TechForing
Shaping Tomorrow's Cybersecurity

Cybersecurity Training Program

Course Overview

This course aims to enhance the skill of an IT Professional/ Programmer and Security Engineer to an advance level where they will learn hands on practical about IT Security, how hackers perform real life attacks , how to prevent them and do incidence response with 360 degree in depth digital forensic analysis.

This course has three different levels which can be taken at once or step by step.

1. **Short**
   Duration: 2 Weeks (10 Working Days, 2 to 4 hrs/ Day)
   Reference No: Module 1 to 12

2. **Medium**
   Duration: 4 Weeks (20 Working Days, 2 to 4 hrs/ Day)
   Reference No: Module 1 to 20

3. **Long**
   Duration: 8 Weeks (40 Working Days, 2 to 4 hrs/ Day)
   Reference No: Module 1 to 40

Cybersecurity Training for Non IT Professionals

Course Overview

These days, every business needs cybersecurity training for employees to prevent security breach and to stay in sync with the latest cyber threats. We have online and on your business premise class facilities to collectively aware your IT team or employees about the best cybersecurity practices and policies.

The curriculum for this course can be found at the end of this document.

Course Delivery Option

- Onsite Instructor-Led Training

Our Cybersecurity trainers visit corporate houses, company offices, educational institutes, and law enforcement agencies to provide hands-on training.

- Online Instructor-Led Training

Suitable for remotely working employees or anyone unable to attend the onsite training.

About Instructors

Our Instructors are Industry Expert.
We have cybersecurity experts worldwide with top security certifications like C|EH, CHFI, CISA, CISSP, Security+. They worked with various Government and non-government agencies, providing security support with Data Protection. The fantastic work ethic and quality of service they possess are reflected in our clientele.

They understand the tech arena and well-versed with all the latest potential cyber threats that can occur in an organization. We, Techforing, want to use this wealth of knowledge in educating the IT sector and every individual with their data privacy.

Upon client's request TechForing can provide both national and international instructors.

Why Choose TechForing Academy

- **Learn from the Experts**

Top-class instructors booming with confidence, who hold C|EH, CHFI, CISA, CISSP, and Security+ certifications, will conduct the classes.

- **Skills Development and Assessment**

The trainee will be able to learn about the latest cybersecurity tools and techniques and assess the IT infrastructure of his workplace.

- **Hands on practice**

Virtual labs, assignments, and practice tests are just what you need to stay on track with real-world experiences

- **Industry Recognition**

Collaborating with the best expands your professional network and helps you gain more exposure in the cybersecurity industry.

Course Curriculum (IT Professionals)

Short

Best program to develop basic foundation of IT Security and overall best practices along with in depth hands on practical in web, network and system VAPT.

1. Cybersecurity Foundations

2. Payment card fraud
   - Application fraud
   - Account takeover
   - Social engineering fraud
   - Skimming
   - Unexpected repeat billing
   - Spam & Phishing
   - Corporate Account Takeover (CATO)
   - Automated Teller Machine (ATM) Cash Out
   - Credential Stuffing

3. Foot Printing and Enumeration
   - What is Foot Printing
   - Objectives of Foot Printing
   - What is Enumeration
   - Information gathering Tool: Web Data Extractor
   - Finding an organization's details / domain name / Internal & Public and Restricted URLs
   - Finding an organization's Server details
   - Finding the details of domain registration
   - Finding the location of servers
   - Tracking e-mail communications

4. Penetration Testing Tools
   - Introduction with penetration testing tools
   - Hacking Web servers and Web applications
   - Uses of Proxy Tools: Burp-Suite, Live HTTP Headers
   - Uses of Exploitation Tools: SQL map

5. SQL Injection -01 (Introduction & Basic SQLi)
   - What is SQL Injection and Why Occurs?
   - Types of SQL Injection
   - Impact of SQLi
   - Understanding SQL injection

- Detection of SQL injection
- Finding Suitable Injecting Point
- Conduct Injection, Disclosing Database, Tables and Column

