- **Student Introduction**
- **Computer Network and Defense Fundamentals**
  - Network Fundamentals
  - Network Components
  - TCP/IP Networking Basics
  - TCP/IP Protocol Stack
  - IP Addressing
  - Computer Network Defense (CND)

- **Network Security Threats, Vulnerabilities, and Attacks**
  - Essential Terminologies
  - Network Security Concerns
  - Network Security Vulnerabilities
  - Network Reconnaissance Attacks
  - Network Access Attacks
  - Denial of Service (DoS) Attacks
  - Distributed Denial-of-Service Attack (DDoS)
  - Malware Attacks

- **Network Security Controls, Protocols, and Devices**
  - Fundamental Elements of Network Security
  - Network Security Controls
  - User Identification, Authentication, Authorization and Accounting
  - Types of Authorization Systems
  - Authorization Principles
  - Cryptography
  - Security Policy
  - Network Security Devices
  - Network Security Protocols

- **Network Security Policy Design and Implementation**
  - What is Security Policy?
  - Hierarchy of Security Policy
  - Characteristics of a Good Security Policy
  - Contents of Security Policy
  - Typical Policy Content
  - Policy Statements
  - Steps to Create and Implement Security Policies
  - Considerations Before Designing a Security Policy
  - Design of Security Policy
  - Policy Implementation Checklist
  - Types of Information Security Policy

- Review of Security Policy Examples on the Enterprise
- Implementing Policies using the Group Policy

- **Physical Security**
  - Physical Security Concepts
  - Access Control Authentication Techniques
  - Physical Security Controls
  - Other Physical Security Measures
  - Workplace Security
  - Personnel Security: Managing Staff Hiring and Leaving Process
  - Laptop Security Tool: EXO5
  - Environmental Controls
  - Physical Security: Awareness /Training
  - Physical Security Checklists

- **Host Security**
  - Host Security
  - Windows Security Baselining
  - OS Security
  - Host based IDS
  - Data Encryption
  - Linux Security
  - Securing Network Servers
  - Hardening Routers and Switches
  - Syslog Server for Log Collection
  - Application/software Security
  - Data Security
  - Data Loss Prevention (DLP)
  - Virtualization Security

- **Secure Firewall Configuration and Management**
  - Firewalls and Concerns
  - What Firewalls Does?
  - What should you not Ignore?
  - Firewall Limitations
  - How Does a Firewall Work?
  - Firewall Rules
  - Types of Firewalls
  - Firewall Technologies
  - Firewall Topologies
  - Firewall Rule Set & Policies
  - Firewall Implementation

- Firewall Administration
- Firewall Logging and Auditing
- Firewall Anti-evasion Techniques
- Why Firewalls are Bypassed?
- Full Data Traffic Normalization
- Data Stream-based Inspection
- Vulnerability-based Detection and Blocking
- Firewall Security Recommendations and Best Practices
- Firewall Security Auditing Tools

- **Secure IDS Configuration and Management Intrusions and IDPS**
  - IDS
  - Types of IDS Implementation
  - IDS Deployment Strategies
  - Types of IDS Alerts
  - IPS
  - IDPS Product Selection Considerations
  - IDS Counterparts

- **Secure VPN Configuration and Management**
  - Understanding Virtual Private Network (VPN)
  - How VPN works?
  - Why to establish VPN?
  - VPN components
  - VPN concentrators
  - Types of VPN
  - VPN Categories
  - Selecting Appropriate VPN
  - VPN Core Functions
  - VPN Technologies
  - VPN Topologies
  - Common VPN Flaws
  - VPN Security
  - Quality of Service and Performance in VPNs

- **Wireless Network Defense**
  - Wireless Terminologies
  - Wireless Standard
  - Wireless Topologies
  - Components of Wireless Network
  - WEP (Wired Equivalent Privacy) Encryption
  - WPA (Wi-Fi Protected Access) Encryption

- WPA2 Encryption
- WEP vs. WPA vs. WPA2
- Wi-Fi Authentication Method
- Wireless Network Threats
- Bluetooth Threats
- Wireless Network Security
- Wi-Fi Discovery Tools
- Assessing Wireless Network Security
- WPA Security Assessment Tool
- Wi-Fi Vulnerability Scanning Tools
- Configuring Security on Wireless Routers
- Additional Wireless Network Security Guidelines

- **Network Traffic Monitoring and Analysis**
- Network Traffic Monitoring and Analysis (Introduction)
- Network Monitoring: Positioning your Machine at Appropriate Location
- Network Traffic Signatures
- Packet Sniffer: Wireshark
- Detecting OS Fingerprinting Attempts
- Detecting PING Sweep Attempt
- Detecting ARP Sweep/ ARP Scan Attempt
- Detecting TCP Scan Attempt
- Detecting SYN/FIN DDOS Attempt
- Detecting UDP Scan Attempt
- Detecting Password Cracking Attempts
- Detecting FTP Password Cracking Attempts
- Detecting Sniffing (MITM) Attempts
- Detecting the Mac Flooding Attempt
- Detecting the ARP Poisoning Attempt
- Additional Packet Sniffing Tools
- Network Monitoring and Analysis
- Bandwidth Monitoring

- **Network Risk and Vulnerability Management**
- What is Risk?
- Risk Levels
- Risk Matrix
- Key Risk Indicators (KRI)
- Risk Management Phase
- Enterprise Network Risk Management
- Vulnerability Management

- **Data Backup and Recovery**
  - Introduction to Data Backup
  - RAID Technology
  - Storage Area Network (SAN)
  - Network Attached Storage (NAS)
  - Selecting Appropriate Backup Method
  - Choosing the Right Location for Backup
  - Backup Types
  - Conducting Recovery Drill Test
  - Data Recovery
  - Windows Data Recovery Tool
  - RAID Data Recovery Services
  - SAN Data Recovery Software
  - NAS Data Recovery Services

- **Network Incident Response and Management**
  - Incident Handling and Response
  - Incident Response Team Members: Roles and Responsibilities
  - First Responder
  - Incident Handling and Response Process
  - Overview of IH&R Process Flow