

**EC-Council**

**Network  
Security  
Administrator** <sup>TM</sup>

**EC-Council**  
**Network  
Security Administrator**

### **Course Description**

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 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.

### **Who Should Attend**

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

### **Prerequisites**

This course is a prerequisite for the CEH program.

### **Duration:**

5 days (9:00 – 5:00)

### **Certification**

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

### **Course Outline** v3

#### **Module: Fundamentals of Network**

1. Key elements of network
  - 1.1. Nodes
  - 1.2. The Network Backbone

### 1.3. Segments

### 1.4. Subnets

## 2. Logical Elements of Network

### 2.1. IP Addresses

#### 2.1.1. IP Address Space

#### 2.1.2. Assignment of IP Address

##### 2.1.2.1. Prefix Based Addressing

##### 2.1.2.2. Pre Interface based Assignment

##### 2.1.2.3. Virtual Addresses

##### 2.1.2.4. Dynamic Addressing

##### 2.1.2.5. Static Addressing

### 2.2. Domain Name System

#### 2.2.1. Domain Names

#### 2.2.2. Creating a new Domain Name

#### 2.2.3. Components Of DNS

##### 2.2.3.1. Domain Namensraum

##### 2.2.3.2. Name servers

##### 2.2.3.3. Resolver

##### 2.2.3.4. Securing DNS Services

### 2.3. Gateways

#### 2.3.1. Working of Gateway

#### 2.3.2. Functional Categories of Gateway Devices

##### 2.3.2.1. Data Gateway

##### 2.3.2.2. Multimedia Gateway

##### 2.3.2.3. Home Control Gateway

## 3. Types of network media

### 3.1. Wired media or Bounded Network Media

### 3.1.1. Twisted pair cable

#### 3.1.1.1.1. Shielded Twisted Pair

#### 3.1.1.1.2. Unshielded Twisted Pair

### 3.1.2. Coaxial cable or copper cable

### 3.1.3. Fiber-optic cable

### 3.1.4. Plenum and PVC cable

## 3.2. Wireless Transmission

### 3.2.1. Infrared transmission

### 3.2.2. Microwave Transmission

### 3.2.3. Satellite Transmission

## 4. Media Access Methods

### 4.1.1. Multiplexed Media Access

#### 4.1.1.1. TDM

#### 4.1.1.2. FDM

### 4.1.2. Polling

### 4.1.3. Token-Based Media Access

#### 4.1.3.1. CSMA/CD

#### 4.1.3.2. CSMA/CA

#### 4.1.3.3. Contention Domains

## 5. OSI Model

### 5.1. Physical Layer

### 5.2. Data Link Layer

### 5.3. Network Layer

### 5.4. Transport Layer

### 5.5. Session Layer

### 5.6. Presentation Layer

### 5.7. Application Layer

## 6. TCP/IP Model

### 6.1. Physical Layer

### 6.2. Data Link Layer

#### 6.2.1. Logical Link Control(LLC)

#### 6.2.2. Media Access Control (MAC)

### 6.3. Network Layer

### 6.4. Transport Layer

### 6.5. Application Layer

## 7. Transmission Modes

### 7.1. Simplex

### 7.2. Half Duplex

### 7.3. Full Duplex

## 8. Types of Transmission

### 8.1. Serial Data Transmission

### 8.2. Parallel Data Transmission

### 8.3. Unicast Transmission

### 8.4. Multicast Transmission

## 9. Logical Network Classification

### 9.1. Client Server networking

### 9.2. Peer to peer networking

### 9.3. Mixed Mode Networking

## 10. Network Topologies

### 10.1. Bus

#### 10.1.1. Linear Bus

#### 10.1.2. Distributed Bus

### 10.2. Star or Hub

#### 10.2.1. Extended Star

10.2.2. Distributed Star

10.3. Star-Wired ring

10.4. Ring

10.5. Mesh

10.6. Tree

10.7. Hybrid Topology

## 11. Physical Network Classification

11.1. LAN

11.1.1. Ethernet

11.1.2. Intranet

11.2. WAN

11.3. MAN

11.3.1. Internet

11.4. PAN

11.5. CAN

11.6. GAN

## 12. Network Equipments

12.1. Network Interface Cards

12.2. Access Points

12.3. Switches

12.4. Concentrators/hub

12.5. Modem

12.6. Router

12.7. Brouter

12.8. Bridges

12.9. Adapters

12.10. Network Load Balancers

- 12.11. Repeaters
- 12.12. Gateways
- 12.13. Transceivers
- 12.14. Converters
- 12.15. Terminals

## **Module: Network Protocols**

- 1. Introduction to protocols
- 2. Implementing Network protocols
  - 2.1. Introduction to TCP/IP
  - 2.2. Configuring TCP/IP
  - 2.3. Configuring Network Links
  - 2.4. Managing TCP/IP
  - 2.5. Network Classes
    - 2.5.1. Class A
    - 2.5.2. Class B
    - 2.5.3. Class C
    - 2.5.4. Class D
    - 2.5.5. Class E
  - 2.6. Terminal Emulation Protocol (TELNET) of TCP/IP
  - 2.7. TELNET: Vulnerabilities
  - 2.8. Network News Transfer Protocol
  - 2.9. Network News Transfer Protocol: Vulnerabilities
- 3. Application Layer Protocols
  - 3.1. Boot Strap Protocol (BOOTP)
  - 3.2. Data Link Switching Client Access Protocol(DCAP)
  - 3.3. Dynamic Host Configuration Protocol (DHCP)

3.4. Domain Name System(service) Protocol (DNS)

3.5. File Transfer Protocol (FTP)

3.6. Trivial FTP

3.7. (FTP) and Trivial FTP: Vulnerabilities

3.8. Network Time Protocol

3.9. Network News Transfer Protocol

3.10. Simple Network Management Protocol(SNMP) and Its Versions

3.11. Internet Relay Chat Protocol(IRCP)

3.12. Service Location Protocol(SLP)

3.13. Hyper Text Transfer Protocol (HTTP)

3.14. Hyper Text Transfer Protocol Secure (HTTPS)

4. Presentation Layer Protocol

4.1. Light Weight Presentation Protocol(LWPP)

5. Session Layer Protocol

5.1. Remote Procedure Call Protocol(RPC)

6. Transport Layer Protocols

6.1. Reliable Data Protocol(RDP)

6.2. Transmission Control Protocol(TCP)

6.3. User Datagram Protocol(UDP)

6.4. TCP, UDP: Attacks and Countermeasures

7. Network Layer Protocols

7.1. Routing Protocols

7.1.1. Border Gateway Protocol(BGP)

7.1.2. Exterior Gateway Protocol(EGP)

7.1.3. Internet Protocol and its versions

7.1.4. Internet Control Message Protocol(ICMP) &V6

7.1.5. The Internet Group Management Protocol (IGMP)

7.1.6. ICMP Router Discovery Protocol(IRDP)

7.1.7. Mobility Support Protocol for IP(Mobile IP)

7.1.8. Network Address Resolution Protocol

7.1.9. Next Hop Resolution Protocol

7.1.10. Open Shortest Path First(OSPF) protocol

7.1.11. Routing Information Protocol

## 7.2. Multicasting Protocols

7.2.1. Border Gateway Multicast Protocol

7.2.2. Distance Vector Multicast Protocol

7.2.3. Internet Group Management Protocol

## 7.3. Other Network Protocols

7.3.1. The NetBEUI Protocol

7.3.2. The IPX/SPX Protocol

7.3.2.1. Service Advertisement Protocol

7.3.2.2. IPX/SPX Node Address

7.3.2.3. IPX/SPX Server Address

7.3.2.4. IPX Frame Types

7.3.2.5. NWLink Protocol

7.3.3. The AppleTalk Protocol

7.3.4. Remote Authentication Dial-in User Service(RADIUS)

## 8. Data link Layer Protocol

8.1. Address Resolution Protocol(ARP)

8.1.1. Vulnerabilities and Security Measures

8.2. Network Address Resolution Protocol (NARP)

8.3. Reverse Address Resolution Protocol(RARP)

8.4. Serial Line Protocol (SLP)

8.5. High Level Data Link Control (HDLC) Protocol

## 8.6. Point-to-Point Protocol (PPP)

### **Module: Protocol Analysis**

1. Overview of TCP/IP
  - 1.1. Streams
  - 1.2. Reliable delivery
  - 1.3. Network adaption
  - 1.4. Flow control
2. Relation to other Protocol
3. Tcp/ip Protocol suite
  - 3.1. Physical And Data link Layer
  - 3.2. Network Layer
  - 3.3. Transport layer
  - 3.4. Application Layer
4. TCP
  - 4.1. Tcp header format
    - 4.1.1. Source port
    - 4.1.2. Destination port
    - 4.1.3. Sequence Number
    - 4.1.4. Acknowledgement Number
    - 4.1.5. Data offset
    - 4.1.6. Reserved
    - 4.1.7. Control Bits
    - 4.1.8. Window
    - 4.1.9. Checksum
    - 4.1.10. Urgent Pointer
    - 4.1.11. Options
    - 4.1.12. Data

## 4.2. TCP Interface

### 4.2.1. User/TCP Interface

#### 4.2.1.1. User /TCP Commands

4.2.1.1.1. Open

4.2.1.1.2. Send

4.2.1.1.3. Receive

4.2.1.1.4. Close

4.2.1.1.5. Status

4.2.1.1.6. Abort

### 4.2.2. TCP/lower -level Interface

### 4.2.3. TCP/lower –level Commands

4.2.3.1. Open call

4.2.3.2. Listen state

4.2.3.3. Send Call

4.2.3.4. Receive Call

4.2.3.5. Close Call

4.2.3.6. Abort Call

4.2.3.7. Status call

## 4.3. Algorithms in TCP

4.3.1. Appropriate byte Counting(ABC)

4.3.2. Additive Increase Multiplicative Decrease(AIMD)

4.3.3. Selective Acknowledgement(SACK)

4.3.4. TCP Friendly Rate Control(TFRC)

## 4.4. TCP Checksum Calculation

## 4.5. Performance Estimation in TCP

4.5.1. Round Trip Time Estimation

## 4.6. Problems related to TCP

- 4.6.1. Packet Replication
- 4.6.2. Checksum Error
- 4.6.3. Out of order data delivery
- 4.6.4. Bottleneck Bandwidth
- 4.6.5. Packet Loss

