CND: Certified Network Defender

Course ID #: 1275-235-ZZ-W

Hours: 35

Course Content

Course Description:

Certified Network Defender (CND) is a vendor-neutral, hands-on, instructor-led comprehensive network security certification training program. It is a skills-based, lab intensive program based on a job-task analysis and cybersecurity education framework presented by the National Initiative of Cybersecurity Education (NICE). The course has also been mapped to global job roles and responsibilities and the Department of Defense (DoD) job roles for system/network administrators. The course is designed and developed after extensive market research and surveys.

The program prepares network administrators on network security technologies and operations to attain Defense-in-Depth network security preparedness. It covers the Protect, Detect and Respond approach to network security. The course contains hands-on labs, based on major network security tools and techniques which will provide network administrators real world expertise on current network security technologies and operations. The study-kit provides you with over 10 GB of network security best practices, assessments and protection tools. The kit also contains templates for various network policies and a large number of white papers for additional learning.

At Course Completion:

After competing this course:

- Students will learn about various network security controls, protocols, and devices.
- Students will be able to troubleshoot their network for various network problems.
- Students will be able to identify various threats on organization network.
- Students will learn how to design and implement various security policies for their organizations.
- Students will learn the importance of physical security and be able to determine and implement various physical security controls for their organizations.
- Students will be able to harden security of various hosts individually in the organization's network.
- Students will be able to choose appropriate firewall solution, topology, and configurations to harden security through firewall.
- Students will be able to determine appropriate location for IDS/ISP sensors, tuning IDS for false positives and false negatives, and configurations to harden security through IDPS technologies.
- Students will be able to implement secure VPN implementation for their organization.
- Students will be able to identify various threats to a wireless network and learn how to mitigate them.
- Students will be able to monitor and conduct signature analysis to detect various types of attacks and policy violation activities.
- Students will be able to perform risk assessment, identify vulnerability assessment with the method of scanning through various scanning tools, and generate detailed reports on the risk.

- Students will be able to provide first response to the network security incident and assist IRT team and forensics investigation team in dealing with the incident.

Why Certified Network Defender:

Organizational focus on cyber defense is more important than eve a cyber breaches have a far greater financial impact and can cause broad reputational damage.

Despite best efforts to prevent breaches, many organizations are still being compromised. Therefore organizations must have, as part of their defense mechanisms, trained network engineers who are focused on protecting, detecting, and responding to the threats on their networks.

Network administrators spends a lot of time with network environments, and are familiar with network components, traffic, performance and utilization, network topology, location of each system, security policy, etc.

So, organizations can be much better in defending themselves from vicious attacks if the IT and network administrators equipped with adequate network security skills. Thus Network administrator can play a significant role in network defense and become first line of defense for any organization.

Target Students:

- Network Administrators
- Network Security Administrators
- Network Security Engineers
- Network Defense Technicians
- CND Analysts
- Security Analysts
- Security Operators
- Anyone who is involved in network operations.

Prerequisites:

N/A

CND: Certified Network Defender

Course ID #: 1275-235-ZZ-W

Hours: 35

Topics:

Module 01: Computer Network and Defense Fundamentals

- Network Fundamentals
  - Computer Network
  - Types of Network
  - Major Network Topologies
- Network Components
  - Network Interface Card (NIC)
  - Repeater
  - Hub Switches
  - Router
  - Bridges
  - Gateways
- TCP/IP Networking Basics
  - Standard Network Models: OSI Model
  - Standard Network Models: TCP/IP Model
  - Comparing OSI and TCP/IP
- TCP/IP Protocol Stock
  - Domain Name System (DNS)
  - DNS Packet Format
  - Transmission control Protocol (TCP)
    - TCP Header Format
    - TCP Services
    - TCP Operation
    - Three-way Handshake
  - User Datagram Protocol (UDP)
    - UDP Operation
  - IP Header
    - IP Header: Protocol Field
    - What is Internet Protocol v6 (IPv6)?
    - IPv6 Header
  - Internet Control Message Protocol (ICMP)
    - Format of an ICMP Message
  - Address Resolution Protocol (ARP)
    - ARP Packet Format
  - Ethernet
  - Fiber Distributed Data Interface (FDDI)
  - Token Ring
    - IP Addressing
  - Classful IP Addressing
  - Address Classes
  - Reserved IP Address
  - Subnet Masking
    - Subnetting
    - Supersubnetting
- IPv6 Addressing
    - Difference between IPv4 and IPv6
    - IPv4 compatible IPv6 Address
- Computer Network Defense (CND)
  - Computer Fundamental Attributes
  - What CND is NOT
  - CND Layers
    - CND Layers: Technologies
    - CND Layer 2: Operations
    - CND Layer 3: People
  - Blue Teaming
  - Network Defense-In-Depth
  - Typical Secure Network Design
- CND Triad
- CND Process
- CND Actions
- CND Approaches

