NETWORK SECURITY ADMINISTRATOR

Course: ENSA; Duration: 5 Days; Instructor-led

WHAT YOU WILL LEARN

This course looks at the network security in defensive view. The ENSA program is designed to provide fundamental skills needed to analyze the internal and external security threats against a network, and to develop security policies that will protect an organization's information. Students will learn how to evaluate network and Internet security issues and design, and how to implement successful security policies and firewall strategies. In addition, they will learn how to expose system and network vulnerabilities and defend against them.

AUDIENCE

System administrators, Network administrators and anyone who is interested in network security technologies.

PREREQUISITES

REQUIRED PREREQUISITES:

This course is a prerequisite for the CEH program.

CERTIFICATION

The ENSA 312-38 exam will be conducted on the last day of training. Students need to pass the online Prometric exam to receive the ENSA certification.

COURSE OBJECTIVES

Upon the completion of this course, students will be able to :

- Evaluate network and internet security issues and design
- Implement successful security policies and firewall strategies
- Expose system and network vulnerabilities and defend against them

COURSE OUTLINES

Module 1 - Fundamentals Of Computer Network

- Key elements of network
  - Nodes
  - The Network Backbone
  - Segments
  - Subnets
- Logical Elements of Network
  - IP Addresses
    - IP Address Space
    - Assignment of IP Address
      - Prefix Based Addressing
      - Pre Interface based Assignment
      - Virtual Addresses
      - Dynamic Addressing
      - Static Addressing
  - Domain Name System
    - Domain Names
    - Creating a new Domain Name
    - Components Of DNS
      - Domain Namensraum
      - Name servers
      - Resolver
      - Securing DNS Services
  - Gateways
    - Working of Gateway
    - Functional Categories of Gateway Devices
      - Data Gateway
      - Multimedia Gateway
      - Home Control Gateway
- Types of network media
  - Historical vs. Current communication Methodology
  - Asynchronous vs synchronous
  - Wired media or Bounded Network Media
    - Dedicated line
  - Optical remanence
  - Magnetic remanence
    - Twisted pair cable
      - Shielded Twisted Pair
      - Unshielded Twisted Pair
    - Coaxial cable or copper cable
    - Fiber-optic cable
    - Plenum and PVC cable
  - Wireless Transmission
    - Infrared transmission
    - Microwave Transmission
    - Satellite Transmission
    - Line of Sight
    - Radio frequency (e.g., bandwidth)
  - Public switched network
  - Emanations security
- Media Access Methods
  - Multiplexed Media Access
    - TDM
    - FDM
  - Polling
  - Token-Based Media Access
    - CSMA/CD
    - CSMA/CA
    - Contention Domains
  - Automated Information Systems (AIS)
    - Historical vs. Current Technology
    - Hardware
      - Distributed vs. stand-alone
      - Micro, mini, mainframe processors
      - Components
        - Input, output, central processing unit (CPU)
  - Software
  - Memory
    - Sequential
    - Random
    - Volatile vs. nonvolatile
- Critical information characteristics
  - Confidentiality

  - Integrity
  - Availability
- Information states
  - Transmission
  - Storage
  - Processing
- Operations Security (OPSEC)
  - OPSEC process
  - INFOSEC and OPSEC interdependency
  - Unclassified indicators
  - OPSEC surveys/OPSEC planning
- Object reuse(computer security)
- OSI Model
  - Physical Layer
  - Data Link Layer
  - Network Layer
  - Transport Layer
  - Session Layer
  - Presentation Layer
  - Application Layer
- Transmission Modes
  - Simplex
  - Half Duplex
  - Full Duplex
- Types of Transmission
  - Serial Data Transmission
  - Parallel Data Transmission
  - Unicast Transmission
  - Multicast Transmission
- Logical Network Classification
  - Client Server networking
  - Peer to peer networking
  - Mixed Mode Networking
- Network Topologies
  - Sharing of data
  - Sharing of devices
  - File servers
  - Bus
    - Linear Bus
    - Distributed Bus
  - Star or Hub
    - Extended Star
    - Distributed Star
  - Star-Wired ring
  - Ring
  - Mesh
  - Tree
  - Hybrid Topology
- Physical Network Classification
  - LAN
  - WAN
  - MAN
  - PAN
  - CAN
  - GAN
- Network Equipments
  - Network Interface Cards
  - Access Points
  - Switches
  - Concentrators/hub
  - Modem
  - Asynchronous vs. synchronous
  - Router
  - Brouter
  - Bridges
  - Adapters
  - Network Load Balancers
  - Repeaters
  - Gateways
  - Transceivers
  - Converters
  - Terminals

Module 2 - Network Protocols

- Introduction to protocols
- Implementing Network protocols
  - Introduction to TCP/IP
  - Configuring TCP/IP
  - Configuring Netware Links
  - Managing TCP/IP
  - Network Classes
    - Class A
    - Class B
    - Class C
    - Class D
    - Class E
  - Terminal Emulation Protocol (TELNET) of TCP/IP
  - TELNET: Vulnerabilities
  - Network News Transfer Protocol
  - Network News Transfer Protocol: Vulnerabilities
- Application Layer Protocols
  - Voice Over Internet Protocol (VoIP)
  - Boot Strap Protocol (BOOTP)
  - Data Link Switching Client Access Protocol(DCAP)
  - Dynamic Host Configuration Protocol (DHCP)
  - Domain Name System(service) Protocol (DNS)
  - File Transfer Protocol (FTP)
  - Trivial FTP (TFTP)
  - FTP and Trivial FTP: Vulnerabilities
  - Network Time Protocol
  - Network News Transfer Protocol
  - Simple Network Management Protocol(SNMP) and Its Versions
  - Internet Relay Chat Protocol(IRCP)
  - Service Location Protocol(SLP)
  - Hyper Text Transfer Protocol (HTTP)
  - Hyper Text Transfer Protocol Secure (HTTPs)
- Presentation Layer Protocol
  - Light Weight Presentation Protocol(LWPP)
- Session Layer Protocol
  - Remote Procedure Call Protocol(RPC)
- Transport Layer Protocols
  - Reliable Data Protocol(RDP)
  - Transmission Control Protocol(TCP)
  - User Datagram Protocol(UDP)
  - TCP, UDP: Attacks and Countermeasures
- Network Layer Protocols
  - Routing Protocols
    - Border Gateway Protocol(BGP)
    - Exterior Gateway Protocol(EGP)
    - Internet Protocol and its versions
    - Internet Control Message Protocol(ICMP) &V6

        - The Internet Group Management Protocol (IGMP)
        - ICMP Router Discovery Protocol(IRDP)
        - Mobility Support Protocol for IP(Mobile IP)
        - Network Address Resolution Protocol
        - Next Hop Resolution Protocol
        - Open Shortest Path First(OSPF) protocol
        - Routing Information Protocol
    - Multicasting Protocols
        - Border Gateway Multicast Protocol
        - Distance Vector Multicast Protocol
        - Internet Group Management Protocol
    - Other Network Protocols
        - The NetBEUI Protocol
        - Remote Authentication Dial-in User Service(RADIUS)
        - VoIP
- Data link Layer Protocol
    - Address Resolution Protocol(ARP)
        - Vulnerabilities and Security Measures
    - Network Address Resolution Protocol (NARP)
    - Reverse Address Resolution Protocol(RARP)

