CERTIFIED INFORMATION SECURITY EXPERT L-2 NETWORK SECURITY

1. NETWORK TOPOLOGY

- Introduction to network topology
- Why do we need Network topology?
- Types of network topology
- Issues and Problems in network topology
- Cable Connections
- Configuration of network
- Installation & Configuration of NIC

2. OPEN SYSTEMS INTERCONNECTIVITY MODEL

- Purpose of OSI model
- Need of OSI model
- Why it is used?
- 7 OSI Layers
- Interaction between the OSI Layer
- OSI Reference Model
- Data encapsulation in TCP/IP
- Advantages & Disadvantages of OSI model

3. TCP/IP IN-DEPTH

- Introduction to TCP/IP
- What is TCP/IP?
- Protocol architecture
- TCP/IP Protocol
- Modified 5 layer model
- Subnetting
- Advantages & Disadvantages of TCP/IP
- Configuration of TCP/IP

4. WAP, NAT & DNS

- Functions of NAT
- NAT Configuration
- Configuring Dynamic NAT
- DNS Introduction
- What is Domain Name?
- DNS Overview
- What services does it provide?
- How does it Operate?

5. INTERNET ROUTING

- Introduction to Internet routing
- Infrastructure
- Function of Router
- Types of Internet Routing
- IP Routing Process
- Routing Matrices
- Multicasting

6. ADVANCED PORT SCANNING

- What are ports & what is Port scanning
- How is Port scanning carried?
- Objective of Scanning
- Advanced Port Scanning Types
- Tools Used
- Port Knocking
- Protect Your identity
- How to be Untraceable

7. SNIFFING ATTACKS

- Introduction to sniffing
- Objectives of Sniffing
- How to sniff
- Tools Usage
- Ways to sniff
- Protocol Vulnerabilities to Sniffing
- Detecting Sniffers
- Prevention Techniques

8. MASQUERADING ATTACKS

- Introduction to Masquerading Attacks
- Different Ways to Masquerade
- Tools to Masquerade
- Detecting Masquerading Attacks

9. ADVANCED DOS AND DDOS

- What are DOS and DDOS Attacks?
- Understanding the working of Denial of services
- Examine Symptoms of DOS Attacks
- Modes of Attack
- Assess DOS Attack Techniques
- Prevention and detection Techniques
- DOS/DDOS Penetration testing
- Classification of DOS/DDOS Attacks

10. SESSION HIJACKING

- Introduction to Session Hijacking
- Sniffing Attack Methods
- Key Session Hijacking Techniques
- Sniffing vs. Hijacking
- Types of Session Hijacking
- Session Hijacking in OSI Model
- Session Sniffing
- Man in middle attack

11. NETWORK OPERATIONS SECURITY CENTER

- Introduction to NOSC
- NOSC General Process
- Need of NOSC
- NOSC Location

- NOSC Staff
- NOSC Operations
- Advantages and disadvantages of NOSC

12. NETWORK TRAFFIC ANALYSIS

- Introduction to Network Traffic Analysis
- Need of Network Traffic Analyzer
- Components of Network Traffic Analyzer
- Implementation of Network Traffic Analyzer
- Classification of Network traffic Analyzing
- WAN Traffic Analyzing
- Network Traffic Anomalies
- Advantages and disadvantages

13. NETWORK VULNERABILITY ASSESSMENT

- Introduction to Vulnerability Assessment
- Need of Vulnerability Assessment
- Vulnerability Detection
- Vulnerability Assessment
- Vulnerability Assessment Procedure
- Advanced Vulnerability Assessment
- Vulnerability Management

14. NETWORK PENETRATION TESTING

- Network Penetration Testing
- Objectives of Network Penetration Testing
- Difference Between P.T. and V.T.
- Types of Network Penetration Testing
- WHOIS
- Information gathered by WHOIS
- Wireshark
- NMAP showing open ports

15. INTRUSION DETECTION SYSTEM

- Introduction to IDS
- Types of IDS
- Difference between NIDS and HIDS
- Snort Intrusion Detection System
- Advantages and Disadvantages of IDS

16. SNORT 101

- Snort IDS- A Brief Overview
- Snort Architecture
- Packet Sniffer mode
- Preprocessor
- Detection Engine
- Packet logger mode
- NIDS Mode
- Snort Rules

17. OSSEC

- Introduction to OSSEC

- OSSEC Intrusion Detection System
- OSSEC Components
- OSSEC Features
- OSSEC Installation and configuration
- Advantages and Disadvantages of OSSEC

18. INTRUSION PREVENTIVE SYSTEM

- Introduction to IPS
- Difference between IPS & IDS
- Deep Packet Inspection
- Types of IPS
- Honeypot
- Defense in Depth