Module 2: Network Security Threats Vulnerabilities, and Attacks

- Essential Terminologies
  - Threats
  - Vulnerabilities
  - Attacks
- Network Security Concerns
  - Why Network Security Concern Arises?
  - Fundamental Network Security Threats
  - Types of Network Security Threats

    - Where they arise from?
    - How does network security breach affects business continuity?
- Network Security Vulnerabilities
    - Types of Network Security Vulnerabilities
    - Technological Vulnerabilities
    - Configuration Vulnerabilities
    - Security Policy Vulnerabilities
    - Types of Network Security Attacks
- Network Reconnaissance Attacks
    - Reconnaissance Attacks
        - ICMP Scanning
        - Ping Sweep
        - DNS Footprinting
        - Network Range Discovery
        - Network Topology Identification
        - Network Information Extraction Using Nmap Scan
        - Port Scanning
        - Network Sniffing
        - How an Attacker Hacks the Network Using Sniffers
        - Social Engineering Attacks
- Network Access Attacks
    - Password Attacks
    - Password Attack Techniques
        - Dictionary Attack
        - Brute Forcing Attacks
        - Hybrid Attack
        - Birthday Attack
        - Rainbow Table Attack
    - Man-in-the-Middle Attack
    - Replay Attack
    - Smurf Attack
    - Spam and Spim
    - Xmas Attack
    - Pharming
    - Privilege Escalation
    - DNS Poisoning
    - DNS Cache Poisoning
    - ARP Poisoning
    - DHCP Attacks: DHCP Starvation Attacks
        - DHCP Spoofing Attack
    - Switch Port Stealing
    - Spoofing Attacks
        - MAC Spoofing/Duplicating
- Denial of Service (DoS) Attacks
- Distributed Denial-of-Service Attack (DDoS)
- Malware Attacks
    - Malware
        - Types of Malware: Trojan
        - Types of Malware: Virus and Armored Virus
    - Malware Attacks
        - Adware
        - Spyward
        - Rootkits
        - Backdoors
        - Logic Bomb
        - Botnets
        - Ransomware
        - Polymorphic Malware

Module 3: Network Security Controls, Protocols, and Devices

- Fundamental Elements of Network Security
    - Network Security Controls
    - Network Security Protocols
    - Network Security Perimeter Appliances
- Network Security Controls
    - Access Control
        - Access Control Terminology
        - Access Control Principles
        - Access Control System: Administrative Access Control
        - Access Control System: Physical Access Controls

    - Access Control System: Technical Access Controls
  - Types of Access Control
    - Discretionary Access Control (DAC)
    - Mandatory Access Control (MAC)
    - Role-Based Access
  - Network Access Control (NAC)
  - NAC Solutions
- User Identification, Authentication, Authorization and Accounting
- Types of Authentication
  - Password Authentication
  - Two-Factor Authentication
  - Biometrics
  - Smart Card Authentication
  - Single Sign-On (SSO)
- Types of Authorization Systems
  - Centralized Authorization
  - Implicit Authorization
  - Decentralized Authorization
  - Explicit Authorization
- Authorization Principles
  - Least Privilege
  - Separation of Duties
- Cryptography
  - Encryption
    - Symmetric Encryption
    - Asymmetric Encryption
  - Hashing: Data Integrity
  - Digital Signatures
  - Digital Certificates
  - Public Key Infrastructure (PKI)
- Security Policy
  - Network Security Policy
  - Key Consideration for Network Security Policy
  - Types of Network Security Policies
- Network Security Devices
  - Firewalls
  - DMZ
  - Virtual Private Network (VPN)
  - Proxy Server
    - Advantages of using Proxy Servers
    - Proxy Tools
  - Honeypot
    - Advantages of using Honeypots
    - Honeypot Tools
  - Intrusion Detection System (IDS)
  - Intrusion Prevention System (IPS)
  - IDS/IPS Solutions
  - Network Protocol Analyzer
    - How it Works
    - Advantages of using Network Protocol Analyzer
    - Network Protocol Analyzer Tools
  - Internet Content Filter
    - Advantages of using Internet Content Filters
    - Internet Content Filters
  - Integrated Network Security Hardware
- Network Security Protocols
    - Transport Layer
    - Network Layer
    - Application Layer
    - Data Link Layer
  - RADIUS
  - TACACS+
  - Kerbros
  - Pretty Good Service (PGP) Protocol
  - S/MIME Protocol
    - How it Works
    - Difference between PGP and S/MIME
  - Secure HTTP
  - Hyper Text Transfer Protocol Secure (HTTPS)

