EC-Council Network Security Administrator
Version 4 is CNSS 4011 Approved
Course Description

The EC-Council’s Network Security Administrator certification looks at the network security in defensive view while the CEH certification program looks at the security in offensive mode. 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.

The ENSA Course is for experienced hands in the industry and is backed by a curriculum designed by the best in the field. Students can gain greater industry acceptance as seasoned Network Security professional. Students learn to configure firewalls, intrusion detection systems and AV systems. Develop effective security policy in the company.

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.

Who Should Attend

This course will significantly benefit System Administrators, System Engineers, Firewall Administrators, Network Managers, IT Managers, IT Professionals 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 Network Security Administrator certification exam 312-38 will be conducted on the last day of training. Students need to pass the online Prometric exam to receive ENSA certification.

Course Outline v4

Module I: Fundamentals of Computer 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. Historical vs. Current communication Methodology
   3.2. Asynchronous vs synchronous
   3.3. Wired media or Bounded Network Media
      3.3.1. Dedicated line
   3.4. Optical remanence
   3.5. Magnetic remanence
      3.5.1. Twisted pair cable
         3.5.1.3.1. Shielded Twisted Pair
         3.5.1.3.2. Unshielded Twisted Pair
      3.5.2. Coaxial cable or copper cable
      3.5.3. Fiber-optic cable
      3.5.4. Plenum and PVC cable
   3.6. Wireless Transmission
      3.6.1. Infrared transmission
      3.6.2. Microwave Transmission
      3.6.3. Satellite Transmission
3.6.4. Line of Sight
3.6.5. Radio frequency (e.g., bandwidth)

3.7. Public switched network
3.8. Emanations security

4. Media Access Methods
   4.8.1. Multiplexed Media Access
      4.8.1.1. TDM
      4.8.1.2. FDM
   4.8.2. Polling
   4.8.3. Token-Based Media Access
      4.8.3.1. CSMA/CD
      4.8.3.2. CSMA/CA
      4.8.3.3. Contention Domains

5. Automated Information Systems (AIS)
   5.1. Historical vs. Current Technology
   5.2. Hardware
      5.2.1. Distributed vs. stand-alone
      5.2.2. Micro, mini, mainframe processors
      5.2.3. Components
         5.2.3.1. Input, output, central processing unit (CPU)
   5.3. Software
   5.4. Memory
      5.4.1. Sequential
      5.4.2. Random
      5.4.3. Volatile vs. nonvolatile

6. Critical information characteristics
   6.1. Confidentiality
   6.2. Integrity
6.3. Availability

7. Information states
   7.1. Transmission
   7.2. Storage
   7.3. Processing

8. Operations Security (OPSEC)
   8.1. OPSEC process
   8.2. INFOSEC and OPSEC interdependency
   8.3. Unclassified indicators
   8.4. OPSEC surveys/OPSEC planning

9. Object reuse (computer security)

10. OSI Model
    10.1. Physical Layer
    10.2. Data Link Layer
    10.3. Network Layer
    10.4. Transport Layer
    10.5. Session Layer
    10.6. Presentation Layer
    10.7. Application Layer

11. Transmission Modes
    11.1. Simplex
    11.2. Half Duplex
    11.3. Full Duplex

12. Types of Transmission
    12.1. Serial Data Transmission
    12.2. Parallel Data Transmission
    12.3. Unicast Transmission
    12.4. Multicast Transmission
13. Logical Network Classification
   13.1. Client Server networking
   13.2. Peer to peer networking
   13.3. Mixed Mode Networking

14. Network Topologies
   14.1. Sharing of data
   14.2. Sharing of devices
   14.3. File servers
   14.4. Bus
      14.4.1. Linear Bus
      14.4.2. Distributed Bus
   14.5. Star or Hub
      14.5.1. Extended Star
      14.5.2. Distributed Star
   14.6. Star-Wired ring
   14.7. Ring
   14.8. Mesh
   14.9. Tree
   14.10. Hybrid Topology

15. Physical Network Classification
   15.1. LAN
   15.2. WAN
   15.3. MAN
   15.4. PAN
   15.5. CAN
   15.6. GAN

16. Network Equipments
   16.1. Network Interface Cards
16.2. Access Points
16.3. Switches
16.4. Concentrators/hub
16.5. Modem
16.6. Asynchronous vs. synchronous
16.7. Router
16.8. Brouter
16.9. Bridges
16.10. Adapters
16.11. Network Load Balancers
16.12. Repeaters
16.13. Gateways
16.14. Transceivers
16.15. Converters
16.16. Terminals

**Module II: Network Protocols**

1. Introduction to protocols
2. Implementing Network protocols
   2.1. Introduction to TCP/IP
   2.2. Configuring TCP/IP
   2.3. Configuring Netware 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. Voice Over Internet Protocol (VoIP)

3.2. Boot Strap Protocol (BOOTP)

3.3. Data Link Switching Client Access Protocol (DCAP)

3.4. Dynamic Host Configuration Protocol (DHCP)

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

3.6. File Transfer Protocol (FTP)

3.7. Trivial FTP (TFTP)

3.8. FTP and Trivial FTP: Vulnerabilities

3.9. Network Time Protocol

3.10. Network News Transfer Protocol

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

3.12. Internet Relay Chat Protocol (IRCP)

3.13. Service Location Protocol (SLP)


3.15. 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. Remote Authentication Dial-in User Service(RADIUS)  
7.3.3. VoIP  
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)
Module III: 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. Network Interface Layer
   3.2. Internet Layer
   3.3. Transport layer
   3.4. Application Layer
4. Windowing
5. Sliding Window
6. Acknowledgement
7. TCP
   7.1. Tcp header format
      7.1.1. Source port
      7.1.2. Destination port
      7.1.3. Sequence Number
      7.1.4. Acknowledgement Number
      7.1.5. Data offset
      7.1.6. Reserved
      7.1.7. Control Bits
      7.1.8. Window
      7.1.9. Checksum
      7.1.10. Urgent Pointer
      7.1.11. Options
      7.1.12. Data
7.2. TCP Interface
   7.2.1. User/TCP Interface
      7.2.1.1. User /TCP Commands
         7.2.1.1.1. Open
         7.2.1.1.2. Send
         7.2.1.1.3. Receive
         7.2.1.1.4. Close
         7.2.1.1.5. Status
         7.2.1.1.6. Abort
   7.2.2. TCP/lower -level Interface
   7.2.3. TCP/lower –level Commands
      7.2.3.1. Open call
      7.2.3.2. Listen state
      7.2.3.3. Send Call
      7.2.3.4. Receive Call
      7.2.3.5. Close Call
      7.2.3.6. Abort Call
      7.2.3.7. Status call

7.3. Algorithms in TCP
   7.3.1. Appropriate byte Counting(ABC)
   7.3.2. Additive Increase Multiplicative Decrease(AIMD)
   7.3.3. Selective Acknowledgement(SACK)
   7.3.4. TCP Friendly Rate Control(TFRC)

