CYBER ZONE
TECHNOLOGIES (P) LTD

AN ISO 9001 : 2008 CERTIFIED COMPANY

Global Learning and Development Services

Cyber Zone Technologies (P) Ltd (An ISO 9001 : 2008 Certified company) is leading company which is currently working in domains which involve Information Security, Cyber Crime – training and investigations, Ethical Hacking and Professional training in various I.T domains. Having expertise in Cyber security domain and Police trainings, Cyber Zone is going to extend its wings in Software and Web development sector, Publication, Outsourcing, Online Courses, and Boot Camps etc. So be part of our team and join hands with us to achieve new heights in your respective domain.

Our Services Includes

- Vulnerability Assessment and Penetration Testing.
- Network Testing and Security Audits.
- LAN Management and Maintenance.
- Cyber Crime Investigation and Forensics.
- Customized Trainings which include On Campus, Off Campus, Summer Training, Industrial Training and Boot Camps.
- Corporate Training and Faculty Development Programs.
- Outsourcing various project of I.T sector, Web and Software Development.

www.cyberzone.org.in

Advanced Certification in Cyber & Information Security

Course Objectives: This training program is specially designed to give trainee a very concrete base to make their career in Information Security and related domains such as Ethical Hacking, Information security, Network security, Penetration testing etc. By equipping trainee with all the nitty-gritty involved in this domain.

- To make very clear and concrete image of Ethical Hacking Domain under standards rules and laws.
- To provide all conceptual and practical knowledge to counter all types of cyber-attacks in a professional manner.
- To provide training on real time situations to have better understanding of every minute concept.
- Special emphasis on Standard operational Procedure followed in any testing process (Vulnerability Assessment and Penetration Testing).

Course Benefits:-

- Class apart content and modules.
- Greater emphasis on practical and real scenario.
- Industry relevant practices and standard working procedures.
- Project work on each module to test the grip on particular topic.
- Testing and Auditing on live system to have better concept.

Carrier Benefits:-

- A strong foundation for long term carrier in Information Security Domain.
- An edge for your competitors as an extra knowledge and Area of work.
- Emerging carrier, high market value with evergreen scope and rise.
- Huge demand in Private as well as in Government Sectors to counter Cyber Attacks.

Benefits for Law Enforcement Agencies:-

- Will help in protecting all digital assets of their Agency.
- Maintaining and applying All Standard Security policies in their organization.
- Countering all types of Cyber-attacks by self -testing basis (Penetration Testing).
- Induction in various departments as I.T officers, Cyber Crime Cells and Digital investigation Agencies.

Job Profile:

InfoSec consultant ,Vulnerability Tester , Information Security Auditor, Penetration Tester, Computer Forensic Investigator ,Forensic Analyst , Security Analyst ,IT Officer, Cyber Crime Investigator etc.

Time duration: 1 Year

Training methodology: On – Campus, Boot Camp, and Online – Mode, weekend days, etc)

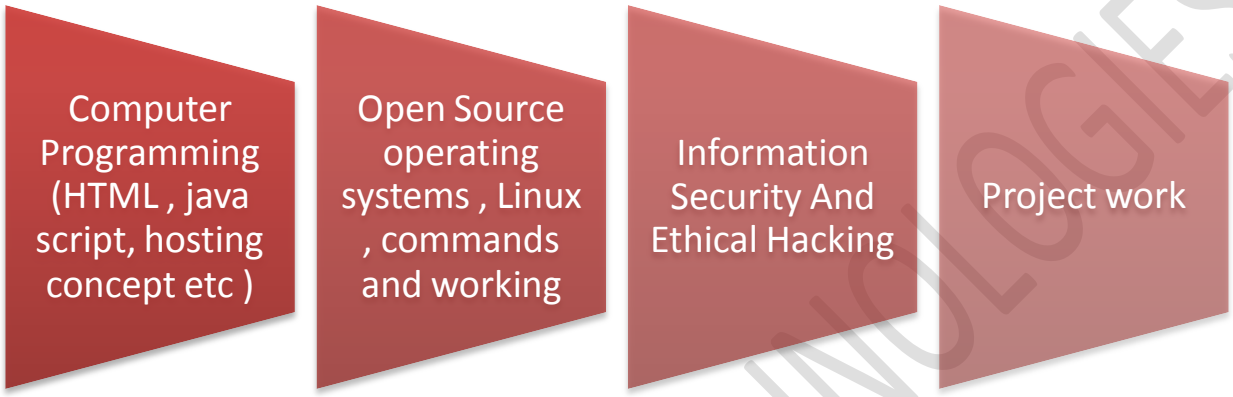
(For Law Enforcement Agencies Personnel's one to one option is also available in applicable cases).