Module 3 - Protocol Analysis

- Overview of TCP / IP
    - Streams
    - Reliable Delivery
    - Network Adaption
    - Flow Control
- Relation to other Protocol
- TCP / IP Protocol Suite
    - Network Interface Layer
    - Internet Layer
    - Transport Layer
    - Application Layer
- Windowing
- Sliding Window
- Acknowledgement
- TCP
    - TCP Header Format
        - Source Port
        - Destination Port
        - Sequence Number
        - Acknowledgement Number
        - Data Offset
        - Reserved
        - Control Bits
        - Window
        - Checksum
        - Urgent Pointer
        - Options
        - Data
    - TCP Interface
        - User / TCP Interface
            - User / TCP Commands
                - Open
                - Send
                - Receive
                - Close
                - Status
                - Abort
        - TCP / Lower-Level Interface
        - TCP / Lower–Level Commands
            - Open Call
            - Listen State
            - Send Call
            - Receive Call
            - Close Call
            - Abort Call
            - Status call
    - Algorithms in TCP
        - Appropriate Byte Counting (ABC)
        - Additive Increase Multiplicative Decrease (AIMD)
        - Selective Acknowledgement (SACK)
        - TCP Friendly Rate Control (TFRC)
    - TCP Checksum Calculation
    - Performance Estimation in TCP
        - Round Trip Time Estimation
    - Problems related to TCP
        - Packet Replication
        - Checksum Error
        - Out of order data delivery
        - Bottleneck Bandwidth
        - Packet Loss
- IP
    - Overview of IP
    - IP Header Format
        - Version
        - IHL
        - Type of Service
            - Precedence
            - Delay
            - Throughput
            - Reliability
    - Total Length
    - Identification
    - Flags
    - Fragment Offset
    - Time to live
    - Protocol
    - Header Checksum
    - Source Address / Destination Address
    - Options
    - Data
- IP Addressing
- IP Datagram
    - Maximum Transmission Unit
    - Fragmentation
    - Encapsulation
    - Formatting
    - Reassembly
    - Delivery
    - Routing
    - Multicasting
    - Encapsulating Security Payload
        - Modes in ESP
            - Tunnel modes
            - Transport mode
- IPv6
- IPv6 Header
    - Version
    - Priority
    - Flowlabel
    - Payload Length
    - Next Header

- Hop limit
- Source Address
- Destination address

- IPv6 Specification
- Addressing
- Packet Tunneling
- Multicast
- Hop by Hop Option

Module 4 – Hardening Physical Security

- Need for physical security
- Security Statistics
- Physical Security Breach Incidents
  - Who is Accountable for Physical Security?
- Factors Affecting Physical Security
- Physical Security Threats
  - Environmental threats
    - Floods
    - Fire
    - Earthquakes
  - Man Made threats
    - Terrorism
    - Wars
    - Bombs
    - Dumpster Diving
  - Prevention & Detection of physical hazards
- Premises Security
  - Office Security
    - Reception Area
    - Authenticating individuals
      - Personal Access Control
        - Smart Cards
        - Proximity Cards
      - Biometrics
        - Process of Biometrics
        - Accuracy of Biometrics
        - Applications of Biometrics
          - Fingerprint Verification
          - Hand Geometry
          - Voice Recognition
          - Retina Scanning
          - Iris Scanning
            - Panasonic Authenticam
          - Facial Recognition
          - Biometric Signatures
        - Further Biometrics technology
      - Techniques for Compromising Biometrics
    - Workplace security
    - Filtered power
    - Stand-alone systems and peripherals
    - Environmental controls (humidity and air conditioning)
    - Protected distributed systems
    - Personnel Security Practices and Procedures
      - Position sensitivity
      - Employee clearances
      - Access authorization/verification (need-to-know)
      - Systems maintenance personnel
      - contractors
    - Controlling system access: Desktop security
      - Workstation security
      - Laptop Theft: Security Statistics
      - Laptop Theft
      - Laptop Security Countermeasures
      - Laptop Security Tools
      - Laptop Tracker - XTool Computer Tracker
    - Tools to Locate Stolen Laptops
    - Securing Network Devices
      - Server Security
      - Securing Backup devices
        - Physical Access to the Boot CD-ROM and Floppy Drives
    - Other equipment, such as fax, and removable media
  - CCT (Close Circuit Televisions/Cameras)
  - Parking Area
- EPS (Electronic Physical Security)
- Challenges in Ensuring Physical Security
  - Countermeasures
  - Fencing
  - Security force
  - Watch Dogs
  - Locks and Keys
  - Physical Security: Lock Down USB Ports
  - Tool: DeviceLock
  - Blocking the Use of USB Storage Devices
  - Track Stick GPS Tracking Device
  - USB Tokens
    - TEMPEST
      - shielding
      - grounding
      - attenuation
      - banding
      - filtered power
      - cabling
      - Zone of control/zoning
      - TEMPEST separation
  - Fire Safety: Fire Suppression, Gaseous Emission Systems
    - Fire Detection
    - Failures of Supporting Utilities: Heating Ventilation, Air Condition
    - Failures of Supporting Utilities: Power Management and Conditioning
  - Uninterruptible Power Supplies
- Mantrap
  - Mantrap: Diagrammatical Representation
- Physical Security Checklist

Module 5 -Network Security

- Overview of Network Security
- The need for Network Security
- The goals of Network Security
- Security Awareness
- Functions of Network Security Administrator
  - Develop, Maintain and Implement IT Security
  - Maintain and Implement Firewalls
  - Monitor and Secure Network and Servers
  - Monitor Critical System Files
  - Backup the Files

  - Administrative Security Procedural Controls
    - External marking of media
    - Destruction of media
    - Sanitization of media
    - Construction, changing, issuing and deleting passwords
    - Transportation of media
    - Reporting of computer misuse or abuse
    - Emergency destruction
    - Media downgrade and declassification
    - Copyright protection and licensing
  - Documentation, logs and journals
    - Attribution
    - Repudiation
- Communication Security (COMSEC)
  - Functions of COMSEC custodian
  - identify and inventory COMSEC material
  - access, control and storage of COMSEC material
  - report COMSEC incidents
  - destruction procedures for COMSEC material
- Functions of INFOSEC Officer
- Functions of information resources management staff
- program or functional managers
- security office
- senior management
- system manager and system staff
- telecommunications office and staff
- Functions of audit office
- Functions of OPSEC managers
- Role of end users
- Network Security at:
  - Public vs private
  - Dial-up vs dedicated
  - Privileges (class, nodes)
  - Traffic analysis
  - End-to-end access control
- Transmission Security
  - Frequency hopping
  - Masking
  - Directional signals
  - Burst transmission
  - Optical systems
  - Spread spectrum transmission
  - Covert channel control (crosstalk)
  - Dial back
  - Line authentication
  - Line-of-sight
  - Low power
  - Screening
  - Protected wireline
- Legal Elements
  - Criminal prosecution
  - fraud, waste and abuse
  - Evidence collection and preservation
  - Investigative authorities
- Countermeasures: cover and deception
  - HUMINT
  - Technical surveillance countermeasures
- Reporting security violations

Module 6 - Security Standards Organizations

- Internet Corporation for Assigned Names and Numbers (ICANN)
- International Organization for Standardization (ISO)
- Consultative Committee for Telephone and Telegraphy (CCITT)
- International Telecommunication Union (ITU)
- American National Standards Institute (ANSI)
- Institute of Electronics and Electrical Engineers (IEEE)
- Electronic Industries Association
- National Center for Standards and Certification Information (NIST)
- World Wide Web Consortium (W3C)
- Web Application Security Consortium (WASC)

Module 7 - Security Standards

- Introduction to Internet Standards
- Standards Creation Committee
- Internet Standards
  - RFC Evolution
  - Types and Submissions
  - Obtaining RFCs
- Cabling Standards
  - EIA / TIA - 568
  - UTP Categories
  - Cable Specifications
  - Electronic Industries Association
- Specification Standards