7.4. TCP Checksum Calculation

7.5. Performance Estimation in TCP
   7.5.1. Round Trip Time Estimation

7.6. Problems related to TCP
   7.6.1. Packet Replication
   7.6.2. Checksum Error
7.6.3. Out of order data delivery
7.6.4. Bottleneck Bandwidth
7.6.5. Packet Loss

8. IP

8.1. Overview of IP

8.2. IP Header Format
   8.2.1. Version
   8.2.2. IHL
   8.2.3. Type of Service
      8.2.3.1. Precedence
      8.2.3.2. Delay
      8.2.3.3. Throughput
      8.2.3.4. Reliability
   8.2.4. Total Length
   8.2.5. Identification
   8.2.6. Flags
   8.2.7. Fragment Offset
   8.2.8. Time to live
   8.2.9. Protocol
   8.2.10. Header Checksum
   8.2.11. Source Address/ Destination Address
   8.2.12. Options
   8.2.13. Data

8.3. IP Addressing

8.4. IP datagram
   8.4.1. Maximum Transmission Unit
   8.4.2. Fragmentation
   8.4.3. Encapsulation
   8.4.4. Formatting
   8.4.5. Reassembly
8.4.6. Delivery
8.4.7. Routing
8.4.8. Multicasting
8.4.9. Encapsulating Security Payload
   8.4.9.1. Modes in ESP
      8.4.9.1.1. Tunnel modes
      8.4.9.1.2. Transport mode
8.5. IPv6
8.6. IPv6 Header
   8.6.1. Version
   8.6.2. Priority
   8.6.3. Flowlabel
   8.6.4. Payload Length
   8.6.5. Next Header
   8.6.6. Hop limit
   8.6.7. Source Address
   8.6.8. Destination address
8.7. IPv6 Specification
8.8. Addressing
8.9. Packet Tunneling
8.10. Multicast
8.11. Hop by Hop option

**Module IV: Hardening Physical Security**

1. Need for physical security
2. Security Statistics
3. Physical Security Breach Incidents
   3.1. Who is Accountable for Physical Security?
4. Factors Affecting Physical Security
5. **Physical Security Threats**
   5.1. **Environmental threats**
      5.1.1. Floods
      5.1.2. Fire
      5.1.3. Earthquakes
   5.2. **Man Made threats**
      5.2.1. Terrorism
      5.2.2. Wars
      5.2.3. Bombs
      5.2.4. Dumpster Diving
   5.3. **Prevention & Detection of physical hazards**

6. **Premises Security**
   6.1. **Office Security**
      6.1.1. Reception Area
      6.1.2. Authenticating individuals
         6.1.2.1. Personal Access Control
            6.1.2.1.1. Smart Cards
            6.1.2.1.2. Proximity Cards
         6.1.2.2. Biometrics
            6.1.2.2.1. Process of Biometrics
            6.1.2.2.2. Accuracy of Biometrics
            6.1.2.2.3. Applications of Biometrics
               6.1.2.2.3.1. Fingerprint Verification
               6.1.2.2.3.2. Hand Geometry
               6.1.2.2.3.3. Voice Recognition
               6.1.2.2.3.4. Retina Scanning
               6.1.2.2.3.5. Iris Scanning
                  6.1.2.2.3.5.1. Panasonic Authenticam
6.1.2.2.3.6. Facial Recognition
6.1.2.2.3.7. Biometric Signatures
6.1.2.2.4. Further Biometrics technology
6.1.2.3. Techniques for Compromising Biometrics

6.1.3. Workplace security
6.1.4. Filtered power
6.1.5. Stand-alone systems and peripherals
6.1.6. Environmental controls (humidity and air conditioning)
6.1.7. Protected distributed systems

   6.1.8.1. Position sensitivity
   6.1.8.2. Employee clearances
   6.1.8.3. Access authorization/verification (need-to-know)
   6.1.8.4. Systems maintenance personnel
   6.1.8.5. Contractors

6.1.9. Controlling system access: Desktop security
   6.1.9.1. Workstation security
   6.1.9.2. Laptop Theft: Security Statistics
   6.1.9.3. Laptop Theft
   6.1.9.4. Laptop Security Countermeasures
   6.1.9.5. Laptop Security Tools
   6.1.9.6. Laptop Tracker - XTool Computer Tracker

6.1.10. Tools to Locate Stolen Laptops
6.1.11. Securing Network Devices
   6.1.11.1. Server Security
   6.1.11.2. Securing backup devices
   6.1.11.3. Physical access to the Boot CD-ROM and Floppy Drives
6.1.12. Other equipment, such as fax, and removable media
6.2. CCT (Close Circuit Televisions/Cameras)

6.3. Parking Area

7. EPS (Electronic Physical Security)

8. Challenges in Ensuring Physical Security

8.1. Countermeasures

8.2. Fencing

8.3. Security force

8.4. Watch Dogs

8.5. Locks and Keys

8.6. Physical Security: Lock Down USB Ports

8.7. Tool: DeviceLock

8.8. Blocking the Use of USB Storage Devices

8.9. Track Stick GPS Tracking Device

8.10. USB Tokens

8.10.1. TEMPEST

8.10.1.1. shielding

8.10.1.2. grounding

8.10.1.3. attenuation

8.10.1.4. banding

8.10.1.5. filtered power

8.10.1.6. cabling

8.10.1.7. Zone of control/zoning

8.10.1.8. TEMPEST separation

8.11. Fire Safety: Fire Suppression, Gaseous Emission Systems

8.11.1. Fire Detection

8.11.2. Failures of Supporting Utilities: Heating Ventilation, Air Condition

8.11.3. Failures of Supporting Utilities: Power Management and Conditioning

8.12. Uninterruptible Power Supplies
9. Mantrap

9.1. Mantrap: Diagrammatical Representation

Physical Security Checklist

**Module V: 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
5.6. Administrative Security Procedural Controls
   5.6.1. External marking of media
   5.6.2. Destruction of media
   5.6.3. Sanitization of media
   5.6.4. Construction, changing, issuing and deleting passwords
   5.6.5. Transportation of media
   5.6.6. Reporting of computer misuse or abuse
   5.6.7. Emergency destruction
   5.6.8. Media downgrade and declassification
   5.6.9. Copyright protection and licensing
5.7. Documentation, logs and journals
   5.7.1. Attribution
   5.7.2. Repudiation
6. Communication Security (COMSEC)
   6.1. Functions of COMSEC custodian
   6.2. identify and inventory COMSEC material
   6.3. access, control and storage of COMSEC material
   6.4. report COMSEC incidents
   6.5. destruction procedures for COMSEC material
7. Functions of INFOSEC Officer
8. Functions of information resources management staff
9. program or functional managers
10. security office
11. senior management
12. system manager and system staff
13. telecommunications office and staff
14. Functions of audit office
15. Functions of OPSEC managers
16. Role of end users
17. Network Security at:
   17.1. Public vs private
   17.2. Dial-up vs dedicated
   17.3. Privileges (class, nodes)
   17.4. Traffic analysis
   17.5. End-to-end access control
18. Transmission Security
   18.1. Frequency hopping
   18.2. Masking
   18.3. Directional signals
   18.4. Burst transmission
   18.5. Optical systems
18.6. Spread spectrum transmission
18.7. Covert channel control (crosstalk)
18.8. Dial back
18.9. Line authentication
18.10. Line-of-sight
18.11. Low power
18.12. Screening
18.13. Protected wireline

