LCC INTERNATIONAL UNIVERSITY

Cybint

Week 1

- Introduction to the Bootcamp
- Overview of the Cybersecurity Landscape and Industry
- Basics of Computer and Device Hardware, Software, Operating Systems and Processes
- Basics of Networking Traffic, Hardware Components and Topology
- Network Communication Principles and Methods

Week 2

- Network and Routing Protocols / Services
- Packet Level Traffic Analysis
- Hands-on Operation of a Computer Network and Equipment, Monitoring and Analyzing Network Traffic Flow, Patterns and Performance
- Hands-on Creation and Analysis of Critical Network Servers.

Week 3

- Hands-on Creation and Analysis of Telnet, Web, Data and Active Directory Servers
- Hands-on Analysis of Network Topologies, Network Mapping and OS Fingerprinting
- Telecommunication Concepts and Range
- System and Network Admin Concepts, Management Principles and Controls
- Hands-on Creation and Use of Virtual Machines and Bootable USB OS

Week 4

- Overview of Threats, Classes, Attackers, Tactics, and Application Security Risks (OWASP)
- Hands-on Communications Security through Encrypting and Decrypting Data and Medias
- Hands-on Backup and Recovery of Data, Devices and Servers
- Network Security Principles, Methods, Protocols, Components and Architectures

Week 5

- Hands-on Assessment of Access Controls and Hardening Techniques to Ensure a Network's Security
- Hands-on Configuration and Utilization of a Firewall (on Windows, Linux and Hardware Firewall)
- Hands-on Configuration and Utilization of a Network/Host Intrusion Detection/Prevention System to Alert and Prevent Malicious Activity on a Network

Week 6

- Hands-on Configuration and Utilization of a Security Information and Event Management System to Correlate, Research, Analyze Logs and Provide Timely Detection of Misuse, Threats and Malicious Activity on the Network
- Hands-on Malware Detection, Analysis, Isolation and Removal

Week 7

- Cyber-Forensic Investigation Methodologies, Mindset, Tools
- Hands-on Forensics Investigation: Logs, System Files, Media, Memory Dump and Traffic Monitoring and Analysis

Week 8

- Overview of Network Vulnerabilities, Associated Attacks; Ethical Hacking Methodologies, Stages, Principles, Tools and Techniques
- Hands-on Conducting of Vulnerability and Compliance Scanning; and Correction Recommendation
- Hands-on Performing Incident Response, Damage Assessment, Incident Triage, Tracking and Reporting

Week 9

- Full Day Scenarios: Hands-on Protecting a Network from a Range of Cyber-Attacks (DDoS, SQL Injection, XSS, Ransomware, MiTM, ARP Poisoning, etc.)

Week 10

- Analysis of System Security and Organizational Posture Trends
- Analysis of Cyber-Defense Trends and Staying at the Cutting Edge of the Industry
- Performing of Security Design and Architecture Evaluation and Ensuing Recommendation

Week 11

- Hands-on Process of the Whole Chain of Custody for Handling Digital Evidence
- Hands-on Performing of Static and Dynamic Analysis of Drive Images and other Data Sources, Recovery and Mitigation/Remediation of an Enterprise System

Week 12

- Risk and Security Management Processes and Security Models
- Cybersecurity and Privacy Principles
- Advising on Disaster Recovery, Contingency and Continuity
- Summary and Presentation by Bootcampers
- Technical and Soft-Skill Preparation of a Job Interview Final Hands-on Scenario