- Transport Layer Security (TLS)
- Internet Protocol Security (IPsec)

Module 4: 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
    - Enterprise Information Security Policy (EISP)
    - Issue Specific Security Policy (ISSP)
    - System Specific Security Policy (SSP)
- Internet Access Policies
  - Promiscuous Policy
  - Permissive Policy
  - Paranoid Policy
  - Prudent Policy
- Acceptable-Use Policy
- User-Account Policy
- Remote-Access Policy
- Information-Protection Policy
- Firewall-Management Policy
- Special-access Policy
- Network-Connection Policy
- Business-Partner Policy
- Email Security Policy
- Passwords Policy
- Physical Security Policy
- Information System Security Policy
- Bring Your Own Devices (BYOD) Policy
- Software/Application Security Policy
- Data Backup Policy
- Confidential Data Policy
- Data Classification Policy
- Internet Usage Policies
- Server Policy
- Incidence Response Plan (IRP)
- User Access Control Policy
- Switch Security Policy
- Intrusion Detection and Prevention (IDS/IPS) Policy
- Personal Device Usage Policy
- Encryption Policy
- Router Policy
- Security Policy Training and Awareness
- ISO Information Security Standards
  - ISO/IEC 27001:2013: Information Technology – Security Techniques-Information Security Management Systems – Requirements
  - ISO/IEC 27033: Information Technology – Security Techniques –Network Security
- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Information Security Acts
- Sarbanes Oxley Act (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- The Digital Millennium Copyright Act (DMCS)
- Federal Information Security Management Act (FISMA)
- Other Information Security Acts and Laws
  - Cyber Law in Different Countries

Module 5: Physical Security

- Physical Security
  - Need for Physical Security
  - Factors Affecting Physical Security
  - Physical Security Controls
    - Administrative Controls
    - Physical Controls
    - Technical Controls
  - Physical Security Controls
    - Location and Architecture Considerations
    - Fire Fighting Systems
    - Physical Barriers
    - Security Personnel
- Access Control Authentication Techniques
  - Authentication Techniques
  - Knowledge Factors
  - Ownership Factors
  - Biometric Factors
- Physical Security Controls
  - Physical Locks
  - Mechanical Locks:
  - Digital Locks:
  - Combination Locks:
  - Electronic/Electric/Electromagnetic Locks:
  - Concealed Weapon/Contraband Detection Devices
  - Mantrap
  - Security Labels and Warning Signs
  - Alarm System
  - Video Surveillance
  - Physical Security Policies and Procedures
- Other Physical Security Measures
  - Lighting System
  - Power Supply
- Workplace Security
  - Reception Area
  - Server/Backup Device Security
  - Critical Assets and Removable Devices
  - Securing Network Cables
  - Securing Portables Mobile Devices
- Personnel Security: Managing Staff Hiring and Leaving Process
- Laptop Security Tool: EX05
    - Laptop Tracking Tools
- Environmental Controls
  - Heating, Ventilation, and Air Conditioning
  - Electromagnetic Interference (EMI) Shielding
  - Hot and Cold Aisles
- Physical Security: Awareness/Training
- Physical Security Checklists

