# EC-Council Network Security Administrator (ENSA)

## Course Introduction — 4m

Course Introduction

## Module 01 - Fundamentals of the Network — 3h 11m

Fundamentals of the Network
Key Elements of a Network
Nodes
The Network Backbone
Segments
Subnets
Logical Elements of a Network
IP Addresses
IP Address Space
Assignment of IP Addresses
Prefix Based Addressing
Pre Interface Based Assignment
Virtual Addresses
Dynamic Addressing
Dynamically Assigning IP Addresses
Static Addressing
Assigning Static IP Addresses
Demo - Configuring IP Addresses
Domain Name System
Domain Names
Creating a New Domain Name
Components of DNS
Name Servers
Resolver
Securing DNS Services
Demo - DNS
Gateways
Data Gateway
Multimedia Gateway
Home Control Gateway
Types of Network Media
Types of Network Media: Asynchronous vs. Synchronous
Wired Media or Bounded Network Media
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
Public Switched Network (PSN)
Emanations Security and Line of Sight
Radio Frequency
Media Access Methods

Multiplexed Media Access
Time Domain Multiplexing (TDM)
Frequency Division Multiplexing (FDM)
Token-Based Media Access
Carrier Sense Multiple Access/Collision Detection (CSMA/CD)
Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)
Contention Domains
Automated Information Systems (AIS)
Input, Output, Central Processing Unit (CPU)
Memory
Critical Information Characteristics
Operations Security (OPSEC)
INFOSEC and OPSEC Interdependency
Object Reuse (Computer Security)
Optical Remanence
Magnetic Remanence
Transmission Modes
Simplex Transmission
Half Duplex Transmission
Full Duplex Transmission
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 Topology
Network Topologies
Sharing of Data
Sharing of Devices
File Servers
Bus Topology
Linear Bus
Distributed Bus
Star Topology
Star Wired Ring Topology
Mesh Topology
Ring Topology
Tree Topology
Hybrid Topology
Classifying the Networks
Physical Network Classification
Network Equipment
Network Interface Cards (NICs)
Access Points and Switches
Concentrators/Hub
Modem
Network Equipment: Asynchronous vs. Synchronous
Router
Brouter
Bridge
ISDN Terminal Adapters
Repeaters

Multiplexer
Gateway
Other Network Devices
Module 01 Review

## Module 02 - Network Protocols 2h 29m

Network Protocols
Introduction to Network Protocols
Common Protocol Numbers
Internet Protocol (IP)
Internet Protocol: Attacks and Countermeasures
Implementing Network Protocols
Network Classes
Application Layer: TELNET
Implementing Application Layer Protocols
BOOT Strap Protocol (BOOTP)
Dynamic Host Configuration Protocol (DHCP)
Data Link Switching Client Access Protocol (DCAP)
DCAP Client/Server Model
Domain Name System (Service) Protocol (DNS)
File Transfer Protocol (FTP)
Trivial File Transfer Protocol (TFTP)
FTP, TFTP Vulnerabilities
Network Time Protocol (NTP)
Network News Transfer Protocol (NNTP)
Simple Network Management Protocol (SNMP)
Internet Relay Chat Protocol (IRCP)
Service Location Protocol (SLP)
Types of Messages
Hyper Text Transfer Protocol (HTTP)
Hyper Text Transfer Protocol Secure (HTTPS)
Demo - Network Protocols
Implementing Presentation Layer Protocols
Implementing Session Layer Protocol
Implementing Transport Layer Protocols
Transmission Control Protocol (TCP)
User Datagram Protocol (UDP)
TCP, UDP: Attacks and Countermeasures
Reliable Data Protocol (RDP)
Implementing Network Layer Protocols
Routing Protocols
Border Gateway Protocol (BGP)
Internet Control Message Protocol (ICMP)
ICMP Message Structure
TYPES Defined
Internet Group Management Protocol (IGMP)
IGMP
ICMP Router Discovery Protocol (IRDP)
Mobile Support Protocol for IP
Next Hop Resolution Protocol (NHRP)
Open Shortest Path First (OSPF) Protocol
Demo - OSPF
Routing Information Protocol (RIP)
Multicasting Protocols
The NetBEUI Protocol
Remote Authentication Dial-In User Service Protocol (RADIUS)

