Certified Network Defense (CND)
Course certification training

Course Agenda

Index

Course Curriculum

Module 01: Computer Network and Defense Fundamentals

1. Network Fundamentals

- Computer Network
- Types of Network
- Major Network Topologies

2. Network Components

- Network Interface Card (NIC)
- Repeater
- Hub
- Switches
- Router
- Bridges
- Gateways

3. TCP/IP Networking Basics

- Standard Network Models: OSI Model
- Standard Network Models: TCP/IP Model
- Comparing OSI and TCP/IP

4. TCP/IP Protocol Stack

- 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

5. IP Addressing

- Classful IP Addressing
- Address Classes
- Reserved IP Address
- Subnet Masking
    - Subnetting
    - Supernetting
- IPv6 Addressing
    - Difference between IPv4 and IPv6
    - IPv4 compatible IPv6 Address

6. Computer Network Defense (CND)

- Computer Fundamental Attributes
- What CND is NOT
- CND Layers
    - CND Layer 1: Technologies
    - CND Layer 2: Operations
    - CND Layer 3: People
- Blue Teaming
- Network Defense-In-Depth
- Typical Secure Network Design

7. CND Triad

8. CND Process

9. CND Actions

10. CND Approaches

Module 02: 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 arises 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

- Reconnaissance Attacks: ICMP Scanning
- Reconnaissance Attacks: Ping Sweep
- Reconnaissance Attacks: DNS Footprinting
- Reconnaissance Attacks: Network Range Discovery
- Reconnaissance Attacks: Network Topology Identification
- Reconnaissance Attacks: Network Information Extraction using Nmap Scan
- Reconnaissance Attacks: Port Scanning
- Reconnaissance Attacks : Network Sniffing
- How an Attacker Hacks the Network Using Sniffers
- Reconnaissance Attacks : 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 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
- Spyware
- Rootkits
- Backdoors
- Logic Bomb

- Botnets
- Ransomware
- Polymorphic malware

Module 03: 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
- Types of Authentication: Two-factor Authentication
- Types of Authentication : Biometrics
- Types of Authentication : Smart Card Authentication
- Types of 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 04: 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 (SSSP)

- 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
- Wireless Network 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)
- Information Security Acts: Gramm-Leach-Bliley Act (GLBA)
- Information Security Acts: The Digital Millennium Copyright Act (DMCA) and Federal
- Information Security Management Act (FISMA)
- Other Information Security Acts and Laws
- Cyber Law in Different Countries

Module 05: 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
- Physical Security Controls: Fire Fighting Systems
- Physical Security Controls: Physical Barriers
- Physical Security Controls: Security Personnel
- Access Control Authentication Techniques
- Authentication Techniques: Knowledge Factors
- Authentication Techniques: Ownership Factors
- Authentication Techniques: 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 Portable Mobile Devices
- Personnel Security: Managing Staff Hiring and Leaving Process
- Laptop Security Tool: EXO5
- 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 06: 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: Example
  - 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
  - AlienVault Unified Security Management (USM)
  - Tripwire
  - Additional Host Based IDSes

- File System Security: Setting Access Controls and Permission to Files and Folders
- Creating and Securing a Windows file share
- File 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 Switches
- Hardening Routers: Recommendations
- Hardening Switches
- o Hardening Switches-Recommendations
- Logs Review and Audit: Syslog
- 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 07: 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

- 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
- Deploying Firewall Implementation
- Managing and Maintaining Firewall Implementation
- Firewall Administration
- Firewall Administration: Deny Unauthorized Public Network Access

- Firewall Administration: Deny Unauthorized Access Inside the Network
- Firewall Administration: Restricting Client's Access to External Host
- Firewall Logging and Auditing
- Firewall Logging
- Firewall Logs
- 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
- 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 08: 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 IDS is 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/False Negative Rate
- 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
  - Placement 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 Costs
- 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 09: Secure VPN Configuration and Management

- Understanding Virtual Private Network (VPN)
- How VPN works?
- Why to Establish VPN ?
- 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 VPNs
- 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
- IP VPN 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 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
- Access 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

- Omnidirectional Antenna
- Yagi 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 Process Using a Centralized Authentication Server
- Wireless Network Threats
- War Driving
- Client Mis-association
- Unauthorized Association
- HoneySpot Access Point (Evil Twin) Attack
- Rogue Access Point Attack
- Misconfigured Access Point Attack
- Ad Hoc 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 NetSurveyor
- Vistumbler and NetStumbler
- Locating Rogue Access points
- Protecting from Denial-of-Service Attacks: Interference
- Assessing Wireless Network Security
- Wi-Fi Security Auditing Tool: AirMagnet WiFi Analyzer
- WPA Security Assessment Tool
- Elcomsoft Wireless Security Auditor
- Cain & Abel
- Wi-Fi Vulnerability Scanning Tools
- Deploying Wireless IDS (WIDS) and Wireless IPS (WIPS)
- Typical Wireless IDS/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-based 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 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
- 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 & 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 with Parity
- 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 Backup Management Tools
- Network Attached Storage (NAS)

- Types of NAS Implementation
- Integrated NAS System
- Gateway NAS System
- Selecting Appropriate Backup Method
- Hot Backup(Online)
- Cold Backup(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
- EASEUS Data Recovery Wizard
- PC INSPECTOR File Recovery
- Data Recovery Tools for MAC OS X
- RAID Data Recovery Services
- SAN Data Recovery Software
- NAS Data Recovery Services

}**Module 14: Network Incident Response and Management**

- Incident 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