## 5. IP

### 5.1. Overview of IP

### 5.2. IP Header Format

#### 5.2.1. Version

#### 5.2.2. IHL

#### 5.2.3. Type of Service

##### 5.2.3.1. Precedence

##### 5.2.3.2. Delay

##### 5.2.3.3. Throughput

##### 5.2.3.4. Reliability

#### 5.2.4. Total Length

#### 5.2.5. Identification

#### 5.2.6. Flags

#### 5.2.7. Fragment Offset

#### 5.2.8. Time to live

#### 5.2.9. Protocol

#### 5.2.10. Header Checksum

#### 5.2.11. Source Address/ Destination Address

#### 5.2.12. Options

#### 5.2.13. Data

### 5.3. IP Addressing

### 5.4. IP datagram

5.4.1. Maximum Transmission Unit

5.4.2. Fragmentation

5.4.3. Encapsulation

5.4.4. Formatting

5.4.5. Reassembly

5.4.6. Delivery

5.4.7. Routing

5.4.8. Multicasting

5.4.9. Encapsulating Security Payload

5.4.9.1. Modes in ESP

5.4.9.1.1. Tunnel modes

5.4.9.1.2. Transport mode

5.5. IPv6

5.6. IPv6 Header

5.6.1. Version

5.6.2. Priority

5.6.3. Flowlabel

5.6.4. Payload Length

5.6.5. Next Header

5.6.6. Hop limit

5.6.7. Source Address

5.6.8. Destination address

5.7. IPv6 Specification

5.8. Addressing

5.9. Packet Tunneling

5.10. Multicast

**5.11. Hop by Hop option**

5.12.

**Module: IEEE standards**

1. Introduction to IEEE standards
2. IEEE LAN Protocol Specification
  - 2.1. 802-Overview And Architecture
  - 2.2. 802.1-Briding And Management
  - 2.3. 802.2-Logical Link Control(LLC)
  - 2.4. 802.3-CSMA/CD(Ethernet)
  - 2.5. 802.4-Token Passing Bus
  - 2.6. 802.5-Token Passing Ring
  - 2.7. 802.6-DQDB Access Method
  - 2.8. 802.7-Broad Band LAN
  - 2.9. 802.10-Security
  - 2.10. 802.11-Wireless LAN(WLAN)
  - 2.11. 802.12-Demand Priority Access
  - 2.12. 802.15-Wireless Personal Area Networks (WPAN)
  - 2.13. 802.16-Broad Band Wireless MAN (WMAN)
  - 2.14. 802.17-Resilliant Packet Ring Work Group
3. Wireless Networking Standards
  - 3.1. IEEE Standards
  - 3.2. 802.1X
  - 3.3. 802.11 Architecture
  - 3.4. 802.11 Standards (Wi-Fi Standard)
    - 3.4.1. 802.11a
    - 3.4.2. 802.11b
    - 3.4.3. 802.11e
    - 3.4.4. 802.11g

3.4.5. 802.11h

3.4.6. 802.11i standards

3.4.7. 802.11n

3.5. 802.15

3.6. 802.16

3.7. Wi-MAX

3.8. ETSI Standards

3.9. HIPERLAN

3.10. HIPERMAN

### **Module: Network Security**

1. Overview of Network Security
2. The need for network security
3. The goals of network security
4. Security awareness
5. Functions of Network security administrator
  - 5.1. Develop, Maintain and implement IT security
  - 5.2. Maintain and implement firewalls
  - 5.3. Monitor and secure network and servers
  - 5.4. Monitor critical system files
  - 5.5. Backup the files

### **Module: Security Standards Organizations**

1. Internet Corporation for Assigned Names and Numbers (ICANN)
2. International Organization for Standardization (ISO)
3. Consultative Committee For Telephone and Telegraphy(CCITT)
4. International Telecommunication Union(ITU)
5. American National Standards Institute(ANSI)
6. Institute Of Electronics and Electrical Engineers(IEEE)

7. Electronic Industries Association
8. National Center for Standards and Certification Information (NIST)
9. World Wide Web Consortium (W3C)

### **Module: Security Standards**

1. Introduction to Standards
2. Introduction to Internet Standards
3. Standards Creation Committee
4. Internet Standards
  - 4.1. RFC Evolution
  - 4.2. Types and Submissions
  - 4.3. Obtaining RFCs
5. Cabling Standards
  - 5.1. EIA/TIA -568
  - 5.2. UTP Categories
  - 5.3. Cable Specifications
  - 5.4. Electronic Industries Association
6. Specification Standards

### **Module: Security Policy**

1. Security Policy overview
2. Concept Of Security Policy
3. Key Security Elements
4. Security Awareness Programs
  - 4.1. Trainings
  - 4.2. Meetings
5. Goals of security Policies
6. Vital role of a security policy
7. Classification of Security policy

- 7.1. User policies
  - 7.1.1. Password Management policy
- 7.2. IT policies
- 7.3. General Policies
- 7.4. Partner Policies
- 7.5. Types of Security Policies: Issues Specific Policies
- 8. Policy design
- 9. Contents of Security Policy
- 10. Privacy and Confidentiality
- 11. Security levels
  - 11.1. Separation of duties, dual controls, job rotation
- 12. Security organization and policy development
- 13. Security policy features
- 14. Configuration of security policy
- 15. Implementation of security policy
- 16. Incident Handling and Escalation Procedures
- 17. Security operations and life cycle management
- 18. Securing Assets
- 19. Defining Responses to Security Violations
- 20. Presenting and Reviewing the Process
- 21. Compliance with Law and Policy
  - 21.1. Intellectual Property
  - 21.2. Legal Issues
  - 21.3. Describing the Electronic Communications Privacy Act
- 22. Transborder encryption issues
- 23. Points To Remember While Writing Security Policy

**Module: Hardening Physical Security**

1. Need for physical security
2. Security Statics
3. Physical Security Breach Incidents
4. Who is Accountable for Physical Security?
5. Factors Affecting Physical Security
6. Physical Security Threats
  - 6.1. Environmental threats
    - 6.1.1. Floods
    - 6.1.2. Fire
    - 6.1.3. Earthquakes
  - 6.2. Man Made threats
    - 6.2.1. Terrorism
    - 6.2.2. Wars
    - 6.2.3. Bombs
    - 6.2.4. Dumpster Diving
7. Prevention & Detection of physical hazards
8. Premises Security
  - 8.1. Office Security
    - 8.1.1. Reception Area
    - 8.1.2. Authenticating individuals
      - 8.1.2.1. Personal Access Control
        - 8.1.2.1.1. Smart Cards
        - 8.1.2.1.2. Proximity Control
      - 8.1.2.2. Biometrics
        - 8.1.2.2.1. Process of Biometrics
        - 8.1.2.2.2. Accuracy of Biometrics
        - 8.1.2.2.3. Applications of Biometrics

8.1.2.2.3.1. Fingerprint Verification

8.1.2.2.3.2. Hand Geometry

8.1.2.2.3.3. Voice Recognition

8.1.2.2.3.4. Retina Scanning

8.1.2.2.3.5. Iris Scanning

8.1.2.2.3.5.1. Panasonic Authenticati

8.1.2.2.3.6. Facial Recognition

8.1.2.2.3.7. Biometric Signatures

8.1.2.2.4. Further Biometrics technology

8.1.2.2.5. Techniques for Compromising Biometrics

## 8.2. Workplace security

### 8.2.1. Controlling system access: Desktop security

8.2.1.1. Workstation security

8.2.1.2. Laptop Theft: Security Statistics

8.2.1.3. Laptop Theft

8.2.1.4. Laptop Security Countermeasures

8.2.1.5. Laptop Security Tools

8.2.1.6. Laptop Tracker - XTool Computer Tracker

8.2.1.7. Tools to Locate Stolen Laptops

### 8.2.2. Securing Network Devices

8.2.2.1. Server Security

8.2.2.2. Securing Backup devices

8.2.2.3. Physical Access to the Boot CD-ROM and Floppy Drives

8.2.2.4. Other equipment, such as fax, and removable media

## 8.3. CCT (Close Circuit Televisions/Cameras)

## 8.4. Parking Area

# 9. EPS (Electronic Physical Security)

- 10. Challenges in Ensuring Physical Security
- 11. Countermeasures
  - 11.1. Fencing
  - 11.2. Security force
  - 11.3. Watch Dogs
  - 11.4. Locks and Keys
  - 11.5. Physical Security: Lock Down USB Ports
  - 11.6. Tool: DeviceLock
  - 11.7. Blocking the Use of USB Storage Devices
    - 11.8. Track Stick GPS Tracking Device
    - 11.9. USB Tokens
    - 11.10. TEMPEST
    - 11.11. Fire Safety: Fire Suppression, Gaseous Emission Systems
      - 11.11.1. Fire Safety: Fire Detection
      - 11.11.2. Failures of Supporting Utilities: Heating Ventilation, Air Condition
      - 11.11.3. Failures of Supporting Utilities: Power Management and Conditioning
    - 11.12. Uninterruptible Power Supplies
- 12. Mantrap
  - 12.1. Mantrap: Diagrammatical Representation
- 13. Physical Security Checklist

