the knowledge, skills and abilities to succeed in the cyber security workforce... today

Required Student Demonstration of Competencies and Tasks

» Students are required to meet all performance requirements before leaving training. Any deviation from a 100% success rate indicates that a student will not be fully competent in job performance. Therefore we quantify job role competencies in the classroom and actively follow-up on any deficiencies to ensure student success

COMTECH™

CYB300

CYBER SECURITY AWARENESS

CYB300 - Cyber Security Awareness introduces students to fundamental issues faced by cyber security professionals.

Beginning with the identification and definition of vulnerabilities, malware and hacker methodology, this two-day course proceeds to explain appropriate defenses and mitigation processes to secure and defend information systems.

TARGET AUDIENCE

Professionals seeking a fundamental understanding of cyber security issues, appropriate defense measures & industry-recommended mitigation processes

OBJECTIVE

Provide detailed-discussion & hands-on practical application in the identification/classification of vulnerabilities & malware; explanation of the hacker threat & methodology & explore best-practice procedures & processes associated with security appliances & applications

COMTECH™

MODULE 1

Vulnerabilities & Malware introduces students to the types of vulnerabilities and malware that are prevalent in today's cyber security landscape.

Topics List

- Types of Vulnerabilities
- Types of Malware

MODULE 2

Hacker Methodology & Threats provides background information regarding ways hackers exploit networks and networked devices. Discussions also include topics related to various threat actors like social engineers and insiders, and the various techniques these threat actors use to solicit information and/or damage/disrupt information systems.

Topics List

- Hacker Methodology & Mindset
- Social Engineering & Insider Threat
- Physical Security Threat

MODULE 3

Scanning & Assessment provides an overview of the various types of network and host-based scans required to assess and enumerate information systems, as well as, to aide in the identification of vulnerable services/applications.

Topics List

- Network Scanning
- Vulnerability Assessment

MODULE 4

Defense in Depth introduces students to industry "best-practices" detailed through the implementation of a multi-pronged defense posture.

Topics List

- Defense Mechanisms
- Introduction to Intrusion
- Detection/Prevention Systems
- Security Logs
- Personal Security Products
- Password Mechanisms
- Application Security

MODULE 5

Security Responsibilities & the Future of Cyber Security examines the different security responsibilities levied on an organization. These responsibilities include those outlined by local, state and federal law, as well as, those responsibilities which come as a result of adherence to industry guidelines or internal policies, processes and procedures.

Topics List

- Security and Responsibilities
- Digital Forensics Basics
- Future Trends in Cyber Security

LNX200

FUNDAMENTALS OF LINUX SECURITY

Fundamentals of Linux Security for System Administrators teaches students basic Linux command line usage and filesystem structure, how to configure, evaluate and troubleshoot common management services used on today's Linux systems, and well as how to configure and test a Linux-based firewall. Linux System Administrators are often responsible for managing systems containing critical or sensitive data and infrastructure. The ability to securely and effectively manage Linux systems is paramount to the System Administrator job role. Completion of this module will prepare students to handle the basic requisite tasks associated with configuring, managing and

PREREQUISITE KNOWLEDGE

Before completing this lesson, students should:

- Have familiarity with basic Linux commands
- Have a basic understanding of the Linux directory structure

OBJECTIVE

After completing this module, students will be able to: Perform basic command line usage and syntax • Perform package management on Linux • Identify basic file system structure • Identify and describe common management services on Linux, and the use case for each • Configure and troubleshoot various common management services on Linux • Evaluate the strengths and weaknesses of various service configurations • Perform service hardening on common Linux management services • Configure Linux-based firewall

COMTECH™

ACTIVITIES & SUPPORTING MATERIAL

I. TOPICS

- Linux Command Line
- Linux File System Structure
- Telnet
- SSH
- VNC and SSH tunneling
- Fail2Ban
- Firewalls w/UFW, firewalld

II. LAB ACTIVITIES

- Lab 1: Basic Linux Command Line Usage
- Lab 2: Basic Linux Filesystem Structure
- Lab 3: Telnet Traffic Capture
- Lab 4: Installing OpenSSH server, configuring sshd
- Lab 5: SSH Keypairs, SSH Keypair Passphrases, and exporting SSH public keys to remote machine
- Lab 6: Fail2Ban Setup and Analysis
- Lab 7: Setting up a firewall with UFW and firewalld

III. SUPPORTING MATERIAL

- Video 1: Telnet Vulnerability Demo via Wireshark Capture
- Video 2: SSH Passphrase Strength cracking

RESOURCES

I. HARDWARE

- Internet-connected laptop running a modern web browser

II. SOFTWARE

- Telnet
- SSH
- VNC
- Fail2Ban
- UFW
- firewalld
- Guacamole

ASSESSMENT

I. FORMATIVE

- Multiple choice (or other format) questions in the video that will verify the learning for each submodule

II. SUMMATIVE

- Capstone Lab:
- Student's will exploit a novel application that has several vulnerabilities that have various levels of filtering and difficulty in exploiting

DEV300

HARDENING PHP WEB APPS

Web applications are routinely the source of many security vulnerabilities, especially as more and more move to the cloud. However, this is despite the fact it is often simple to fix most web applications vulnerabilities, before the code is released into the wild. The 'Hardening PHP Web Apps' course walks students through the list of the OWASP Top Ten vulnerabilities common in web application code and demonstrates various methods of secure coding to harden web applications. Specifically, the course focuses on examples A1 through A8 of the top ten list.

PREREQUISITE KNOWLEDGE

Before taking this course, students should be able to:

- Write web applications in PHP
- Identify basic and advanced examples of the OWASP Top Ten vulnerabilities
- Describe basic mitigation guidelines for fixing basic OWASP Top Ten vulnerabilities

OBJECTIVE

Examine a web application design and implementation and identify potential vulnerabilities.

Remediate the vulnerability by modifying the underlying code.