Module 8 - Security Policy

- Security Policy Overview
- Concept of Security Policy
- Key Security Elements
- Security Awareness Programs
  - Trainings
  - Meetings
  - Goals of Security Policies
- Vital Role of a Security Policy
- Classification of Security Policy
  - User Policies
    - Password Management policy
    - IT Policies
  - General Policies
  - Partner Policies
  - Types of Security Policies : Issues Specific Policies
  - Policy Design
- Contents of Security Policy
- Privacy and Confidentiality
- Security Levels
  - Separation of Duties, Dual Controls and Job Rotation
  - Security Organization and Policy Development
- Agency Specific AIS and Telecommunications Policies
  - Points of contact
  - References
- Configuration of security policy
- National Policy and Guidance
  - AIS security

  - Communications security
  - Employee accountability for agency information
- Implementation of security policy
- Incident Handling and Escalation Procedures
- Security operations and life cycle management
  - Securing Assets
  - Requirements definition (e.g architecture)
  - Development
  - Design review and systems test
  - Demonstration and validation (testing)
  - Implementation
  - Security (e.g certification and accreditation)
  - Operations and maintenance (e.g configuration management)
- Defining Responses to Security Violations
- Presenting and Reviewing the process
- Compliance with Law and Policy
  - Intellectual Property
  - Describing the Electronic Communications Privacy Act
- Transborder encryption issues
- Points to remember while writing security policy
- Issues-specific security policy (ISSP)
  - E-mail Security Policies
  - Hacking
- Creating and managing ISSPs

Module 9 – IEEE Standards

- Introduction to IEEE standards
- IEEE LAN Protocol Specification
  - 802-Overview And Architecture
  - 802.1-Briding And Management
  - 802.2-Logical Link Control(LLC)
  - 802.3-CSMA/CD(Ethernet)
  - 802.4-Token Passing Bus
  - 802.5-Token Passing Ring
  - 802.6-DQDB Access Method
  - 802.7-Broad Band LAN
  - 802.10-Security
  - 802.11-Wireless LAN(WLAN)
  - 802.12-Demand Priority Access
  - 802.15-Wireless Personal Area Networks (WPAN)
  - 802.16-Broad Band Wireless MAN (WMAN)
  - 802.17-Resilliant Packet Ring Work Group
- Wireless Networking Standards
  - IEEE Standards
  - 802.1X
  - 802.11 Architecture
  - 802.11 Standards (Wi-Fi Standard)
    - 802.11a
    - 802.11b
    - 802.11e
    - 802.11g
    - 802.11h
    - 802.11i standards
    - 802.11n
  - 802.15
  - 802.16
  - Wi-MAX
  - IEEE p1451 Standard
  - ETSI Standards
  - HIPERLAN
  - HIPERMAN

Module 10 - Network Security Threats

- Current Statistics
  - Defining Terms : Vulnerability, Threats and Attacks
- Types of Attackers
- Classification of Hackers
- Techniques
  - Spamming
  - Revealing Hidden Passwords
  - War Dialing
  - War Diving
  - War Chalking
  - War Flying
  - Wire Tapping
  - Scanning
    - Port Scanning
    - Network Scanning
    - Vulnerability Scanning
  - Sniffing
    - Active Sniffing
    - Passive Sniffing
  - Network Reconnaissance
  - Social Engineering
- Common Vulnerabilities and Exposures (CVE)
  - Threats
  - Trojan
  - Virus
    - IRC Bot
  - Worms
  - Logic Bombs
  - Eavesdropping
  - Phishing
- Attacks
  - Smurfing
  - Man-in-the-Middle Attacks
  - Denial of Service
  - DDoS
  - Buffer Overflow
  - Zero Day Attacks
  - Jamming
  - Password Attacks
    - Brute Force Password Attacks
  - Spoofing
  - Session Hijacking
  - Web Page Defacement
  - Recording Key Strokes
  - Cracking Encrypted Passwords
  - Revealing Hidden Password
- Hiding Evidence of an Attack
- Problems Detecting Network Attacks
- Network Scanning Tools :
  - The Netstat Tool
  - Nmap
  - NetscanTool
  - Superscan
  - hping

Module 11 - Intrusion Detection System (IDS) And Intrusion Prevention

Systems (IPS)

- Introduction to IDS
- History of Intrusion Detection
- Intrusion Detection Concepts
  - Architecture
  - Monitoring Strategies
  - Analysis Type
  - Timing
  - Goal of Detection
  - Control Issues
- IDS for an Organization
  - Selecting an IDS
  - Deploying an IDS
  - Maintaining an IDS
- Characteristics of IDS
  - Importance of IDS
- Aggregate Analysis with IDS
- Types of IDS
  - Network based IDS
    - NIDS Architecture
      - Traditional Sensor-Based
      - Distributed Network Node
    - Operational Concept
      - Tip off
      - Surveillance
      - Forensic Workbench
    - Network-Based Detection
      - Unauthorized Access
      - Data Resource Theft
      - Denial of Service
      - Password Download
      - Malformed Packet
      - Packet Flooding
    - Tool : NetRanger
    - Tool : Bro
    - Tool : Arpwatch (in Linux)
    - Tool : Psad (in Linux)
    - Tool : ippl (in Linux)
  - Host Based IDS
    - HIDS Architecture
      - Centralized Host Based
      - Distributed Real Time Host Based
    - Operational Concept
      - Tip Off
      - Surveillance
      - Damage Assessment
      - Compliance
    - Host Based Detection
      - Abuse of Privilege Attack Scenarios
      - Critical data Access and Modification
      - Changes in Security Configuration
    - Tool : Host Sentry
    - Tool : KFSensor
    - Tool : LIDS
    - Tool : SNARE
    - Tool : Tiger(in Linux)
  - Host Based IDS vs Network Based IDS
  - The Hybrid IDS Framework
    - Prelude IDS
      - Components
      - Interaction between Prelude components
        - Relaying
        - Reverse Relaying
        - Tool: Libasfe
  - Distributed IDS
    - Introduction and Advantages
    - Components
  - Protocol Intrusion Detection System
  - Network Behavior Analysis (NBA)
  - Unified Thread Management
- Deployment of IDS
- Types of Signatures
  - Network Signatures
  - Host Based Signatures
  - Compound Signatures
- True / False-Positive / Negative
- Major Methods of Operation
  - Signature Based Detection
  - Anomaly Based Detection
- IDS Tool
  - Snort
  - BlackICE
  - M-ICE
  - Secure4Audit (auditGUARD)
  - Emerald
  - Nides
  - SECUREHOST
  - GFI EventsManager
- Intrusion Prevention System
  - Intrusion Prevention Strategies
  - IPS Deployment Risks
  - Flexible Response with Snort
    - Snort Inline Patch
  - Controlling your Border
- Information Flow in IDS and IPS
  - Raw Packet Capture
  - Filtering
  - Packet Decoding
  - Storage
  - Fragment Reassembly
  - Stream Reassembly
  - Stateful Inspection of TCP Sessions
  - Firewalling
- IPS Tool
  - Sentivist
  - StoneGate IPS
  - McAfee
- IDS Vs IPS
- Intrustion Detection Checklist

Module 12 - Firewalls

- Firewalls : Introduction
- Security Features
  - Securing Individual Users
  - Perimeter Security for Networks
- Multiple Components of Firewall
- Firewall Operations
- Software Firewall
- Hardware Firewall
- Types of Firewalls
  - IP Packet Filtering Firewall
  - Circuit-Level Gateway
  - Application Level Firewalls
- Pix Firewall
- Basic features of PIX firewall

