



CYB101:

Cybersecurity Academy Bootcamp

CyberCamp - The trusted source for cybersecurity training and certifications, driven by world-class Israeli experts.

Table of Contents

[Table of Contents](#)

[Course Description](#)

[Target Audience](#)

[Prerequisites](#)

[Certification](#)

[Training Objectives](#)

[Job Roles](#)

[Laptop Requirements](#)

[Training Outline](#)

[Module - Introduction](#)

[Module - Setting Up a Personal Lab](#)

[Module - Linux Administration and Security](#)

[Module - Computer Networking Fundamentals](#)

[Module - Python Programming](#)

[Module - Attacking and Defending Networks](#)

[Module - Digital Forensics and Incident Response](#)

[Module - Real-World Project](#)

[Module - Penetration Testing](#)

[Module - Windows Administration and Security](#)

[Module - Web Application Security](#)

[Module - Job Preparation](#)

[Module - Final Exam and Certification](#)

Course Description

CYB101: Cybersecurity Academy Bootcamp

CyberCamp's training provides a wide knowledge base and a set of powerful tools for each learner, enabling graduates to start functioning in a variety of junior security positions. Through building a personal lab and practicing tens of real-world challenges during the course, learners will acquire invaluable skills to give them a strong base for becoming distinguished security professionals, delivering unmatched value to corporations that employ them.

Target Audience

- Anyone pursuing a career as a cybersecurity professional.

Prerequisites

- STEM Diploma or Degree (Science, Technology, Engineering, and Mathematics)
- English level: B2, C1, or C2
- Basic competence in computer programming (Java / Python / C# / C++ etc.)
- Passing the CyberCamp Online Admission Test

Certification

After successfully completing this training, participants will be entitled to the **CyberCamp Certified Security Professional** certificate.

This program provides hands-on training and preparation for the following industry certifications:

- **CompTIA - Security+**
- **EC-Council - CEH (Certified Ethical Hacker)**

Participants can take the exams independently after the course ends.

Training Objectives

By the end of this course, participants will:

- Get a solid technical foundation in the fields of **Linux, Windows, Networking, Host and Network Exploitation, Web Application Security, and Incident Response.**
- Possess the skills necessary to carry out independent penetration tests against applications and networks.
- Gain knowledge of administering SIEM solutions.
- Gain knowledge of SOC processes, technologies, and workflows.
- Be able to recognize attacker tools, tactics, and procedures to identify indicators of compromise (IOCs).
- Be able to monitor and analyze logs and alerts from a variety of different technologies (IDS/IPS, end-point protection, servers, and hosts).
- Be able to utilize a set of security tools for analyzing networks, attacking, and protecting systems.
- Be able to gather detailed information about devices in a network.
- Be able to discover, exploit, and mitigate MITM attacks.
- Be able to discover, exploit, and mitigate web application vulnerabilities.
- Be able to secure systems, mitigating the attacks shown throughout the course.

Job Roles

At the end of the course, graduates will be ready to start the following job roles at a junior level:

- Security/SOC Analyst (Tier I+)
- Security Engineer/Architect
- Penetration Tester
- System Administrator
- Threat Intelligence Analyst
- Cybersecurity Consultant
- Technical Security Manager

Laptop Requirements

- CPU: 64-bit Intel i5/i7
- RAM: 8 GB RAM minimum
- Hard Drive Free Space: 100 GB Free space
- Operating System: Windows / macOS / Linux

Training Outline

Module - Introduction

- Course Overview and Goals

Module - Setting Up a Personal Lab

- What is Virtualization?
- Virtualization Software Overview
 - Creating a Virtual Machine
 - Creating and Using Snapshots
- Installing Kali as a Virtual Machine
- Installing Windows as a Virtual Machine
- Creating a Linux Cloud Server

Module - Linux Administration and Security

- Introduction to UNIX/Linux
 - The Kernel
 - The Shell
 - The Terminal
 - Linux Distributions
- Command Line Basics
 - man pages
 - Directories
 - Files
 - **Bonus: Problem Solving Methodology**
- File Contents
- Linux File Tree