COMTECH™

MODULE	LECTURE	LABS
0	Introduction	
1	A1: Injection	Lab 1.1: Stopping SQL Injection with validation and prepared statements Lab 1.2: Stopping OS Command Injection with Data Validation
2	A2: Broken Authentication	Lab 2.1: Implementing Proper Authentication in PHP Lab 2.2: Enabling Google Authenticator in a PHP Web Application
3	A3: Sensitive Data Exposure	Lab 3.1: Password Hashing in PHP Lab 3.2: Proper error handling in PHP
4	A4: XML External Entities	Lab 4: Defending against XXE in PHP
5	A5: Broken Access Control	Lab 5.1: Basic Access Control in PHP Lab 5.2: Preventing Directory Traversal and LFI with Whitelisting in PHP
6	A6: Security Misconfiguration	Lab 6: Securing the PHP configuration
7	A7: Cross Site Scripting	Lab 7: Preventing XSS in PHP
8	A8: Insecure Deserialization	Lab 8: Secure Serialization in PHP
9	CSRF	Lab 9.1: Defending Against CSRF in PHP
10	File Upload Protection	Lab 9.2: Securely Handling File Uploads in PHP
11	Capstone	Lab 10: Capstone: Securing a Web Application From Top to Bottom in PHP

DEV400

INTRODUCTION TO PROGRAMMING C

DEV 400 - Introduction to Programming C offers a fast-paced computer science course for students without programming experience. Students learn to write in the language used for operating systems, embedded processors, micro-controllers, assemblers, exploits and network drivers. This course focuses on solving problems using C, by teaching its fundamental principles, and techniques used in software engineering.

DEV400 assumes no prior programming experience.

TARGET AUDIENCE

Individuals with or without programming experience

OBJECTIVE

Provide an introduction to writing language for operating systems, embedded processors, micro-controllers, assemblers, exploits and network drivers

COMTECH™

DAY 1

Day 1 begins by introducing how computers work and how C programs are processed by a computer. Students learn how to apply the software development model to solve programming problems. The format of C programs, data types, and variables is discussed, and students also learn how to program arithmetic expressions, assign values to variables, and read data into a program and display the results. Students learn about top-design to develop algorithms and program structure. Self-check exercises and labs challenge students to use the newly-learned information in context.

Topics List

- Operating system, machine language, assembly language and high-level languages
- Format and elements of a C program
- Various data types
- Arithmetic expressions and problem solving
- Format strings
- Functions
- Modular programming
- Common programming errors

DAY 2

Day 2 discusses control structures and how to manipulate program execution and control flow. Students learn to make comparisons and code the logic behind conditionals. The labs challenge students to use a variety of control structures like sequence, selection, and repetition.

Topics List

- Control structures
- Compare numbers, compare characters and strings
- "If" statements
- Decision algorithms
- Switch statement and various alternatives
- Case Study: Utility Bill; Problem: Write a program to compute a customer's utility bill based on numerous factors

DAY 3

Students learn why repetition is an important concept in programming. The Repetition and Loops lectures and labs teach students how to use repetition in their programs to gain efficiencies. Counting, sentinel-controlled and flag-controlled loops and the usefulness of nested loops are discussed. Traditional for, while, and do-while statements for creating loops are covered in-depth.

Topics List

- Loop design and infinite loops
- Counting Loops, sentinel-controlled loops, flag-controlled loops
- For, while, do-while statements
- Nested loops
- Outer and inner loop control variables
- Case Study: Bisection Method for Finding Roots; Problem: Develop a function to approximate the root of a mathematical function containing an odd number of roots

DAY 4

The Pointers lectures and labs expose students to indirect addressing. Reading from and writing to files using file pointers and comparing call-by-value and call-by-reference methods are discussed. Finally the student will learn how to pass information to and get information back from functions.

Topics List

- Pointers
- Indirect addressing
- File I/O using pointers
- Call methods for functions
- Modularize program with functions
- Working with pointers and functions
- Case Study: Solar-heated House; Problem: Design a program to estimate size of collecting area needed to support a solar-heated house

DAY 5

The Array Pointers lectures and labs teach students how to use arrays and how C implements arrays as pointers. Students learn how to access values in arrays, and how to process data in arrays using loops. Searching arrays is introduced and multi-dimensional arrays are described as a solution for storing tables of data.

Capstone Exercise

- Arrays
- Relationship between arrays and pointers
- Process array data with loops
- Function and array interaction
- Searching and sorting arrays
- Case Study: Summary of Business Revenue; Problem: Regional medical center needs software to track its revenue by unit and quarter

DEV400

INTRODUCTION TO PROGRAMMING C

DEV550

PYTHON FOR PENTESTERS

DEV550 – Python for Pentesters is an intermediate level course designed for pentesters who want to use Python to build specialized tools. This challenging course will expose students to target scanning, enumeration, exploit development, web application attacks, and persistence mechanisms through Python scripting.

Upon completion, students will have built an arsenal of over 20 penetration testing tools.

TARGET AUDIENCE

This course is designed for students who have basic programming/scripting experience in C or Python, knowledge of networking concepts, and knowledge of penetration testing methods and hacking tools

OBJECTIVE

Provide students with the knowledge necessary to analyze technical situations, solving them through the development of Python tools

COMTECH™

DAY 1

Introduction to building pentesting tools in Python. Students will review Python fundamentals and will develop target scanning and enumeration tools using modules from the Python Standard Library as well as third party modules.

Topics List

- Python Fundamentals
- Socket Module
- I/O Functionality
- User Input
- Application Banner Grabbing
- HTTP Methods
- Nmap Module

DAY 2

Students will begin the day by creating custom scanners using the Nmap module. They will develop algorithms to parse complex data sets and build additional functionality into their custom tools.

Topics List

- Building Custom Scanners
- Parsing Nmap Data
- Exception Handling
- Enhancing Tool Functionality
- OS Module
- Introduction to Exploit Development

DAY 3

Students will begin the day by taking a deep look at x86 memory architecture, operating system controls and debugging. Students will then learn how to construct exploits against stack-based buffer overflows, as well as how to embed shellcode into their Python scripts.

