CYBER ZONE
TECHNOLOGIES (P) LTD

AN ISO 9001 : 2008 CERTIFIED COMPANY

Detailed Description about course module wise:

Module 1: Basics of Networking and Major Protocols

1.1 Networks and its Types.
1.2 Network Topologies
1.3 Major Protocols and their Functions
1.4 OSI Reference Model
1.5 Concept of I.P Address and its Classification
1.6 Some important Network Devices
1.7 Virtualization and its Implementation (Virtual Box)
1.8 Practice & Assignment on Networking

Module 2: Ethical hacking and Cyber Crime

2.1 Introduction to Ethical Hacking
2.2 Hackers and their Types
2.3 Phases of Hacking
2.4 Some live cases of Hacking
2.5 Cyber-crime and its current situation
2.6 Motive of Cyber frauds and Attacks
2.7 Cyber Crime Laws
2.8 Assignment

Module 3: Information Gathering (Foot Printing & Reconnaissance)

3.1 What is Foot printing?
3.2 Objectives of Foot printing
3.3 Foot printing Threats
3.4 Information Gathering with Networking skills
3.5 Information Gathering using Sites and Tools
3.6 Role of Information Gathering In Hacking World
3.7 Information Gathering Methodology of Hackers
3.8 Footprinting through Social media
3.9 Finding Website History & Other Information
3.10 Countermeasures
3.11 Practice & Assignment on Information Gathering

Module 4: Google Database Hacking & Advanced Google Hacking

4.1 Using Google as Hacking Tool (Google Hacks)
4.2 Mails Password Hacking By Google
4.3 Sensitive Files Steeling from Google
4.4 Google Hacks Tool
4.5 Passwords Steeling By Google
4.6 Google Introduction & Features
4.7 Google Search Technique
4.8 Google Basic Operators
4.9 Google Advanced Operators
4.10 Protect your information from Google
4.11 Practice & Assignment onGoogle Database Hacking

Module 5: Operating System Hacking & Security

5.1 Window Password Cracking
5.2 Bypass Login Password
5.3 View System Account
5.4 Reset Admin Password
5.5 Syskey Password
5.6 Create Backdoor in System
5.7 Security Against Windows Hacking
5.8 Folder Security & others Tips
5.9 Practice & Assignment on OS Hacking & Security

Module 6: Hacking By Trojans, Backdoors & Viruses

6.1 What Is Trojan?
6.2 Trojans Attack Cases
6.3 Types of Trojans
6.4 Binding Trojan In Different Files
6.5 How Attacker Make Undetectable Trojans
6.6 Different Way a Trojan Can get Into A system
6.7 Controlling System Remotely By Trojans
6.8 Analysis of Trojans/Virus
6.9 Security Issues Against Trojans Attack
6.10 Removing Trojans Manually and Automatic
6.11 Practice & Assignment

Module 7: Sniffing & Network Monitoring

7.1 What is Sniffing?
7.2 How a Sniffer Works?
7.3 Types of Sniffing
7.4 Protocols Vulnerable to Sniffing
7.5 Man-in-the-Middle Attacks
7.6 Mac Flooding

7.7 ARP and RARP
7.8 MAC Spoofing
7.9 ARP Poisoning Techniques
7.10 DNS Poisoning Techniques
7.11 Password Sniffing Tools
7.12 Session Capture Sniffer
7.13 Email Message Sniffer
7.14 Additional Sniffing Tools
7.15 How an Attacker Hacks the Network Using Sniffers?
7.16 How to Defend Against Sniffing?
7.17 Sniffing Prevention Techniques
7.18 Practice & Assignment

Module 8: Virus, Worms, Spyware & Analysis

8.1 What is virus, worm and spyware
8.2 History of virus and worm
8.3 Different characteristics and functioning of virus
8.4 Basic symptoms of virus-like attack
8.5 Difference Between Virus and Worm & Spyware
8.6 Indications of Virus and Worm & Spyware
8.7 Basic Working and Access Methods of Virus and Worm
8.8 Various Damages Caused by Virus and Worm
8.9 Virus and Worm &their Infection
8.10 Various Virus Detection Techniques (Manually & Automatic)
8.11 Virus and Worm Incident Response
8.12 Practice & Assignment

Module 9: Hacking Email Accounts (Advance)

9.1 Basic ways of password hacking, keylogging etc
9.2 Cookies Stealing (Session Hijacking)
9.3 System Cookie Hacking
9.4 Cookie Hacking From All or Any Browsers
9.5 Browser Cookie Hacking
9.6 Browser Tab Cookie Hacking
9.7 Advanced Phishing , Desktop Phishing
9.8 Email Spoofing Attack
9.9 Analyze the Vulnerability of Email Servers
9.10 Countermeasures
9.11 Practice & Assignment

Module 10: Data Hiding Techniques (Steganography & Cryptography)

10.1 What is Steganography?
10.2 History
10.3 Steganography today
10.4 Steganography tools

10.5 Steganalysis
10.6 What is Steganalysis?
10.7 Types of analysis
10.8 Identification of Steganographic files
10.9 Cracking Steganography programs
10.10 Forensics/Anti-Forensics
10.11 Conclusions
10.12 Cryptography
10.13 Encryption and Decryption
10.14 Cryptographic Algorithms
10.15 Practice & Assignment

