CERTIFIED CYBERSECURITY PROFESSIONAL SYLLABUS

MODULE CONTENT	LAB PROCEDURES
1.PHYSICAL ASSET SECURITY	
Access control, Physical Security Controls, Locks and Keys, Standard Key-Locking Deadbolts, Cipher Locks, Control Relays, Authentication Systems, Smart card/RFID/biometric scanners, IDS/IPS, Video Surveillance, Environmental Security Activities.	■ Introduction to Physical Security Systems ■ Physical Security Zoning ■ Video Surveillance Systems ■ Remote Access Control ■ Remote Monitoring ■ Security Notification Systems
2.LOCAL HOST SECURITY	
Physically securing personal computing devices, software-based firewalls, and Internet Browser Security options. Securing Outer Perimeter Portals, BIOS Security Sub systems, Inner Perimeter Access, inner perimeter protection, OS Kernel Security, Password Security, Physical Authentication Devices, Data Encryption, Software-Based Local Firewalls, Malicious Software Protection, Anti spyware, hardening OS.	■ BIOS/CMOS Security Configuration ■ Local Login and User Configuration ■ Managing NTFS Permissions and File Encryption ■ Auditing and Viewing Logs ■ Local (Software) Firewall Configuration ■ Data Backup and Restore, ■ Additional OS Hardening
3.LOCAL NETWORK SECURITY	
OSI Security, Network topologies, protocols, servers, server security, Server Room Door Locks, Configuring/Hardening Server Operating Systems, Establishing User and Group Accounts, Distributed Intrusion Detection Architectures, Network Bridges, Copper Cabling, Fibre Optic Cabling, Wireless Networking security.	■ Managing Network Users ■ Wireless Router Configuration ■ Network Device Configuration ■ Managing Linux Users and Groups ■ Network Device Logging ■ Network Intrusion Detection
4.INTERNET SECURITY	
Authentication protocols, data cryptography, and data encryption techniques, examines Virtual Private Networks (VPNs) and firewalls, System Auditing and Event Logging as tools, along with different types of Intrusion Detection Systems (IDS). Basic internet concepts, IP Traffic, Unicasts, Broad casts and Multi-casts, Network Address Translation, Port Forwarding or Mapping, Network Segmentation, Firewalls, Proxy Servers, Extranets, DMZs, IP and MAC Authentication, Encryption, Cryptography, Vulnerabilities, DOS attacks.	■ Configuring IPSec for Communication ■ Steganography ■ Using the Encrypting File System ■ Introduction to Command-Line Network Analysis Utilities ■ File Hashing ■ Application Whitelisting/Blacklisting ■ Introduction to Wireshark ■ Managing Local Machine Certificates
5.ENTERPRISE IT NETWORK SECURITY	
Enterprise networking, security topologies, Seven Layer Network Security Model, enterprise server security, corporate cyber security policies, Risk Mitigation, Environmental Security Activities, Employee Awareness and Training.	■ Introduction to Network Switches ■ Introduction to Hardware Firewalls ■ Router Security ■ VLAN Operation ■ Inter-VLAN Routing ■ Creating Standard Access Control Lists ■ Creating a DMZ ■ Performing a Risk Assessment

6.INDUSTRIAL OT NETWORK SECURITY	
Closed Loop /open loop/ dedicated/distributed Control Systems, Asynchronous Serial Standards, Ethernet Networking, MODBUS, DNP3, ICCP, OPC, Utility Generation and Distribution Control Networks, Industrial Threats, Substation Security.	■ Introduction to Industrial Process Control Systems ■ Exploring ICS Network Structures ■ ICS Access Vulnerabilities ■ Exploring ICS/Enterprise Network Vulnerabilities ■ Segregating ICS Networks ■ Defending Against Brute Force Attacks ■ Protecting ICS Networks Using Switch Security
7.MEDICAL IoT NETWORK SECURITY	
Waiting Room Wi-Fi, VoIP Phone Systems, Medical Records Security, HIPAA, and healthcare data security, Radiology Information Systems, Digital Imaging and Communications in Medicine, Medical Diagnostic Instrumentation, IoT Health and Fitness Applications.	■ Introduction to Wearable Medical Devices ■ Bluetooth Reconnaissance ■ WiFi Reconnaissance ■ Ethernet Reconnaissance ■ SQL Injection (Database Security) ■ Risk Identification Network Vulnerability Scanning ■ Network and Server Hardening
8.ETHICAL HACKING	
Ethical and Legal Hacking, Hackers and Crackers, Cyber-criminals, Insider Threats , Network Enumeration Tools, Physical Techniques, Psychological Social Engineering, Pentest Process, IP Header Manipulation, UDP Flood At tacks, MAC Spoofing, DoS vs. DDoS At tacks, Rogue Access Points.	■ Credential Harvesting ■ Denial of Service ■ Password Cracking ■ Protocol Sniffing ■ Software Keylogging ■ Practicing Physical Social Engineering Techniques ■ Remote Access Trojans ■ Vulnerability Scanning and Exploitation