- Shell Expansion
 - Commands and Arguments
 - Control Operators
- Shell variables
 - Shell Embedding and Options
 - Shell History
 - File Globbing
- Pipes and Commands
 - I/O Redirection
 - Filters
 - Basic Unix Tools
 - Command Line Challenge
 - Regular Expressions
 - Regular Expressions Challenge
- Command-Line Environment
 - tmux
 - vim
 - **Bonus: Touch Typing**
 - **Bonus: Mouseless Computer Control**
- Bash Scripting
 - Introduction
 - Loops
 - Parameters
- Local User Management
 - Introduction to Users
 - User Management
 - User Passwords
 - User Profiles
 - Groups
- File Security
 - Standard File Permissions
 - Advanced File Permissions
 - Access Control Lists
 - File Links
- Processes
 - Introduction

- Process Priorities
- Background Jobs
- Linux System Administration
 - Scheduling
 - Logging
 - Memory Management
 - Resource Monitoring
 - Package Management

Module - Computer Networking Fundamentals

- Introduction to Networking
 - The OSI Model
 - Key Networking Terms
- Packet Sniffing with Wireshark
- Advanced Wireshark Filtering and Analysis
 - Identifying Malicious Content and Streams
 - Extracting and Repairing Content from PCAP files
- Physical Layer
- Data Link Layer
 - MAC
 - ARP
 - Ethernet
- Network Layer
 - Network Addresses
 - IP (IPv4, IPv6)
 - Network Masks
 - Routing
 - ICMP
- Transport Layer
 - TCP
 - UDP
- Session and Presentation Layer
 - Logical Ports
- Application Layer
 - Socket Programming - TCP/UDP Client and Server
 - DHCP, DNS, FTP, HTTP, HTTPS, SNMP, SSH, Telnet, TLS/SSL

- Networking Conclusion - A Journey of a Packet

Module - Python Programming

- Python Refresher
 - Variables and Data Types
 - Flow Control
 - Functions
 - Modules
 - Exceptions
 - Debugging
 - Files
 - Encoding
 - Package Management
- Python Programming for Security
 - OWASP Python Security Project
 - Implementing 'ps' using Python and /proc
 - Creating a Port Scanner

Module - Attacking and Defending Networks

- Introduction - Cyber Attack Process
 - MITRE ATT&CK Framework
 - Cyber Kill Chain
- Network Anonymity
 - Proxy Servers
 - proxychains
 - Tor
- Network Attack Detection and Prevention
 - Denial-of-Service Attacks
 - MITM Attacks
 - IP Spoofing
 - ARP Spoofing
 - DNS Spoofing
 - Bypassing HTTPS (Protocol Downgrade Attacks)
 - Javascript Code Injection
 - Detecting ARP Poisoning Attacks

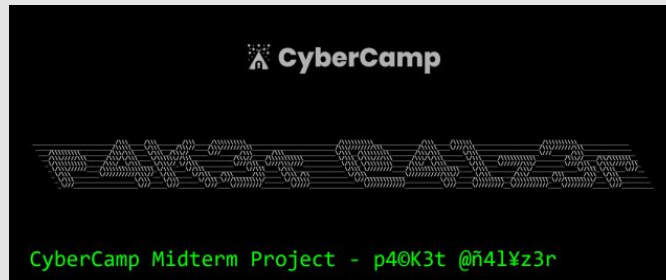
- Detecting Suspicious Network Activity
- Preventing MITM Attacks
- Firewalls
 - Next-Generation Firewalls
 - Web Application Firewalls
 - iptables Refresher
- IDS/IPS
 - SNORT
 - Suricata
- Techniques for Evading IDS/IPS