Module 11: Hiding Identity

11.1 Internet Privacy,Proxy Privacy & Email Privacy
11.2 Cookies & Examining Information
11.3 How Google Stores Personal Information
11.4 (a) Web request
11.5 (b)Internet protocol address
11.6 (c) Browser type
11.7 (d) Date and time request
11.8 Unique cookie ID
11.9 Web Browser bugs
11.10 Internet relay chat
11.11 Anonymous surfing
11.12 Anonymous Browsing Toolbar
11.13 Real Time Cleaner
11.14 Protecting Search Privacy
11.15 Tips for Internet Privacy
11.16 Countermeasures
11.17 Practice & Assignment

Module 12: Proxy Server & Virtual Private Network (VPN) Technology

12.1 Use of Proxy
12.2 Why Hacker use Proxy
12.3 How we open Block website in Your College
12.4 Convert Your Machine As Proxy Server With Https Proxy
12.5 Disadvantage of Proxy
12.6 How Proxy Hack Your Passwords
12.7 What is Better then Proxy
12.8 What Is VPN?
12.9 Why We Use VPN
12.10 Advantage & Disadvantage of VPN
12.11 Free VPN
12.12 Countermeasures
12.13 Practice & Assignment

Module 13: Hacking By USB & Live Devices

13.1 Introduction USB Devices
13.2 USB Attacks
13.3 USB Hacking Tools
13.4 Create Your USB Device As Hacking Tool
13.5 Hacking By Live USB OS Devices
13.6 USB Security Tools
13.7 Countermeasures
13.8 Practice & Assignment

Module 14: Denial-of-service Attack

14.1 What is a Denial of Service Attack?
14.2 What is Distributed Denial of Service Attack
14.3 Symptoms of a DOS Attack
14.4 Shutdown Network & Website By DOS Attack
14.5 Manually DOS Attack
14.6 Automatic DOS Attack
14.7 DOS Attack Techniques
14.8 Detection Techniques
14.9 DDOS Attack Countermeasures
14.10 DOS/DDOS Protection at ISP Level
14.11 Advanced DDOS Protection
14.12 Practice & Assignment on DOS Attack

Module 15: Firewalls, Honeypots, IDS, IPS

15.1 Types of Firewall
15.2 Firewall Identification
15.3 Intrusion Detection Tool
15.4 Types of IDS
15.5 Intrusion Prevention Tool
15.6 Types of IPS
15.7 Honeypot Overview
15.8 Practice & Assignment

Module 16: Social Engineering

16.1 What is Social Engineering
16.2 Behaviors Vulnerable to Attacks
16.3 Why is Social Engineering Effective?
16.4 Warning Signs of an Attack
16.5 Phases in a Social Engineering Attack
16.6 Impact on the Organization
16.7 Common Targets of Social Engineering
16.8 Types of Social Engineering
16.9 Common Intrusion Tactics and Strategies for Prevention
16.10 Social Engineering Through Impersonation on Social Networking Sites

16.11 Risks of Social Networking to Corporate Networks
16.12 Social Networking Frauds
16.13 Identity Theft Countermeasures
16.14 Practice & Assignment

Module 17: Mobile Hacking

17.1 Call Forging
17.2 SMS Forging
17.3 Android Phone Vulnerability
17.4 Some Tricks And Tips
17.5 Countermeasures
17.6 Practice & Assignment

Module 18: Credit Card Frauds, Cases & Security

18.1 What is Credit Card Fraud?
18.2 Credit Card Cases
18.3 Type of Credit Card
18.4 Vulnerability in merchant website.
18.5 Vulnerability of Some Payment Gateway
18.6 Detection of Credit Card Fraud
18.7 Security Against Credit Card Fraud
18.8 Countermeasures
18.9 Practice & Assignment

Module 19: Website & Database Hacking Attacks

19.1 Introduction of Website & Database
19.2 Authentication Process of Web Application
19.3 Attack On Website & Web Application
19.4 OWSAP Top 10
19.5 SQL Injection attacks
19.6 Retrieve Data From Website like Username & Passwords
19.7 SQL Injection in MySql Database
19.8 Attacking Against SQL Servers
19.9 SQL Injection:-Authentication Bypassing
19.10 Maintaining Access On Website
19.11 Uploading Shell ,Viruses & Trojans On Website
19.12 XSS attacks :- (a) Reflected (b) Persistence
19.13 IIS Attack
19.14 LFI attacks
19.15 RFI attacks
19.16 Countermeasures
19.17 Assignment

Module 20: Penetration Testing & Vulnerability Assessment

20.1 What is Web Server?
20.2 How We Create a Webserver (Wamp Server etc...)
20.3 How it's Work
20.4 Web Server Vulnerability
20.5 Exploit Against Web servers
20.6 Hacking Web Server Techniques
20.7 What is Vulnerability?
20.8 Method of finding Vulnerability
20.9 Web Application Threats
20.10 What is Penetration Testing?
20.11 Penetration Testing Methodologies
20.12 Countermeasures
20.13 Practice & Assignment on VAPT

Module 21: Wi-Fi Hacking & Countermeasures

21.1 Introduction of Wi-Fi& Its Protocols
21.2 Setup & Optimizing Wireless Client
21.3 Hacking and Cracking Wireless LAN
21.4 Stealing Data After Cracking Wi-Fi Key
21.5 Securing & Managing Wireless LAN
21.6 Make Deep Security with WPA2
21.7 Wi-Fi Protected Access
21.8 Router &Wi-Fi Security
21.9 Countermeasures
21.10 Practice & Assignment

Module 22: Some Real Cyber Crime cases and their case study

Module 23: Hands on Some Important tools of Hackers Kit

Module 24: Important links and web portals

Module 25: Industry Visits and Interaction from various Experts

Module 26: Final Project.