Voice Over Internet Protocol (VoIP)
VoIP Implementation Types
Implementing Data Link Layer Protocols
Address Resolution Protocol (ARP)
Reverse Address Resolution Protocol (RARP)
Network Address Resolution Protocol (NARP)
Module 02 Review

## Module 03 - Protocol Analysis 1h 39m

Protocol Analysis
TCP/IP Protocol Suite
TCP/IP: Network Interface Layer
TCP/IP: Internet Layer
TCP/IP: Transport Layer
TCP/IP: Application Layer
Acknowledgement
Windowing
Positive Acknowledgement and Retransmission
Demo - Protocol Analyzer
TCP Header Format
Algorithms in TCP
TCP Checksum Calculation
Performance Estimation in TCP
Problems Related to TCP
Internet Protocol (IP)
IP Header Format
IP Datagram
Encapsulating Security Payload (ESP)
Modes in ESP
eNotes: Modes in ESP
Demo - Headers
IPv6
IPv6 Header Format
Internet Protocol v4 Addressing
eNotes: Internet Protocol v4 Addressing
Packet Tunneling
IP Multicasting
Hop By Hop Option
Module 03 Review

## Module 04 - Hardening Physical Security 52m

Hardening Physical Security
Physical Security
Need for Physical Security
Internet Security
Factors Affecting Physical Security
Types of Attackers
Physical Security Threats
Nature / Environment Threats
Man-Made Threats
Dumpster Diving
Premise Security
Office Security
Reception Area
Authenticating Individuals
Smart Cards

Physical Security Checklist: Proximity Card
Biometrics
Fingerprint Verification
Hand Geometric
Voice Recognition
Retina Scanning
Iris Scanning
Facial Recognition
Workplace Security
Access Authorization
System Maintenance Personnel
Contractors
Desktop Security
Laptop Theft: Countermeasures
Laptop Security: Information Security Countermeasures
Server Security
Securing Backup Devices
Challenges in Ensuring Physical Security
Physical Security Countermeasures
Locks and Keys
Uninterruptible Power Supplies
Mantrap
Physical Security Checklist
Module 04 Review

## Module 05 - Network Security 1h 20m

Network Security
Overview of Network Security
The Security, Functionality, and Ease of Use Triangle
The Need for Security
Goals of Network Security
Security Awareness
Functions of Network Security Administrator
Demo - Threat Assessment
Administrative Security Procedural Controls
Demo - Sanitizing Media
Demo - Strong Passwords
Documentation, Logs and Journals
Functions of Information Security (INFOSEC) Officer
Security Office and Senior Management
System Manager and System Staff
Functions of the Audit Office
Network Security: Public vs. Private and Dial-up vs. Dedicated
Network Security
Transmission Security
Legal Elements
Countermeasures: Cover and Deception
Reporting Security Violations
Module 05 Review

## Module 08 - Security Policy 46m

Security Policy
Overview of Security Policy
Concept of Security Policy
Key Elements of Security Policy
Conducting Security Awareness Programs

Defining the Purpose and Goals of Security Policy
Classification Systems
Security Framework
Role of Security Policy
Classification of Security Policy
Design of Security Policy
Contents of Security Policy
Privacy and Confidentiality
Security Levels
Separation of Duties, Dual Controls, Job Rotation
Least Privilege
Security Organization and Policy Development
Configuring of Security Policy
Implementing Security Policies
Incident Handling and Escalation Procedures
Understanding Assets
Development
Demonstration and Validation
Implementation
Security (e.g. Certification and Accreditation)
Operations and Maintenance (e.g., Configuration Management)
Presenting and Reviewing the Process
Points to Remember While Writing a Security Policy
Module 08 Review

## Module 09 - IEEE Standards 55m

IEEE Standards
802 - Overview and Architecture
802.1 - Bridging and Management
eNotes: Bridging and Management
Demo - Switch Operation
802.2 - Logical Link Control (LLC)
802.3 - CSMA/CD (Ethernet)
eNotes: 802.3 - CSMA/CD (Ethernet)
IEEE 802.5 - Token Ring Passing
IEEE 802.11 - Wireless LAN (WLAN)
Wireless Networking Standards
802.1X
802.11 (Wi-Fi Standard)
802.11 Architecture
802.11a
802.11b
802.11g
802.11i
802.11n
IEEE 802.15 Wireless Personal Area Network: Bluetooth
802.16
Wi-MAX
Module 09 Review