Topics List

- x86 Memory Architecture
- Exploit Mitigation Controls
- Fuzzing
- Debugging
- Shellcode
- Constructing Exploits

DAY 4

Students will learn about common web application vulnerabilities, reconnaissance methods and attack vectors. Students will then write code to identify and exploit Standard Query Language (SQL) and Cross-Site Scripting (XSS) vulnerabilities to reveal server-side details, as well as to find directory traversal vulnerabilities.

Topics List

- Web Application Vulnerabilities
- Web Application Reconnaissance
- HTTP Authentication
- SQL Vulnerabilities
- XSS Vulnerabilities
- Directory Traversal Vulnerabilities

DAY 5

On the final day of class, students will learn how to conduct post-exploitation pillaging and employ persistence techniques. They will then learn how to build reverse shells, send encoded data via HTTP requests, and control their persistence tool via command and control mechanisms.

Topics List

- Command and Control Systems
- Persistence
- Subprocess Module
- Encoding and Decoding Data
- Data Exfiltration

FOR300

BASIC DIGITAL MEDIA FORENSICS

FOR300 - Basic Digital Media Forensics provides an introduction to media collection, imaging and analysis. Students will discuss file systems, partition structures and data storage to better understand how and where data is stored on multiple types of digital media, as well as the best methods to access it.

The course is an optimal starting point for individuals looking to expand their forensic knowledge and outlines a number of ways to achieve forensic goals while ensuring all processes are completed in a forensically-sound manner. Chain of custody and evidence handling is addressed, as well as what to do and what not to do when dealing with 'live' evidence.

TARGET AUDIENCE

Professionals looking to broaden their cyber skills or begin developing a strong skill set within the forensic community

OBJECTIVE

Provide a solid understanding of what is considered valuable digital media used as forensic evidence for an investigation, including how data is stored, retrieved and analyzed

COMTECH™

DAY 1

During the first lesson, students will learn about setting up a Forensic workspace. In addition, students will learn about preparing target media to ensure a forensically sound process prior
to imaging.

Topics List

- Preparation of target media/wiping using dc3dd
- Forensic imaging using FTK Imager
- Identification and discussion of various digital media that has been and could be useful in a forensic investigation

DAY 2

A lesson consisting of Incident response and acquisition. Students will also learn about forensic tools, windows file systems, and partition structures.

Topics List

- Forensic imaging of different media using FTK Imager
- Forensic analysis of a raw image using autopsy
- Exifdata analysis

DAY 3

Students will become more familiar with Forensics for Windows, and learn the value of metadata, and exifdata in forensic analysis.

Topics List

- Forensic analysis of a raw image using autopsy
- Exifdata analysis
- Viewing of data in a hex editor

DAY 4

Students will learn the proper techniques for Forensic reporting
and documentation.

Topics List

- Lab will begin by conducting analysis on another dd image
- Answering a line of questions that pertains to that provided image
- Conduct imaging and analysis of a smaller image
- Draft a comprehensive forensic report

DAY 5

Review all submitted forensic reports at the end of Day 4 and discuss items of concern within both the processes and the reporting.

Capstone Exercise

Students will conduct a forensically-sound acquisition and analysis of assigned media. After which, they will be required to write a comprehensive
forensic report.

FOR400

FUNDAMENTALS OF NETWORK FORENSICS

FOR400 - Fundamentals of Network Forensics expands on acquired networking knowledge and extends in to the computer forensic mindset. Students will learn about common devices used in computer networks and where useful data may reside. Students will also learn how to collect that data for analysis using hacker methodology.

Additionally, the course covers information related to common exploits involved in Windows server systems and common virus exploits. Students will learn how to recognize exploit traffic, and the difference between attacks and poor network configuration.

TARGET AUDIENCE

Professionals looking to either broaden their cyber skills or begin developing a skill set within the network defense community

OBJECTIVE

Provide an understanding of devices used to set up computer networks, where useful data may reside within the network, and how the data is stored and retrieved to acquire analysis

COMTECH™

DAY 1

Students will learn to understand and demonstrate the use of a standard methodology for exploitation, the concepts of various software threats and the techniques expected of a professional hacker.

Topics List

- Hacker mindset and steps of an attack
- Hacker techniques
- Tools used for exploitation
- Packet capturing and analysis
- Tools used for network analysis

DAY 2

Students will identify protocols helpful when performing network forensics. Students will gain an understanding of filters and how they can help identify specific packets of interest. Students will setup Ethernet ports for capturing data and analyze traffic using Snort to identify malicious activity.

Topics List

- Filtering traffic and protocol analysis
- Comparing file hashes to identify malicious files
- Parsing network traffic to identify malicious files and attacker activity
- Network devices, packet capturing in a switched environment
- Configuring Ethernet ports on an IDS
- Advantages of internal and external IDS placement
- Running Snort
- Examining Snort rules and using Snort to analyze packet capture files

DAY 3

Students will learn how to edit Snort configuration files to use local rules, edit rules files and write custom rules to detect malicious activity, command shells and malware. Students analyze traffic using Snort as an intrusion detection system. Students will learn to recognize anomalous activity in web, FTP authentication and access logs in Linux and Windows.

Topics List

- Editing Snort configuration files
- Editing Snort rules files
- Writing custom Snort rules to detect malicious activity
- Analyzing traffic using Snort as an IDS
- Recognizing anomalous activity in Linux and Windows logs

DAY 4

Students will learn how to recognize anomalous activity in Linux and Windows. Student will understand how to detect evidence of an attack using incident response toolkits as well as native tools to view process lists, established connections, scheduled jobs, and account activity.

DAY 5

Students will demonstrate the ability to identify attacker IP addresses, exfiltrated data, malware, method of compromise, accounts used, and document observed activity in an executive summary and timeline
of events.

FOR410

MOBILE DEVICE FORENSICS

FOR410 - Mobile Device Forensics provides an introduction to mobile devices and the value that they offer in forensic investigations. The class addresses the methods used to store data, as well as the areas of the mobile device where data is stored and how to access it. The class will also discuss mobile device removable media and the role it plays with the mobile device.