Note: This training module is only for the purpose of knowledge based learning and not for any other purpose. The management and mentors of cyber zone will not be responsible for any illegal/Unlawful activity done by any trainee. The term ethical hacking actually means testing in a positive manner for checking loopholes present in various IT Systems. Our purpose of ethical hacking is to evaluate the security

Advanced Certification in Cyber and Information Security

Course Outline

Major Classification:



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 Proxy Server
1.7 Virtual Private Network (VPN)
1.8 Some important Network Devices
1.9 Virtualization and its Implementation (Virtual Box)
1.10 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 on Google 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 13: Hacking By USB & Live Devices

12.1 Introduction USB Devices
12.2 USB Attacks
12.3 USB Hacking Tools
12.4 Create Your USB Device As Hacking Tool
12.5 Hacking By Live USB OS Devices
12.6 USB Security Tools
12.7 Countermeasures
12.8 Practice & Assignment

Module 15: Firewalls, Honeypots, IDS, IPS

13.1 Types of Firewall
13.2 Firewall Identification
13.3 Intrusion Detection Tool
13.4 Types of IDS
13.5 Intrusion Prevention Tool
13.6 Types of IPS
13.7 Honeypot Overview
13.8 Assignment

Module 16: Social Engineering

14.1 What is Social Engineering
14.2 Behaviors Vulnerable to Attacks
14.3 Why is Social Engineering Effective?
14.4 Warning Signs of an Attack
14.5 Phases in a Social Engineering Attack
14.6 Impact on the Organization
14.7 Common Targets of Social Engineering
14.8 Types of Social Engineering
14.9 Common Intrusion Tactics and Strategies for Prevention
14.10 Social Engineering Through Impersonation on Social Networking Sites
14.11 Risks of Social Networking to Corporate Networks

14.12 Social Networking Frauds
14.13 Identity Theft Countermeasures
14.14 Assignment

Module 19: Website & Database Hacking Attacks

15.1 Introduction of Website & Database
15.2 Authentication Process of Web Application
15.3 Attack On Website & Web Application
15.4 OWSAP Top 10
15.5 SQL Injection attacks
15.6 Retrieve Data From Website like Username & Passwords
15.7 SQL Injection in MySql Database
15.8 Attacking Against SQL Servers
15.9 SQL Injection:-Authentication Bypassing
15.10 Maintaining Access On Website
15.11 Uploading Shell ,Viruses & Trojans On Website
15.12 XSS attacks :- (a) Reflected (b) Persistence
15.13 IIS Attack
15.14 LFI attacks
15.15 RFI attacks
15.16 Countermeasures
15.17 Assignment

Module 20: Penetration Testing & Vulnerability Assessment

16.1 What is Web Server?
16.2 How We Create a Webserver (Wamp Server etc...)
16.3 How it's Work
16.4 Web Server Vulnerability
16.5 Exploit Against Web servers
16.6 Hacking Web Server Techniques
16.7 What is Vulnerability?
16.8 Method of finding Vulnerability
16.9 Web Application Threats
16.10 What is Penetration Testing?
16.11 Penetration Testing Methodologies
16.12 Countermeasures
16.13 Assignment on VAPT

Module 21:Wi-Fi Hacking & Countermeasures

17.1 Introduction of Wi-Fi& Its Protocols
17.2 Setup & Optimizing Wireless Client
17.3 Hacking and Cracking Wireless LAN
17.4 Stealing Data After Cracking Wi-Fi Key
17.5 Securing & Managing Wireless LAN
17.6 Make Deep Security with WPA2
17.7 Wi-Fi Protected Access
17.8 Router &Wi-Fi Security

17.9 Countermeasures
17.10 Assignment

Note:

- ✓ Each project module has to be submitted by the trainee separately as part of course – curriculum.
- ✓ Regular test, online activity and participation are also must to fulfill the course criteria.
- ✓ Confidentiality and integrity of the course should be maintained in a professional manner.
- ✓ Trainees have to follow all the instruction as laid by the company guidelines at the start of the course.
- ✓ Certificate will only be generated on obtaining no dues and after submitting all the project on given time.