## **Module: Network Security Threats**

- 1. Current Statistics
- 2. Defining Terms: Vulnerability, Threats, and Attacks
- 3. Types of Attackers
- 4. Classification of Hackers
- 5. Techniques
  - 5.1. Spamming

5.2. Revealing hidden passwords

5.3. War Dialing

5.4. War Diving

5.5. War Chalking

5.6. War Flying

5.7. Wire Tapping

5.8. Scanning

5.8.1. Port Scanning

5.8.2. Network Scanning

5.8.3. Vulnerability Scanning

5.9. Sniffing

5.9.1. Active Sniffing

5.9.2. Passive Sniffing

5.10. Network Reconnaissance

5.11. Social Engineering

6. Common Vulnerabilities and Exposures (CVE)

7. Threats

7.1. Trojan

7.2. Virus

7.2.1. IRC bot

7.3. Worms

7.4. Logic Bombs

7.5. Eavesdropping

7.6. Phishing

8. Attacks

8.1. Smurfing

8.2. Man-in-the-Middle Attacks

8.3. Denial of service

8.4. DDoS

8.5. Buffer Overflow

8.6. Zero Day Attacks

8.7. Jamming

8.8. Password Attacks

8.8.1. Brute Force Password Attacks

8.9. Spoofing

8.10. Session Hijacking

8.11. Web Page Defacement

8.12. Recording Key Strokes

8.13. Cracking Encrypted Passwords

8.14. Revealing Hidden Password

9. Hiding Evidence of an Attack

10. Problems Detecting Network Attacks

11. Network Scanning Tools:

11.1. The Netstat Tool

11.2. Nmap

11.3. NetscanTool

11.4. Superscan

11.5. hping

## **Module: Intrusion Detection System (IDS) and Intrusion Prevention Systems (IP)**

1. Introduction to IDS

2. History of Intrusion Detection

3. Intrusion Detection Concepts

3.1. Architecture

3.2. Monitoring Strategies

3.3. Analysis type

3.4. Timing

3.5. Goal of detection

3.6. Control Issues

4. IDS for an Organization

4.1. Selecting an IDS

4.2. Deploying an IDS

4.3. Maintaining an IDS

5. Characteristics of IDS

6. Importance of IDS

7. Aggregate Analysis with IDS

8. Types of IDS

8.1. Network based IDS

8.1.1. NIDS Architecture

8.1.1.1. Traditional Sensor-Based

8.1.1.2. Distributed Network Node

8.1.2. Operational Concept

8.1.2.1. Tip off

8.1.2.2. Surveillance

8.1.2.3. Forensic Workbench

8.1.3. Network-Based Detection

8.1.3.1. Unauthorized Access

8.1.3.2. Data Resource Theft

8.1.3.3. Denial of Service

8.1.3.4. Password Download

8.1.3.5. Malformed Packet

8.1.3.6. Packet Flooding

8.1.4. Tool: NetRanger

8.1.5. Tool: Bro

8.1.6. Tool: Arpwatch (in Linux)

8.1.7. Tool: Psad(in Linux)

8.1.8. Tool: ippl(in Linux)

## 8.2. Host Based IDS

### 8.2.1. HIDS Architecture

8.2.1.1. Centralized Host Based

8.2.1.2. Distributed Real Time Host Based

### 8.2.2. Operational Concept

8.2.2.1. Tip Off

8.2.2.2. Surveillance

8.2.2.3. Damage Assessment

8.2.2.4. Compliance

### 8.2.3. Host Based Detection

8.2.3.1. Abuse of Privilege Attack Scenarios

8.2.3.2. Critical data Access and Modification

8.2.3.3. Changes in Security Configuration

### 8.2.4. Tool: Host sentry

8.2.5. Tool: KFSensor

8.2.6. Tool: LIDS

8.2.7. Tool: SNARE

8.2.8. Tool: Tiger(in Linux)

## 8.3. Host Based IDS Vs Network Based IDS

## 8.4. The Hybrid IDS Framework

### 8.4.1. Prelude IDS

8.4.1.1. Components

## 8.4.1.2. Interaction between Prelude components

### 8.4.1.2.1. Relaying

### 8.4.1.2.2. Reverse Relaying

### 8.4.1.2.3. Tool: Libasfe

## 8.5. Distributed IDS

### 8.5.1. Introduction and Advantages

### 8.5.2. Components

## 8.6. Protocol Intrusion Detection System

## 8.7. Network Behavior Analysis (NBA)

## 8.8. Unified Thread Management

## 9. Deployment of IDS

## 10. Types of Signatures

### 10.1. Network signatures

### 10.2. Host based signatures

### 10.3. Compound Signatures

## 11. True/False-Positive/Negative

## 12. Major Methods of Operation

### 12.1. Signature Based Detection

### 12.2. Anomaly Based Detection

## 13. IDS Tool

### 13.1. Snort

### 13.2. BlackICE

### 13.3. M-ICE

### 13.4. Secure4Audit (auditGUARD)

### 13.5. Emerald

### 13.6. Nides

### 13.7. SECUREHOST

13.8. GFI EventsManager

14. Intrusion Prevention System

14.1. Intrusion Prevention Strategies

14.2. IPS Deployment Risks

14.3. Flexible response with Snort

14.3.1. Snort Inline Patch

14.4. Controlling your Border

15. Information Flow in IDS and IPS

15.1. Raw Packet Capture

15.2. Filtering

15.3. Packet Decoding

15.4. Storage

15.5. Fragment Reassembly

15.6. Stream Reassembly

15.7. Stateful Inspection of TCP Sessions

15.8. Firewalling

16. IPS Tool

16.1. Senticist

16.2. StoneGate IPS

16.3. McAfee

17. IDS Vs IPS

## **Module: Firewalls**

1. Firewalls: Introduction

2. Security features

2.1. Securing individual users

2.2. Perimeter security for networks

3. Multiple components of Firewall

4. Firewall Operations
5. Software Firewall
6. Hardware Firewall
7. Types of Firewalls
  - 7.1. Packet Filtering Firewall
  - 7.2. IP Packet Filtering Firewall
  - 7.3. TCP Packet Filtering Firewall
  - 7.4. Circuit-Level Gateway
  - 7.5. Application Level Firewalls
  - 7.6. Application Packet Filtering Firewall
  - 7.7. Stateful Multilayer Inspection Firewall
  - 7.8. Network Level Firewalls
8. Pix Firewall
9. Basic features of PIX firewall
10. ADvanced Features of PIX firewall
11. Firewall Features
12. Establishing Rules and Restrictions for your Firewall
13. Firewall Configuration Strategies
14. Scalability
15. Productivity
16. Firewall Architecture
  - 16.1. Dual-Homed Host Architecture
  - 16.2. Screened Host Architecture
  - 16.3. Screened Subnet Architecture
17. Handling threats and security tasks
18. Protection against hacking
19. Centralization and Documentation

- 20. Multi-layer firewall protection
- 21. Firewall deployment strategies
  - 21.1. Screened Host
  - 21.2. Two router with one firewall
  - 21.3. Introduction to Demilitarized Zone(DMZ)
  - 21.4. DMZ screened subnet
  - 21.5. Multi firewall DMZ
    - 21.5.1. Two firewalls, One DMZ
    - 21.5.2. Two firewalls, Two DMZ
  - 21.6. Screening Router
  - 21.7. Dual homed host
- 22. Specialty firewalls and Reverse firewalls
- 23. Advantages of using Firewalls
- 24. Disadvantages of using Firewalls
- 25. Threats
  - 25.1. Firewalking
  - 25.2. Banner Grabbing
  - 25.3. Placing Backdoors Through Firewalls
- 26. Limitations of Firewalls
- 27. Personal Firewall Software
  - 27.1. ZoneAlarm Pro
  - 27.2. PC-Cillin
  - 27.3. Norton Personal Firewall
  - 27.4. McAfee Personal Firewall
  - 27.5. Windows Personal Firewall
- 28. Personal Firewall Hardware
  - 28.1. Linksys and Netgear