Module 6: Host Security

- Host Security
  - Common Threats Specific to Host Security
  - Where do they come from?
  - Why Host Security?
  - Before Configuring Host Security: Identify Purpose of each Host
  - Host Security Baselining
- OS Security
  - Operating System Security Baselining
  - Common OS Security Configurations
  - Windows Security
    - Windows Security Baselining: Examples
    - Microsoft Baseline Security Analyzer (MBSA)
    - Setting up BIOS Password
    - Auditing Windows Registry
    - User and Password Management
    - Disabling Unnecessary User Accounts
    - Configuring User Authentication
  - Patch Management

    - Configuring an Update Method for Installing Patches
    - Patch Management Tools
  - Disabling Unused System Services
  - Set Appropriate Local Security Policy Settings
  - Configuring Windows Firewall
  - Protecting from Viruses
    - Antivirus Software
  - Protecting from Spywares
    - Antispywares
  - Email Security: AntiSpammers
    - Spam Filtering Software
  - Enabling Pop-Up Blockers
  - Windows Logs Review and Audit
    - Log Review Recommendations
    - Event IDs in Windows Event Log
  - Configuring Host-Based IDS/IPS
    - Host Based IDS: OSSEC
    - Alien Vault Unified Security Management (USM
    - Tripwire
    - Additional Host Based IDSes
  - FileSystem Security: Setting Access Controls and Permission to Files and Folders
    - Creating and Securing a Windows File Share
  - Files and File System Encryption
    - EFS Limitations
    - Data Encryption Recommendations
    - DATA Encryption Tools
- Linux Security
  - Linux Baseline Security Checker: Buck-Security
  - Password Management
  - Disabling Unnecessary Services
  - Killing Unnecessary Processes
  - Linux Patch Management
  - Understanding and Checking Linux File Permissions
    - Changing File Permissions
    - Common File Permission Settings
    - Check and Verify Permissions for Sensitive Files and directories
  - Host-Based Firewall Protection with Iptables
  - Linux Log Review and Audit
    - Common Linux Log Files
    - System Log Viewer
    - Log Events to Look For
- Securing Network Servers
  - Before Hardening Servers
  - Hardening Web Server
  - Hardening Email Server: Recommendations
  - Hardening FTP Servers: Recommendations
- Hardening Routers and Switchers
  - Hardening Routers: Recommendations
  - Hardening Switches
    - Hardening Switches-Recommendations
  - Logs Review and Audit: Syslog Server
  - GFI EventsManager: Syslog Server
- Application/Software Security
  - Application Security
    - Application Security Phases
    - Application Security: Recommendations
- Data Security
  - What is Data Loss Prevention (DLP)
    - Best Practices to Prevent Data Loss
    - List of DLP Solution Vendors
    - Data Leak/Loss Prevention Tools

- Virtualization Security
  - Virtualization Terminologies
  - Introduction to Virtualization
  - Characteristics of Virtualization
  - Benefits of Virtualization
  - Virtualization Vendors
  - Virtualization Security
    - Virtualization Security Concern
  - Securing Hypervisor
  - Securing Virtual Machines
    - Implementing Software Firewall
    - Deploying Anti-Virus Software
    - Encrypting the Virtual Machines
  - Secure Virtual Network Management
    - Methods to Secure Virtual Environment
    - Virtualization Security Best Practices for Network Defenders
    - Best Practices for Virtual Environment Security

Module 7: Secure Firewall Configuration and Management

- Firewalls and Concerns
- What Firewall Does?
- What should you NOT Ignore?: Firewall Limitations
- How Does a Firewall Work?
- Firewall Rules
- Types of Firewalls
  - Hardware Firewall
  - Software Firewall
- Firewall Technologies
  - Packet Filtering Firewall
  - Circuit Level Gateway
  - Application Level Firewall
  - Stateful Multilayer Inspection Firewall
    - Multilayer Inspection Firewall
  - Application Proxy
  - Network Address Translation
  - Virtual Private Network
- Firewall Topologies
  - Bastion Host
  - Screened Subnet
  - Multi-Homed Firewall
  - Choosing Right Firewall Topology
- Firewall Rule Set & Policies
  - Build an Appropriate Firewall Ruleset
  - Blacklist vs. Whitelist
  - Example: Packet Filter Firewall Ruleset
  - Implement Firewall Policy
  - Periodic Review of Firewall Policies
- Firewall Implementation
  - Before Firewall Implementation and Deployment
  - Firewall Implementation and Deployment
  - Planning Firewall Implementation
  - Factors to Consider Before Purchasing any Firewall Solution
  - Configuring Firewall Implementation
  - Testing Firewall Implementation
  - Managing and Maintaining Firewall Implementation
- Firewall Administration
  - Deny Unauthorized Public Network Access
  - Deny Unauthorized Access Inside the Network
  - Restricting Client's Access to External Hots
- Firewall Logging and Auditing
  - Firewall Logging
  - Firewall Logs
- Firewall Anti-Evasion Techniques
- Why Firewalls are Bypassed?
- Full Data Traffic Normalization
- Data Stream-Basted Inspection
- Vulnerability-Based Detection and Blocking