19. Legal Elements
19.1. Criminal prosecution
19.2. Fraud, waste and abuse
19.3. Evidence collection and preservation
19.4. Investigative authorities

20. Countermeasures: cover and deception
20.4.1. HUMINT
20.4.2. Technical surveillance countermeasures

21. Reporting security violations

Module VI: 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 VII: Security Standards
1. Introduction to Internet Standards
2. Standards Creation Committee
3. Internet Standards
   3.1. RFC Evolution
   3.2. Types and Submissions
   3.3. Obtaining RFCs
4. Cabling Standards
   4.1. EIA/TIA -568
   4.2. UTP Categories
   4.3. Cable Specifications
   4.4. Electronic Industries Association
5. Specification Standards

Module VIII: 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
   4.3. Goals of security Policies
5. Vital role of a security policy
6. Classification of Security policy
   6.1. User policies
       6.1.1. Password Management policy
6.1.2. IT policies
6.2. General Policies
6.3. Partner Policies
6.5. Policy design
7. Contents of Security Policy
8. Privacy and Confidentiality
9. Security levels
   9.1. Separation of duties, dual controls, job rotation, least privilege
   9.2. Security organization and policy development
10. Agency Specific AIS and Telecommunications Policies
    10.1. Points of contact
    10.2. References
11. Configuration of security policy
12. National Policy and Guidance
    12.1. AIS security
    12.2. Communications security
    12.3. Employee accountability for agency information
13. Implementation of security policy
14. Incident Handling and Escalation Procedures
15. Security operations and life cycle management
    15.1. Securing Assets
    15.2. Requirements definition (e.g., architecture)
    15.3. Development
    15.4. Design review and systems test
    15.5. Demonstration and validation (testing)
    15.6. Implementation
    15.7. Security (e.g., certification and accreditation)
15.8. Operations and maintenance (e.g., configuration management)

16. Defining Responses to Security Violations

17. Presenting and Reviewing the Process

18. Compliance with Law and Policy
   18.1. Intellectual Property
   18.2. Describing the Electronic Communications Privacy Act

19. Transborder encryption issues

20. Points To Remember While Writing Security Policy

   21.1. E-mail Security Policies
   21.2. Hacking

22. Creating and Managing ISSPs

Module IX: **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. IEEE p1451 Standard
3.9. ETSI Standards
3.10. HIPERLAN
3.11. HIPERMAN

Module X: Network Security Threats
1. Current Statistics
   1.1. Defining Terms: Vulnerability, Threats, and Attacks
2. Types of Attackers
3. Classification of Hackers
4. Techniques
4.1. Spamming
4.2. Revealing hidden passwords
4.3. War Dialing
4.4. War Diving
4.5. War Chalking
4.6. War Flying
4.7. Wire Tapping
4.8. Scanning
   4.8.1. Port Scanning
   4.8.2. Network Scanning
   4.8.3. Vulnerability Scanning
4.9. Sniffing
   4.9.1. Active Sniffing
   4.9.2. Passive Sniffing
4.10. Network Reconnaissance
4.11. Social Engineering
5. Common Vulnerabilities and Exposures (CVE)
   5.1. Threats
   5.2. Trojan
   5.3. Virus
      5.3.1. IRC bot
   5.4. Worms
   5.5. Logic Bombs
   5.6. Eavesdropping
   5.7. Phishing
6. Attacks
   6.1. Smurfing
   6.2. Man-in-the-Middle Attacks
6.3. Denial of service
6.4. DDoS
6.5. Buffer Overflow
6.6. Zero Day Attacks
6.7. Jamming
6.8. Password Attacks
   6.8.1. Brute Force Password Attacks
6.9. Spoofing
6.10. Session Hijacking
6.11. Web Page Defacement
6.12. Recording Key Strokes
6.13. Cracking Encrypted Passwords

7. Hiding Evidence of an Attack
8. Problems Detecting Network Attacks

9. Network Scanning Tools:
   9.1. The Netstat Tool
   9.2. Nmap
   9.3. NetscanTool
   9.4. Superscan
   9.5. Hping

Module XI: Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS)
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
   5.1. Importance of IDS
6. Aggregate Analysis with IDS
7. Types of IDS
   7.1. Network based IDS
      7.1.1. NIDS Architecture
         7.1.1.1. Traditional Sensor-Based
         7.1.1.2. Distributed Network Node
      7.1.2. Operational Concept
         7.1.2.1. Tip off
         7.1.2.2. Surveillance
         7.1.2.3. Forensic Workbench
      7.1.3. Network-Based Detection
         7.1.3.1. Unauthorized Access
         7.1.3.2. Data Resource Theft
         7.1.3.3. Denial of Service
         7.1.3.4. Password Download
         7.1.3.5. Malformed Packet
         7.1.3.6. Packet Flooding
      7.1.4. Tool: NetRanger
7.1.5. Tool: Bro
7.1.6. Tool: Arpwatch (in Linux)
7.1.7. Tool: Psad (in Linux)
7.1.8. Tool: ippl (in Linux)

7.2. Host Based IDS

7.2.1. HIDS Architecture
   7.2.1.1. Centralized Host Based
   7.2.1.2. Distributed Real Time Host Based

7.2.2. Operational Concept
   7.2.2.1. Tip Off
   7.2.2.2. Surveillance
   7.2.2.3. Damage Assessment
   7.2.2.4. Compliance

7.2.3. Host Based Detection
   7.2.3.1. Abuse of Privilege Attack Scenarios
   7.2.3.2. Critical data Access and Modification
   7.2.3.3. Changes in Security Configuration

7.2.4. Tool: Host sentry
7.2.5. Tool: KFSensor
7.2.6. Tool: LIDS
7.2.7. Tool: SNARE
7.2.8. Tool: Tiger (in Linux)

7.3. Host Based IDS vs. Network Based IDS

7.4. The Hybrid IDS Framework

7.4.1. Prelude IDS
   7.4.1.1. Components
   7.4.1.2. Interaction between Prelude components
       7.4.1.2.1. Relaying
7.4.1.2.2. Reverse Relaying