28.2. SonicWall and Watchguard

28.3. Cisco's PIX

28.4. Netscreen

29. Firewall Log Analysis

29.1. Firewall Analyzer

29.1.1.1. Firewall Logs

29.1.1.2. Automatic Firewall Detection

29.1.1.3. Firewall Log Import

29.1.1.4. Firewall Log Archiving

29.2. Firewall Tools

29.2.1.1. Firewall Builder

29.2.1.2. Fwanalog

29.2.1.3. Wflogs

30. Comparison of Various Firewall Products

31. T-REX Open Source Firewall

32. SQUID

33. WinGate

34. Symantec Enterprise Firewall

35. Firewall Testers

35.1. Firewalk

35.2. FTester

35.3. Firewall Leak Tester

## **Module: Packet Filtering and Proxy Servers**

1. Application layer gateway

1.1. Network Address Translation

1.2. Packet Filtering

1.2.1. Approaches

1.2.2. Architecture

1.2.3. Packet Sequencing and Prioritization

1.2.4. Packet cataloging

1.2.5. Packet Fragmentation

1.2.6. Analyzing Packet Fragmentation

1.2.7. Analyzing Packet Signatures

1.2.7.1. Signature Analysis

1.2.7.2. Common Vulnerabilities and Exposure

1.2.7.3. Signatures

1.2.7.4. Normal Traffic Signatures

1.2.7.5. Abnormal Traffic Signatures

1.2.8. IP Header

1.2.9. Configuring

1.2.10. Types of Filtering

1.2.10.1. Stateful Packet Filtering

1.2.10.2. Stateless Packet Filtering

1.2.10.3. Dynamic Packet Filtering

1.2.11. Filtering rules

1.2.11.1. Packet Filter Rules That Cover Multiple Variations

1.2.11.2. Packet Filter Rules That Cover ICMP

1.2.11.3. Packet Filter Rules That Block Ping Packets

1.2.11.4. Packet Filter Rules That Enable Web Access

1.2.11.5. Packet Filter Rules That Enable DNS

1.2.11.6. Packet Filter Rules That Enable FTP

1.2.11.7. Packet Filter Rules That Enable E-Mail

1.2.12. Advantages/Disadvantages of filtering

1.2.13. Flags used

### 1.2.13.1. TCP

1.2.13.1.1. Urgent Flag

1.2.13.1.2. Ack Flag

1.2.13.1.3. Push Flag

1.2.13.1.4. Reset Flag

1.2.13.1.5. Syn flag

1.2.13.1.6. Fin Flag

### 1.2.13.2. UDP

1.2.13.2.1. Control Flag

## 2. Proxy servers

### 2.1. Role of Proxy Server

2.1.1. Routed Environment

2.1.2. Network Environment

2.1.3. Blocking URLs and unblocking URLs

### 2.2. Proxy Control

2.2.1. Transparent Proxies

2.2.2. Non-transparent Proxies

2.2.3. Socks Proxy

### 2.3. Authentication Process

2.3.1. Authentication Configuration

2.3.2. Types of Authentication

### 2.4. Firewall

2.4.1. Firewalls Based on Proxy

2.4.1.1. Application Proxy firewall

### 2.5. Installation & configuration

### 2.6. Administration and management of Proxy servers

### 2.7. Security and access control

- 2.8. Reorganizing the Single-Point-of-Failure (SPOF)
- 2.9. Reverse Proxies
- 2.10. How Proxy Servers Differ From Packet Filters
- 2.11. Performance enhancement, monitoring, and troubleshooting