- Firewall Security Recommendations and Best Practices
    - Secure Firewall Implementation: Best Practices
    - Secure Firewall Implementation: Recommendations
    - Secure Firewall Implementation: Do's and Don'ts
- Firewall Security Auditing Tools
    - Firewall Analyzer
    - Firewall Tester: Firewalk
    - FTester
    - Wingate
    - Symantec Enterprise Firewall
    - Hardware Based Firewalls
    - Software Based Firewalls

Module 8: Secure IDS Configuration and Management

- Intrusions and IDPS
    - Intrusions
        - General Indications of Intrusions
    - Intrusion Detection and Prevention Systems (IDPS)
        - Why do We Need IDPS?
- IDS
    - Role of IDS in Network Defense
    - IDS Functions
    - What Events do IDS Examine?
    - What IDSis NOT?
    - IDS Activities
    - How IDS Works?
    - IDS Components
        - Network Sensors
        - Alert Systems
        - Command Console
        - Response System
        - Attack Signature
        - Database
    - Intrusion Detection Steps
    - Types of IDS Implementation
        - Approach-Based IDS
            - Anomaly and Misuse Detection Systems
        - Behavior- Based IDS
        - Protection-Based IDS
        - Structure-Based IDS Analysis Timing Based IDS
        - Source Data Analysis Based IDS
    - IDS Deployment Strategies
        - Staged IDS Deployment
        - Deploying Network-Based IDS
    - Types of IDS Alerts
        - True Positive (Attack – Alert)
        - False Positive (No Attack – Alert)
        - False Negative (Attack – No Alert)
        - True Negative (No Attack – No Alert
        - Dealing with False Positive/Alarm
            - What should be the Acceptable Levels of False Alarms?
        - Calculating False Positive Alerts with Cisco Secure IPS
        - Dealing with False Negative
        - Excluding False Positive Alerts with Cisco Secure IPS
        - Characteristics of a Good IDS
        - IDs mistakes that should be avoided
    - IPS
        - IPS Technologies
        - IPS Placement
        - IPS Functions
        - Need of IPS
        - IDS vs. IPS
        - Types of IPS
            - Network-Based IPS
            - Host-Based IPS
            - Wireless IPS
            - Network Behavior Analysis (NBA) System

- Network-Based IPS
  - Network-Based IPS: Security Capabilities
  - Placements of IPS Sensors
- Host-Based IPS
  - Host-Based IPS Architecture
- Wireless IPS
  - WLAN Components and Architecture
  - Wireless IPS: Network Architecture
  - Security Capabilities
  - Management
- Network Behavior Analysis (NBA) System
  - NBA Components and Sensor Locations
  - NBA Security Capabilities

- IDPS Product Selection Considerations
  - General Requirements
  - Security Capability Requirements
  - Performance Requirements
  - Management Requirements
  - Life Cycle Cost
- IDS Counterparts
  - Complementing IDS
  - Vulnerability Analysis or Assessment Systems
    - Advantages & Disadvantages of Vulnerability Analysis
  - File Integrity Checkers
    - File Integrity Checkers Tools
  - Honey Pot & Padded Cell Systems
    - Honey Pot and Padded Cell System Tools
  - IDS Evaluation: snort
  - IDS/IPS Solutions
  - IDS Products and Vendors