7.4.1.2.3. Tool: Libsafe

7.5. Distributed IDS
    7.5.1. Introduction and Advantages
    7.5.2. Components

7.6. Protocol Intrusion Detection System

7.7. Network Behavior Analysis (NBA)

7.8. Unified Thread Management

8. Deployment of IDS

9. Types of Signatures
    9.1. Network signatures
    9.2. Host based signatures
    9.3. Compound Signatures

10. True/False-Positive/Negative

11. Major Methods of Operation
    11.1. Signature Based Detection
    11.2. Anomaly Based Detection

12. IDS Tool
    12.1. Snort
    12.2. BlackICE
    12.3. M-ICE
    12.4. Secure4Audit (auditGUARD)
    12.5. Emerald
    12.6. Nides
    12.7. SECUREHOST
    12.8. GFI EventsManager

13. Intrusion Prevention System
    13.1. Intrusion Prevention Strategies
13.2. IPS Deployment Risks
13.3. Flexible response with Snort
   13.3.1. Snort Inline Patch
13.4. Controlling your Border
14. Information Flow in IDS and IPS
   14.1. Raw Packet Capture
   14.2. Filtering
   14.3. Packet Decoding
   14.4. Storage
   14.5. Fragment Reassembly
   14.6. Stream Reassembly
   14.7. Stateful Inspection of TCP Sessions
   14.8. Firewalling
15. IPS Tool
   15.1. Sentivist
   15.2. StoneGate IPS
   15.3. McAfee
16. IDS vs. IPS
17. Intrusion Detection Checklist

Module XII: 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. IP Packet Filtering Firewall
   7.2. Circuit-Level Gateway
   7.3. Application 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. Firewall Architecture
   15.1. Dual-Homed Host Architecture
   15.2. Screened Host Architecture
   15.3. Screened Subnet Architecture
16. Handling threats and security tasks
17. Protection against hacking
18. Centralization and Documentation
19. Multi-layer firewall protection
20. Firewall deployment strategies
   20.1. Screened Host
   20.2. Two router with one firewall
   20.3. Introduction to Demilitarized Zone(DMZ)
   20.4. DMZ screened subnet
   20.5. Multi firewall DMZ
      20.5.1. Two firewalls, One DMZ
      20.5.2. Two firewalls, Two DMZ
20.6. Screening Router
20.7. Dual homed host
21. Specialty firewalls and Reverse firewalls
22. Advantages of using Firewalls
23. Disadvantages of using Firewalls
24. Threats
   24.1. Firewalking
   24.2. Banner Grabbing
   24.3. Placing Backdoors Through Firewalls
25. Limitations of Firewalls
26. Personal Firewall Software
   26.1. ZoneAlarm Pro
   26.2. Norton Personal Firewall
   26.3. McAfee Personal Firewall
   26.4. Windows Personal Firewall
27. Personal Firewall Hardware
   27.1. Linksys and Netgear
   27.2. Cisco’s PIX
28. Firewall Log Analysis
   29.1. Firewall Analyzer
   29.1.1. Firewall Logs
   29.1.1.2. Automatic Firewall Detection
   29.1.1.3. Firewall Log Import
   29.1.1.4. Firewall Log Archiving
29. Firewall Tools
   29.2.1. Firewall Builder
   29.2.2. 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 XIII: 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. Packet Sequencing and Prioritization
      1.2.3. Packet Fragmentation
      1.2.4. Analyzing Packet Fragmentation
      1.2.5. Analyzing Packet Signatures
         1.2.5.1. Signature Analysis
         1.2.5.2. Signatures
         1.2.5.3. Normal Traffic Signatures
         1.2.5.4. Abnormal Traffic Signatures
      1.2.6. IP Header
      1.2.7. Configuring
      1.2.8. Types of Filtering
         1.2.8.1. Stateful Packet Filtering
         1.2.8.2. Stateless Packet Filtering
         1.2.8.3. Dynamic Packet Filtering
1.2.9. Filtering rules
1.2.10. Advantages/Disadvantages of filtering
1.2.11. Flags used
   1.2.11.1. TCP
      1.2.11.1.1. Urgent Flag
      1.2.11.1.2. Ack Flag
      1.2.11.1.3. Push Flag
      1.2.11.1.4. Reset Flag
      1.2.11.1.5. Syn flag
      1.2.11.1.6. Fin Flag
   1.2.11.2. UDP
      1.2.11.2.1. 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. Types of Authentication
   2.4. Firewall
      2.4.1. Firewalls Based on Proxy
         2.4.1.1. Application Proxy firewall
   2.5. Administration and management of Proxy servers
   2.6. Security and access control
2.7. Reverse Proxies

2.8. How Proxy Servers Differ From Packet Filters

Module XIV: 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
   1.9. Disabling Accounts
   1.10. Disabling Unnecessary Services
   1.11. Handling Backups
   1.12. Role of Bastion host
   1.13. 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 Honeypot
3. Honeynet
  3.8.1. Architecture of Honeynet
  3.8.2. Types of Honeynet
Module XV: 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
5.1.4. 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
   9.2. Primary Modem Failure
   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

10. Troubleshooting Modems
10.1. External Modems
10.2. Internal Modems

Module XVI: Troubleshooting Network

1. Introduction to troubleshooting
2. A Troubleshooting Methodology
   2.1. Troubleshooting Strategies
      2.1.1. Recognizing Symptoms
      2.1.2. Understanding The Problem
         2.1.2.1. System Monitoring Tools
            2.1.2.1.1. Network Monitor
            2.1.2.1.2. Performance Monitors
            2.1.2.1.3. Protocol Analyzer
            2.1.2.1.4. The Protocol Analysis Process
         2.1.2.2. Testing the Cause of the problem
      2.1.3. Solving Problem
   2.2. Device Manager
   2.3. Troubleshooting Network Communication
      2.3.1. Identifying Communication Problems
      2.3.2. Using Ping and Traceroute
      2.3.3. Exploring Network Communications
      2.3.4. Find Path Information
      2.3.5. Access point Interface
      2.3.6. Identify Communication Capabilities
      2.3.7. Load balancing
         2.3.7.1. Configuration Best Practices for windows 2000, windows Server
            2.3.7.1.1. General consideration
            2.3.7.1.2. Security ad Manageability
2.3.7.1.3. High Availability

2.3.7.2. Troubleshooting Network Load Balancing

2.3.7.3. Problems and Solutions

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

2.3.8.1. Network adapter is unplugged

2.4. Network adapter has limited or no connectivity

2.5. Network adapter is connected, but you can’t reach the Internet

2.6. Troubleshooting Connectivity

2.6.1. Causes for connectivity Problem

2.6.2. Troubleshooting Physical Problems

2.6.3. Troubleshooting Link Status

2.6.4. Physical Troubleshooting Tools

2.6.5. Troubleshooting the Topology

2.6.6. Troubleshooting the Fault Domain

2.6.7. Tracing connectivity

2.6.7.1. ipconfig

2.7. Performance Measurement Tool

2.7.1. Host Monitoring Tool

2.7.2. Point Monitoring tool

2.7.3. Network Monitoring Tool

3. Troubleshooting Network devices

3.1. Windows PC Network Interface Card

3.2. Troubleshooting Cisco Aironet Bridge

3.3. Troubleshooting bridges using the Virtualization Engine

3.4. Troubleshooting BR350 (Bridge)

3.5. Diagnosing Repeater and Gateway Problems

3.6. Troubleshooting Hubs and Switches

3.7. Troubleshooting cable modem
3.8. Troubleshooting DSL or LAN Internet Connection
3.9. Troubleshooting a Universal Serial Bus Device
3.10. Troubleshooting IEEE 1394 Bus Devices