Students will cover network technology as well as three tools specifically designed for mobile device acquisition. Upon completion of an extensive hands-on experience, the student will draft a comprehensive forensic report, ensuring all actions were documented and conducted in a

TARGET AUDIENCE

Professionals looking to broaden their cyber forensics skills or individuals that will begin working with mobile devices and acquiring data from them, as well as their removable components

OBJECTIVE

Provide students with an understanding of how mobile devices actually work and store data, and what data can be of forensic value, as well as how certain types of damage can determine what data can be acquired from the device

COMTECH™

DAY 1	DAY 2	DAY 3
Students will be introduced to mobile device hardware and architecture. **Topics List** » Using faraday » Preparing target media using dc3dd » Acquiring a SIM card and saving to target media » Creating a forensic image of removable media using dc3dd	Students will learn about cell phone acquisition and exploitation and become familiar with various mobile device acquisition tools. **Topics List** » Exifdata analysis » Viewing data in hex editor » Conducting forensic analysis on previously imaged media	Students will learn the correct methods for forensic reporting and documentation. **Topics List** » Device acquisitions following forensically sound methodologies » Drafting of forensic report

DAY 4

Students will review the results from the forensic reports that have been submitted and acquisitions completed. Students will also go through a review of the course material.

Capstone Exercise

Students will utilize the knowledge and skills acquired throughout the course, in a hands on lab exercise.

IR500

INCIDENT RESPONSE

IR500 - Incident Response equips students with the needed tools to implement robust defense-in-depth practices within the workplace. IR provides detailed training on proper documentation and planning for computer network defense.

The course exposes students to a variety of real-world scenarios and provides hands-on experience in event detection and recovery in an enterprise environment.

TARGET AUDIENCE

IT and Cyber Security professionals looking to acquire hands-on experience, in the identification of and recovery from security events, and to establish and maintain a robust computer network defense posture

OBJECTIVE

Provide in-depth exposure to network and systems intrusion protection methods, what to do before, during and after an event,, and how to recover from events and strengthen organizational security

COMTECH™

DAY 1

Day 1 introduces students to sound IR concepts focusing on proper awareness of information systems and networks, clear and up-to-date documentation and effective use of risk management theory.

Topics List

- IR today
- Network mapping and awareness
- Standard documentation requirements and options
- System and network baselining practices
- Wisdom of security auditing
- Proactive vs. reactive action
- Risk management and defense

DAY 2

Students use the tools learned on Day 1 to detect a possible incident and conduct a full-spectrum analysis on a selection of corporate network systems in order to judge impact and threat to business or company data.

Topics List

- Incident detection approaches
- Baselining saves the day
- Practices for analyzing an incident
- Approaches for confirming an incident
- Using all logs for impact analysis
- Techniques for analyzing files

DAY 3

Students learn to formulate a fully-realized recovery plan based on data received on a confirmed cyber incident on their company network. They will contain and eradicate threats to the network and use security auditing tools to verify success . Recovery efforts will be completed by verifying no new vulnerabilities were introduced to the network. Day 3 ends with students reporting on details of the event identification, response and recovery to organizational management.

Topics List

- Incident Recovery Plans
- Testing recovery options before/after rollout
- Standard Operating Procedures and Recovery Plans
- Approaches for confirming an incident
- Using all logs for impact analysis
- Techniques for analyzing files
- Reporting to management

DAY 4

Students apply forensically-sound principles to image a machine and recover useful information from additional imaged systems. Students participate in the recovery experience and are required to update a response plan.

Topics List

- Real world recoveries
- Forensic imaging and analysis
- Maintaining clear communications
- Post-incident actions and lessons learned
- Updating documentation to prep for the next cycle

DAY 5

Day 5 comprises a full-spectrum IR scenario that requires students to recover from a series of attacks discovered on a corporate network. They must scope the impacted systems, create a mitigation plan, harden weak defenses and conduct recovery efforts. This final exercise replicates a variety of network services, hardware, and configurations. The capstone reinforces exposure to tools and techniques learned during the previous four days.

Capstone Exercise

All the material covered in the course will be put to use in the final exercise.

MAL400

FUNDAMENTALS OF MALWARE ANALYSIS

MAL400 - Fundamentals of Malware Analysis is an introductory course that exposes students to the theoretical knowledge and hands-on techniques for analyzing malware.

Students will learn how to identify and analyze software that causes harm to users, computers and networks as part of an overall cyber defense and incident response plan. Understanding how malware works and what it was designed to do is crucial to thwarting future attacks.

TARGET AUDIENCE

New malware analysts looking to increase their arsenal of techniques, or others looking to break into the malware analysis field

OBJECTIVE

To obtain the basic skills needed for the identification and analysis of software that causes harm to users, computers and networks

COMTECH™

DAY 1

Introduction to the overall malware analysis process and methodology. Students define terminology, learn specific malware types and cover fundamental approaches of analysis, in addition to learning how to effectively analyze program code/structure to determine function. Students are challenged with three labs.

Day 1 ends with a detailed overview of setting up and using a safe virtual environment for malware analysis.

Topics List

- Malware analysis techniques
- Identification via antivirus tools and hashing
- Analyzing strings, functions, and headers
- Use a variety of virtual machines, settings and configurations

DAY 2

Day 2 focuses on easy-to-use techniques to dynamically analyze malicious programs by running them in a lab. Students learn to observe true behavior of malware and determine its purpose and functionality via live demos and three challenging specimens they must analyze.

Day 2 centers around how malware interacts with the victim's OS by looking at network activity, registry changes and interactions with the file system.

Topics List

- Use of Procmon, Process Explorer and Regshot to understand malicious behavior
- Fake network services to aid analysis
- Traffic analysis
- Network connections
- X86 architecture

DAY 3

Day 3 closes behavioral analysis and ends with a final fourth lab.

Students then begin X86 assembly language. This module is crucial for learning follow-on analysis techniques using debuggers and disassemblers. Students learn key concepts in assembly language to assist follow-on analysis with IDA Pro. IDA Pro is introduced as a disassembler and reverse engineering tool.