## **Module: Bastion Host and Honeypots**

### 1. Bastion Hosts

#### 1.1. Principles

#### 1.2. Need of Bastion host

#### 1.3. Building a Bastion Host

##### 1.3.1. Selecting the Host Machine

###### 1.3.1.1. Memory Considerations

###### 1.3.1.2. Processor Speed

###### 1.3.1.3. Selecting the OS

#### 1.4. Configuring Bastion Host

#### 1.5. Locating Bastion Host

##### 1.5.1. Physical Location

##### 1.5.2. Network Location

##### 1.5.3. Configuring Bastion Host

##### 1.5.4. Making the Host Defend Itself

#### 1.6. Securing the Machine Itself

#### 1.7. Making the Host Defend Itself

#### 1.8. Selecting Services to be Provided

##### 1.8.1. Special Considerations for UNIX System

##### 1.8.2. Special Considerations for Windows System

#### 1.9. Disabling Accounts

#### 1.10. Disabling Unnecessary Services

#### 1.11. Limiting Ports

1.12. Handling Backups

1.13. Role of Bastion host

1.14. Bastion Host security policy

## 2. Honeypot

2.1. History of Honeypot

2.2. Value of Honeypot

2.3. Types of Honeypots

2.3.1. Production

2.3.2. Research

2.4. Classifying Honeypots by Interaction

2.4.1. Low-Interaction Honeypots

2.4.2. Medium-Interaction Honeypots

2.4.3. High-Interaction Honeypots

2.5. Examples of Honeypots

2.5.1. Backofficer Friendly

2.5.2. Specter

2.5.3. Honeyd

2.5.4. Homemade

2.5.5. Mantrap

2.5.6. Honeynet

2.6. Use of Honeypot

2.6.1. Preventing Attacks

2.6.2. Detecting Attacks

2.6.3. Responding to attacks

2.7. Homemade Honeypot

2.7.1. Port Monitoring Honeypots

2.7.2. Jailed Environment

### 2.7.3. Mantrap

## 2.8. Advantages and Disadvantages of Honey pot

## 3. Honeynet

### 3.1.1. Architecture of Honeynet

### 3.1.2. Types of Honeynet

#### 3.1.2.1. Distributed Honeynet

#### 3.1.2.2. GEN I Honeynet

#### 3.1.2.3. Gen II Honeynet

#### 3.1.2.4. Virtual Honeynet

### 3.1.3. Legal Issues related

## **Module: Securing Modems**

### 1. Introduction to Modems

### 2. Origin of Modems

### 3. Modem Features

### 4. Types of Modems

#### 4.1. Hardware Modems

##### 4.1.1. Internal Direct Connect Modem

###### 4.1.1.1. Advantages and Disadvantages of Internal Direct Modem

##### 4.1.2. External Direct Connect Modem

###### 4.1.2.1. Advantages and Disadvantages of External Direct Modem

#### 4.2. Optical Modems

#### 4.3. Short Haul Modems

#### 4.4. Smart Modem

#### 4.5. Controller Less Modem

#### 4.6. Acoustic Modem

##### 4.6.1. Advantages and Disadvantages of acoustic modem

#### 4.7. Null modems

## 5. Modem Security

### 5.1.1. Additional Security to modems

5.1.1.1. Password modems

5.1.1.2. Callback modems

5.1.1.3. Encrypting modems

5.1.1.4. Caller-ID and ANI schemes

5.1.2. Modem Security should be a priority for the telephony managers

5.1.3. SecureLogix provides Solutions for Modems Security

5.1.4. Make modem Security simple with robust Management Tool

## 6. Categorizing Modem Access

6.1. Dial out Access

6.2. Dial In Access

## 7. Modem Attacks

7.1. Spoofing Attacks

7.2. Call Forwarding Attacks

7.3. War Dialing

## 8. Modem Risks

8.1. War Dialers

8.2. Packet Sniffing

## 9. Modem Failure Symptoms

9.1. Modem Firmware Failure

9.1.1. Random modem Lock ups due to bug in firmware

9.1.2. Newer Firmware upgrades reduced the number of such lockups

9.2. Primary Modem Failure

9.2.1. No Longer drops all modems

9.2.2. Just the one Modem is lost

9.3. Reasons for modem Connection Failure

9.3.1. Modem Incompabilities

9.3.2. Buggy Modem Firmware

9.3.3. Bad Phone line

9.3.4. Misconfigured Modems or communication software

9.3.5. Temporary Modem Failures

9.4. Some Common Failures

9.4.1. Modem Not Responding

9.4.2. Modem Damaged

9.4.3. Modem Not Compatible

9.4.4. System Crashes

10. Troubleshooting Modems

10.1. External Modems

10.2. Internal Modems

## **Module: Troubleshooting Network**

1. Introduction to troubleshooting

2. Troubleshooting Network devices

2.1. Windows PC Network Interface Card

2.2. Troubleshooting Cisco Aironet Bridge

2.3. Troubleshooting bridges using the Virtualization Engine

2.4. Troubleshooting BR350 (Bridge)

2.5. Diagnosing Repeater and Gateway Problems

2.6. Troubleshooting Hubs and Switches

2.7. Troubleshooting cable modem

2.8. Troubleshooting DSL or LAN Internet Connection

2.9. Troubleshooting a Universal Serial Bus Device

2.10. Troubleshooting IEEE 1394 Bus Devices

3. Troubleshooting Network Slowdowns

3.1. NetBios Conflicts

3.2. IP Conflicts

3.3. Bad NICs

3.4. DNS Errors

3.5. Insufficient Bandwidth

3.6. Excessive Network Based Application

3.7. Daisy Chaining

3.8. Spyware Infestation

4. Troubleshooting Wireless devices

4.1. Checking the Led Indicators

4.2. Checking Basic setting

4.3. SSID

4.4. WEP Keys

4.5. Security Setting

5. A Troubleshooting Methodology

5.1. Overview of Troubleshooting

5.2. Troubleshooting Strategies

5.2.1. Recognizing Symptoms

5.2.2. Understanding The Problem

5.2.2.1. System Monitoring Tools

5.2.2.1.1. Network Monitor

5.2.2.1.2. Performance Monitors

5.2.2.1.3. Protocol Analyzer

5.2.2.1.4. The Protocol Analysis Process

5.2.3. Testing the Cause of the problem

5.2.4. Solving Problem

5.3. Device Manager

## 5.4. Troubleshooting Network Communication

### 5.4.1. Identifying Communication Problems

### 5.4.2. Using Ping and Traceroute

### 5.4.3. Exploring Network Communications

### 5.4.4. Find Path Information

### 5.4.5. Access point Interface

### 5.4.6. Identify Communication Capabilities

### 5.4.7. Load balancing

#### 5.4.7.1. Configuration Best Practices for windows 2000,wir Server

##### 5.4.7.1.1. General consideration

##### 5.4.7.1.2. Security ad Manageability

##### 5.4.7.1.3. High Availability

#### 5.4.7.2. Troubleshooting Network Load Balancing

#### 5.4.7.3. Problems and Solutions

### 5.4.8. How to isolate networking problems (Windows XP): Network Adapter

#### 5.4.8.1. Network adapter is unplugged

#### 5.4.8.2. Network adapter has limited or no connectivity

#### 5.4.8.3. Network adapter is connected, but you can't reac Internet

## 5.5. Troubleshooting Connectivity

### 5.5.1. Causes for connectivity Problem

### 5.5.2. Troubleshooting Physical Problems

### 5.5.3. Troubleshooting Link Status

### 5.5.4. Physical Troubleshooting Tools

### 5.5.5. Troubleshooting the Topology

### 5.5.6. Troubleshooting the Fault Domain

### 5.5.7. Tracing connectivity

#### 5.5.7.1. ipconfig

### 5.6. Performance Measurement Tool

#### 5.6.1. Host Monitoring Tool

#### 5.6.2. Point Monitoring tool

#### 5.6.3. Network Monitoring Tool

## 6. TCP/IP Troubleshooting Utilities

### 6.1. Troubleshooting with IP Configuration Utilities

### 6.2. Troubleshooting with Ping

### 6.3. Troubleshooting with Tracert

### 6.4. Troubleshooting with Arp

### 6.5. Troubleshooting with Telnet

### 6.6. Troubleshooting with Nostat

### 6.7. Troubleshooting with Netstat

### 6.8. Troubleshooting with FTP

### 6.9. Troubleshooting with Nslookup

### 6.10. Troubleshooting NTP

## 7. Troubleshooting Tools

### 7.1. Hardware-Based Troubleshooting Tools

### 7.2. Network Technician's Hand Tools

### 7.3. The POST Card

### 7.4. Memory Testers

### 7.5. Electrical Safety Rules

### 7.6. Wire Crimpers

### 7.7. Punch Down Tools

### 7.8. Circuit Testers

### 7.9. Voltmeters

### 7.10. Cable Testers

7.11. Crossover Cables

7.12. Hardware Loopback Plugs

7.13. LED Indicator Lights

7.14. Tone Generators

## **Module: Hardening Routers**

1. Introduction to Routers

2. Routing Metrics

3. Multiple Routing

4. Types of Routers

5. Routing Algorithms

6. Internet work Operating Systems (IOS)

7. IOS: FEATURES

8. Routing Principles

8.1. The ARP Process

8.2. LAN – to- LAN Routing Process

8.3. LAN –to- WAN Routing Process

9. Modes Of Operation

9.1. User Mode

9.2. Enable Mode

9.3. Global Configuration MODE

10. IP Routing

10.1. Configuring IP and IP routing

10.2. Configuring RIP

11. IP Source Routing

12. Configuration of Routers

12.1. External configuration sources

12.2. Internal configuration sources

- 12.3. Router Initiation
- 12.4. Loading the configuration files
- 12.5. Configuring from the TFTP Server
- 12.6. The Setup Configuration Mode
- 12.7. CLI configuration mode
- 13. Router Configuration Modes
  - 13.1. Global Configuration mode
  - 13.2. Interface Configuration mode
  - 13.3. Line Configuration Mode
  - 13.4. Privilege EXEC mode
  - 13.5. ROM Monitor mode
  - 13.6. User EXEC Mode
- 14. Finger Tool
- 15. Disabling the auxiliary and closing extra interfaces
- 16. BOOTp service
- 17. TCP and UDP small servers
- 18. Disabling Proxy ARP
- 19. Disabling SNMP
- 20. Disabling NTP
- 21. Hardening a Router
  - 21.1. Configuring a banner
    - 21.1.1. Passwords and secrets
    - 21.1.2. Encrypting passwords
    - 21.1.3. Creating end user accounts
    - 21.1.4. Setting session time-out periods
- 22. Cisco Discovery Protocol
  - 22.1. Configuring CDP

## 22.2. Logging Concept

### 22.2.1. Log Priority

### 22.2.2. Configuring Logging

### 22.2.3. Timestamping

## 22.3. Cisco Logging Options

### 22.3.1. Console Logging

### 22.3.2. Buffered Logging

### 22.3.3. Terminal Logging

### 22.3.4. Syslog Logging

### 22.3.5. SNMP Logging

## 23. Filtering Network Traffic

## 24. Access Control List

### 24.1. Basics of ACL

### 24.2. Creating Access Control List

### 24.3. ACL Types

### 24.4. Monitoring ACL

### 24.5. Implementing ACL

### 24.6. Securing Routers: ACL

## 25. Log System Error Messages

## 26. Securing Routers: Committed Access Rate

## 27. Securing Routers: Secure Shell

### 27.1. Authentication methods

### 27.2. Configuring SSH

### 27.3. Default Locations of Secure Shell Files

#### 27.3.1. Generating the Host Key

#### 27.3.2. Ciphers and MAC's

#### 27.3.3. Compression

27.3.4. Configuring Root Logins

27.3.5. Restricting User Logins

28. Router Commands

28.1. Configuring Router Interface setting

28.2. Managing Router Configuration

28.3. Reviewing IP Traffic and Configuring static Routers

29. Types of Routing

29.1. Distance Vector Routing

29.2. Link State Routing

30. Routing Protocols

30.1. Routing Information Protocol (RIP)

30.2. Interior Gateway Routing Protocol (IGRP)

30.3. Enhanced Interior Gateway Routing Protocol (EIGRP)

30.4. Open Shortest Path First (OSPF)

30.5. Border Gateway Protocol (BGP)

31. Routing Table Maintenance Protocol (RTMP)

32. Troubleshooting a router

32.1. Troubleshooting tools

32.2. Troubleshooting with network management tools

32.3. Troubleshooting IP Connectivity in Routers

32.4. Troubleshooting PPP

32.5. Troubleshooting Frame Relay

32.6. Troubleshooting X.25

32.7. Troubleshooting ISDN

33. Components of router security

34. Router security: testing tools

**Module: Hardening Operating Systems**

1. BIOS security
2. Windows Registry
  - 2.1. Registry Editor
  - 2.2. Rootkit Revealer
3. Configuring Windows Services
  - 3.1. E-mail Services
  - 3.2. Regional settings
  - 3.3. Virtual Servers
  - 3.4. Share Point Portal Server
  - 3.5. Antivirus Protection
4. Process
5. Resource Access
  - 5.1. Managing Access control
  - 5.2. Resource Access Privileges
  - 5.3. Access Lists
6. Discretionary Access Control List (DACL)
7. Privileges
8. Objects And Permissions
9. Rights Vs Permissions
10. NTFS File System Permissions
11. Encryption File System
12. Windows Network Security
  - 12.1. Computer Management
  - 12.2. File Management
  - 12.3. Security Configuration And Analysis Tool
  - 12.4. Firewalls
13. Windows infrastructure features

- 13.1. Active Directory
- 13.2. Group Policy
- 13.3. Share Security
- 13.4. Dynamic DNS updates
- 14. Kerberos Authentication And Domain Security
- 15. Trust Relationships Between Domains
- 16. IP Security
  - 16.1. Problems With IP Security
- 17. Windows Security Tools
  - 17.1. Update System
  - 17.2. Antivirus
  - 17.3. Anti Spyware
  - 17.4. Anti Spam
- 18. Windows
  - 18.1. Windows Server 2003
    - 18.1.1. Windows 2003 Infrastructure Security
    - 18.1.2. Windows 2003 Authentication
    - 18.1.3. Windows 2003 Security Configuration Tools
    - 18.1.4. Windows 2003 Resource Security
    - 18.1.5. Windows 2003 Auditing and Logging
    - 18.1.6. Windows 2003 EFS
    - 18.1.7. Windows 2003 Network Security
- 19. Windows Certificate Authorities
- 20. Certificate Authority Requirements
  - 20.1. Major Functions of a CA Hierarchy
  - 20.2. Certificate Standard and Format
  - 20.3. Implement Microsoft Certificate Authorities