- Advanced Features of PIX firewall
- Firewall Features
- Establishing Rules and Restrictions for your Firewall
- Firewall Configuration Strategies
- Scalability
- Productivity
- Firewall Architecture
  - Dual-Homed Host Architecture
  - Screened Host Architecture
  - Screened Subnet Architecture
- Handling Threats and Security Tasks
- Protection against Hacking
- Centralization and Documentation
- Multi-Layer Firewall Protection
- Firewall Deployment Strategies
  - Screened Host
  - Two router with One Firewall
  - Introduction to Demilitarized Zone (DMZ)
  - DMZ Screened Subnet
  - Multi Firewall DMZ
    - Two Firewalls, One DMZ
    - Two Firewalls, Two DMZ
  - Screening Router
  - Dual Homed Host
- Specialty Firewalls and Reverse Firewalls
- Advantages of using Firewalls
- Disadvantages of using Firewalls
- Threats
  - Firewalking
  - Banner Grabbing
  - Placing Backdoors through Firewalls
- Limitations of Firewalls
- Personal Firewall Software
  - ZoneAlarm Pro
  - Norton Personal Firewall
  - McAfee Personal Firewall
  - Windows Personal Firewall
- Personal Firewall Hardware
  - Linksys and Netgear
  - Cisco's PIX
- Firewall Log Analysis
  - Firewall Analyzer
    - Firewall Logs
    - Automatic Firewall Detection
    - Firewall Log Import
    - Firewall Log Archiving
  - Firewall Tools
    - Firewall Builder
    - Wflogs
- Comparison of various Firewall Products
- T-REX Open Source Firewall
- SQUID
- WinGate
- Symantec Enterprise Firewall
- Firewall Testers
  - Firewalk
  - FTester
  - Firewall Leak Tester

Module 13 - Packet Filtering And Proxy Servers

- Application Layer Gateway
  - Network Address Translation
  - Packet Filtering
    - Approaches
    - Packet Sequencing and Prioritization
    - Packet Fragmentation
    - Analyzing Packet Fragmentation
    - Analyzing Packet Signatures
      - Signature Analysis
      - Common Vulnerabilities and Exposure
      - Signatures
      - Normal Traffic Signatures
      - Abnormal Traffic Signatures
    - IP Header
    - Configuring
    - Types of Filtering
      - Stateful Packet Filtering
      - Stateless Packet Filtering
      - Dynamic Packet Filtering
    - Filtering Rules
    - Advantages / Disadvantages of filtering
    - Flags used
      - TCP
        - Urgent Flag
        - Ack Flag
        - Push Flag
        - Reset Flag
        - Syn Flag
        - Fin Flag
      - UDP
        - Control Flag
- Proxy Servers
  - Role of Proxy Server
    - Routed Environment
    - Network Environment
    - Blocking URLs and unblocking URLs
  - Proxy Control
    - Transparent Proxies
    - Non-transparent Proxies
    - Socks Proxy
  - Authentication Process
    - Authentication Configuration
      - Types of Authentication
  - Firewall
    - Firewalls based on Proxy
  - Administration and Management of Proxy Servers
  - Security and Access Control
  - Reverse Proxies
  - How Proxy Servers differ from Packet Filters

Module 14 - Bastion Host And Honeypots

- Bastion Hosts
  - Principles
  - Need of Bastion Host
  - Building a Bastion Host
    - Selecting the Host Machine
      - Memory Considerations
      - Processor Speed
      - Selecting the OS
  - Configuring Bastion Host
  - Locating Bastion Host
    - Physical Location
    - Network Location

        - Configuring Bastion Host
        - Making the Host Defend itself
        - Securing the Machine itself
        - Making the Host Defend itself
    - Selecting Services to be provided
        - Special Considerations for UNIX System
    - Disabling Accounts
    - Disabling Unnecessary Services
    - Limiting Ports
    - Handling Backups
    - Role of Bastion host
    - Bastion Host Security Policy
- Honeypot
    - History of Honeypot
    - Value of Honeypot
    - Types of Honeypots
        - Production
        - Research
    - Classifying Honeypots by Interaction
        - Low-Interaction Honeypots
        - Medium-Interaction Honeypots
        - High-Interaction Honeypots
    - Examples of Honeypots
        - Backofficer Friendly
        - Specter
        - Honeyd
        - Homemade
        - Mantrap
        - Honeynet
    - Use of Honeypot
        - Preventing Attacks
        - Detecting Attacks
        - Responding to Attacks
    - Homemade Honeypot
        - Port Monitoring Honeypots
        - Jailed Environment
        - Mantrap
    - Advantages and Disadvantages of Honeypot
- Honeynet
    - Architecture of Honeynet
    - Types of Honeynet
        - Distributed Honeynet
        - GEN I Honeynet
        - Gen II Honeynet
        - Virtual Honeynet
    - Legal Issues Related

Module 15 - Securing Modems

- Introduction to Modems
- Origin of Modems
- Modem Features
- Types of Modems
    - Hardware Modems
        - Internal Direct Connect Modem
    - Advantages and Disadvantages of Internal Direct Modem
        - External Direct Connect Modem
    - Advantages and Disadvantages of External Direct Modem
    - Optical Modems
    - Short Haul Modems
    - Smart Modem
    - Controller Less Modem
    - Acoustic Modem
        - Advantages and Disadvantages of Acoustic Modem
    - Null Modems
- Modem Security
    - Additional Security to Modems
        - Password Modems
        - Callback Modems
        - Encrypting Modems
        - Caller-ID and ANI Schemes
    - Modem Security should be a priority for the Telephony Managers
    - SecureLogix provides Solutions for Modems Security
    - Make Modem Security simple with Robust Management Tool
- Categorizing Modem Access
    - Dial Out Access
    - Dial In Access
- Modem Attacks
    - Spoofing Attacks
    - Call Forwarding Attacks
    - War Dialing
- Modem Risks
    - War Dialers
    - Packet Sniffing
- Modem Failure Symptoms
    - Modem Firmware Failure
    - Primary Modem Failure
    - Reasons for modem Connection Failure
        - Modem Incompabilities
        - Buggy Modem Firmware
        - Bad Phone line
        - Misconfigured modems or communication software
        - Temporary Modem Failures
    - Some common Failures
        - Modem Not Responding
        - Modem Damaged
        - Modem Not Compatible
- Troubleshooting Modems
    - External Modems
    - Internal Modems

Module 16 - Troubleshooting Network

- Introduction to troubleshooting
- A Troubleshooting Methodology
    - Troubleshooting Strategies
        - Recognizing Symptoms
        - Understanding The Problem
            - System Monitoring Tools
                - Network Monitor
                - Performance Monitors
                - Protocol Analyzer
                - The Protocol Analysis Process
            - Testing the Cause of the problem
        - Solving Problem
    - Device Manager
    - Troubleshooting Network Communication
        - Identifying Communication Problems
        - Using Ping and Traceroute
        - Exploring Network Communications
        - Find Path Information