Considerable time is spent on familiarization with the UI and IDA's numerous features. Plenty of code snippets, demos and two IDA familiarization labs help the student understand both assembly language and how to use IDA Pro.

Topics List

- Stack vs. Heap
- Registers, flags & basic instructions
- Conditionals, flow control instructions & jumps
- IDA Pro UI intro
- Disassembly window (Text vs. Graph Mode)
- Jumping to memory addresses

DAY 4

IDA Pro Introductions continues on Day 4 with the identification and analysis of more complex functions. Students are gradually exposed to more complex malware and its disassembly to build confidence and skills. Students learn techniques needed to identify, categorize and analyze high-level functionality of assembly code. Two labs challenge students to identify a variety of C code constructs in malware specimens as part of an overarching analysis strategy.

Topics List

- Cross-references in code
- Function identification, analysis & renaming
- Imports, exports & structs
- Searching through disassembly
- Code & data redefinition
- Deeper function analysis

DAY 5

Students spend their final day analyzing two malicious programs to further solidify analysis skills focusing on the identification of C code constructs in assembly, and how these high-level constructs correlate to other aspects of the program and its behavior. An instructor-led review of all major topics will be conducted and any final questions will be answered.

After the course, students have 90 days to challenge the optional CYBRScore-enabled certification associated with MAL400. The certification presents a malware specimen to the challenger that must be analyzed using the techniques and tools learned in this course. Our behind-the-scenes scoring engine will track progress throughout against a rubric of core skills that must be demonstrated in the hands-on analysis.

MAL400

FUNDAMENTALS OF MALWARE ANALYSIS

MAL500

REVERSE ENGINEERING MALWARE

MAL500 - Reverse Engineering Malware is an intermediate course that exposes students to the theoretical knowledge and hands-on techniques to analyze malware of greater complexity.

Students will learn to analyze malicious Windows programs, debug user-mode and kernel-mode malware with WinDbg, identify common malware functionality, in addition to reversing covert and encoded malware.

TARGET AUDIENCE

Junior malware analysts and reverse engineers who want to increase their skills to better understand more complex malicious code

OBJECTIVE

Provide students with a working knowledge of analyzing malicious Windows programs, debugging user-mode & kernel-mode malware, identifying common malware functionality, & other related topics

COMTECH™

DAY 1

Malware targeting Windows victims is prolific, and understanding how this malware interacts with the complex Windows operating system and API is a challenge not to be taken lightly.

In the first part of this course, students dive straight into Windows API and its myriad functions, inputs, and outputs as they relate to reverse engineering malware targeted against Windows victims. Networking APIs, as well as threads and mutexes are examined in-depth. The day is spent trying to solve the Gordian knot that is Windows malware.

Topics List

- Windows API
- Handles & file system functions
- Common registry functions & autoruns
- Networking APIs
- Processes, threads & mutexes
- COM objects

DAY 2

Being able to debug a program is crucial to reverse engineering and malware analysis. On Day 2 students are introduced to the concept of debugging and extensively exposed to OllyDbg, its functionality, tools and plugins. Breakpoints, and tracing are used as part of the overall reversing process to unravel complex malware specimens.

Topics List

- Kernel vs. User-mode debugging
- Software & hardware breakpoints
- Modifying program execution & patching
- OllyDbg overview
- Memory maps
- Executing code, breakpoints & tracing
- OllyDbg plugins

DAY 3

On Day 3, students are introduced to the broad and complex topic of kernel debugging. This includes core principles of this interesting sub-topic, as well as a demonstration of how to configure an environment, analyze kernel objects, and look at rootkits. Day 3 closes with the discovering and reversing of a variety of malicious functionality malware executes across several labs.

Topics List

- Kernel debugging with WinDbg
- Configuring kernel debugging environment
- Analyzing functions, structures and driver objects
- Rootkit analysis
- Downloaders, launchers & backdoors
- Analyzing various persistence mechanisms & user-mode rootkits

DAY 4

Day 4 switches gears and delves into the complex world of covert malware. Students learn about a variety of techniques malware uses to hide its activities, and how to identify indicators of this type of activity. Process injection, hooks, and detours are looked at as part of this interesting module of the course.

Topics List

- Covert malware
- Abusing resource section of PE file
- Process injection & process replacement
- Windows hooks & detours
- APC injection from kernel space

DAY 5

On the final day of class, students learn how malware authors use a variety of encoding mechanisms to obfuscate data, and how to analyze them. XOR, BASE64 and custom encoding mechanisms are explored and analyzed.

After the course, students have 90 days to challenge the optional CYBRScore-enabled certification associated with MAL400. The certification presents a malware specimen to the challenger that must be analyzed using the techniques and tools learned in this course. Our behind-the-scenes scoring engine will track progress throughout against a rubric of core skills that must be demonstrated in the hands-on analysis.

Topics List

- Analyzing encoding algorithms
- XOR, BASE64 & custom encoding
- Common crypto algorithms
- KANAL
- Custom decoding scripts in Python
- Instrumentation for generic decryption

MAL500

REVERSE ENGINEERING MALWARE

MAL600

ADVANCED MALWARE ANALYSIS

MAL600 - Advanced Malware Analysis is an advanced course that exposes students to the theoretical knowledge and hands-on techniques to reverse engineer malware designed to thwart common reverse engineering techniques.

Students will learn how to identify and analyze the presence of advanced packers, polymorphic malware, encrypted malware, and malicious code that has been armored with cryptors, anti-debugging and anti-reverse engineering.

TARGET AUDIENCE

Mid-level malware analysts & reverse engineers, as well as programmers who want a different professional perspective as a means of better protecting their tools & intellectual property

OBJECTIVE

Provide an in-depth understanding of identifying & analyzing the presence of advanced packers, polymorphic malware, encrypted malware & malicious code

COMTECH™

DAY 1

The course begins by examining a variety of network signatures associated with malware. Understanding the networking aspect is important because malware almost always uses network connectivity to infect, persist, receive command and control instructions, and exfiltrate data.