Module - Digital Forensics and Incident Response

- The SOC - Security Operations Center
 - Modern SOC Components: People, Processes, and Technology
 - SOC Ethics
 - SIEM, EDR, and SOAR
 - SOC Analyst - A Daily Overview
 - Identity and Access Management
 - Data Loss Prevention (DLP)
 - Workplace Security Awareness
- Incident Response
 - Preparing for an Incident
 - Incident Response Lifecycle
- Digital Forensics
 - **Team challenge: Windows Image Forensic Investigation**
 - Toolkit: Autopsy, RegRipper, FTK Imager
- Security Logging and Monitoring
 - Local and Centralized Logging
 - Security Information and Event Management (SIEM)
 - Installing and Configuring Splunk on a Windows Server
 - Transformation Commands
 - Reports, Dashboards, and Alerts
 - Detecting Ransomware with Splunk

Module - Real-World Project

- **Building an Intrusion Detection System from Scratch**
 - Working with Scapy (Packet manipulation tool)



Module - Penetration Testing

- Introduction to Penetration Testing
 - Terminology
 - The Phases of a Penetration Test
- Information Gathering - Passive
 - Open Source Intelligence Gathering (OSINT)
 - Google Hacking
 - Shodan
 - Information Gathering - Active
 - Host discovery
 - Port and Service Scanning
 - Nmap and Zenmap
 - Finding Unlisted Files and Directories
 - Social Engineering for Information Gathering
 - Maltego
 - SEToolkit
 - HiddenEye
 - Enumeration Vectors
 - Default Passwords
 - SNMP Enumeration
- Threat Modeling and Vulnerability Analysis
 - Vulnerability Scanners
 - Nessus, Nexpose, OpenVAS
- Server-Side Exploitation
 - Bind, Reverse, and Encrypted Shells

- The Metasploit Framework
- Client-Side Exploitation
 - Creating a Backdoor
 - Delivering a Backdoor
 - Protecting Against Delivery Methods
 - Exploiting a System Through a Malicious Update
 - Browser Exploitation
 - BeEF
 - Hiding Malware Inside Innocent Files
 - Trojan Detection
- Post Exploitation and Reporting
 - Privilege Escalation Techniques (Linux and Windows)
 - Pivoting
 - Maintaining Access

Module - Windows Administration and Security

- Introduction to Windows
- Command Line Basics
- Batch Scripting
- Windows Registry
- Permissions
- Workgroup
- Powershell for Hackers
- Sysinternals Suite
- Windows Domain and Active Directory

Module - Web Application Security

- Introduction to Web Applications
 - Web Servers
 - Web Application Architecture
 - Web Application Technologies
- Client-Side Development - HTML, CSS, and Javascript
 - HTML5
 - Tags
 - Nesting Elements - Hierarchy

- HTML Attributes
 - Forms
- DOM - Document Object Model
- CSS3
- JavaScript
 - Manipulating the DOM
 - Ajax
 - jQuery
- Server-Side Development
 - Common Server Side Programming Languages
 - PHP
 - Variables, Loops, Functions, and Classes
 - Object Serialization
 - PHP and HTTP
 - Exploitable PHP Functions
 - Sessions
 - Using PDOs to Connect to a Database
 - Databases Introduction
 - Relational / SQL
 - Non-Relational / NoSQL
- Web Application Reconnaissance Tools
- Finding and Exploiting the OWASP Top 10 and Common Web App Attacks
 - SQL Injection
 - OS Command Injection
 - Path Traversal
 - Local File Inclusion
 - Remote File Inclusion
 - Cross-Site Request Forgery (CSRF)
 - Broken Authentication
 - Sensitive Data Exposure
 - XXE - XML External Entities
 - Broken Access Control
 - Security Misconfigurations
 - XSS - Cross-Site Scripting
 - Insecure Deserialization
 - Using Components with Known Vulnerabilities

- OWASP Open SAMM
- Discovering Vulnerabilities Automatically
 - ZAP, Nikto, w3af

Module - Job Preparation

- Networking
- LinkedIn Profile
- Personal Portfolio Website
- Resume Preparation
- Interview Preparation
- Job Search Strategy
- Continuous Learning Resources

Module - Final Exam and Certification

- Final Evaluation Exam and Certification
- Course Conclusion
- Graduation