## Module 10 - Network Security Threats 1h 28m

Network Security Threats
Defining Terms: Vulnerability, Threats and Attacks
Types of Attacks
Classification of Hackers
Network Attack Techniques: Spamming

Network Attack Techniques: Revealing Hidden Passwords
Network Attack Techniques: War Driving, War Chalking and War Flying
Network Attack Techniques: Wiretapping
Network Attack Techniques: Scanning
Types of Scanning
Demo - Network Scanning
Network Attack Techniques: Sniffing
Types of Sniffing
Demo - Sniffing
Network Attack Techniques: Reconnaissance
Network Attack Techniques: Social Engineering
Common Vulnerabilities and Exposures (CVE)
Threat: Trojan
Threat: Virus
Threat: Worm
Logic Bomb
Threat: Eavesdropping
Threat: Phishing
Attack: Smurfing
Attack: Rootkit
Man in the Middle Attack
eNotes: Man in the Middle Attack
Demo - Man-in-the-Middle
Denial of Service (DoS) Attack
Distributed Denial of Service Attack (DDoS)
Buffer Overflow Attack
Zero-Day Attack
Password Attacks
Spoofing Attack
Session Hijacking
Attack: Web Page Defacement
Recording Keystrokes or Keystroke Loggers
Attack: Cracking Encrypted Passwords
Cain and Abel Tool
Attack: SQL Injection
Hiding Evidence of an Attack
Network Scanning Tools
Netstat Tool
Nmap Scanning Tool
Module 10 Review

## Module 11 - Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) — 1h 1m

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)
Understanding Intrusion Detection Concepts
Intrusion Detection Concept
IDS Concept: Architecture
IDS Concept: Monitoring Strategies
IDS Concept: Analysis Type
IDS Concept: Timing Analysis
IDS Concept: Goals of IDS
Choosing an IDS for an Organization
Characteristics of IDS
Identifying the Importance of IDS
Understanding the Types of IDS
Network-Based IDS (NIDS)

NIDS Architecture
Traditional Sensor-Based Architecture
Distributed Network Node
Network-Based Detection
Host-Based IDS (HIDS)
HIDS Architecture
HIDS Operational Concept
Host-Based Detection
Network-Based IDS Vs Host-Based IDS
Distributed IDS: Introduction and Advantages
Components of Distributed IDS
Protocol Intrusion Detection System
Network Behavior Analysis (NBA)
Unified Threat Management (UTM)
Deployment IDS
Types of Signatures: Network Signatures
Types of Signatures: Host-Based Signatures
Types of Signatures: Compound Signatures
True/False-Positive/Negative
Major Methods of Operation
Intrusion Prevention System
Intrusion Prevention Strategies
IPS Deployment Risks
Information Flow in IDS and IPS
eNotes: Information Flow in IDS and IPS
IDS and IPS
Module 11 Review

## Module 12 - Firewalls 1h 11m

Firewalls
Firewalls: Introduction
Security Features
Multiple Components of a Firewall
Firewall Operations
Software Firewall
Demo - Software Firewall
Hardware Firewall
Types of Firewalls: IP Packet Filter Firewall
Types of Firewall: Circuit Level Gateway
Types of Firewall: Application Level Firewall
Types of Firewalls: Network Level Firewalls
Firewall Features
Establishing Rules and Restrictions for Your Firewall
Firewall Configuration Strategies
Scalability
Firewall Architecture: Dual Homed Host Architecture
Firewall Architecture: Screened Host Architecture
Firewall Architecture: Screened Subnet Architecture
Handling Threats and Security Tasks
Centralization and Documentation
Multi-Layer Firewall Protection
Firewall Deployment Strategies: Screened Host
Two Routers with One Firewall
DMZ Screened Subnet
Figure: DMZ Screened Subnet
Multi Firewall DMZ