Module 9: Secure VPN Configuration and Management

- Understanding Virtual Private Network (VPN)
- How VPN works?
- Why to Establish VNP?
- VPN Components
  - VPN Client
  - Tunnel Terminating Device
  - Network Access Server (NAS)
  - VPN Protocol
- VPN Concentrators
  - Functions of VPN Concentrator
- Types of VPN
  - Client-to-Site (Remote-Access) VPNs
  - Site-to-Site VPNs
  - Establishing Connections with VPN
- VPN Categories
  - Hardware VPN
    - Hardware VPN Products
  - Software VPNs
    - Software VPN Products
- Selecting Appropriate VPN
- VPN Core Functions
  - Encapsulation
  - Encryption
  - Authentication
- VPN Technologies
- VPN Topologies
  - Hub-and-Spoke VPN Topology
  - Point-to-Point VPN Topology
  - Full Mesh VPN Topology
  - Star Topology
- Common VPN Flaws
  - VPN Fingerprinting
  - Insecure Storage of Authentication Credentials by VPN Clients
  - Username Enumeration Vulnerabilities
  - Offline Password Cracking
  - Man-in-the-Middle
  - Attacks

- Lack of Account Lockout
- Poor Default Configurations
- Poor Guidance and Documentation

- VPN Security
  - Firewalls
  - VPN Encryption and Security Protocols
    - Symmetric Encryption
    - Asymmetric Encryption
  - Authentication for VPN Access
    - VPN Security: IPsec Server
    - AAA Server
  - Connection to VPN: SSH and PPP
  - Connection to VPN: Concentrator
  - VPN Security – Radius
- Quality of Service and Performance in VPNs
  - Improving VPN Speed
  - Quality of Service (QOS) in VPNs
  - SSL VPN Deployment Considerations
    - Client Security
    - Client Integrity Scanning
    - Sandbox
    - Secure Logoff and Credential Wiping
    - Timeouts and Re-Authentication
    - Virus, Malicious code and Worm Activity
    - Audit and Activity Awareness
    - Internal Network Security Failings
  - SLAs for VPN
  - IPVPN Service Level Management
  - VPN Service Providers
  - Auditing and Testing the VPN
    - Testing VPN File Transfer
  - Best Security Practices for VPN Configuration
    - Recommendations for VPN Connection

Module 10: Wireless Network Defense

Wireless Terminologies

- Wireless Terminologies
- Wireless Networks
  - Advantages of Wireless Networks
  - Disadvantages of Wireless Networks
- Wireless Standard
- Wireless Topologies
  - Ad-Hoc Standalone Network Architecture (IBSS – Independent Basic Service Set)
  - Infrastructure Network Topology (Centrally Coordinated Architecture / BSS – Basic Service Set)
- Typical Use of Wireless Networks
  - Extension to a Wired Network
  - Multiple Access Points
  - LAN-to LAN Wireless Network
  - 3G Hotspot
- Components of Wireless Network
  - Assess Point Wireless Cards (NIC)
  - Wireless Modem
  - Wireless Bridge
  - Wireless Repeater
  - Wireless Router
  - Wireless Gateways
  - Wireless USB Adapter
  - Antenna
    - Directional Antenna
    - Parabolic Grid Antenna
    - Dipole Antenna
    - Omnidirection Antenna
    - Yagi Antenna
    - Reflector Antenna
- WEP (Wired Equivalent Privacy) Encryption
- WPA (Wi-Fi Protected Access) Encryption
- WPA2 Encryption
- WEP vs. WPA vs. WPA2

