Description of the course (English):

Earn your Cybersecurity certificate in 8 weeks.

Become a Cybersecurity Expert with our comprehensive and world-class Online Cybersecurity Bootcamp. Build your skillset and get CompTIA Security+ Certification. Get excellent career advice from our experienced professionals and mentors.

Cybersecurity Bootcamp Benefits:

Cybersecurity professionals must be 100% knowledgeable and experienced in the skills and nuances of the domain, including a wide range of security components and technologies. We've packaged this critical knowledge and skills into our Cybersecurity Bootcamp Certification course. Here's how this course impacts your career:

- You're Day-1 ready when you leave the program and have the foundational knowledge and experience needed to grow your career into leadership positions.
- You learn from working professionals who are active in the tech landscape and give authentic feedback on today's tech and hiring landscapes; you have insight into what's really out there.
- You have a network of professionals, both technical and non-technical, committed to supporting your growth and advancement even after you graduate.
- You can get your career started quickly and with minimal investment; you'll be working and earning a paycheck in six months or less.

URL of Course: Cybersecurity Bootcamp | Best Cyber Security Online Bootcamps

Cost: $7,995 USD

Mode: Virtual
Duration: 8 Weeks
Name: CYBERSECURITY BOOTCAMP

Course Contents:

Module 1: Cybersecurity Fundamentals

- Explain the center data confirmation (IA) standards.
- Identify the key segments of cybersecurity engineering.
- Apply cybersecurity engineering standards.
- Describe hazard the executives procedures and practices.
- Identify security instruments and solidifying procedures.
- Distinguish framework and application security dangers and vulnerabilities.
- Describe various classes of assaults.
- Define kinds of occurrences including classifications, reactions, and timetables for the reactions.
- Describe new and developing IT and IS advances.
- Analyze dangers and dangers inside setting of the cybersecurity engineering.
- Appraise cybersecurity episodes to apply fitting reaction.
- Evaluate basic leadership results of cybersecurity situations.
- Access extra outer assets to enhance information on cybersecurity.

Module 2: Systems Administration - Windows & Linux

- Linux Administration
  - Install the Linux operating system and configure peripherals
  - Perform and modify startup and shutdown processes
  - Configure and maintain essential networking services
  - Create and maintain system users and groups
  - Understand and administer file permissions on directories and regular files
  - Plan and create disk partitions and file systems
  - Perform maintenance on file systems
  - Identify and manage Linux processes
  - Automate tasks with cron
  - Perform backups and restoration of files
  - Work with system log files
  - Troubleshoot system problems
  - Analyze and take measures to increase system performance
  - Configure file sharing with NFS

  - Configure Samba for file sharing with the Windows clients
  - Setting up a basic Web server
  - Understand the components for setting up a LAMP server
  - Implement basic security measures
  -
- Windows Administration
  - How to use Windows 10 and Server 2016.
  - How to use Local users and groups.
  - What are Servers and Clients.
  - What do we mean with networking (Routers,Switches)
  - What are Public and Private Ip Addresses.
  - What are Public DNS zones and Private DNS zones?
  - What are Active Directory Domains and why do Enterprises use them.
  - How to use Active Directory users and groups.
  - How to enable Sharing and NTFS rights.
  - How to use Group Policy.
  - Preparing for upgrades and migrations
  - Managing disks in Windows Server
  - Managing volumes in Windows Server
  - Overview of Hyper-V
  - Defining levels of availability
  - Backing up and restoring the Windows Server 2016 operating system and data by using Windows Server B

Module 3: CompTIA Network+

- Explain the OSI and TCP/IP Models.
- Explain the properties of network traffic.
- Install and configure switched networks.
- Configure IP networks.
- Install and configure routed networks.
- Configure and monitor ports and protocols.
- Explain network application and storage issues.
- Monitor and troubleshoot networks.
- Explain network attacks and mitigations.
- Install and configure security devices.
- Explain authentication and access controls.
- Deploy and troubleshoot cabling solutions.
- Implement and troubleshoot wireless technologies.
- Compare and contrast WAN technologies.
- Use remote access methods.
- Identify site policies and best practices.

Module 4: CompTIA Security+

- Identify security threats
- Harden internal systems and services
- Harden internetwork devices and services
- Secure network communications
- Manage a PKI
- Manage certificates
- Enforce an organizational security policy
- Monitor the security infrastructure

Exam Voucher Included

Module 5: Python Programming

- Create working Python scripts following best practices
- Use python data types appropriately
- Read and write files with both text and binary data
- Search and replace text with regular expressions
- Get familiar with the standard library and its work-saving modules
- Use lesser known but powerful Python data types
- Create "real-world", professional Python applications
- Work with dates, times, and calendars
- Know when to use collections such as lists, dictionaries, and sets
- Understand Pythonic features such as comprehensions and iterators
- Write robust code using exception handling

Module 6: C)PEH - Certified Professional Ethical Hacker

- Course Introduction
- Introduction to Ethical Hacking
- Linux Fundamentals
- Protocols
- Cryptography
- Password Cracking
- Malware
- Security Devices
- Information Gathering – Passive Reconnaissance
- Social Engineering
- Active Reconnaissance
- Vulnerability Assessment
- Network Attacks
- Hacking Servers
- Hacking Web Technologies
- Hacking Wireless Technologies
- Maintaining Access and Covering Tracks

Exam Voucher Included

Module 7: CompTIA CySA+

- Assess information security risk in computing and network environments.
- Analyze reconnaissance threats to computing and network environments.
- Analyze attacks on computing and network environments.
- Analyze post-attack techniques on computing and network environments.
- Implement a vulnerability management program.
- Collect cybersecurity intelligence.
- Analyze data collected from security and event logs.
- Perform active analysis on assets and networks.
- Respond to cybersecurity incidents.
- Investigate cybersecurity incidents.
- Address security issues with the organization's technology architecture

Exam Voucher Included

Module 8: CompTIA PenTest+

- Plan and scope penetration tests.
- Conduct passive reconnaissance.
- Perform non-technical tests to gather information.
- Conduct active reconnaissance.
- Analyze vulnerabilities.
- Penetrate networks.
- Exploit host-based vulnerabilities.
- Test applications.
- Complete post-exploit tasks.
- Analyze and report pen test results

Module 9: CCSP - Certified Cloud Security Professional

- Architectural concepts and design requirements
- Cloud data security
- Cloud platform and infrastructure security
- Cloud application security
- Operations
- Legal and compliance

Career Success

- Career Success: Preparing for the Job Search
- Building a network and using it to Land Interviews
- Career Success: Resume, Cover Letter, LinkedIn Review
- Career Success: Interview Prep (Technical and Non-Technical)
- Mock Interviews
- Graduation