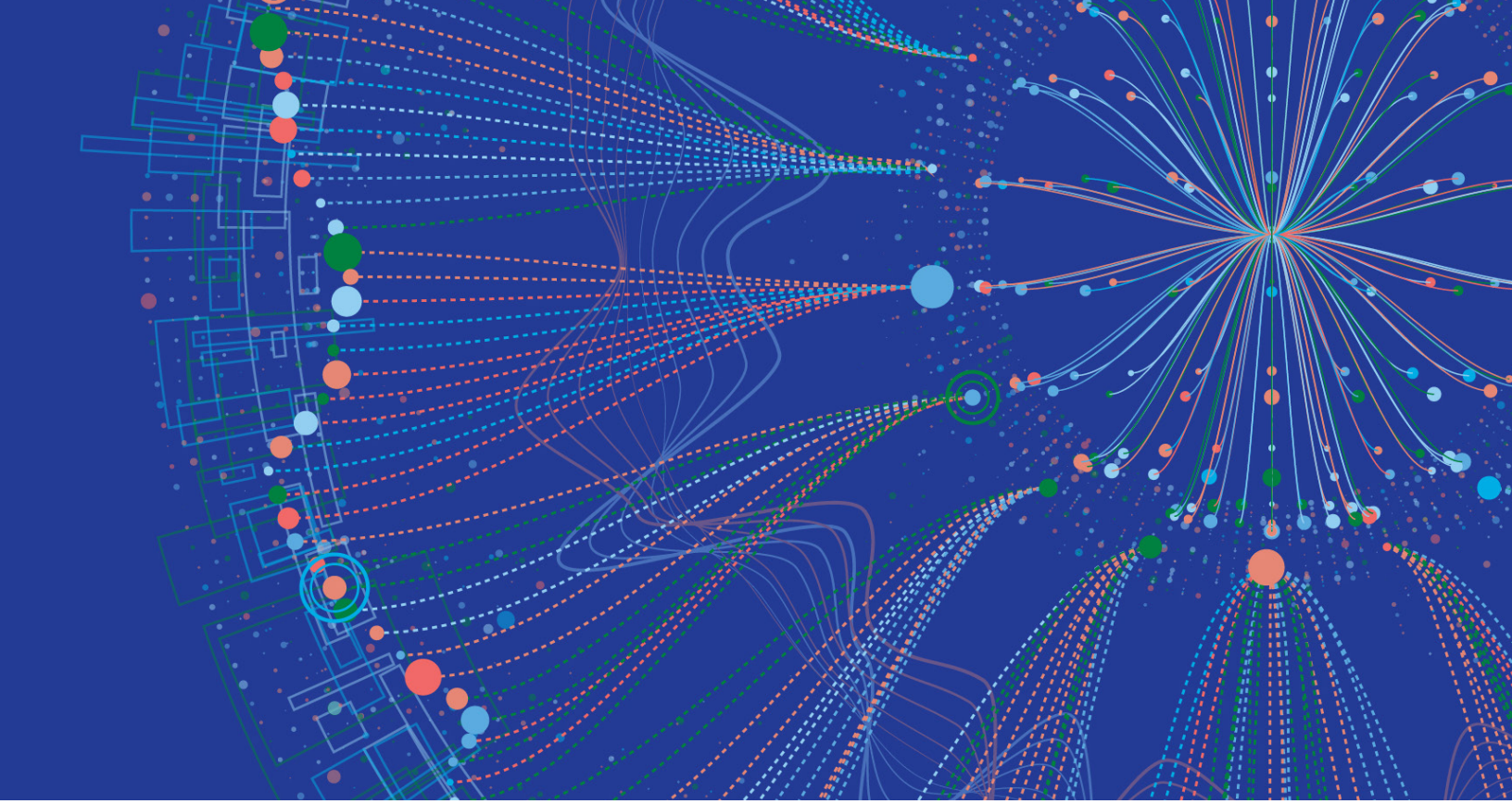

PEN550 Advanced Pentest Bootcamp

Course Overview

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.

Objectives

- 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.

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.

Estimated Course Length: 24 hours

Day 1

Intro to Pentesting and Scanning Lecture

Topics List

- Scanning
- Specialized Linux Port Scans
- Vulnerability Scanning
- Scanning and Enumeration
- Metasploit Fundamentals
- Post Exploitation and Pivoting

Day 2

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

Day 3

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

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

Day 5

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

About CyberStronger

Comtech provides cybersecurity solutions and services tailored to training and workforce development. The CyberStronger product portfolio was created by a team of former National Intelligence Community members who all possess the necessary hands-on, practical cybersecurity experience and abilities required to meet the needs of our demanding customer base. Our experts share the intellectual curiosity to constantly ask the 'why' and 'how' as they develop and deliver truly unique products and services to help close the growing cybersecurity skills gap. The Comtech CyberStronger offerings include off-the-shelf and custom training, hands-on skills labs, and competency-based assessments mapped to cybersecurity job roles.

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