## 20.4. Implement a Microsoft Enterprise Root CA

## 21. Desktop Management

### 21.1. Troubleshoot User Logons

### 21.2. Troubleshoot User Configuration

### 21.3. Troubleshoot System performance

## 22. File Management

### 22.1. Troubleshooting Access to Files And Folders

### 22.2. Troubleshooting Access to Shared Files And Folders

### 22.3. Troubleshooting Access to Offline Files and Folders

## 23. Security Issues

### 23.1. Troubleshooting User Account Control

### 23.2. Troubleshooting Windows Firewall

### 23.3. Troubleshooting Windows Defender and Locators

## 24. Linux

### 24.1. User and File system Security Administration

#### 24.1.1. Security

##### 24.1.1.1. Data Security

##### 24.1.1.2. Network Security

#### 24.1.2. OS Security Measures

##### 24.1.2.1. Linux Update Agent

##### 24.1.2.2. Configuring Unix Services

#### 24.1.3. User Management

##### 24.1.3.1. etc/password fields

##### 24.1.3.2. etc/shadow fields

#### 24.1.4. Account Security

##### 24.1.4.1. Password Security

##### 24.1.4.1.1. Shadow Password

24.1.4.2. Guest Account

24.1.4.3. User Account

24.1.4.4. etc/password fields

24.1.4.5. etc/shadow fields

24.1.4.6. etc/gshadow

24.1.4.7. etc/group

24.1.5. File System and Navigation

24.1.6. File And Directory Permissions

24.1.6.1. Default Directories

24.1.7. Network Interface configuration

24.1.8. Security Scripting

24.1.9. Useful Linux Security Tools

25. Linux Certificate Authorities

25.1. Introduction to Linux Certificate Authorities

25.2. Certificate Authorities for Linux

25.3. Preparing to Install a CA

25.4. Open LDAP

25.5. Using CATool

26. Pluggable Authentication Module

26.1. Configuring PAM

26.2. Pam Configuration Files

26.3. PAM Framework

26.4. Security With PAM

27. Network Information Services

28. Group Management Utilities

29. Network File System

30. Permission Management Tools

31. System Logger Utility

32. Unix Security

32.1. UNIX Security Checklist v2.0

33. Macintosh Security

33.1. Enterprise Security

33.1.1. Using Kerberos Authentication

33.1.2. Rendezvous Security

33.2. Application Security

33.2.1. Restricting User Capabilities

33.2.2. Command Line administration Tools

## **Module: Patch Management**

1. Introduction

2. The Patch Concept

3. Patch Sources

4. Patch testing

5. Patch Monitoring and Management

5.1. Create a Change Process

5.2. Monitor the Patch Process

6. Consolidating Patches on Red hat Network

6.1. Configuring the Proxy Server

6.2. Configuring the Proxy Client

7. Red Hat Up2date Patch Management Utility Installation Steps

8. Red Hat Up2date Patch Management: Command Line Interface

8.1. Security Patch Compliance

8.2. Distribution

8.3. Discovery and zero-touch inventory

8.4. Client Adoption

## 8.5. Troubleshoot Security Patch Management

## 8.6. Reporting

# 9. Patch Management Process

## 9.1. Identification

## 9.2. Assessment Phase

### 9.2.1. Inventory

### 9.2.2. Base Lining

## 9.3. Phase

## 9.4. Obtainment

## 9.5. Testing

## 9.6. Deploy Phase

### 9.6.1. Deployment Preparation

### 9.6.2. Deployment of the Patch

## 9.7. Confirmation

# 10. Windows Update Services

# 11. Microsoft Patch Management Tool: Microsoft Baseline Security Analyzer

## 11.1. MBSA: Scanning Updates in GUI Mode

## 11.2. MBSA: Scanning Updates in Command-line version

# 12. Patch Management Tool

## 12.1. Selecting a Tool

### 12.1.1. Learning Curve

### 12.1.2. Platform Support

### 12.1.3. System targeting

### 12.1.4. Ease of Use

### 12.1.5. Connection Sensitivity

### 12.1.6. Deployment Schedule

### 12.1.7. Cost

## 12.2. Patch Management Tools

12.2.1. Microsoft Baseline Security Analyzer

12.2.2. Qchain

12.2.3. BES Patch Management

12.2.4. Shavlik HFNetChkPro 5

12.2.5. PatchLink Update

12.2.6. SecureCentral™ PatchQuest

## **Module: Log Analysis**

1. Introduction to Log Analysis

2. Overview of log analysis

3. Audit Events

4. Log Types

4.1. Content

4.2. Source

4.3. Format

5. Log Files

5.1. Access\_log

5.1.1. Variables of Access\_log

5.2. Analysis of logs

5.2.1. access\_log

5.2.1.1. Domain type

5.2.1.2. Hours

5.2.1.3. Hits

5.2.1.4. Threading

5.2.1.4.1. Entrance

5.2.1.4.2. Exit

5.2.1.4.3. Clock Analysis

#### 5.2.1.4.4. Download Time

### 5.2.2. agent log

#### 5.2.2.1. Browser

#### 5.2.2.2. Version

#### 5.2.2.3. Operating System

### 5.2.3. error\_log

#### 5.2.3.1. Error 404

#### 5.2.3.2. Stopped Transmission

#### 5.2.3.3. Cross Reference

### 5.2.4. refer log

#### 5.2.4.1. Referral

##### 5.2.4.1.1. Missing Links

### 5.2.5. TCPDump logs

## 5.3. Web Server Log Analysis

### 5.3.1. Analog

### 5.3.2. Mach5 FastStat Analyzer

### 5.3.3. Web Trends

### 5.3.4. Happy Log

### 5.3.5. Net Merit

### 5.3.6. Click Tracks

### 5.3.7. Word Tracker

## 5.4. Apache Logs

## 5.5. IIS Logs

## 6. Limitations of log files

## 7. System Log Aggregation, Statistics And Analysis

### 7.1. Introduction To Syslog

### 7.2. Estimating log quantities and log system requirements

- 7.3. Back-hauling your logs
- 7.4. Building a central loghost
- 7.5. Parsing and normalizing
- 7.6. Bayesian spam filters for logging
- 7.7. Storage and rotation
- 7.8. Databases and logs
- 7.9. Graphing log data
- 7.10. Alerting
- 7.11. Legalities of logs as evidence

## 8. Overview of logging

- 8.1. Secure Audit Logging
- 8.2. Setting Up Remote Logging
- 8.3. Linux Process Tracking
- 8.4. Windows Logging
  - 8.4.1. Logging on Windows loghosts
  - 8.4.2. NTsyslog
  - 8.4.3. Remote Logging in Windows
- 8.5. Application Logging
- 8.6. Extended Logging
- 8.7. Firewall Logging

## 9. Monitoring for Intrusion and Security Event

- 9.1. Importance of Time Synchronization
- 9.2. Passive Detection Methods
  - 9.2.1. EventCombMT
  - 9.2.2. Event Collection
- 9.3. Scripting

## 10. Investigating Log Files

10.1. Log file Codes

10.2. Log File Information

10.3. Log Messages

11. Importance of log review

11.1. Optimizing system and network Performance

11.2. Identifying security incidents, policy violations, fraudulent activities, and operational problems

11.3. Performing audits and forensic analyses

11.4. Supporting internal investigations

11.5. Establishing baselines

11.6. Identifying operational trends and long-term problems

12. Log Analysis Tools

12.1. UserLock

12.2. WSTOOI

12.3. Auditing tools

12.3.1. ASDIC

12.3.2. Tenshi

12.3.3. SpoofMAC

12.3.4. Gentle MAC PRO

12.3.5. Log Manager

12.4. Generic Log Parsing Tools

12.4.1. LogSentry

12.4.2. SL2

12.4.3. Flog

12.4.4. Simple Log Clustering Tool(SLCT)

12.4.5. xlogmaster

12.4.6. GeekTool (mac O.S)

12.4.7. Dumpel.exe (Windows O.S)

12.4.8. Watchlog

12.4.9. LogDog

12.5. Log File Rotation Tools

12.5.1. LogController

12.5.2. Newsyslog

12.5.3. Spinlogs

12.5.4. Trimlog

12.5.5. System Log Rotation Service(SLRS)

12.5.6. Bzip2

13. How to Secure Logs(Log Security)

13.1. Limit Access To Log Files

13.2. Avoid Recording Unneeded Sensitive data

13.3. Protect Archived Log Files

13.4. Secure The Processes That Generate the Log Entries

13.5. Configure each log source to behave appropriately when logging errors occur

13.6. Implement secure mechanisms for transporting log data from the system to centralized log management servers

## **Module: Application Security**

1. Importance of Application Security

2. Why Is Web Security So Difficult?

3. Application Threats and Counter Measures

4. Web Applications

4.1. Managing Users

4.2. Managing Sessions

4.2.1. Cookies

4.2.1.1. What is in a Cookie

4.2.1.2. Working of a Cookie

4.2.1.3. Persistent Vs Non-Persistent

4.2.1.4. Secure Vs Non-Secure

4.2.2. Session Tokens

4.2.2.1. Session Tokens

4.2.2.2. Authentication Tokens

4.3. Encrypting Private Data

4.4. Event Logging

4.4.1. What to Log

4.4.2. Log Management

5. Embedded Application Security (EMBASSY)

5.1. TCP/IP security Technology

5.2. IPSec And SSL Security

5.3. IPSec And SSL Security In Embedded Systems

5.4. Network Security For Embedded Applications

5.5. Embedded Network Security Hardware Instructions

6. Secure Coding

6.1. Common Errors

6.1.1. Buffer Overflow

6.1.2. Format String Vulnerabilities

6.1.3. Authentication

6.1.4. Authorization

6.1.5. Cryptography

6.2. Best Practices For Secure Coding

6.2.1. Distrust User Input

6.2.2. Input Validation

6.2.3. Magic Switches

6.2.4. Malicious Code Detection

## **Module: Web Security**

1. Overview of Web Security
2. Common Threats On Web
  - 2.1. Identity theft
  - 2.2. Spam Mail
  - 2.3. Distributed Denial of Service(DDoS)
  - 2.4. Reflection Dos Attack
  - 2.5. Parasitic Malware
  - 2.6. Bots
  - 2.7. Cross Site Request Forgery
  - 2.8. Session Hijacking
  - 2.9. Smurf attack
  - 2.10. FTP bounce
  - 2.11. RSS/Atomic Injection
  - 2.12. DNS Attack
  - 2.13. Content Spoofing
  - 2.14. Logical Attacks
  - 2.15. Buffer Overflow
  - 2.16. IP and Routing Protocol Spoofing
3. Identifying Unauthorized Devices
4. Restrictive Access
5. Network Addresses
  - 5.1. Altering the Network Addresses
6. Tracking the Connectivity: Tracert/Traceroute
7. Testing the Traffic Filtering Devices
8. Installing and Protecting IIS
9. Client Authorization