Multi Firewall DMZ: Two Firewalls, One DMZ
Multiple Firewall DMZs: Two Firewalls, Two DMZs
Screening Router
Dual Homed Host
Specialty Firewalls and Reverse Firewalls
Advantages of Using Firewalls
Disadvantages of Using Firewalls
Threats: Firewalking
Threats: Banner Grabbing
Limitations of Firewalls
Firewall Log Analysis
Firewall Tester: Firewalk
Module 12 Review

## Module 13 - Packet Filtering and Proxy Server 53m

Packet Filtering and Proxy Server
Application Layer Gateway
Network Address Translation
Demo - NAT
Packet Filtering
Approaches to Packet Filtering
Packet Sequencing
Packet Prioritization
Packet Fragmentation
Analyzing Packet Fragmentation
Signature Analysis
Stateful Packet Filtering
Stateless Packet Filtering
Demo - Packet Filters
Dynamic Packet Filtering
Advantages of Filtering
Disadvantages of Filtering
Transmission Control Protocol (TCP)
TCP: URG Flag
TCP: ACK Flag
TCP: PSH Flag
TCP: RST Flag
TCP: SYN Flag
TCP: FIN Flag
eNotes: TCP Three Way Handshake
User Datagram Protocol (UDP)
Module 13 Review

## Module 14 - Bastion Host and Honeypots 24m

Bastion Host and Honeypots
Building Honeypots
Value of Honeypot
Production Honeypot
Research Honeypot
Categorizing the Honeypots Based on Levels of Interaction
Low-Interaction Honeypot
Medium-Interaction Honeypot
High-Interaction Honeypot
Uses of Honeypot
Uses of Honeypot: Preventing Attacks
Uses of Honeypot: Detecting Attacks

Uses of Honeypot: Responding to Attacks
How to Create a Homemade Honeypot
Port-Monitoring Homemade Honeypots
Demo - Honeypots
Jailed Environment Homemade Honeypots
Mantrap
Advantages and Disadvantages of Honeypots
Legal Issues Related to Honeypots
Building a Honeynet
Architecture of Honeynet
Module 14 Review

## Module 16 - Troubleshooting Network 1h 20m

Troubleshooting Network
Introduction to Troubleshooting
Troubleshooting Strategy
Recognizing Symptoms
Analyzing Symptoms
Understanding the Problem
System Monitoring Tools
Network Monitor
Demo - Monitoring Network Traffic
Testing the Cause of the Problem
Solving the Problem
Troubleshooting Network Devices
Windows PC Network Interface Card
Demo - Network Troubleshooting
Troubleshooting RF
Diagnosing Gateway
Troubleshooting Hubs and Switches
Troubleshooting Network Slowdowns
IP Conflicts
Bad NICs
DNS Errors
Insufficient Bandwidth
Troubleshooting Wireless Devices
Checking the LED Indicators
Checking Basic Setting
Device Manager
Demo - Device Manager
Troubleshooting Network Communication
Identifying Communication Problems
Using Ping
Variations in the PING Utility
Using TraceRT
eNotes: TraceRT
Network Adapter Troubleshooting
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
How to Overcome the Connectivity Problem
Causes of Connectivity Problems
Troubleshooting Physical Problems
Troubleshooting Link Status

Performance Measurement Tool
TCP/IP Troubleshooting Utilities
Troubleshooting with Ping
Troubleshooting with ARP
Troubleshooting with Netstat
Troubleshooting with Nslookup
Demo - Troubleshooting Tools
eNotes: Life of a Packet
Troubleshooting Tools
Hardware Based Troubleshooting Tools
Hardware Loopback Plugs
Module 16 Review

