Cyber Security Specialist Program Syllabus

05.2021

Course Description

This 480 hour online training program will provide a foundational understanding of core topics and concepts, as well as introductory labs, projects and a cyber range. Upon completion of the course students will earn NexGenT Cyber Security Professional (NCSP) and CompTIA Security+ certifications.

Live Instruction: Part-Time programs include 10 hours of live instruction each week and a total student commitment of 20 hours per week. Full-Time programs include 24 hours of live instruction each week and a total student commitment of 40 hours per week. Instructors and mentors are available outside of class as needed for additional support and 1:1 mentoring.

Part 1. Introduction to Networking for Cyber Security

Two week introductory computer networking training. This section provides the foundational networking knowledge required to transition into the NexGenT Cyber Security Associate course. Students will complete labs using the Cisco Packet Tracer application for simulating real-world networks and learning basic skills with Cisco IOS command line. The course includes the following two modules:

1. Core Networking Concepts:
   Frames, MAC addresses and broadcast domains and transitions into IPv4/IPv6, ARP, routing and wireless LANs.

2. Systems and Security:
   Virtualization, cloud technologies and operating systems, networking security concepts including Access Control Lists, WLAN security, firewalls, IDS/IPS, VPNs, network attacks and hardening techniques.

Part 2. NexGenT Cyber Security Associate

This section includes 8 knowledge-based modules with over 25 virtualized labs for real-world skills training. As a final project at the end of this section, students are given a real-world cyber security scenario where they must develop a feasible solution to mitigate the given problem and perform a professional presentation on the solution. Upon final project and written exam completion, students are awarded the NexGenT Cyber Security Associate (NCSA).

Hands-on real-world lab simulation experiences. Twenty-five virtualized labs are designed to teach the following skills: Scanning Networks, Social Engineering, Certificate Management, Encryption, Wireshark, Hacking Wireless Networks, Vulnerability Scanning, Network Vulnerabilities, Protocols & Services, Keyloggers, Sniffers, System Hacking, Password Cracking Tools, IDS Evasion,, Firewalls, Honeypots, and PKI Concepts.

Modules:

1. Identify and Analyze Threats:
   Overview of the cyber security ecosystem, understanding of threat actors and attacks. Exploration of various toolkits and how they fit into common cyber security frameworks.

2. Cryptography:
   Fundamentals of cryptography and practical uses, as well as behind the scenes look at these algorithms and how they are useful.

3. Network Security:
   Common security implementations and common weaknesses, typically overlooked low hanging fruit that provide ways to raise threat awareness.

4. Secure Protocols:
   Understanding of the basic protocols and best practices needed to create a security focused organization. Defensive tactics to raise the bar.

5. Symptoms of Compromise:
   Recognizing symptoms of an attack, what to expect in different scenarios for efficient problem diagnosis, understanding what went wrong and how to prevent it in the future.

6. Tools:
   Cyber toolkits, which tools are available and how to apply them for all of the various security solutions and strategies.

7. Testing Infrastructure:
   Practical applications of attacking your own infrastructure to help defend it. How to identify your organization's weaknesses to help mitigate and define changes to be made.

8. Incident Response:
   What to do in the event of a security breach. The security team playbook, planning, and how to respond to certain events.

Part 3. NexGenT Cyber Security Professional

The NexGenT Cyber Security Professional (NCSP) is based on real-world skills which are vetted through the Cyber Range and intermediate knowledge on cyber security topics. Students earn the NCSP upon demonstration that they have learned the necessary real-world skills, are able to apply them, and have been skills checked in various missions and cyber range scenarios to validate their entry-level cyber security skillset. To obtain the NCSP students must both pass a knowledge-based exam and prove their skills in the cyber range.

Projects:
Virtualized projects built with reality-based missions that build upon the students' networking and cyber security skill sets for the final cyber range Skills Qualification Check (SQC). Example missions are simulations of attacks such as ransomware, spear phishing, disabling botnets, defending a financial institution, and defending against web attacks.

Cyber Range:
Students learn to defend against malicious threats in real-world lab simulations using our state-of-the-art Cyber Range. Here we cover scenarios that mimic ransomware, botnets, password cracking, reverse shells, launching payloads, and a comprehensive review of all types of red / blue team scrimmages. This will help build preparedness by allowing students to test drive incident response playbooks in a real-world situation. This type of immersive training builds situational awareness, which leads to on-the-ground experience and offers numerous benefits including real-time feedback and cross-functional training.

NCSP Skills Qualification Check
During this final week all students are scheduled to perform their live SQC (Skills Qualification Check) to verify skills. Upon successful completion the candidate will be awarded the NexGenT Cyber Security Professional (NCSP).. Students are tested with a cumulative exam and a final cyber range mission based on learned skills that prove their job readiness.

Part 4. CompTIA Security+
Students are prepared for and complete the CompTIA Security + exam. Aligned to the latest trends and techniques, the CompTIA Security+ covers the most core technical knowledge in risk assessment and management, incident response, forensics, enterprise networks, hybrid/cloud operations, and security controls.. This global certification validates the baseline knowledge necessary to perform core security functions and pursue an IT security career.