Students are asked to spend a significant amount of time reversing malicious command and control structure parsing routines to better understand the overall network activity, and how to identify and stop it.

Topics List

- Indications of malware activity
- Network countermeasures
- Snort & complex signatures
- Hiding in the noise by mimicking existing protocols
- Client initiated beacons
- Networking code & encoding data
- Networking from an attacker's perspective

DAY 2

Day 2 focuses on anti-disassembly techniques employed by malware authors to thwart analysis. Students learn about various techniques, like jump instructions with the same target, jump instructions with a constant condition and more. More complex techniques like return pointer abuse and misusing structured exception handlers give the student new conceptual knowledge.

This knowledge will help complete three complex hands-on challenges: identifying false conditional branches, improperly disassembled code, and return pointer abuse.

Topics List

- Defeating disassembly algorithms
- Same target jumps & constant condition jumps
- Rogue opcodes
- Multi-level inward jumping sequences
- Patching binaries to defeat return pointer abuse
- SEH abuse
- Reversing armored code designed to thwart stack frame analysis

DAY 3

Anti-debugging is used by malware authors to determine when their malware is under the control of a debugger or to thwart debugging efforts. On Day 3 students learn how Windows API can be used to detect debugger use, and how malware manually checks structs. Checking the ProcessHeap and NTGlobal flags is reviewed, as well as how some malware checks the analysis system for debugging tool residue in the registry.

The module concludes with a discussion of TLS callbacks, and exceptions to disrupt debugger use.

Topics List

- Using Windows API functions to detect debuggers
- PEB checks, ProcessHeap flag & NTGlobal flag
- TLS Callbacks
- Exceptions and Interrupts
- PE Header vulnerabilities
- OutputDebugString vulnerability

DAY 4

Although the presence of anti-virtual machine techniques seems to be declining, Day 4 is spent discussing how to identify various methods used by malware authors.

Students also learn how to manually unpack malware by finding tail jumps, the original entry point (OEP) and rebuilding Import Address Tables (IAT).

Topics List

- Anti-VM techniques & memory artifacts
- Red pill & no pill techniques
- Unpacking stub, tail jump, OEP & import resolution
- Manual IAT rebuilds
- Tips & tricks for dealing with several common packers

DAY 5

On the final day of class, students learn how to identify and reverse C++ code, in addition to conducting shellcode analysis. Virtual functions and the concept of polymorphism are discussed to prepare students to identify and reverse vtables using their cross references.

Position-independent shellcode is examined, as well as how to identify execution location. Day 5 ends with a look at 64-bit malware and the challenges analysts face when reversing this type of code.

Topics List

- Shellcode analysis, position independent-code & call/pop
- Shellcode use of LoadLibraryA & GetProcAddress for dynamic function location
- C++ Analysis
- Overloading functions, mangling and vtables
- Challenges of identifying inheritance between classes
- 64-bit malware, general-purpose & special-purpose registers
- X64 calling convention & exception handling

MAL600

ADVANCED MALWARE ANALYSIS

PEN300

OWASP TOP 10 EXPLOITATION BOOTCAMP

Hackers routinely exploit web applications, especially as more services move to the cloud, despite the fact companies can easily fix most vulnerabilities within web applications before releasing their code to the wild. The “Web Application Exploitation” course teaches students about the most common web vulnerabilities (OWASP Top 10) in modern web applications, why they often exist, and several methods to test for their existence.

PREREQUISITE KNOWLEDGE

Before taking this course, students should be familiar with:

- Networking applications and protocol analysis
- SQL statements
- Knowledge of Linux command line interface

OBJECTIVE

To define the top ten vulnerabilities that are common to web applications. Analyze a simple web application to search for the presence of the top ten web vulnerabilities. Identify techniques to mitigate the presence of the top ten web vulnerabilities.

COMTECH™

MODULE	LECTURE	LABS
0	Introduction	
1	A1: Injection	Introduction To OWASP Top Ten: A1 - Injection
2	A2: Broken Authentication	Introduction To OWASP Top Ten: A2 - Broken Authentication
3	A3: Sensitive Data Exposure	Introduction To OWASP Top Ten: A3 - Sensitive Data Exposure
4	A4: XML External Entities	Introduction To OWASP Top Ten: A4 - XML External Entities
5	A5: Broken Access Control	Introduction To OWASP Top Ten: A5 - Broken Access Control
6	A6: Security Misconfiguration	Introduction To OWASP Top Ten: A6 - Security Misconfiguration
7	A7: Cross Site Scripting	Introduction To OWASP Top Ten: A7 - Cross Site Scripting
8	A8: Insecure Deserialization	Introduction To OWASP Top Ten: A8 - Insecure Deserialization
9	A9: Using Components With Known Vulnerabilities	Introduction To OWASP Top Ten: A9 - Using Components With Known Vulnerabilities
10	A10: Insufficient Logging and Monitoring	Introduction To OWASP Top Ten: A10 - Insufficient Logging and Monitoring
11	Capstone	Introduction To OWASP Top Ten: Capstone

PEN450

HACKING AND WEB EXPLOITATION BOOTCAMP

Offensive Cyber Security tools and techniques are necessary to understand if you are either engaging in offensive activities or defending against them. It is also important to understand the basics of defense as well, either to employ them or to know their limitations and shortcomings. This course will introduce the student to these tools and techniques, with 2 days spent on basic penetration testing techniques, 1 day on basic web application attacks, 1 day on defensive measures and cryptographic techniques, and the last day spent on a live Attack and Defend exercise, in which the students will team up in a shared environment and go head to head with the other students, attacking the shared machines, and when successful, defending them from the

PREREQUISITE KNOWLEDGE

Before taking this course, students should be familiar with:

- Basics of Cyber Security
- Be comfortable using Windows and Linux

OBJECTIVE

Learn how to use the basic tools of pentesting and web application security testing. Learn how to find vulnerabilities in applications and exploit them. Learn how to deploy basic defenses and what defenders may do to track down an attacker.