## Module 17 - Hardening Router 1h 6m

Hardening Router
Introduction to Routers
Routing Metrics
Multiple Routing
Types of Routes
Routing Algorithms
Demo - Dynamic Routes
Routing Principles
IP Routing
Demo - Static Routes
IP Source Routing
Router Configuration
External Configuration Sources
Internal Configuration Sources
Router Initiation
Setup Configuration Mode
Finger Tool
Disabling the Auxiliary Services and Closing Extra Interfaces
Demo - Router Configuration
Bootstrap Service (BOOTP Service)
TCP and UDP Small Servers
Disabling Proxy ARP
Disabling Simple Network Management Protocol (SNMP)
Disabling Network Time Protocol (NTP)
Hardening a Router
Display Notifications on Banners
Passwords and Secrets
Setting Session Timeout Periods
Cisco Discovery Protocol
Logging Concept
Timestamping
Console Logging
Buffered Logging
Terminal Logging
Filtering Network Traffic
Access Control List (ACL)
Creating a Standard ACL
Demo - Hardening Router
Logging System Error Messages
Enabling System Error Message Logging
How to Secure the Routers
Committed Access Rate

SSH: Securing Routers
SSH: Authentication Methods
Router Commands
Configuring Router Interface Settings
How to Troubleshoot a Router
Troubleshooting Tools
Troubleshooting IP Connectivity in Routers
Components of Router Security
Module 17 Review

## Module 18 - Hardening Operating System 1h 28m

Hardening Operating System
BIOS Security
Windows Registry
Configuring Windows Services
Process
Need to Know Controls
Malicious Logic Protection
Assurance
Discretionary Access Control List (DACL)
Objects and Permissions
Rights vs. Permission
NTFS File System Permissions
Encryption File System (EFS)
Demo - File Security
Windows Infrastructure Features
Kerberos Authentication and Domain Security
Trust Relationships Between Domains
IPSecurity
Windows 2003 Security Configuration Tools
Demo - SCW
Windows 2003 Resource Security
Windows 2003 Network Security
User and File System Security Administration
Security: Data Security and Network Security
OS Security Measures: Linux Update Agent
User Management
Account Security
File System and Navigation
File and Directory Permissions
Demo - Linux
Pluggable Authentication Module (PAM)
PAM Framework
Security with PAM
Network Information Services (NIS)
Group Management Utilities
Permission Management Tools
System Logger Utility
UNIX Security Checklist
Using Kerberos Authentication
eNotes: Kerberos
Restricting User Capabilities
Module 18 Review

## Module 19 - Patch Management 31m

Patch Management
Introduction to Patch Management
Change Management Rules
Types of Patches Defined by Microsoft
The Patch Concept
Patch Testing
Understanding Patch Monitoring and Management
Understanding the Process of Patch Management
Microsoft Patch Management Process: Identification
Microsoft Patch Management Process: Assessment
Microsoft Patch Management Process: Obtainment
Demo - MBSA
Microsoft Patch Management Process: Testing
Microsoft Patch Management Process: Deployment
Microsoft Patch Management Process: Confirmation
Implementing the Windows Update Services
Demo - Windows Update
Windows Server Update Services (WSUS)
Features: WSUS Client Side, Server Side Components
Working with Patch Management Tools
Selecting a Tool
Patch Management Tool: Microsoft Baseline Security Analyzer (MBSA)
Module 19 Review

## Module 21 - Application Security 47m

Application Security
Importance of Application Security
Why Web Security is So Difficult?
Application Threats
Application Dependant Guidance
Cookies
Working of Cookies
Persistent vs. Non-Persistent Cookie
Session Tokens
Authentication Tokens
Encrypting Private Data
Demo - Drive Encryption
Countermeasures to Threats
Securing Voice Communications
Demo - Securing Voice Communication
Securing Data Communication
Securing of Keying Material
IPSec and SSL Security
Writing Secure Coding Practice
Secure Coding - Common Errors
Common Error: Buffer Overflow
Demo - Metasploit
Common Error: Format String Vulnerabilities
Common Error: Authentication
Common Error: Authorization
Common Error: Cryptography
Best Practices for Secure Coding
Remote Administration Security
Programming Standards and Controls
Threat Modeling

Input and Output of Threat Modeling
Module 21 Review

## Module 22 - Web Security 42m

Web Security
Understanding the Various Types of Network Threats
Common Threats on Web
Demo - Web Security Evaluation
Identity Theft
Email Security Risks: Spam
FTP Bounce
DNS Attack
Content Spoofing
Logical Attacks
Restrictive Access
Network Addresses
Altering the Network Address
Client Authorization
Client Side Data
Overview of Server Side Data
Client Authentication
Client Authentication: User's Approach
Client Authentication: Authentication Techniques
Input Data Validation
Demo - Application Security
Browser Hijacking
Common Gateway Interface (CGI)
CGI Script
CGI Script: Mechanisms and Variables
CGI Operations
Module 22 Review