4. Troubleshooting Network Slowdowns
   4.1. NetBios Conflicts
   4.2. IP Conflicts
   4.3. Bad NICs
   4.4. DNS Errors
   4.5. Insufficient Bandwidth
   4.6. Excessive Network Based Application
   4.7. Daisy Chaining
   4.8. Spyware Infestation

5. Troubleshooting Wireless devices
   5.1. Checking the Led Indicators
   5.2. Checking Basic setting
   5.3. SSID
   5.4. WEP Keys
   5.5. Security Settings

6. Troubleshooting Methodology

7. TCP/IP Troubleshooting Utilities
   7.1. Troubleshooting with IP Configuration Utilities
   7.2. Troubleshooting with Ping
   7.3. Troubleshooting with Tracert
   7.4. Troubleshooting with Arp
   7.5. Troubleshooting with Telnet
   7.6. Troubleshooting with Nbstat
   7.7. Troubleshooting with Netstat
   7.8. Troubleshooting with FTP
7.9. Troubleshooting with Nslookup
7.10. Troubleshooting NTP
7.11. Troubleshooting Tools
7.12. Hardware-Based Troubleshooting Tools
7.13. Network Technician’s Hand Tools
7.14. The POST Card
7.15. Memory Testers
7.16. Electrical Safety Rules
7.17. Wire Crimpers
7.18. Punch Down Tools
7.19. Circuit Testers
7.20. Voltmeters
7.21. Cable Testers
7.22. Crossover Cables
7.23. Hardware Loopback Plugs
7.24. LED Indicator Lights
7.25. Tone Generators

Module XVII: 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

33. Components of router security

34. Router security: testing tools

Module XVIII: 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
   3.6. Process
4. Resource Access
   4.1. Managing Access control
   4.2. Resource Access Privileges
   4.3. Access Lists
   4.4. Need-to-know controls
   4.5. Malicious logic protection
   4.6. Assurance
5. Discretionary Access Control List (DACL)
6. Objects And Permissions
7. Rights Vs Permissions
8. NTFS File System Permissions
9. Encryption File System
10. Windows Network Security
   10.1. Firewalls
11. Modes of Operation (Describes the security conditions under which the system actually functions)
   11.1. Dedicated security mode
   11.2. System-high security mode
   11.3. Compartmented security mode
   11.4. Multilevel security mode
12. AIS
   12.1. Hardware
   12.2. Software
   12.3. Firmware
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
   18.1.5. 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. Implement Microsoft Certificate Authorities
   20.2. Implement a Microsoft Enterprise Root CA

21. Desktop Management
   21.1. Concept of least privilege
   21.2. Internal labeling
   21.3. Troubleshoot User Logons
   21.4. Troubleshoot User Configuration
   21.5. Troubleshoot System performance

22. File Management
   22.1. Troubleshooting Access to Files And Folders
   22.2. Troubleshooting Access to Shared Files And Folders

23. Linux
   23.1. User and File system Security Administration
      23.1.1. Security
         23.1.1.1. Data Security
         23.1.1.2. Network Security
      23.1.2. OS Security Measures
         23.1.2.1. Linux Update Agent

http://www.eccouncil.org
23.1.2.2. Configuring Unix Services
23.1.2.3. Guest Account
23.1.2.4. User Account
23.1.2.5. etc/password fields
23.1.2.6. etc/shadow fields
23.1.2.7. etc/gshadow
23.1.2.8. etc/group

23.1.3. File System and Navigation
23.1.4. File And Directory Permissions
23.1.4.1. Default Directories
23.1.5. Network Interface configuration
23.1.6. Security Scripting

24. Pluggable Authentication Module
24.1. Configuring PAM
24.2. Pam Configuration Files
24.3. PAM Framework
24.4. Security With PAM

25. Network Information Services
26. Group Management Utilities
27. Permission Management Tools
28. System Logger Utility
29. Unix Security
29.1. UNIX Security Checklist v2.0
30. Macintosh Security
31. Vista security
31.1. Upgrading from XP to Windows Vista
31.2. Installing Windows Vista
31.3. Securing Windows Vista
Module XIX: Patch Management

1. Introduction
2. The Patch Concept
3. Patch testing
4. Patch Monitoring and Management
   4.1. Create a Change Process
   4.2. Monitor the Patch Process
5. Consolidating Patches on Red hat Network
   5.1. Configuring the Proxy Server
   5.2. Configuring the Proxy Client
6. Red Hat Up2date Patch Management Utility Installation Steps
7. Red Hat Up2date Patch Management: Command Line Interface
   7.1. Security Patch Compliance
   7.2. Distribution
   7.3. Discovery and zero-touch inventory
   7.4. Client Adoption
   7.5. Troubleshoot Security Patch Management
8. Reporting
9. Patch Management Process
   9.1. Identification
   9.2. Assessment Phase
      9.2.1. Inventory
      9.2.2. Base Lining
   9.3. Obtainment
   9.4. Testing
   9.5. Deploy Phase
      9.5.1. Deployment Preparation
9.5.2. Deployment of the Patch

9.6. Confirmation

10. Windows Update Services
   10.1. Microsoft Software Update Services (SUS)
   10.2. Windows Server Update Services (WSUS)
   10.3. WSUS VS SMS 2003
   10.4. Role of SMS in Patch Management Process

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. Microsoft Baseline Security Analyzer
   12.3. Qchain
   12.4. BES Patch Management
   12.5. Shavlik HFNetChkPro 5
   12.6. PatchLink Update
   12.7. SecureCentral™ PatchQuest