        - Access point Interface
        - Identify Communication Capabilities
        - Load balancing
            - Configuration Best Practices for windows 2000,windows Server
                - General consideration
                - Security ad Manageability
                - High Availability
            - Troubleshooting Network Load Balancing
            - Problems and Solutions
        - How to isolate networking problems (Windows XP): Network Adapter
            - Network adapter is unplugged
    - Network adapter has limited or no connectivity
    - Network adapter is connected, but you can't reach the Internet
    - Troubleshooting Connectivity
        - Causes for connectivity Problem
        - Troubleshooting Physical Problems
        - Troubleshooting Link Status
        - Physical Troubleshooting Tools
        - Troubleshooting the Topology
        - Troubleshooting the Fault Domain
        - Tracing connectivity
            - ipconfig
    - Performance Measurement Tool
        - Host Monitoring Tool
        - Point Monitoring tool
        - Network Monitoring Tool
- Troubleshooting Network devices
    - Windows PC Network Interface Card
    - Troubleshooting Cisco Aironet Bridge
    - Troubleshooting bridges using the Virtualization Engine
    - Troubleshooting BR350 (Bridge)
    - Diagnosing Repeater and Gateway Problems
    - Troubleshooting Hubs and Switches
    - Troubleshooting cable modem
    - Troubleshooting DSL or LAN Internet Connection
    - Troubleshooting a Universal Serial Bus Device
    - Troubleshooting IEEE 1394 Bus Devices
- Troubleshooting Network Slowdowns
    - NetBios Conflicts
    - IP Conflicts
    - Bad NICs
    - DNS Errors
    - Insufficient Bandwidth
    - Excessive Network Based Application
    - Daisy Chaining
    - Spyware Infestation
- Troubleshooting Wireless devices
    - Checking the Led Indicators
    - Checking Basic setting
    - SSID
    - WEP Keys
    - Security Settings
- Troubleshooting Methodology
- TCP/IP Troubleshooting Utilities
    - Troubleshooting with IP Configuration Utilities
    - Troubleshooting with Ping
    - Troubleshooting with Tracert
    - Troubleshooting with Arp
    - Troubleshooting with Telnet
    - Troubleshooting with Nbstat
    - Troubleshooting with Netstat
    - Troubleshooting with FTP
    - Troubleshooting with Nslookup
    - Troubleshooting NTP
    - Troubleshooting Tools
    - Hardware-Based Troubleshooting Tools
    - Network Technician’s Hand Tools
    - The POST Card
    - Memory Testers
    - Electrical Safety Rules
    - Wire Crimpers
    - Punch Down Tools
    - Circuit Testers
    - Voltmeters
    - Cable Testers
    - Crossover Cables
    - Hardware Loopback Plugs
    - LED Indicator Lights
    - Tone Generators

Module 17 - Hardening Routers

- Introduction to Routers
- Routing Metrics
- Multiple Routing
- Types of Routers
- Routing Algorithms
- Internet Work Operating Systems (IOS)
- IOS : Features
- Routing Principles
    - The ARP Process
    - LAN– to-LAN Routing Process
    - LAN–to-WAN Routing Process
- Modes Of Operation
    - User Mode
    - Enable Mode
    - Global Configuration MODE
- IP Routing
    - Configuring IP and IP routing
    - Configuring RIP
- IP Source Routing
- Configuration of Routers
    - External Configuration Sources
    - Internal Configuration Sources
    - Router Initiation
    - Loading the Configuration Files
    - Configuring from the TFTP Server
    - The setup Configuration Mode
    - CLI Configuration Mode
- Router Configuration Modes
    - Global Configuration Mode
    - Interface Configuration Mode
    - Line Configuration Mode
    - Privilege EXEC Mode
    - ROM Monitor Mode
    - User EXEC Mode
- Finger Tool
- Disabling the Auxiliary and Closing extra Interfaces
- BOOTp Service
- TCP and UDP Small Servers
- Disabling Proxy ARP

- Disabling SNMP
- Disabling NTP
- Hardening a Router
  - Configuring a Banner
    - Passwords and Secrets
    - Encrypting Passwords
    - Creating End User Accounts
    - Setting Session Time-Out Periods
- Cisco Discovery Protocol
  - Configuring CDP
  - Logging Concept
    - Log Priority
    - Configuring Logging
    - Timestamping
  - Cisco Logging Options
    - Console Logging
    - Buffered Logging
    - Terminal Logging
    - Syslog Logging
    - SNMP Logging
- Filtering Network Traffic
- Access Control List
  - Basics of ACL
  - Creating Access Control List
  - ACl Types
  - Monitoring ACL
  - Implementing ACL
  - Securing Routers : ACL
- Log System Error Messages
- Securing Routers : Committed Access Rate
- Securing Routers : Secure Shell
  - Authentication Methods
  - Configuring SSH
  - Default Locations of Secure Shell Files
    - Generating the Host Key
    - Ciphers and MAC's
    - Compression
    - Configuring Root Logins
    - Restricting User Logins
- Router Commands
  - Configuring Router Interface Setting
  - Managing Router Configuration
  - Reviewing IP Traffic and Configuring Static Routers
- Types of Routing
  - Distance Vector Routing
  - Link State Routing
- Routing Protocols
  - Routing Information Protocol (RIP)
  - Interior Gateway Routing Protocol (IGRP)
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
  - Open Shortest Path First (OSPF)
  - Border Gateway Protocol (BGP)
- Routing Table Maintenance Protocol (RTMP)
- Troubleshooting a Router
  - Troubleshooting Tools
  - Troubleshooting with Network Management Tools
  - Troubleshooting IP Connectivity in Routers
- Components of Router Security
- Router Security : Testing Tools

Module 18 - Hardening Operating Systems

- BIOS Security
- Windows Registry
  - Registry Editor
  - Rootkit Revealer
- Configuring Windows Services
  - E-mail Services
  - Regional Settings
  - Virtual Servers
  - Share Point Portal Server
  - Antivirus Protection
  - Process
- Resource Access
  - Managing Access control
  - Resource Access Privileges
  - Access Lists
  - Need-to-know controls
  - Malicious logic protection
  - Assurance
- Discretionary Access Control List (DACL)
- Objects and Permissions
- Rights vs Permissions
- NTFS File System Permissions
- Encryption File System
- Windows Network Security
  - Firewalls
- Modes of Operation (Describes the security conditions under which the system actually functions)
  - Dedicated security mode
  - System-high security mode
  - Compartmented security mode
  - Multilevel security mode
- AIS
  - Hardware
  - Software
  - Firmware
- Windows infrastructure features
  - Active Directory
  - Group Policy
  - Share Security
  - Dynamic DNS updates
- Kerberos Authentication And Domain Security
- Trust Relationships Between Domains
- IP Security
  - Problems With IP Security
- Windows Security Tools
  - Update System
  - Antivirus
  - Anti Spyware
  - Anti Spam
- Windows
  - Windows Server 2003
    - Windows 2003 Infrastructure Security
    - Windows 2003 Authentication
    - Windows 2003 Security Configuration Tools
    - Windows 2003 Resource Security
    - Windows 2003 Auditing and Logging
    - Windows 2003 EFS
    - Windows 2003 Network Security
- Windows Certificate Authorities
- Certificate Authority Requirements

- Implement Microsoft Certificate Authorities
- Implement a Microsoft Enterprise Root CA

- Desktop Management
  - Concept of least privilege
  - Internal labeling
  - Troubleshoot User Logons
  - Troubleshoot User Configuration
  - Troubleshoot System performance
- File Management
  - Troubleshooting Access to Files And Folders
  - Troubleshooting Access to Shared Files And Folders
- Linux
  - User and File system Security Administration
    - Security
      - Data Security
      - Network Security
    - OS Security Measures
      - Linux Update Agent
      - Configuring Unix Services
      - Guest Account
      - User Account
      - etc/password fields
      - etc/shadow fields
      - etc/gshadow
      - etc/group
    - File System and Navigation
    - File And Directory Permissions
      - Default Directories
    - Network Interface configuration
    - Security Scripting
- Pluggable Authentication Module
  - Configuring PAM
  - Pam Configuration Files
  - PAM Framework
  - Security With PAM
- Network Information Services
- Group Management Utilities
- Permission Management Tools
- System Logger Utility
- Unix Security
  - UNIX Security Checklist v2.0
- Macintosh Security
- Vista security
  - Upgrading from XP to Windows Vista
  - Installing Windows Vista
  - Securing Windows Vista