19. FIREWALLS

- Introduction to Firewall
- Firewall Rules
- Firewall Process
- Types of Firewalls
- Scalability and Productivity of Firewall
- Adding Functions to Firewall
- Configuring Firewall
- Adding Software and Patches

20. OS HARDENING FOR NETWORKS

- OS Hardening
- SSL and TCP/IP
- TLS
- Changing IP and MAC Address
- IPSec
- Security for Linux and MAC Address
- System Network Architecture
- APPC Security

21. CRYPTOGRAPHY

- Introduction
- Concepts and Techniques
- Symmetric Key algorithms and AES
- Asymmetric key Algorithms digital signatures and RSA
- Digital Certificates and Public key Infrastructure (PKI)
- Internet Security Protocol (Kerberos)
- User Authentication and Kerberoes

22. SYMMETRIC KEY ENCRYPTION

- Introduction to Symmetric Key Encryption
- Data Encryption Standards
- Objectives of Symmetric Key Encryption
- Issues with Symmetric key Encryption
- Advantages and disadvantages of symmetric key encryption
- Problems with Symmetric key Encryption
- Why do we need SKE?

 SKE Implementation

23. Asymmetric Key Encryption

 Introduction to Asymmetric key Encryption
 Keys Type
 Implementation
 Security of Asymmetric Key Encryption
 Problems using Asymmetric Key Encryption
 Asymmetric Keys Encryption working
 Need of Asymmetric key Encryption
 Advantages and Disadvantages of AKE

24. HASH FUNCTIONS

 Introduction to Hash Functions
 How are Hash Functions built?
 Attacks on Hash functions
 Types of Hashing
 Problems with Hash functions
 Security of Hash functions

25. TRUST MODEL

 Introduction to Trust Models
 Types of Trust
 Trust prediction problem
 Proposed models
 Problems in Trust models

26. VLAN-Security

 Introduction to VLAN
 VLAN IDs
 VTP
 Types of VLAN
 Advantages and Disadvantages of VLAN

27. VPN(VIRTUAL PRIVATE NETWORK)

 Introduction to VPN
 Categories of VPN
 Types of VPN
 Components of VPN
 VPN working
 Advantages and disadvantages of VPN

28. WIRELESS NETWORKS- INTRODUCTION

 Introduction to Wireless Networks
 History of Wireless Networks
 Types of Wireless Networks
 HiperLAN
 Wireless Architecture
 Ad hoc Routing Protocols
 Wireless security

29. RADIO FREQUENCY ESSENTIALS

 Introduction to RF

 RF Characterstics
 Bluetooth RF
 Bluetooth Essentials
 Bluetooth RF measurements
 Research Problem
 System Setup
 Software Implementation

30. WIRELESS SECURITY- BASICS

 Introduction to Wireless Security
 Types of Wireless security WEP/WPA/WPA2
 WEP Basics and workings
 WEP Security Limitations
 How to crack WEP
 WPA/WPA2 Basics and workings
 WPA/WPA2 Security limitations
 How to crack WPA/WPA2

31. WIRELESS THREATS

 Different types of wireless threats
 War Chalking
 Management Nightmare
 Ignorance
 Man in the middle attacks Monkey jack
 Authentication Missing

32. ATTACKING WIRELESS HOTSPOT AND SECURITY

 Know the Vulnerabilities
 Foot- Printing
 Wireless Scanning and Enumeration
 Gaining Access in 802.11
 War diving Protect your Wireless

33. WEP SECURITY

 Introduction to WEP
 Understand the working of WEP
 Problems with WEP
 Security in WEP
 Solutions to WEP

802.1x
802.11i
WPA
Conclusion

34. WPA/WPA2 SECURITY

 Introduction
 Brief History
 WPA2
 Robust Security Network via 802.1x
 WPA2-PSK
 Data Encryption via AES-CCMP

35. SECURE WIRELESS INFRASTRUCTURE DEPLOYMENT

- Securing a Wireless Network
- Layout of the Design
- Implementing a Wireless Network Using Password Authentication
- Configuring Wireless Network Infrastructure Components
- Testing for errors and security Leaks

36. DNS TUNNELING

- What in DNS?
- Structure of DNS Records
- How DNS tunneling works?
- DNS Tools

37. NETWORK FORENSICS

- What is Computer Forensics?
- Acquire the evidence
- Tracking the offender
- Storage Media
- Encryption and Forensics
- Data Hiding
- Hostile Code

38. EVIDENCE ACQUISITION

- Types of Acquisition
- Digital evidence storage formats
- Acquisition methods
- Contigency planning
- Using acquisition tools
- Validating data acquisition
- RAID acquisition methods
- Remote network acquisition tools

39. OS LOGS AND SPLUNK

- Feature of splunk
- Hands on splunk/working of splunk

40. SUMMARY