**Module XX: Log Analysis**

1. Introduction to Log Analysis
2. Overview of log analysis
3. Audit Events
4. Log Files
   4.1. Apache Logs
   4.2. IIS Logs
       4.2.1. IIS Logger
5. Limitations of log files
6. Monitoring for Intrusion and Security Event
   6.1. Importance of Time Synchronization
   6.2. Passive Detection Methods
       6.2.1. EventCombMT
       6.2.2. Event Collection
   6.3. Scripting
7. Log Analysis Tools
   7.1. UserLock
   7.2. WSTOOI
   7.3. Auditing tools
       7.3.1. ASDIC
       7.3.2. Tenshi
       7.3.3. SpoofMAC
       7.3.4. Gentle MAC PRO
       7.3.5. Log Manager
   7.4. Generic Log Parsing Tools
       7.4.1. LogSentry
       7.4.2. SL2
       7.4.3. Flog
       7.4.4. Simple Log Clustering Tool(SLCT)
       7.4.5. xlogmaster
7.4.6. GeekTool (mac O.S)
7.4.7. Dumpel.exe (Windows O.S)
7.4.8. Watchlog
7.4.9. LogDog
7.5. Log File Rotation Tools
   7.5.1. LogController
   7.5.2. Newsyslog
   7.5.3. Spinlogs
   7.5.4. System Log Rotation Service (SLRS)
   7.5.5. Bzip2
8. How to Secure Logs (Log Security)
   8.1. Limit Access To Log Files
   8.2. Avoid Recording Unneeded Sensitive data
   8.3. Protect Archived Log Files
   8.4. Secure The Processes That Generate the Log Entries
   8.5. Configure each log source to behave appropriately when logging errors occur
   8.6. Implement secure mechanisms for transporting log data from the system to the centralized log management servers
9. Inc setting up of Servers: IIS & Apache

Module XXI: Application Security
1. Importance of Application Security
2. Why Is Web Security So Difficult?
3. Application Threats and Counter Measures
4. Application dependent guidance
5. Web Applications
   5.1. Managing Users
   5.2. Managing Sessions
5.2.1. Cookies
  5.2.1.1. What is in a Cookie
  5.2.1.2. Working of a Cookie
  5.2.1.3. Persistent Vs Non-Persistent
  5.2.1.4. Secure Vs Non-Secure

5.2.2. Session Tokens
  5.2.2.1. Session Tokens
  5.2.2.2. Authentication Tokens

5.3. Encrypting Private Data

5.4. Event Logging
  5.4.1. What to Log
  5.4.2. Log Management

  6.1. acquisition
  6.2. design review and systems test performance (ensure required safeguards are operationally adequate)
  6.3. determination of security specifications
  6.4. evaluation of sensitivity of the application based upon risk analysis
  6.5. management control process (ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into significant modifications to existing applications)
  6.6. systems certification and accreditation process

7. Telecommunications Systems
  7.1. Hardware
  7.2. Software

  7.3. Vulnerability and threat that exist in a telecommunications system
  7.4. Countermeasures to threats

8. Securing voice communications
9. Securing data communications
10. Securing of keying material
11. Transmission security countermeasures (e.g., callsigns, frequency, and pattern forewarning protection)
12. Embedded Application Security (EMBASSY)
   12.1. TCP/IP security Technology
   12.2. IPSec And SSL Security
   12.3. IPSec And SSL Security In Embedded Systems
   12.4. Network Security For Embedded Applications
   12.5. Embedded Network Security Hardware Instructions
13. Secure Coding
   13.1. Common Errors
      13.1.1. Buffer Overflow
      13.1.2. Format String Vulnerabilities
      13.1.3. Authentication
      13.1.4. Authorization
      13.1.5. Cryptography
   13.2. Best Practices For Secure Coding
      13.2.1. Distrust User Input
      13.2.2. Input Validation
      13.2.3. Magic Switches
      13.2.4. Malicious Code Detection
   13.3. Programming standards and controls
   13.4. Change controls
   13.5. Internal labeling
14. Threat modeling
Module XXII: 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. Bots
   2.6. Cross Site Request Forgery
   2.7. Session Hijacking
   2.8. Smurf attack
   2.9. FTP bounce
   2.10. RSS/Atomic Injection
   2.11. DNS Attack
   2.12. Content Spoofing
   2.13. Logical Attacks
   2.14. Buffer Overflow
   2.15. 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. IIS Server
   8.1. Installing the IIS server
   8.2. Administering the IIS server
9. Client Authorization
9.1. Certificate Authorities

10. Client-Side Data

11. Server-side data

12. Client Authentication
   12.1. User's Approach
   12.2. Authentication Techniques

13. Input Data Validation

14. Browsing Analysis

15. Browser Security
   15.1. Mozilla Browser
   15.2. Internet Explorer
      15.2.1. Security Setting of Internet Explorer
         15.2.1.1. Configuring Security Zone
         15.2.1.2. Setting up the Internet Zone
         15.2.1.3. Setting up the Intranet Zone
         15.2.1.4. Setting up Trusted and Restricted Sites Zone
         15.2.1.5. Working with domain Name suffixes
         15.2.1.6. Selecting Custom level Settings
         15.2.1.7. Miscellaneous Options
         15.2.1.8. User Authentication
   15.3. Browser hijacking
      15.3.1. Preventing
      15.3.2. Restoring
      15.3.3. Tools:
         15.3.3.1. Stringer
         15.3.3.2. Download Cwshredder
         15.3.3.3. Microsoft Anti Spyware software
   15.4. Browser Analysis
15.4.1. Browser Behavior Analysis
15.4.2. Benefits of Behavior Analysis

15.5. Browser Security Settings
15.5.1. Dynamic Code
15.5.2. Securing Application Code

16. Plug-ins

16.1. Netscape/IE Plug-Ins
16.1.1. Image
   16.1.1.1. IPIX
16.1.2. VRML
16.1.3. Audio
16.1.4. Multimedia
   16.1.4.1. Shockwave
   16.1.4.2. Real Player
   16.1.4.3. Shockwave Flash
   16.1.4.4. Quick Time
16.1.5. Util
   16.1.5.1. Net Zip Plug-in
   16.1.5.2. Asgard Plug-in Wizard
   16.1.5.3. Neptune
16.1.6. Others
   16.1.6.1. Java Plug-in

16.2. Mozilla Firefox Plug-ins
16.2.1. Acrobat Reader
16.2.2. Adobe Flash Player
16.2.3. Java
16.2.4. Quick Time
16.2.5. RealPlayer
16.2.6. Shockwave
16.2.7. Windows Media player
16.2.8. The Validate HTML Plug-ins
16.3. Accessibility Analyzer
16.4. Validate Sites HTML
16.5. Wayback Versions
16.6. Validate P3P
16.7. View In
16.8. BugMe Not
16.9. Webpage Speed Report
16.10. Validate Links (W3C)
16.11. Open Text
16.12. Validate RSS
16.13. Validate CSS
16.14. Validate HTML
17. Common Gateway Interface (CGI)
   17.1. CGI Script
      17.1.1. CGI Mechanism
      17.1.2. Web Servers
      17.1.3. Mechanisms and Variables
      17.1.4. Third part CGI Scripts
      17.1.5. Server Side Includes
   17.2. CGI operation
      17.2.1. Responding To the Client
      17.2.2. Using the Client to call a CGI application
Module XXIII: 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. Examining an E-Mail header
      6.1.2. 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. E-Mail Encryption
   8.1. Centurion mail
   8.2. Kerberos
   8.3. Hush Mail
   8.4. Pretty good privacy
   8.5. Secure Hive
9. Installing WorkgroupMail
10. Configuring Outlook Express
11. Secure Email
12. E-mail Authentication
   12.1. Mail Transfer
12.2. Authenticating Sender