Module 19 - Patch Management

- Introduction
- The Patch Concept
- Patch Testing
- Patch Monitoring and Management
  - Create a Change Process
  - Monitor the Patch Process
- Consolidating Patches on Red Hat Network
  - Configuring the Proxy Server
  - Configuring the Proxy Client
- Red Hat Up2date Patch Management Utility Installation Steps
- Red Hat Up2date Patch Management : Command Line Interface
  - Security Patch Compliance
  - Distribution
  - Discovery and Zero-Touch Inventory
  - Client Adoption
  - Troubleshoot Security Patch Management
- Reporting
- Patch Management Process
  - Identification
  - Assessment Phase
    - Inventory
    - Base Lining
  - Obtainment
  - Testing
  - Deploy Phase
    - Deployment Preparation
    - Deployment of the Patch
  - Confirmation
- Windows Update Services
  - Microsoft Software Update Services (SUS)
  - Windows Server Update Services (WSUS)
  - WSUS VS SMS 2003
  - Role of SMS in Patch Management Process
- Microsoft Patch Management Tool : Microsoft Baseline Security Analyzer
  - MBSA : Scanning Updates in GUI Mode
  - MBSA : Scanning Updates in Command-Line version
- Patch Management Tool
  - Selecting a Tool
    - Learning Curve
    - Platform Support
    - System Targeting
    - Ease of Use
    - Connection Sensitivity
    - Deployment Schedule
    - Cost
  - Patch Management Tools
    - Microsoft Baseline Security Analyzer
    - Qchain
    - BES Patch Management
    - Shavlik HFNetChkPro 5
    - PatchLink Update
    - SecureCentral™ PatchQuest

Module 20 - Log Analysis

- Introduction to Log Analysis
- Overview of log analysis
- Audit Events
- Log Files
  - Apache Logs
  - IIS Logs
    - IIS Logger
- Limitations of log files
- Monitoring for Intrusion and Security Event
  - Importance of Time Synchronization
  - Passive Detection Methods
    - EventCombMT
    - Event Collection
  - Scripting
- Log Analysis Tools
  - UserLock
  - WSTOOl
  - Auditing tools
    - ASDIC

        - Tenshi
        - SpoofMAC
        - Gentle MAC PRO
        - Log Manager
    - Generic Log Parsing Tools
        - LogSentry
        - SL2
        - Flog
        - Simple Log Clustering Tool(SLCT)
        - xlogmaster
        - GeekTool (mac O.S)
        - Dumpel.exe (Windows O.S)
        - Watchlog
        - LogDog
    - Log File Rotation Tools
        - LogController
        - Newsyslog
        - Spinlogs
        - System Log Rotation Service(SLRS)
        - Bzip2
- How to Secure Logs(Log Security)
    - Limit Access To Log Files
    - Avoid Recording Unneeded Sensitive data
    - Protect Archived Log Files
    - Secure The Processes That Generate the Log Entries
    - Configure each log source to behave appropriately when logging errors occur
    - Implement secure mechanisms for transporting log data from the system to the centralized log management servers
- Inc setting up of Servers: IIS & Apache

Module 21 -Application Security

- Importance of Application Security
- Why is Web Security so Difficult?
- Application Threats and Counter Measures
- Application dependent guidance
- Web Applications
    - Managing Users
    - Managing Sessions
        - Cookies
            - What is in a Cookie
            - Working of a Cookie
            - Persistent vs Non-Persistent
            - Secure vs Non-Secure
        - Session Tokens
            - Session Tokens
            - Authentication Tokens
    - Encrypting Private Data
    - Event Logging
        - What to Log?
        - Log Management
- System Life Cycle Management
    - Acquisition
    - Design review and systems test performance (ensure required safeguards are operationally adequate)
    - Determination of security specifications
    - Evaluation of sensitivity of the application based upon risk analysis
    - Management control process (ensure that appropriate administrative, physical,and technical safeguards are incorporated into all new applications and into significant modifications to existing applications)
    - Systems certification and accreditation process
- Telecommunications Systems
    - Hardware
    - Software
    - Vulnerability and threat that exist in a telecommunications system
    - Countermeasures to threats
- Securing voice communications
- Securing data communications
- Securing of keying material
- Transmission security countermeasures (e.g., callsigns, frequency, and pattern forewarning protection)
- Embedded Application Security (EMBASSY)
    - TCP/IP security Technology
    - IPSec And SSL Security
    - IPSec And SSL Security In Embedded Systems
    - Network Security For Embedded Applications
    - Embedded Network Security Hardware Instructions
- Secure Coding
    - Common Errors
        - Buffer Overflow
        - Format String Vulnerabilities
        - Authentication
        - Authorization
        - Cryptography
    - Best Practices For Secure Coding
        - Distrust User Input
        - Input Validation
        - Magic Switches
        - Malicious Code Detection
    - Programming standards and controls
    - Change controls
    - internal labeling
    - Threat modeling

Module 22 - Web Security

- Overview of Web Security
- Common Threats on Web
    - Identity Theft
    - Spam Mail
    - Distributed Denial of Service (DDoS)
    - Reflection Dos Attack
    - Bots
    - Cross Site Request Forgery
    - Session Hijacking
    - Smurf Attack
    - FTP Bounce
    - RSS / Atomic Injection
    - DNS Attack
    - Content Spoofing
    - Logical Attacks
    - Buffer Overflow
    - IP and Routing Protocol Spoofing
- Identifying Unauthorized Devices
- Restrictive Access
- Network Addresses
    - Altering the Network Addresses
- Tracking the Connectivity : Tracert / Traceroute

- Testing the Traffic Filtering Devices
- IIIS Server
  - Installing the IIS server
  - Administering the IIS server
- Client Authorization
  - Certificate Authorities
- Client-Side Data
- Server-side data
- Client Authentication
  - User's Approach
  - Authentication Techniques
- Input Data Validation
- Browsing Analysis
- Browser Security
  - Mozilla Browser
  - Internet Explorer
    - Security Setting of Internet Explorer
      - Configuring Security Zone
      - Setting up the Internet Zone
      - Setting up the Intranet Zone
      - Setting up Trusted and Restricted Sites Zone
      - Working with Domain Name Suffixes
      - Selecting Custom Level Settings
      - Miscellaneous Options
      - User Authentication
  - Browser Hhijacking
    - Preventing
    - Restoring
    - Tools :
      - Stringer
      - Download Cwshredder
      - 14.3.3.3. Microsoft Anti Spyware Software
  - Browser Analysis
    - Browser Behavior Analysis
    - Benefits of Behavior Analysis
  - Browser Security Settings
    - Dynamic Code
    - Securing Application Code
- Plug-Ins
  - Netscape / IE Plug-Ins
    - Image
      - IPIX
    - VRML
    - Audio
    - Multimedia
      - Shockwave
      - Real Player
      - Shockwave Flash
      - Quick Time
    - Util
      - Net Zip Plug-in
      - Asgard Plug-in Wizard
      - Neptune
    - Others
      - Java Plug-In
  - Mozilla Firefox Plug-Ins
    - Acrobat Reader
    - Adobe Flash Player
    - Java
    - Quick Time
    - RealPlayer
    - Shockwave
    - Windows Media player
    - The Validate HTML Plug-Ins
  - Accessibility Analyzer
  - Validate Sites HTML
  - Wayback Versions
  - Validate P3P
  - View In
  - BugMe Not
  - Webpage Speed Report
  - Validate Links (W3C)
  - Open Text
  - Validate RSS
  - Validate CSS
  - Validate HTML
- Common Gateway Interface (CGI)
  - CGI Script
    - CGI Mechanism
    - Web Servers
    - Mechanisms and Variables
    - Third part CGI Scripts
    - Server Side Includes
  - CGI Operation
    - Responding to the Client
    - Using the Client to call a CGI Application