COMTECH™

DAY	LAB ACTIVITY
1	Scanning with Nmap
1	Hping3
1	Vulnerability Scanning with OpenVAS
1	Core Impact Vulnerability Scan
1	Metasploit
1	Post Exploitation and Pivoting
1	Snapd Privilege Escalation Exploit
2	Evasive Maneuvers and Post Exploitation
2	Linux Routing and SSH Tunnels
2	Client-Side Exploitation with Social Engineering
2	Windows Exploitation
2	Linux Exploitation
2	Password Cracking
2	Web Recon Tools

DAY	LAB ACTIVITY
3	Injection
3	Broken Authentication
3	Sensitive Data Exposure
3	Local File Inclusion and Client-side Access Control
3	Security Misconfiguration
3	Cross Site Scripting
3	Insecure Deserialization
3	XML External Entities
3	Using Components with Known Vulnerabilities
3	Insufficient Logging and Monitoring
3	Web Challenge
4	Linux Firewalls
4	Advanced IP Tables
4	Linux Logs
4	Intrusion Detection Systems
4	Basic Network Forensics
4	Attacking Classic Ciphers
4	Breaking Repeated Key XOR Cipher
4	Breaking Weak RSA Keys
4	Steganography
4	Using the OpenSSL CLI Tool
4	Using GPG for Encryption and Key Management
5	Attack and Defend

PEN500

PENTESTING & NETWORK EXPLOITATION

Pentesting & Network Exploitation exposes students to all manner of reconnaissance, scanning, enumeration, exploitation and pillaging for 802.3 networks.

Topics expose students to a variety of recon, discovery, scanning, enumeration, exploitation, post-exploitation, pillaging, covering one's tracks and persistence.

TARGET AUDIENCE

Penetration testers looking to broaden their overall penetration testing skill set, network engineers, system administrators, developers

OBJECTIVE

Provide in-depth exposure and hands-on practice with all facets of 802.3 hacking, vulnerability research, pivoting, exploitation, password/hash cracking, post-exploitation pillaging and methods of setting up persistence on a victim's network

COMTECH™

DAY 1	DAY 2	DAY 3
Day 1 introduces students to host target analysis. Topics include Linux command line, bash scripting and simple programming to enumerate, attack and exploit Linux hosts later in the course. Once Linux is complete, students begin learning basic through intermediate Windows Command Line skills, PowerShell cmdlets and the PowerShell attack framework called PowerPreter.	Students learn how to conduct basic service scans and exploit vulnerable hosts on internal networks through hands-on challenges that force them to replicate a real-world penetration test. They learn how to map, discover and exploit web applications, which requires the tester to understand how they communicate and the role the server plays in the relationship. Students learn how to conduct reconnaissance against a web server, followed by mapping its architecture. They're also challenged with discovering vulnerabilities and misconfigurations for follow-on exploitation.	Students learn how to simulate an insider threat and escape restricted environments by abusing native services and functionality. Students then move to routed attacks against clients that have NAT devices, firewalls and DMZs deployed. They learn how to exploit a variety of web-facing services and gain access to the DMZ. Once in the DMZ they are asked to pillage the hosts and find additional information to assist in pivoting deeper into the network and into network segments that don't touch the web directly.

DAY 4

On Day 4 students learn how to create and host malicious binaries on their own webserver to facilitate network penetration with purpose-built shellcode. Building on techniques and access gained into the DMZ, students are challenged to burrow further into the victims network by adding routes and pivoting into internal network segments by exploiting additional victims. Having exploited a variety of hosts throughout the network deploying persistence is then taught to maintain hard earned access.

Topics List

- Using MSFvenom to create purpose-built binaries with a variety of payloads
- Hosting malware on web server for easy delivery to victims
- Adding routes to additional network segments to facilitate pivoting
- Using post-exploitation Meterpreter tools to pillage various hosts
- Deploying Visual Basic Script for persistence on various victims
- Modifying persistence mechanism to survive reboot

DAY 5

Day 5 deals exclusively with hands-on challenges. Using all the skills, techniques and tools learned during the previous four days to lay waste to the company's network and computers, students will be tasked with owning "the CEO's" computer, and stealing as much sensitive information from the notional corporation as possible. The company's computers contain a wide variety of PII, corporate information and intellectual property for the taking. Can they own the CEO's box? Can they gain access to and modify the company's firewall settings?

Topics List

- Obtaining sensitive, non-public information from the company's computer
- Modifying the company's firewall settings
- Pwning the CEO's computer

PEN540

WIRELESS PENTESTING & NETWORK

PEN540 - Wireless Pentesting and Network Exploitation introduces students to all manner of reconnaissance, scanning, enumeration, exploitation and reporting for 802.11 networks.

The lab topics expose students to a variety of survey, database creation, scripting, and attack methods that can be used to gain a foothold in to a client's network during a penetration test.

TARGET AUDIENCE

Penetration testers looking to broaden their overall penetration testing skill set, wireless engineers, system administrators and developers

OBJECTIVE

Provide in-depth exposure to all facets of 802.11 penetration testing, encryption cracking, post-exploitation pillaging and report writing

COMTECH™

DAY 1

Students will learn how to conduct wireless penetration tests using open source tools against 802.11 a/b/g/n networks. In addition, students will identify characteristics and common vulnerabilities associated with WiFi.

Topics List

- Scoping and Planning WiFi Penetration Tests
- 802.11 Protocols and Standards
- Authentication vs Association
- WiFi Security Solutions
- WiFi Hacking Hardware
- Connectors and Drivers
- Recon and Custom Password Generation with Cupp and CeWL

DAY 2

Students will learn to use open source tools and hardware to conduct both mobile and static 802.11 a/b/g/n surveys. Planning and executing surveys will be covered in depth as well as data management and database management techniques.

Topics List

- Conducting Surveys Using Airodump-ng and Kismet
- Creating SQL Databases of Survey Data
- Specialized SQL and AWK Commands to Manipulate Data for Reporting
- Cracking WEP
- Setting Up MAC Filters
- Bypassing MAC Filters

DAY 3

Students continue their use of Kismet and Airodump-ng to conduct mobile surveys, database the information and create .kml files in order to visualize survey data. Students are then exposed to an in-depth discussion on advanced encryption security processes followed by learning how to use open source tools to exploit the security process.