## Module 23 - Email Security 38m

Email Security
Analyzing the Key Concepts of Electronic Mail
Basics of Email
Types of Email
Components of Email
Components of Email: Headers
Examining an Email Header
Reading Email Header
Opening Attachments
Components of an Email: Recipients and Senders
Components of an Email: Response Targets
Demo - Email Information
Analyzing the Core Elements of Email Encryption
Secure Email
Email Authentication
Email Protocols
Email Security Risks
Email Security Risks: Gateway Virus Scanners
Email Spamming: Protection Against Spam
Email Spamming: Spam Filters
How to Defend Against Email Security Risks?
Tracking Emails
Tracking Emails: ReadNotify

Demo - ReadNotify
Module 23 Review

## Module 24 - Authentication: Encryption, Cryptography and Digital Signatures — 56m

Authentication: Encryption, Cryptography and Digital Signatures
Authentication
Encryption
Encryption Systems
Hashing Algorithm: HMAC
Demo - Hashing
eNotes: Hash
eNotes: HMAC
Hashing Algorithm: MD5
Encryption Algorithms: RSA
Performing RSA Encryption and Decryption
Demo - Encryption
Diffie Hellman Algorithm
Analyzing Popular Encryption Schemes
Symmetric vs. Asymmetric Encryption
Symmetric Key Encryption
Asymmetric Encryption
PGP (Pretty Good Privacy)
X.509
SSL
eNotes: SSL
Understanding IPSec and IPSec Encryption
Choosing Best IPSec Mode for Organizations
The IPSec Process
IPSec Protocol: AH
IPSec Protocol: ESP
Cryptography
Math and Algorithm
Message Authentication
Strength (e.g., Complexity, Secrecy, Characteristics of the Key)
Digital Certificates
X.509 as Authentication Standard
Digital Signature
Features of Digital Signature
Public Key Infrastructure (PKI)
Module 24 Review

## Module 25 - Virtual Private Network — 36m

Virtual Private Network
Virtual Private Network (VPN)
Types of VPN
Tunneling
Types of Tunneling
VPN Tunneling Protocols
PPTP: Introduction
PPTP Security and Disadvantages
Layer Two Tunneling Protocol (L2TP)
Characteristics of L2TP
L2TP Compulsory Tunnel
L2TP Voluntary Tunnel
VPN Security: Encryption

VPN Security: IPSec Server
Demo - IPSec Server
VPN Security: AAA Server
Connection to VPN: SSH & PPP
Connection to VPN: Concentrator
eNotes: VPN
Demo - VPN Concentrator
Pre-Implementation Review-Auditing
Implementation Review-Auditing
Post-Implementation Review and Reporting
Common VPN Flaws
Insecure Storage of Authentication Credentials by VPN Clients
Username Enumeration Vulnerabilities
Module 25 Review

## Module 26 - Wireless Network Security 39m

Wireless Network Security
Introduction to Wireless Networks
Wireless Network Types
Wired vs. Wireless Networks
Types of Wireless Networks: Based on Connection
WLAN (Wireless Local Area Network)
WWAN (Wireless Wide Area Network)
WPAN (Wireless Personal Area Network)
WMAN (Wireless Metropolitan Area Network)
Antennas
Antenna Types
Access Points
Operating Modes of Access Points
Wireless Router
Wireless Range Extender
Wireless Technologies
Personal Communication Services (PCS)
TDMA (Time Division Multiple Access)
CDMA (Code Division Multiple Access)
Bluetooth
Wireless Communications: Satellite Communication Network
Wireless Communications: Cellular Phone Network
Types of Wireless Attacks
Man-in-the-Middle Attacks
Denial-of-Service Attacks
Rogue Access Points
MAC Sniffing and ARP Spoofing
Security Vulnerabilities with Public-Access Wireless Networks
Wired Equivalent Privacy (WEP)
WPA (Wi-Fi Protected Access)
RADIUS Authentication
RADIUS: Security
Troubleshooting Wireless Network
Multipath and Hidden Node
eNotes:  Multipath and Hidden Node
Module 26 Review