Module 23 - E-Mail Security

- Overview of E-mail
- History of E-mail
- Basics of E-Mail
- Types of E-Mail
- Web Based vs POP3 E-mail
- Components of an Email
  - Headers
    - Working of an E-Mail Header
      - Examining an E-Mail Header
      - Reading E-Mail Headers
  - Opening Attachments
  - Reading E-Mails for Different Clients
  - Field Names and Values
  - Address List
  - Recipients and Senders
  - Response Targets and Threading
- E-Mail Servers
- E-Mail Encryption
  - Centurion Mail
  - Kerberos
  - Hush Mail
  - Pretty Good Privacy
  - Secure Hive
- Installing WorkgroupMail
- Configuring Outlook Express
- Secure Email
- Certificate Revocation
- E-mail Authentication
  - Mail Transfer
  - Authenticating Sender
- E-mail Protocols
  - Multipurpose Internet Mail Extensions (MIME) /Secure MIME
  - Pragmatic General Protocol (PGP)
  - Simple Mail Transfer Protocol (SMTP)
  - Post Office Protocol (POP) and its POP3

        - SMTP : Vulnerabilities
    - Internet Message Access Protocol (IMAP)
- Client and Server Architecture
- E-Mail Security Risks
    - Spoofed Addresses
    - Spam
    - Hoaxes
    - Phishing
    - Snarfing
    - Malware
    - E-Mail Spoofing
    - E-Mail Viruses
    - Gateway Virus Scanners
    - Outlook Viruses
    - E-mail Attachment Security
    - E-Mail Spamming
        - Protecting against Spam
        - Spam Filters
    - E-Mail Bombing, Chain Letters
- How to Defend against E-Mail Security Risks
    - Quarantining Suspicious Email
    - Vulnerability check on Email System
- Tools for E-mail Security
    - ClipSecure
    - CryptoAnywhere
    - BCArchive
    - CryptainerLE
    - GfiMailEssentials
    - SpamAware
- Tracking E-mails
    - readnotify

Module 24 – Authentication : Encryption, Cryptography And Digital Signatures

- Authentication
    - Authentication Tokens
    - RSA SecurID
    - Smart Cards
- VeriSign Authentication
- Encryption
    - Encryption Systems
    - Firewalls Implementing Encryption
    - Lack of Encryption
    - Cost of encryption
    - Preserving Data Integrity
    - Maintaining Confidentiality
    - Authentication and Identification
    - Authenticity of N / W Clients
    - Key Based Encryption Systems
        - Symmetric Key
        - Public Key
    - Encryption Algorithms
        - RSA Algorithm
            - Performing RSA Encryption and Decryption
            - Create your RSA Key Pair
            - Creating RSA Keys
        - Diffie Hellman Algorithm
            - Finding Diffie-Hellman Public Keys
        - DSS and DSA
        - ELGAMAL
        - RC2 and RC4
        - IDEA
        - SNEFRU
        - RIPE-MD
        - HAVAL
        - SKIPJACK
        - XOR
        - BLOWFISH
        - camellia
        - Cast Encryption Algorithm
        - Tiny Encryption Algorithm
        - SCA : Size-Changing Algorithms
    - Analyzing Popular Encryption Schemes
        - Symmetric vs Asymmetric Encryption
        - Symmetric Key Encryption
        - Asymmetric Key Encryption
        - Hashing
        - PGP
        - X.509
        - SSL
    - Types of Encryption Algorithms
        - Symmetric Key Encryption
        - Asymmetric Key Encryption
    - Hashing Algorithms
        - IP Sec
        - Understanding IPSec Architecture
        - Components of IPSec
        - Modes
            - Transport Mode
            - Tunnel Mode
            - Choosing Best IPSec Mode for Organizations
        - IPSec Processing
        - Enabling IPSec
        - Algorithms for IPSec
        - Protocols
            - AH
            - ESP
        - Levels of IPSec
            - Client
            - Server
            - Secure Server
        - IPSec Policies
            - IP Filters
            - Filter Action
            - Authentication Methods
            - Tunnel Setting
            - Connection Type
    - Cryptography
        - History of Cryptography
        - Math and Algorithms
        - Message Authentication
            - DES for Encryption
                - DES ECB and CBC Analysis
            - 3DES
            - HMAC / MD5 and SHA for Authentication
        - Strength (e.g., complexity, secrecy, characteristics of the key)
        - Cryptovariable or key
- Digital Certificates
    - Paper Certificates and Identity Cards
    - Authorities that Issue Physical Certificates

  - Difference Between Physical and Digital Certificates
  - Standards For Digital Certificates
  - X.509 as Authentication Standard
  - Public Key Certificate
  - Viewing Digital Certificates
- Certificate Encryption Process
  - Encrypted File System
- Public and Private Keys
  - A Public Key Generated by PGP
  - Choosing the Size of Keys
  - Generating Keys
- Digital Signatures
  - Signature as Identifiers
  - Features of Digital Signatures
  - Digital Signature in practice
  - PKI
- Key management protocols (bundling, electronic key, over-the-air rekeying)

Module 25 - Virtual Private Networks And Remote Networking

- Introduction to Virtual Private Network
- Types of VPN
  - Remote Access VPN's
  - Intranet Access VPN's
  - ExtraNet VPN's
- Tunneling
- Fundamentals of Tunneling
- Tunneling Protocol
- Point to Point Tunneling Protocol (PPTP)
  - Goals and Assumptions
  - Terminology
  - Control Connections
  - Security and Disadvantages
- Layer 2 Tunnel Protocol
  - Characteristics
  - L2TP Header Format
  - L2TP Control Message Header
  - L2TP Data Message
  - L2TP Compulsory Tunnel
  - L2TP Voluntary Tunnel
- VPN Security
  - Encryption
  - IPSec Server
  - AAA Server
- Connection to VPN
  - SSH and PPP
  - Concentrator
  - Other Methods
- Step1 : Setting up VPN
- Step2 : Implement DHCP Services
- Step3 : Create an Enterprise Certificate Authority
- Step 4 : Install IAS
- Step 5 : Configure IAS
- Step 6 : Create a Remote Access Policy
- Step 7 : Configure the VPN Server
- Step 8 : Associate the VPN Server with the DHCP Server
- Step 9 : Configure Remote Clients
- Step 10 : Test The Client Connection
- VPN Policies
- VPN Registrations and Passwords
- Risk Associated with VPN
- Pre Implementation Review – Auditing
- Implementation Review – Auditing
- Post Implementation Review and Reporting
- VPN Product testing
- Common VPN Flaws