- Wi-Fi Authentication Method
  - Open System Authentication
  - Shared Key Authentication
- Wi-Fi Authentication Using a Centralized Authentication Server
- Wireless Network Threats
  - War Driving
  - Client Mis-Association
  - Unauthorized Association
  - HoneySpot Access Point (Evil Twin) Attach
  - Rogue Access Point Attack
  - Misconfigured Access Point Attack
  - AdHoc Connection Attack
  - AP MAC Spoofing
  - Denial-of-Service Attack
  - WPA-PSK Cracking
  - RADIUS Replay
  - ARP Poisoning Attack
  - WEP Cracking
  - Man-in-the-Middle Attack
  - Fragmentation Attack
  - Jamming Signal Attack
- Bluetooth Threats
  - Leaking Calendars and Address Books
  - Bugging Devices
  - Sending SMS Messages
  - Causing Financial Losses
  - Remote Control
  - Social Engineering
  - Malicious Code
  - Protocol Vulnerabilities
- Wireless Network Security
  - Creating Inventory of Wireless Devices
  - Placement of Wireless AP
    - Placement of Wireless Antenna
  - Disable SSID Broadcasting
  - Selecting Stronger Wireless Encryption Mode
  - Implementing MAC Address Filtering
  - Monitoring Wireless Network Traffic
  - Defending Against WPA Cracking
    - Passphrases
    - Client Settings
    - Passphrase Complexity
    - Additional Controls
  - Detecting Rogue Access Points
    - Wireless Scanning:
    - Wired-Side Network Scanning
    - SNMP Polling
- Wi-Fi Discovery Tools
  - InSSIDer and NetWurveyor
  - Vistumbler and NetStumbler
- Locating Rogue Access Points
- Protecting from Denial-of-Service At5tacks: Interference
- Assessing Wireless Network Security
- Wi-Fi Security Auditing Tool: AirMagnet WiFi Analyzer
- WPA Security Assessment Tool
  - Elcomsoft Wireless Security Auditor
  - Cain & Able
- Wi-Fi Vulnerability Scanning Tools
- Deploying Wireless IDS (WIDS) and Wireless IPS (WIPS)
  - Typical Wireless IDP/IPS Deployment
- WIPS Tool
  - Adaptive Wireless IPS
  - AirDefense
- Configuring Security on Wireless Routers
- Additional wireless Network Security Guidelines

Module 11: Network Traffic Monitoring and Analysis

- Network Traffic Monitoring and Analysis (Introduction)
  - Advantages of Network Traffic Monitoring and Analysis
  - Network Monitoring and Analysis: Techniques
    - Router Based
    - Non-Router Based
  - Router Based Monitoring Techniques
    - SNMP Monitoring
    - Netflow Monitoring
  - Non-Router Based Monitoring Techniques
    - Packet Sniffers
    - Network Monitors
- Network Monitoring: Positioning your Machine at Appropriate Location
  - Connecting Your Machine to Managed Switch
- Network Traffic Signatures
  - Normal Traffic Signature
  - Attack Signatures
  - Baselining Normal Traffic Signatures
  - Categories of Suspicious Traffic Signatures
    - Informational
    - Reconnaissance
    - Unauthorized Access
    - Denial of Service
  - Attack Signature Analysis Techniques
    - Content-Based Signatures Analysis
    - Context-Based Signatures Analysis
    - Atomic Signatures-Bases Analysis
    - Composite Signatures-Based Analysis
- Packet Sniffer: Wireshark
  - Understanding Wireshark Components
  - Wireshark Capture and display Filters
  - Monitoring and Analyzing FTP Traffic
  - Monitoring and Analyzing TELNET Traffic
  - Monitoring and Analyzing HTTP Traffic
- Detecting OS Fingerprinting Attempts
  - Detecting Passive OS Fingerprinting Attempts
  - Detecting Active OS Fingerprinting Attempts
    - Detecting ICMP Based OS Fingerprinting
    - Detecting TCP Based OS Fingerprinting
  - Examine Nmap Process for OS Fingerprinting
- Detecting PING Sweep Attempt
- Detecting ARP Sweep/ARP Scan Attempt
- Detecting TCP Scan Attempt
  - TCP Half Open/Stealth Scan Attempt
  - TCP Full Connect Scan
  - TCP Null Scan Attempt
  - TCP Xmas Scan Attempt
- Detecting SYN.FIN DDOS Attempt
- Detecting UDP Scan Attempt
- Detecting 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
  - PRTG Network Monitor
- Bandwidth Monitoring
  - Bandwidth Monitoring – Best Practices
  - Bandwidth Monitoring Tools