Topics List

- Planning and Conducting Mobile WiFi Survey
- GISKimset to Database Survey Information
- Creating Custom SQL Queries
- AWK Tool to Format Output from SQL Queries for Reporting
- GISKismet to Create .kml Files
- Stream and Block Ciphers, Block Cipher Modes
- WPA2 AES-CCMP Security Process
- Cowpatty to Recover WPA2 Passphrase
- Pyrit to Survey and Attack Encryption
- Databasing and Recovering WPA2 Passphrases

DAY 4

Building on the skills learned in the first three days, the students will learn how to conduct Man-in-the-Middle attack using easy-creds and a fake access point. Students will learn how to conduct various types of attacks, traffic capture, and credential harvesting once a victim connects.

DAY 5

The last day of the course comprises a full-spectrum WiFi penetration test that the students must scope, plan and conduct. Final exercise serves to replicate a variety of network hardware, services and configurations, target website for recon, with multiple WiFi access points and clients using a variety of security mechanisms as provided.

PEN550

ADVANCED PENTEST BOOTCAMP

PEN550 Advanced Pentest Bootcamp is and advanced level course designed for pentesters who want to develop competency in scripting and building your own tools. This course provides students a strong foundation in the Python scripting language at the intermediate level while taking the student much deeper into advanced techniques for Penetration testing.

Students who take this course learn how to look at a variety of technical situations and build specialized tools to solve problems. During the course, students create a variety of scripts and tools, to include scanners, exploits, web application attack tools, and more.

TARGET AUDIENCE

This course is designed for students who have completed PEN500 Penetration Testing and Network Exploitation. It is recommended that students have exposure and or working experience (preferred) to scripting languages like Python.

OBJECTIVE

Students will gain access to unprivileged accounts and escalate privilege to exploit and maintain persistence. They will write exploits to leverage against Windows and Linux-based applications and/or systems. Hide sensitive data exfiltration using encryption and test applications via fuzzing to exploit discovered vulnerabilities.

COMTECH™

DAY 1	DAY 2	DAY 3
Intro to Pentesting and Scanning Lecture **Topics List** » Scanning » Specialized Linux Port Scans » Vulnerability Scanning » Scanning and Enumeration » Metasploit Fundamentals » Post Exploitation and Pivoting	Students will begin the day by looking at web recon tools. They will use SQL injection to evaluate paths for access and remote execution. **Topics List** » Web Recon Tools » SQL Injection » Advanced OS Command Injection » Detecting and Exploiting Hard to Find SQL Injections » Advanced Sqlmap » Manual Blind SQL Injection » NoSQL Injection	Students will look at Cross Site Scripting and Cross Site Request Forgery. They will look at other methods of exploiting mis-configurations and Cross Site Execution. **Topics List** » Cross Site Scripting » Cross Site Scripting Filter Evasion » Advanced CSRF » Exploiting Misconfigured CORS » Local File Inclusion » Advanced Local File Inclusion » XML External Entities » XXE to Obtain Arbitrary Files » Out of Band XXE

DAY 4	DAY 5
Students will learn about scripting and Python tools to automate Pentesting. They will look at x86 architecture and other ways to take advantage of the system using software to evaluate large parts of code. **Topics List** » Python Command and Control » x86 Memory Architecture » Basic x86 Assembly and Shellcode » Software Exploitation, Fuzzing, and Buffer Overflows	On the final day of class, students will complete a capstone on web exploitation followed by a capture the flag event. **Topics List** » Advanced Web Exploitation Capstone Lab » Capture the Flag Lab

PEN550

ADVANCED PENTEST BOOTCAMP

PEN600

ADVANCED WEB APPLICATION EXPLOITATION

Web applications are the source of many security vulnerabilities. Because of this, many web developers try to lock down the security of their web applications. However, not all of them do it correctly or completely, leaving certain avenues of attack still open. The Advanced Web Exploitation course explores how to search for, find, and exploit these hard to find vulnerabilities.

Each module will have video lecture content, explaining how to evade common incomplete mitigation strategies and how to find and exploit difficult vulnerabilities. Each module will also have a hands-on lab component, in which the students will have the chance to experiment with advanced techniques, seeing why they work and how they can be modified in whatever unique situation is encountered. Students will then complete a capstone lab that will allow the student to explore a novel web application and perform a multistep attack to exploit it completely.

PREREQUISITE KNOWLEDGE

Before taking this course, students should be familiar with:

- Identify basic examples of the OWASP Top Ten vulnerabilities
- Exploit the basic manifestations of these vulnerabilities

OBJECTIVE

Evade common incomplete filters to achieve the basic attacks. String multiple attacks together to achieve a more difficult objective.

COMTECH™

MODULE	LECTURE	LABS
0	Introduction	
1	Basic Recon Tools	Lab 1: Recon Tools
2	Advanced SQL Injection	Lab 2.1: Detecting and Exploiting Hard to Find SQL Injection Vulnerabilities Lab 2.2: Advanced SQLmap Lab 2.3: Manual Blind SQL Injection Lab 2.4: NOSQL Injection
3	XSS Filter Evasion	Lab 3.1: XSS Filter Evasion Lab 3.2: Exploiting Misconfigured CORS
4	OS Command Injection Filter Evasion	Lab 4: OS Command Injection Filter Evasion
5	Local File Inclusion	Lab 5: Advanced Local File Inclusion
6	Cross Site Request Forgery	Lab 6: Advanced Cross Site Request Forgery
7	XML External Entities	Lab 7.1: XXE to Obtain Arbitrary Files Lab 7.2: Out Of Band XXE
8	Server Side Request Forgery	Lab 8: SSRF for Internal Port Scanning and File Disclosure
9	Insecure Deserialization	Lab 9: Exploiting Insecure Deserialization in Java and Python
10	Capstone	Lab 10: Capstone: Multistage Attack on a Partially Hardened Web Application