Module 26 - Wireless Network Security

- Introduction to Wireless
  - Types of Wireless Networks : WLAN, WWAN, WPAN and WMAN
  - Wired vs Wireless Networks
  - Advantages and Disadvantages of Wireless
- Types of Wireless Networks
  - Based on Type of Connection
  - Based on Geography
- Components of Wireless Network
  - Access Points
  - Wireless Cards
  - Antenna
  - Wireless Desktop Cards
  - Wireless Laptop Cards
  - Wireless USB Adapters
  - Wireless Internet Video Camera
  - Digital Media Adapter
  - Wireless Converters
  - Wireless Print Server
  - Wireless Rechargeable Bluetooth Mouse
  - Wireless Modems
  - Wireless Router
  - Wireless Gateways
  - Wireless USB
  - Wireless Game Adapter
  - Wireless Range Extender
  - GSM Network Devices
    - Mobile Station
    - Base Station Subsystem
    - Base Station controller (BSC)
    - Base Transceiver Station (BTS)
    - Network Subsystem
    - Mobile Switching center
- Wireless Technologies
  - Personal Communication Services (PCS)
  - Time Division Multiple Access (TDMA)
  - Code Division Multiple Access (CDMA)
  - ARDIS
  - BlueTooth
    - Frequency and Data Rates
    - Bluetooth Architecture and Components
  - Ultra Wideband
- Wireless Communications : Examples
  - Satellite Communications
  - Cellular Phone Communications
- Devices using Wireless Communications
  - PDA
  - BlackBerry
- Service Set Identifier (SSID)
- Detecting Wireless Network
  - How to Scan
  - Tool : Kismet
  - Netstumbler
- Types of Wireless Attacks
  - Man in the Middle Attacks

        - Eavesdropping
        - Manipulation
    - Denial of Service or Distributed Denial of Service
    - Social Engineering
    - "Weak Key" Attacks
    - Dictionary Attacks
    - Birthday Attacks
- Wireless Threats
    - Rogue Access Points
    - MAC Sniffing and AP Spoofing
- Overview of Wi-Fi
    - Hotspot
- Open Wi-Fi Vulnerabilities
    - Unauthorized Network Access
    - Eavesdropping
- WLANs in Public Space
    - Security Vulnerabilities with Public Access Wireless Networks
    - Risks Due to Wireless Networks
- Wired Equivalent Privacy
    - WEP Key Cracking Tools
        - WEPCrack
        - AirSnort
        - Aircrack
- WAP
- Wireless Network Attack Tool : AirSnarf
- Tools to detect MAC Address Spoofing : Wellenreiter v2
- WLAN Management
    - Detecting Rogue Points
- Wireless Security
    - Authentication
        - LDAP
            - Communications
        - Multifactor Authentication
        - Authentication Mechanism
            - Kerberos
            - Components
            - Exchanges Of Kerberos Client
    - WPA
    - Security Measures
        - Change the SSID
        - Use Encryption
        - Use a VPN
        - Use a Firewall
    - WLAN Security Policy Development Issues
        - Goals and Characteristics
        - Auditing WLAN Security Policy
    - RADIUS Authentication
        - Security
        - Configuration
- Wireless Auditing
    - Baselining
- DHCP Services
    - Server and Client
- Mobile Security through Certificates
- Certificate Management through PKI
- Trouble Shooting Wireless Network
    - Multipath and Hidden Node
- Wireless Network Security Checklist

Module 27 - Creating Fault Tolerance

- Network Security : Fault Tolerance
- Why Create Fault Tolerance
    - Planning For Fault Tolerance
- Network Security
    - Key Aspect of Fault Tolerance
    - Fault Tolerant Network
- Reasons for Network Failure
    - Viruses and Trojans
    - Intrusion
    - Power Supply Failure
- Reasons For System Failure
    - Crime
    - User Error
    - Environmental
    - Routine Events
- Preventive Measures
    - Physical Security
    - Backups
        - Files Back up
        - Tape Backup – Pros and Cons
    - Practical Tips
    - Setting Privileges
    - Access Rights
    - Partitions
    - Peripherals
    - UPS and Power Generators
    - RAID
        - RAID Level 0 (Striping)
        - RAID Level 1 (Mirroring or Duplexing)
        - RAID Level 2 (Striping with Error Correction Code (ECC))
        - RAID Level 3 (Striping with Parity on a single Drive)
        - RAID Level4 (Striping by block with Parity on a Single Drive)
        - RAID Level 5 (Striping with Parity Information Spread Across Drives)
    - Clustered Servers
    - Simple Server Redundancy
    - Archiving
    - Auditing
        - Anatomy of Auditing
        - Auditing Mechanism
        - Audit Browsing
        - Effectiveness of security breaches
        - Investigation of security breaches
        - Review of audit trails and logs
        - Review of software design standards
        - Review of accountability controls
        - Verification, validation, testing, and evaluation processes
    - Privacy
    - Deployment Testing
    - Circuit Redundancy
    - Offsite Storage
    - Perimeter Security
    - Understanding Vulnerabilities
    - Authentication

Module 28 - Incident Response

- What is an Incident?
- Category of Incident
- Types of Incident

  - Who should I Report an Incident?
- Step by Step Procedure
  - Managing Incidents
- What is an Incident Response?
  - Incident Response Architecture
- Six Step Approach for Incident Handling (PICERF Methodology)
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Follow-up
- Incident Response Team
  - Basic Requirements
  - Ways of Communication
  - Staffing Issues
  - Stages
- Obstacles in Building a Successful Incident Response Team
- Computer Security Incident Response Team
  - Services
    - Reactive Services
    - Proactive Services
    - Security Quality Management Services

Module 29 - Disaster Recovery And Planning

- Overview of Disaster and its Types
- What is a Disaster Recovery?
- Principles of Disaster Recovery
- Types of Disaster Recovery Systems
  - Synchronous Systems
  - Asynchronous Systems
- Backup Site
- Recovery of Small and Large Computer Systems
- Emergency Management
- Disaster Recovery Planning
- Security planning
  - Directives and procedures for NSTISS policy
  - Program budget
- Process of Disaster Recovery Plan
  - Organizing
  - Training
  - Implementing
    - Process
- Disaster Recovery Testing
  - Testing Process
  - Testing Steps
  - Testing Scenarios
- Contingency Planning/Disaster Recovery
- Contingency plan components, agency response procedures and continuity of operations
- Team member responsibilities in responding to an emergency situation
- Guidelines for determining critical and essential workload
- Determination of backup requirements
- Development of procedures for off-site processing
- Development of plans for recovery actions after a disruptive event
- Emergency destruction procedures
- Disaster Recovery Planning Team
  - Training the Disaster Recovery Planning Team
- Business Process Inventory
- Risk Analysis
  - Concept of Risk Analysis
  - Methods of Risk Analysis
  - Process of Risk Analysis
  - Continuous Risk Assessment
  - Techniques to minimize Risk
  - Cost/benefit analysis of controls
  - Implementation of cost-effective controls
- Business Continuity Planning Process
  - Business Impact Analysis
  - Risk Assessment
  - Other Policies, Standards and Process
  - Monitoring
  - Business Continuity Management
- Emergency destruction procedures
- Six myths about Business Continuity Management and Disaster Recovery
- Disaster Prevention

Module 30 - Network Vulnerability Assessment

- Vulnerability Assessment
  - Vulnerability Assessment Services
  - Goals of vulnerability assessment
- Features of a Good Vulnerability Assessment
  - Network Vulnerability Assessment Timeline
  - Network Vulnerability Assessment Team
- Vulnerability Classes
  - Source Of Vulnerabilities
  - Design Flaws
  - Poor Security management
  - Incorrect Implementation
- Choice of Personnel for Network Vulnerability Assessment
- Network vulnerability Assessment Methodology:
  - Phase 1- Acquisition
  - Phase 2 - Identification
  - Phase 3 - Analyzing
  - Phase 4 - Evaluation
  - Phase 5 - Generation
- How to Assess Vulnerability Assessment Tools
- Selecting Vulnerability Assessment Tools
  - SAINT
  - Nessus
  - BindView
  - Nmap
  - Ethereal
  - Retina
  - Sandcat Scanner
  - Vforce
  - NVA-Team Checklist
  - ScanIT Online