13. E-mail protocols
   13.1. Multipurpose Internet Mail Extensions (MIME) / Secure MIME
   13.2. Pragmatic General Protocol (PGP)
   13.3. Simple Mail Transfer Protocol (SMTP)
   13.4. Post Office Protocol (POP) and its POP3
       13.4.1. SMTP: Vulnerabilities
   13.5. Internet Message Access Protocol (IMAP)

14. Client and server architecture

15. E-Mail Security Risks
   15.1. Spoofed Addresses
   15.2. Spam
   15.3. Hoaxes
   15.4. Phishing
   15.5. Snarfing
   15.6. Malware
   15.7. E-Mail spoofing
   15.8. E-Mail viruses
   15.9. Gateway virus scanners
   15.10. Outlook Viruses
   15.11. E-mail Attachment Security
   15.12. E-Mail Spamming
       15.12.1. Protecting against spam
       15.12.2. Spam filters
   15.13. E-Mail Bombing, Chain letters

16. How to defend against E-Mail security risks
   16.1. Quarantining Suspicious Email
   16.2. Vulnerability check on Email System
17. Tools for E-mail Security
   17.1. ClipSecure
   17.2. CryptoAnywhere
   17.3. BCArchive
   17.4. CryptainerLE
   17.5. GfiMailEssentials
   17.6. SpamAware
18. Tracking e-mails
   18.1. readnotify

Module XXIV: Authentication: Encryption, Cryptography and Digital Signatures

1. Authentication
   1.1. Authentication Tokens
   1.2. RSA SecurID
   1.3. Smart Cards
2. VeriSign Authentication
3. Encryption
   3.1. Encryption Systems
   3.2. Firewalls Implementing Encryption
   3.3. Lack of Encryption
   3.4. Cost of encryption
   3.5. Preserving data integrity
   3.6. Maintaining confidentiality
   3.7. Authentication and Identification
   3.8. Authenticity of N/W clients
   3.9. Key Based Encryption Systems
      3.9.1. Symmetric Key
      3.9.2. Public Key
3.10. Encryption Algorithms
   3.10.1. RSA Algorithm
      3.10.1.1. Performing RSA Encryption and Decryption
      3.10.1.2. Create your RSA Key Pair
      3.10.1.3. Creating RSA keys
   3.10.2. Diffie Hellman Algorithm
      3.10.2.1. Finding Diffie-Hellman Public Keys
   3.10.3. DSS and DSA
   3.10.4. ELGAMAL
   3.10.5. RC2 and RC4
   3.10.6. IDEA
   3.10.7. SNEFRU
   3.10.8. RIPE-MD
   3.10.9. HAVAL
   3.10.10. SKIPJACK
   3.10.11. XOR
   3.10.12. BLOWFISH
   3.10.13. camellia
   3.10.14. Cast encryption algorithm
   3.10.15. Tiny encryption algorithm
   3.10.16. SCA: Size-Changing Algorithms
3.11. Analyzing popular encryption schemes
   3.11.1. Symmetric vs Asymmetric Encryption
   3.11.2. Symmetric key encryption
   3.11.3. Asymmetric key encryption
   3.11.4. Hashing
   3.11.5. PGP
   3.11.6. X.509
3.11.7. SSL

3.12. Types of Encryption Algorithms
   3.12.1. Symmetric Key Encryption
   3.12.2. Asymmetric key encryption

3.13. Hashing algorithms
   3.13.1. IPSec
   3.13.2. Understanding IPSec Architecture
   3.13.3. Components of IPSec
   3.13.4. Modes
      3.13.4.1. Transport Mode
      3.13.4.2. Tunnel Mode
      3.13.4.3. Choosing Best IPSec Mode for Organizations
   3.13.5. IPSec Processing
   3.13.6. Enabling IPSec
   3.13.7. Algorithms for IPSec
   3.13.8. Protocols
      3.13.8.1. AH
      3.13.8.2. ESP
   3.13.9. Levels of IPSec
      3.13.9.1. Client
      3.13.9.2. Server
      3.13.9.3. Secure Server
   3.13.10. IPSec Policies
      3.13.10.1. IP Filters
      3.13.10.2. Filter Action
      3.13.10.3. Authentication Methods
      3.13.10.4. Tunnel Setting
      3.13.10.5. Connection Type
4. Cryptography
   4.1. History of Cryptography
   4.2. Math and Algorithms
   4.3. Message Authentication
      4.3.1. DES for Encryption
         4.3.1.1. DES ECB and CBC Analysis
      4.3.2. 3DES
      4.3.3. HMAC/MD5 and SHA for Authentication
   4.4. Strength (e.g., complexity, secrecy, characteristics of the key)
   4.5. Cryptovariable or key

5. Digital Certificates
   5.1. Paper Certificates and Identity Cards
   5.2. Authorities that Issue Physical Certificates
   5.3. Difference Between Physical and Digital Certificates
   5.4. Standards For Digital Certificates
   5.5. X.509 as Authentication Standard
   5.6. Public Key Certificate
   5.7. Viewing digital certificates

6. Certificate Encryption Process
   6.1. Encrypted File System

7. Public and Private Keys
   7.1. A Public Key Generated by PGP
   7.2. Choosing the size of keys
   7.3. Generating Keys

8. Digital Signatures
   8.1. Signature as identifiers
   8.2. Features of Digital Signatures
   8.3. Digital Signature In practice
8.4. PKI
9. key management protocols (bundling, electronic key, over-the-air rekeying)

Module XXV: Virtual Private Networks and Remote Networking

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. Tunneling
   3.1. Fundamentals of Tunneling
4. Point to point Tunneling Protocol(PPTP)
   4.1. Goals And Assumptions
   4.2. Terminology
   4.3. Control Connections
   4.4. Security And Disadvantages
5. Layer 2 Tunnel Protocol
   5.1. Characteristics
   5.2. L2TP Header Format
   5.3. L2TP Control Message header
   5.4. L2TP Data message
   5.5. L2TP Compulsory Tunnel
   5.6. L2TP Voluntary Tunnel
6. VPN Security
   6.1. Encryption
   6.2. IPSec Server
   6.3. AAA Server
7. Connection to VPN
7.1. SSH And PPP
7.2. Concentrator
7.3. Other Methods
8. Step1: Setting Up VPN
9. Step2: Implement DHCP Services
10. Step3: Create An Enterprise Certificate Authority
11. Step 4: Install IAS
12. Step 5: Configure IAS
13. Step 6: Create A Remote Access Policy
14. Step 7: Configure The VPN Server
15. Step 8: Associate The VPN Server With The DHCP Server
16. Step 9: Configure Remote Clients
17. Step 10: Test The Client Connection
18. VPN Policies
19. VPN Registrations And Passwords
20. Risk Associated With VPN
21. Pre Implementation Review – Auditing
22. Implementation Review – Auditing
23. Post Implementation Review And Reporting
24. VPN Product Testing
25. Common VPN Flaws