## 9.1. Certificate Authorities

## 10. Client-Side Data

## 11. Client Authentication

### 11.1. User's Approach

### 11.2. Authentication Techniques

## 12. Input Data Validation

## 13. Browsing Analysis

## 14. Browser Security

### 14.1. Mozilla Browser

### 14.2. Internet Explorer

#### 14.2.1. Security Setting of Internet Explorer

##### 14.2.1.1. Configuring Security Zone

##### 14.2.1.2. Setting up the Internet Zone

##### 14.2.1.3. Setting up the Intranet Zone

##### 14.2.1.4. Setting up Trusted and Restricted Sites Zone

##### 14.2.1.5. Working with domain Name suffixes

##### 14.2.1.6. Selecting Custom level Settings

##### 14.2.1.7. Miscellaneous Options

##### 14.2.1.8. User Authentication

### 14.3. Browser hijacking

#### 14.3.1. Preventing

#### 14.3.2. Restoring

#### 14.3.3. Tools:

##### 14.3.3.1. Stringer

##### 14.3.3.2. Download Cwshredder

##### 14.3.3.3. Microsoft Anti Spyware software

### 14.4. Browser Analysis

14.4.1. Browser Behavior Analysis

14.4.2. Benefits of Behavior Analysis

14.5. Browser Security Settings

14.5.1. Dynamic Code

14.5.2. Securing Application Code

15. Plug-ins

15.1. Netscape/IE Plug-Ins

15.1.1. Image

15.1.1.1. IPIX

15.1.2. VRML

15.1.3. Audio

15.1.4. Multimedia

15.1.4.1. Shockwave

15.1.4.2. Real Player

15.1.4.3. Shockwave Flash

15.1.4.4. Quick Time

15.1.5. Util

15.1.5.1. Net Zip Plug-in

15.1.5.2. Asgard Plug-in Wizard

15.1.5.3. Neptune

15.1.6. Others

15.1.6.1. Java Plug-in

15.2. Mozilla Firefox Plug-ins

15.2.1. Acrobat Reader

15.2.2. Adobe Flash Player

15.2.3. Java

15.2.4. Quick Time

15.2.5. RealPlayer

15.2.6. Shockwave

15.2.7. Windows Media player

15.2.8. The Validate HTML Plug-ins

15.3. Accessibility Analyzer

15.4. Validate Sites HTML

15.5. Wayback Versions

15.6. Validate P3P

15.7. View In

15.8. BugMe Not

15.9. Webpage Speed Report

15.10. Validate Links (W3C)

15.11. Open Text

15.12. Validate RSS

15.13. Validate CSS

15.14. Validate HTML

16. Common Gateway Interface(CGI)

16.1. CGI Script

16.1.1. CGI Mechanism

16.1.2. Web Servers

16.1.3. Mechanisms and Variables

16.1.4. Third part CGI Scripts

16.1.5. Server Side Includes

16.2. CGI operation

16.2.1. Responding To the Client

16.2.2. Using the Client to call a CGI application

**Module: E-mail Security**

1. Overview of E-mail
2. History of E-mail
3. Basics of E-Mail
4. Types of E-Mail
5. Web Based Versus POP3 E-mail
6. Components of an Email
  - 6.1. Headers
    - 6.1.1. Working of an E-Mail header
    - 6.1.2. Examining an E-Mail header
    - 6.1.3. Reading E-Mail headers
  - 6.2. Opening Attachments
  - 6.3. Reading E-Mails for different clients
  - 6.4. Field names and values
  - 6.5. Address list
  - 6.6. Recipients and Senders
  - 6.7. Response targets and threading
7. E-Mail Servers
8. Testing the Email Server
9. E-Mail Encryption
  - 9.1. Centurion mail
  - 9.2. Kerberos
  - 9.3. Hush Mail
  - 9.4. Pretty good privacy
  - 9.5. Secure Hive
10. Installing WorkgroupMail
11. Configuring Outlook Express
12. Secure Email

13. Certificate Revocation
14. E-mail Authentication
  - 14.1. Mail Transfer
  - 14.2. Authenticating Sender
15. E-mail protocols// inc all protocols
  - 15.1. Multipurpose Internet Mail Extensions(MIME) /Secure MIME
  - 15.2. Pragmatic General Protocol(PGP)
  - 15.3. Simple Mail Transfer Protocol(SMTP)
    - 15.3.1. SMTP: Vulnerabilities
  - 15.4. Post Office Protocol(POP) and its POP3
  - 15.5. Internet Message Access Protocol(IMAP)
16. Client and server architecture
17. E-Mail Security Risks
  - 17.1. Spoofed Addresses
  - 17.2. Spam
  - 17.3. Hoaxes
  - 17.4. Phishing
  - 17.5. Snarfing
  - 17.6. Malware
  - 17.7. E-Mail spoofing
  - 17.8. E-Mail viruses
  - 17.9. Gateway virus scanners
  - 17.10. Outlook Viruses
  - 17.11. E-mail Attachment Security
  - 17.12. E-Mail Spamming
    - 17.12.1. Protecting against spam
    - 17.12.2. Spam filters

- 17.13. E-Mail Bombing, Chain letters
- 18. How to defend against E-Mail security risks
  - 18.1. Quarantining Suspicious Email
  - 18.2. Vulnerability check on Email System
- 19. Tools for E-mail Security
  - 19.1. ClipSecure
  - 19.2. CryptoAnywhere
  - 19.3. BCArchive
  - 19.4. CryptainerLE
  - 19.5. GfiMailEssentials
  - 19.6. SpamAware
- 20. Tracking e-mails
  - 20.1. readnotify

## **Module: Authentication: Encryption, Cryptography and Digital Signatures**

- 1. Authentication
  - 1.1. Authentication Tokens
  - 1.2. RSA SecurID
  - 1.3. Smart Cards
- 2. VeriSign Authentication
- 3. Evolution of Encryption
  - 3.1. Introduction to Encryption
  - 3.2. Encryption Systems
  - 3.3. Firewalls Implementing Encryption
  - 3.4. Lack of Encryption
  - 3.5. Cost of encryption
  - 3.6. Preserving data integrity
  - 3.7. Maintaining confidentiality

3.8. Authentication and Identification

3.9. Authenticity of N/W clients

3.10. Key Based Encryption Systems

3.10.1. Symmetric Key

3.10.2. Public Key

3.10.3. Public Key: SSL

3.11. Hashing Algorithms

3.12. Encryption Algorithms

3.12.1. RSA Algorithm

3.12.1.1. Performing RSA Encryption and Decryption

3.12.1.2. Create your RSA Key Pair

3.12.1.3. Creating RSA keys

3.12.1.4. Encrypting and Decrypting with RSA

3.12.1.5. Cracking an RSA Encrypted Message

3.12.2. Diffie Hellman Algorithm

3.12.2.1. Finding Diffie-Hellman Public Keys

3.12.3. DSS and DSA

3.12.4. ELGAMAL

3.12.5. CRYPT(3)

3.12.6. RC2 and RC4

3.12.7. IDEA

3.12.8. SNEFRU

3.12.9. RIPE-MD

3.12.10. HAVAL

3.12.11. SKIPJACK

3.12.12. XOR

3.12.13. BLOWFISH

3.12.14. camellia

3.12.15. Cast encryption algorithm

3.12.16. Tiny encryption algorithm

3.12.17. SCA: Size-Changing Algorithms

3.13. Analyzing popular encryption schemes

3.13.1. Symmetric Vs Asymmetric Encryption

3.13.2. Symmetric key encryption

3.13.3. Asymmetric key encryption

3.13.4. Hashing

3.13.5. PGP

3.13.6. X.509

3.13.7. SSL

3.14. Types of Encryption Algorithms

3.14.1. Symmetric Key Encryption

3.14.2. Password Based Encryption

3.14.3. Asymmetric key encryption

3.15. Hashing algorithms

3.16. IP Sec

3.16.1. Understanding

3.16.2. IPSec Architecture

3.16.3. Components of IPSec

3.16.4. Modes

3.16.4.1. Transport Mode

3.16.4.2. Tunnel Mode

3.16.4.3. Choosing Best IPSec Mode for Organizations

3.16.5. IPSec Processing

3.16.6. Fragmentation

3.16.7. Enabling IPsec

3.16.8. Algorithms for IPsec

3.16.9. Protocols

3.16.9.1. AH

3.16.9.2. ESP

3.16.10. Levels of IPsec

3.16.10.1. Client

3.16.10.2. Server

3.16.10.3. Secure Server

3.16.11. IPsec Protocol Security

3.16.12. IPsec Policies

3.16.12.1. IP Filters

3.16.12.2. Filter Action

3.16.12.3. Authentication Methods

3.16.12.4. Tunnel Setting

3.16.12.5. Connection Type

3.16.13. IPsec Policy Management

3.17. Cryptography

3.17.1. History of Cryptography

3.17.2. Math and Algorithms

3.17.3. Private key Exchange

3.17.4. Public Key Exchange

3.17.5. Message Authentication

3.17.5.1. DES for Encryption

3.17.5.1.1. DES ECB and CBC Analysis

3.17.5.1.2. Private Key Exchange

3.17.5.2. 3DES

### 3.17.5.3. HMAC/MD5 and SHA for Authentication

#### 3.18. Limitations

#### 4. Digital Certificates

- 4.1. Paper Certificates and Identity Cards
- 4.2. Authorities that Issue Physical Certificates
- 4.3. Difference Between Physical and Digital Certificates
- 4.4. Standards For Digital Certificates
- 4.5. X.509 as Authentication Standard
- 4.6. Public Key Certificate
- 4.7. Secret Key Certificate
- 4.8. Viewing digital certificates

#### 5. Certificate Encryption Process

- 5.1. Encrypted File System

#### 6. Public and Private Keys

- 6.1. A Public Key Generated by PGP
- 6.2. Choosing the size of keys
- 6.3. Generating Keys
- 6.4. Using a Key Server that is on a User's Network
- 6.5. Using an Online Key Server

#### 7. Digital Signatures

- 7.1. Signature as identifiers
- 7.2. Features of Digital Signatures
- 7.3. Digital Signature In practice
- 7.4. PKI
- 7.5. Standards of Digital Signatures

### **Module: Virtual Private Networks**

#### 1. Introduction to Virtual Private Network

## 2. Types of VPN

2.1. Remote Access VPN's

2.2. Intranet Access VPN's

2.3. ExtraNet VPN's

## 3. Working of VPN

3.1. Tunneling

3.2. Securing Data

3.3. Making Combination Work

## 4. Tunneling

4.1. Fundamentals of Tunneling

4.2. Tunneling Protocol

## 5. Point to point Tunneling Protocol(PPTP)

5.1. Goals And Assumptions

5.2. Terminology

5.3. Control Connections

5.4. Security And Disadvantages

## 6. Layer 2 Tunnel Protocol

6.1. Characteristics

6.2. L2TP Header Format

6.3. L2TP Control Message header

6.4. L2TP Data message

6.5. L2TP Compulsory Tunnel

6.6. L2TP Voluntary Tunnel

## 7. VPN Security

7.1. Encryption

7.2. IPSec Server

7.3. AAA Server

8. Connection to VPN
  - 8.1. SSH And PPP
  - 8.2. Concentrator
  - 8.3. Other Methods
9. Step1: Setting Up VPN
10. Step2: Implement DHCP Services
11. Step3: Create An Enterprise Certificate Authority
12. Step 4: Install IAS
13. Step 5: Configure IAS
14. Step 6: Create A Remote Access Policy
15. Step 7: Configure The VPN Server
16. Step 8: Associate The VPN Server With The DHCP Server
17. Step 9: Configure Remote Clients
18. Step 10: Test The Client Connection
19. VPN Policies
20. VPN Registrations And Passwords
21. Risk Associated With VPN
22. Pre Implementation Review – Auditing
23. Implementation Review – Auditing
24. Post Implementation Review And Reporting