## Module 27 - Creating Fault Tolerance 33m

Creating Fault Tolerance
Network Security: Fault Tolerance
Why Create Fault Tolerance
Planning for Fault Tolerance
Network Security
Fault Tolerant Network
Reasons for Network Failure
Reasons of System Failure
Reasons of System Failure: Crime
Reasons of System Failure: User Error
Reasons of System Failure: Environmental
Reasons of System Failure: Routine Events
Preventive Measure: Physical Security
Preventive Measure: Backup
Demo - Backups
Preventive Measure: Access Rights
Preventive Measure: Partitions
Preventive Measure: UPS and Power Generators
Preventive Measure: RAID
eNotes: Preventive Measure RAID
Demo - RAID
Preventive Measure: Clustered Servers
Simple Server Redundancy
Preventive Measure: Auditing
Anatomy of Auditing
Auditing Mechanism
Investigation of Security Breaches
Review of Audit Files and Logs
Privacy
Module 27 Review

## Module 28 - Incident Response 20m

Incident Response
What is an Incident?
Category of Incidents
Types of Incidents
To Whom Should I Report an Incident?
Managing Incidents
What is an Incident Response?
Six Step Approach for Incident Handling
Incident Handling Process: Preparation
Incident Handling Process: Detection
Incident Handling Process: Containment
Incident Handling Process: Eradication
Incident Handling Process: Recovery
Incident Handling Process: Follow-Up
Incident Response Team
Incident Response Team: Functional Requirements
Incident Response Team: Ways of Communication
Incident Response Team: Staffing Issues
Obstacles in Building a Successful Incident Response Team
Computer Security Incident Response Team
Proactive Services
Security Quality Management Services
Module 28 Review

## Module 29 - Disaster Recovery and Planning 51m

Disaster Recovery and Planning
Overview of Disaster and Types
What is Disaster Recovery?
Principles of Disaster Recovery
Types of Disaster Recovery Systems: Asynchronous Systems
Types of Disaster Recovery Systems: Synchronous Systems
Backup Sites
Recovery of Small/Large Recovery Systems
Emergency Management
Disaster Recovery Plan
Security Planning
Program Budget
Disaster Recovery Plan: Organizing
Disaster Recovery Plan: Training
Disaster Recovery Plan: Implementing
Disaster Recovery Planning: Process
Disaster Recovery Testing
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
Development of Plans for Recovery Actions After a Disruptive Event
Disaster Recovery Planning Team
Training the Disaster Recovery Team
Risk Analysis
Cost/Benefit Analysis of Controls
Implementation of Cost-Effective Controls
Risk Management
Information Identification
Roles and Responsibilities of all the Players in the Risk Analysis Process
Risk Analysis and/or Vulnerability Assessment Components
Risk Analysis Results Evaluation
Corrective Actions
Business Continuity Planning Process (BCP)
BCP: Business Impact Analysis (BIA)
BCP: Risk Assessment
BCP: Monitoring
BCP: Other Policies, Standards and Processes
Business Continuity Management
Emergency Destruction Procedures
Six Myths About Business Continuity Management and Disaster Recovery
Module 29 Review

## Module 30 - Network Vulnerability Assessment 25m

Network Vulnerability Assessment
Vulnerability Assessment
Goals of Vulnerability Assessment
Features of a Good Vulnerability Assessment
Network Vulnerability Assessment Timeline
Vulnerability Classes
Source of Vulnerabilities
Choice of Personnel for Network Vulnerability Assessment Team (NVAT)
Network Vulnerability Assessment Methodology

Phase I:  Acquisition
Phase II: Identification
Phase III: Analyzing
Phase IV: Evaluation
Phase V: Generating Reports
How to Detect Vulnerability
Selecting Vulnerability Assessment Tools
Demo - Nessus Part 1
Demo - Nessus Part 2
Demo - Nessus Part 3
NVA-Team Checklist
Module 30 Review
Course Closure

**Total Duration:  26h 51m**