Module XXVI: 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
3.12. Wireless Modems
3.13. Wireless Router
3.14. Wireless Gateways
3.15. Wireless USB
3.16. Wireless Game Adapter
3.17. Wireless Range Extender
3.18. GSM Network Devices
   3.18.1. Mobile Station
   3.18.2. Base Station Subsystem
   3.18.3. Base Station controller (BSC)
   3.18.4. Base Transceiver Station (BTS)
   3.18.5. Network Subsystem
   3.18.6. Mobile Switching Center

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
   13.2. Risks Due To Wireless Networks
14. Wired Equivalent Privacy
   14.1. WEP Key Cracking Tools
       14.1.1. WEPCrack
       14.1.2. AirSnort
       14.1.3. Aircrack
15. WAP
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

25. Wireless Network Security Checklist

Module XXVII: Creating Fault Tolerance

1. Network Security: Fault Tolerance
2. Why Create Fault Tolerance
   2.1. Planning For Fault Tolerance
3. Network Security

3.1. Key Aspect of Fault Tolerance

3.2. Fault Tolerant Network

4. Reasons for Network Failure

4.1. Viruses And Trojans

4.2. Intrusion

4.3. Power Supply Failure

5. Reasons For System Failure

5.1. Crime

5.2. User Error

5.3. Environmental

5.4. Routine Events

6. Preventive Measures

6.1. Physical Security

6.2. Backups

6.2.1. Files Back up

6.2.2. Tape Backup – Pros And Cons

6.3. Practical tips

6.4. Setting Privileges

6.5. Access Rights

6.6. Partitions

6.7. Peripherals

6.8. UPS And Power Generators

6.9. RAID

6.9.1. RAID Level 0(Striping)

6.9.2. RAID Level 1(Mirroring or Duplexing)

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

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

6.10. RAID Level 5 (Striping with Parity)

6.11. RAID Level 6 (Distributed Parity)
6.9.5. RAID Level 4 (Striping by block with Parity on a single Drive)
6.9.6. RAID Level 5 (Striping with Parity Information Spread Across Drives)

6.10. Clustered Servers
6.11. Simple Server Redundancy
6.12. Archiving
6.13. Auditing
   6.13.1. Anatomy of Auditing
   6.13.2. Auditing Mechanism
   6.13.3. Audit Browsing
   6.13.4. Effectiveness of security programs
   6.13.5. Investigation of security breaches
   6.13.6. Review of audit trails and logs
   6.13.7. Review of software design standards
   6.13.8. Review of accountability controls
   6.13.9. Verification, validation, testing, and evaluation processes

6.14. Privacy
6.15. Deployment Testing
6.16. Circuit Redundancy
6.17. Offsite Storage
6.18. Perimeter Security
6.19. Understanding Vulnerabilities
6.20. Authentication

**Module XXVIII: Incident Response**
1. What is an Incident
2. Category of Incident
3. Types of Incident
   3.1. Who should I report an Incident
4. Step by Step Procedure
   4.1. Managing Incidents
5. What Is an Incident Response
   5.1. Incident Response Architecture
6. Six Step Approach for Incident Handling (PICERF Methodology)
   6.1. Preparation
   6.2. Identification
   6.3. Containment
   6.4. Eradication
   6.5. Recovery
   6.6. Follow-up
7. Incident Response Team
   7.1. Basic Requirements
   7.2. Ways of Communication
   7.3. Staffing Issues
   7.4. Stages
8. Obstacles in Building a Successful Incident Response Team
9. Computer Security Incident Response Team
   9.1. Services
      9.1.1. Reactive Services
      9.1.2. Proactive Services
      9.1.3. Security Quality Management Services

Module XXIX: 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

   9.1. Directives and procedures for NSTISS policy
   9.2. Program budget

10. Process of Disaster Recovery Plan
    10.1. Organizing
    10.2. Training
    10.3. Implementing
       10.3.1. Process

11. Disaster Recovery Testing
    11.1. Testing Process
    11.2. Testing Steps
    11.3. Testing Scenarios

12. Contingency Planning/Disaster Recovery

13. contingency plan components, agency response procedures and continuity of operations

14. team member responsibilities in responding to an emergency situation

15. guidelines for determining critical and essential workload

16. determination of backup requirements

17. development of procedures for off-site processing

18. development of plans for recovery actions after a disruptive event

19. emergency destruction procedures

20. Disaster Recovery Planning Team
    20.1. Training the Disaster Recovery Planning Team
21. Business Process Inventory

22. Risk Analysis
   22.1. Concept of risk Analysis
   22.2. Methods of Risk Analysis
   22.3. Process of Risk Analysis
   22.4. Continuous Risk Assessment
   22.5. Techniques To minimize Risk
   22.6. Cost/benefit analysis of controls
   22.7. Implementation of cost-effective controls

23. Risk Management
   23.1. Information identification
   23.2. roles and responsibilities of all the players in the risk analysis process
   23.3. risk analysis and/or vulnerability assessment components
   23.4. risk analysis results evaluation
   23.5. corrective actions
   23.6. acceptance of risk (accreditation)

24. Business Continuity Planning Process
   24.1. Business Impact Analysis
   24.2. Risk Assessment
   24.3. Other Policies, standards and process
   24.4. Monitoring
   24.5. Business Continuity Management

25. Emergency destruction procedures

26. Six myths about Business Continuity Management and Disaster Recovery

27. Disaster Prevention
Module XXX: Network Vulnerability Assessment

1. Vulnerability Assessment
   1.1. Vulnerability Assessment services
   1.2. Goals of vulnerability assessment

2. Features of a good vulnerability assessment
   2.1. Network Vulnerability Assessment Timeline
   2.2. Network Vulnerability Assessment Team

3. Vulnerability classes

4. Source Of Vulnerabilities
   4.1. Design Flaws
   4.2. Poor Security management
   4.3. Incorrect Implementation

5. Choice of Personnel for Network Vulnerability Assessment

6. Network vulnerability Assessment methodology:
   6.1. Phase 1- Acquisition
   6.2. Phase 2 - Identification
   6.3. Phase 3 - Analyzing
   6.4. Phase 4 - Evaluation
   6.5. Phase 5 - Generation

7. How to assess vulnerability assessment tools

8. Selecting vulnerability assessment tools
   8.1. SAINT
   8.2. Nessus
   8.3. BindView
   8.4. Nmap
   8.5. Ethereal
   8.6. Retina
   8.7. Sandcat Scanner
8.8. Vforce
8.9. NVA-Team Checklist
8.10. ScanIT Online