Module 12: Network Risk and Vulnerability Management

- What is Risk?
- Risk Levels
  - Extreme/High
  - Medium
  - Low
- Risk Matrix
  - Risk Management Benefits
  - Key Roles and Responsibilities in Risk Management
- Key Risk indicators (KRI)
- Risk Management Phase
  - Risk Identification
    - Establishing Context
    - Quantifying Risks
  - Risk Assessment
    - Risk Analysis
    - Risk Prioritization
  - Risk Treatment
  - Risk Treatment Steps
  - Risk Tracking and Review
- Enterprise Network Risk Management
  - Enterprise Risk Management Framework (ERM)
  - Goals of ERM Framework
  - NIST Risk Management Framework
  - COSO ERM Framework
  - COBIT Framework
  - Risk Management Information Systems (RMIS)
  - Tools for RMIS
  - Enterprise Network Risk Management Policy
  - Best Practices for Effective Implementation of Risk Management
- Vulnerability Management
  - Discovery
  - Asset Prioritization
  - Assessment
    - Advantages of Vulnerability Assessment
    - Requirements for Effective Network Vulnerability Assessment
    - Types of Vulnerability Assessment
    - Steps for Effective External Vulnerability Assessment
    - Vulnerability Assessment Phases
    - Network Vulnerability Assessment Tools
    - Choosing a Vulnerability Assessment Tool
    - Choosing a Vulnerability Assessment Tool: Deployment Practices and Precautions
  - Reporting
    - Sample Vulnerability Management Reports
  - Remediation
    - Remediation Steps
    - Remediation Plan
  - Verification

Module 13: Data Backup and Recovery

- Introduction to Data Backup
  - Backup Strategy/Plan
  - Identifying Critical Business Data
  - Selecting Backup Media
- RAID (Redundant Array of Independent Disks) Technology
  - Advantages/Disadvantages of RAID systems
  - RAID Storage Architecture
  - RAID Level 0: Disk Striping
  - RAID Level 1: Disk Mirroring
  - RAID Level 3: Disk Striping
  - RAID Level 5: Block Interleaved Distributed Parity

- RAID Level 10: Blocks Striped and Mirrored
- RAID Level 50: Mirroring and Striping Across Multiple RAID Levels
- Selecting Appropriate RAID Levels
- Hardware and Software RAIDs
- RAID Usage Best Practices

- Storage Area Network (SAN)
  - Advantages of SAN
  - SAN Backup Best Practices
  - SAN Data Storage and Back up Management Tools
- Network Attached Storage (NAS)
  - Types of NAS Implementation
    - Integrated NAS System
    - Gateway NAS System
- Selecting Appropriate Backup Method
  - Hot Backup (Online)
  - Cold Back up (Offline)
  - Warm Backup (Nearline)
- Choosing the Right Location for Backup
  - Onsite Data Backup
  - Offsite Data Backup
  - Cloud Data Backup
- Backup Types
  - Full/Normal Data Backup
  - Differential Data Backup
  - Incremental Data Backup
  - Backup Types Advantages and Disadvantages
  - Choosing Right Backup Solution
  - Data Backup Software: AOMEI Backupper
    - Data Backup Tools for Windows
    - Data Backup Tools for MAC OS X
- Conducting Recovery Drill Test
- Data Recovery
- Windows Data Recovery Tool
  - Recover My Files
  - IASIUS Data Recovery Wizard
  - PCINSPECTPR File Recovery
  - Data Recover Tools for MAC OS X
- RAID Data recovery Services
- SAN Data Recovery Software
- NAS Data Recovery Services

Module 14: Network Incident Response and Management

- Incident6 Handling and Response
- Incident Response Team Members: Roles and Responsibilities
- First Responder
  - Network Administrators as First Responder
  - What Should You Know?
  - First Response Steps by Network Administrators
    - Avoid Fear, Uncertainty and Doubt (FUD)
    - Make an Initial Incident Assessment
    - Determining Severity Levels
    - Communicate the Incident
    - Contain the Damage: Avoid Further Harm
    - Control Access to Suspected Devices
    - Collect and Prepare Information about Suspected Device
    - Record Your Actions
    - Restrict Yourself from Doing Investigation
    - Do Not Change the State of Suspected Device
    - Disable Virus Protection
- Incident Handling and Response Process

- Overview of IH&R Process Flow
    - Preparation for Incident Handling and Response
    - Detection and Analysis
    - Classification and Prioritization
    - Incident Prioritization
    - Notification and Planning
    - Containment
        - Guidelines for Incident Containment
    - Forensic Investigation
        - Network Forensics Investigation
        - People Involved in Forensics Investigation
        - Typical Forensics Investigation Methodology
    - Eradication and Recovery
        - Countermeasures
        - Systems Recovery
    - Post-Incident Activities
        - Incident Documentation
        - Incident Damage and Cost Assessment
        - Review and Update the Response Policies
    - Training and Awareness