## **Module: Wireless Network Security**

1. Introduction to Wireless
  - 1.1. Types of wireless networks: WLAN, WWAN, WPAN and WMAN
  - 1.2. Wired Vs. Wireless Networks
  - 1.3. Advantages and Disadvantages of Wireless
2. Types of Wireless Networks
  - 2.1. Based on Type of Connection

## 2.2. Based on Geography

### 3. Components of Wireless Network

#### 3.1. Access Points

#### 3.2. Wireless Cards

#### 3.3. Antenna

#### 3.4. Wireless Desktop Cards

#### 3.5. Wireless Laptop Cards

#### 3.6. Wireless USB Adapters

#### 3.7. Wireless Internet Video Camera

#### 3.8. Digital Media Adapter

#### 3.9. Wireless Converters

#### 3.10. Wireless Print Server

#### 3.11. Wireless Rechargeable Bluetooth mouse

### 4. Wireless Technologies

#### 4.1. Personal Communication Services(PCS)

#### 4.2. Time Division Multiple Access(TDMA)

#### 4.3. Code Division Multiple Access(CDMA)

#### 4.4. ARDIS

#### 4.5. BlueTooth

##### 4.5.1. Frequency and Data rates

##### 4.5.2. Bluetooth Architecture and components

#### 4.6. Ultra Wideband

### 5. Wireless Communications: Examples

#### 5.1. Satellite communications

#### 5.2. Cellular phone communications

### 6. Devices using Wireless Communications

#### 6.1. PDA

- 6.2. BlackBerry
- 7. Service Set Identifier (SSID)
- 8. Detecting Wireless Network
  - 8.1. How to scan
  - 8.2. Tool: Kismet
  - 8.3. Netstumbler
- 9. Types of Wireless Attacks
  - 9.1. Man in the Middle Attacks
    - 9.1.1. Eavesdropping
    - 9.1.2. Manipulation
  - 9.2. Denial of Service or Distributed Denial of Service
  - 9.3. Social Engineering
  - 9.4. "Weak key" Attacks
  - 9.5. Dictionary Attacks
  - 9.6. Birthday Attacks
- 10. Wireless Threats
  - 10.1. Rogue Access Points
  - 10.2. MAC Sniffing and AP Spoofing
- 11. Overview of Wi-Fi
  - 11.1. Hotspot
- 12. Open Wi-Fi Vulnerabilities
  - 12.1. Unauthorized Network Access
  - 12.2. Eavesdropping
- 13. WLANs in Public Space
  - 13.1. Security Vulnerabilities With Public Access Wireless Networks
- 14. Risks Due To Wireless Networks
- 15. Wired Equivalent Privacy

## 15.1. WEP Key Cracking Tools

### 15.1.1. WEPCrack

### 15.1.2. AirSnort

### 15.1.3. Aircrack

## 16. Wireless Network Attack Tool: AirSnarf

## 17. Tools to detect MAC Address Spoofing: Wellenreiter v2

## 18. WLAN Management

### 18.1. Detecting Rogue Points

## 19. Wireless Security

### 19.1. Authentication

#### 19.1.1. LDAP

##### 19.1.1.1. Communications

#### 19.1.2. Multifactor Authentication

#### 19.1.3. Authentication Mechanism

##### 19.1.3.1. Kerberos

##### 19.1.3.2. Components

##### 19.1.3.3. Exchanges Of Kerberos Client

### 19.2. WPA

### 19.3. Security Measures

#### 19.3.1. Change the SSID

#### 19.3.2. Use Encryption

#### 19.3.3. Use a VPN

#### 19.3.4. Use a Firewall

### 19.4. WLAN Security Policy Development Issues

#### 19.4.1. Goals And Characteristics

#### 19.4.2. Auditing WLAN Security Policy

### 19.5. RADIUS Authentication

19.5.1. Security

19.5.2. Configuration

20. Wireless Auditing

20.1. Baselining

21. DHCP Services

21.1. Server And Client

22. Mobile Security Through Certificates

23. Certificate Management Through PKI

24. Trouble Shooting Wireless Network

24.1. Multipath and Hidden Node

24.2. Identifying And Resolving Interface Problems

25. Wireless Network Security Checklist

### **Module: Creating Fault Tolerance**

1. Network Security: Fault Tolerance

2. Why Create Fault Tolerance

3. Planning For Fault Tolerance

4. Network Security

4.1. Key Aspect of Fault Tolerance

4.2. Fault Tolerant Network

5. Reasons for Network Failure

5.1. Viruses And Trojans

5.2. Intrusion And Unauthorized Access

5.3. Power Supply Failure

6. Reasons For System Failure

6.1. Crime

6.2. User Error

6.3. Environmental

## 6.4. Routine Events

# 7. Preventive Measures

## 7.1. Physical Security

## 7.2. Backups

### 7.2.1. Files Back up

### 7.2.2. Tape Backup – Pros And Cons

## 7.3. Practical tips

## 7.4. Setting Privileges

## 7.5. Access Rights

## 7.6. Partitions

## 7.7. Peripherals

## 7.8. UPS And Power Generators

## 7.9. RAID

### 7.9.1. RAID Level 0(Striping)

### 7.9.2. RAID Level 1(Mirroring or Duplexing)

### 7.9.3. RAID Level 2(Striping with Error Correction Code(ECC))

### 7.9.4. RAID Level 3(Striping with Parity on a single Drive)

### 7.9.5. RAID Level4(Striping by block with Parity on a single Drive)

### 7.9.6. RAID Level 5(Striping with Parity Information Spread Across Drives)

## 7.10. Clustered Servers

## 7.11. Simple Server Redundancy

## 7.12. Archiving

## 7.13. Auditing

### 7.13.1. Anatomy of Auditing

### 7.13.2. Auditing Mechanism

### 7.13.3. Audit Browsing

## 7.14. Deployment Testing

- 7.15. Circuit Redundancy
- 7.16. Offsite Storage
- 7.17. Perimeter Security
- 7.18. Understanding Vulnerabilities
- 7.19. Authentication
- 7.20. Security Policies

## **Module: Incident Response**

- 1. What is an Incident
- 2. Category of Incident
- 3. Types of Incident
- 4. Who should I report an Incident
- 5. Step by Step Procedure
- 6. Managing Incidents
- 7. What Is an Incident Response
- 8. Incident Response Architecture
- 9. Six Step Approach for Incident Handling (PICERF Methodology)
  - 9.1. Preparation
  - 9.2. Identification
  - 9.3. Containment
  - 9.4. Eradication
  - 9.5. Recovery
  - 9.6. Follow-up
- 10. Incident Response Team
  - 10.1. Basic Requirements
  - 10.2. Ways of Communication
  - 10.3. Staffing Issues
  - 10.4. Stages

11. Obstacles in Building a Successful Incident Response Team

12. Computer Security Incident Response Team

12.1. Services

12.1.1. Reactive Services

12.1.2. Proactive Services

12.1.3. Security Quality Management Services

## **Module: Disaster Recovery and Planning**

1. Overview of Disaster and its types

2. What is a Disaster Recovery

3. Principles of Disaster Recovery

4. Types of Disaster Recovery Systems

4.1. Synchronous Systems

4.2. Asynchronous Systems

5. Backup Site

6. Recovery of Small and Large Computer Systems

7. Emergency Management

8. Disaster Recovery Planning

9. Process of Disaster Recovery Plan

9.1. Organizing

9.2. Training

9.3. Implementing

9.4. Process

10. Disaster Recovery Testing

10.1. Testing Process

10.2. Testing Steps

10.3. Testing Scenarios

11. Disaster Recovery Planning Team

- 11.1. Training the Disaster Recovery Planning Team
- 12. Business Process Inventory
- 13. Risk Analysis
  - 13.1. Concept of risk Analysis
  - 13.2. Methods of Risk Analysis
  - 13.3. Process of Risk Analysis
  - 13.4. Continuous Risk Assessment
  - 13.5. Techniques To minimize Risk
- 14. Business Continuity Planning Process
  - 14.1. Business Impact Analysis
  - 14.2. Risk Assessment
  - 14.3. Other Policies, standards and process
  - 14.4. Monitoring
- 15. Business Continuity Management
- 16. Six myths about Business Continuity Management and Disaster Recovery
- 17. Disaster Prevention

**Module: Network Vulnerability Assessment**

- 1. Statistics of Network Vulnerabilities in 2006
- 2. Vulnerability Assessment
  - 2.1. Vulnerability Assessment services
  - 2.2. Advantages of Vulnerabilities Assessment services
- 3. Goals of vulnerability assessment
- 4. Features of a good vulnerability assessment
  - 4.1. Network Vulnerability Assessment Timeline
  - 4.2. Network Vulnerability Assessment Team
- 5. Vulnerability classes
- 6. Source Of Vulnerabilities

- 6.1. Design Flaws
- 6.2. Poor Security management
- 6.3. Incorrect Implementation
- 7. Choice of Personnel for Network Vulnerability Assessment
- 8. Network vulnerability Assessment methodology:
  - 8.1. Phase 1- Acquisition
  - 8.2. Phase 2 - Identification
  - 8.3. Phase 3 - Analyzing
  - 8.4. Phase 4 - Evaluation
  - 8.5. Phase 5 - Generation
- 9. How to assess vulnerability assessment tools
- 10. Selecting vulnerability assessment tools
  - 10.1. Tools:
    - 10.1.1. SAINT
    - 10.1.2. Nessus
    - 10.1.3. BindView
    - 10.1.4. Nmap
    - 10.1.5. Ethereal
    - 10.1.6. Retina
    - 10.1.7. Sandcat Scanner
    - 10.1.8. Vforce
    - 10.1.9. NVA-Team Checklist
    - 10.1.10. Tool: ScanIT Online