6. SQL Injection -03 (Getting Administrative Access)
    - Conduct Regular/ Union Based Injection
    - Collecting Sensitive Information (email, username, Passwords)
    - Cracking password hashes
    - Finding user or administrator panel
    - Authentication bypass and Gaining access
    - Login as an Admin/ Authorized Person

7. Cryptography and Steganography
    - What is Cryptography?
    - Types of Cryptography
    - Encryption-Decryption techniques
    - Hashing functions
    - Different Types of Encoding Methods
    - Basic concept of steganography
    - Steganography in media files
    - Exif a media to detect malicious codes

8. Web Application vulnerabilities and attack simulation – 01
    - Cross site Scripting(XSS)
    - HTML Injection
    - iFrame Injection
    - LDAP Injection
    - Cross-site request forgery (CSRF)
    - Mail header injection

9. Web Application vulnerabilities and attack simulation – 02
    - Broken Authentication
    - PHP code injection
    - Insecure Direct Object Reference (IDOR)
    - Security Misconfiguration
    - Sensitive data exposure
    - Unrestricted file upload

10. Network penetration testing
    - Introduction to Network Penetration Testing
    - Scanning
    - Router Pentesting
    - Privilege Escalation

- Firewall Bypass
- Anti-Virus Bypass
- Port Forwarding
- Sniffing
- Browser Exploitation

11. System exploitation and vulnerabilities
    - Directory Traversal
    - OS Command Injection
    - Remote command Execution
    - DoS Attack
    - Buffer overflow attacks

12. Defending and Securing Systems
    - Personnel Screening and the Insider Threat
    - Physical and Environmental Security
    - Assessing Threats and Vulnerabilities
    - Information System Protection

Medium (Everything in Short Course and the following)

13. Open source intelligence (OSINT)
    - Online privacy / anonymity tools
    - Counterintelligence techniques used by the criminal elements
    - On line database systems
    - Archiving methodologies and tools and methods for obtaining archived pages & hidden information
    - Advance search methods for blogs and social networks
    - Geolocation methods
    - Image recognition technology
    - Optimizing transfer of large files
    - Best ways to use screen shot capabilities
    - Analyzing, organizing, and preparing of written reports

14. Governance, Risk, and Compliance
    - Governance Framework
    - Board and Senior Management Involvement

15. User Account Management and Access Control

16. Basic operations of Metasploit Framework and System Hacking
    - Understanding Metasploit Framework
    - Basic Concept and Usability

- Using Metasploit framework to attack Windows machines
- Attacking System using vulnerable open ports

17. Phishing and Social Engineering Attacks
    - What is Social Engineering
    - Why is social engineering effective?
    - Phases in a social engineering attack
    - Impact on the organization
    - Common targets of social engineering
    - Types of social engineering
    - What is Phishing
    - Phishing with social engineering
    - Human based social engineering
    - Computer based social engineering
    - Social engineering using SMS
    - Insider attack
    - Social engineering through social networking sites

18. Mobile Application Penetration Testing
    - Understanding Mobile Platform Attack Vector
    - Understanding various Android phone Threats and Attack
    - Understanding Mobile Device Management
    - Mobile Security Guidelines and Security Tools
    - Overview of Mobile Penetration Testing

19. Incident response
    - Information Sharing and Breach Reporting
    - Privacy Breach Notification
    - Endpoint Analysis
    - Binary Analysis
    - Enterprise Hunting
    - Wipe and Rebuild
    - Threat Mitigation Requests

20. Hunting Malware
    - Malware analysis
    - Reverse Engineering

Long (Everything included in Short, Medium Courses and the following)

21. Computer forensics investigation process
    - Investigating Computer Crime
    - Computer Forensics Investigation Methodology
    - Obtain Search Warrant
    - Evaluate and Secure the Scene
    - Collect the Evidence
    - Secure the Evidence
    - Acquire the Data
    - Analyze the Data
    - Assess Evidence and Case
    - Prepare the Final Report
    - Testifying as an Expert Witness

22. Searching and Seizing Computers
    - Searching and Seizing Computers without a Warrant
    - Fourth Amendment's "Reasonable Expectation of Privacy" in Cases Involving Computers: General Principles
    - Exceptions to the Warrant Requirement in Cases Involving Computers
    - Special Case: Workplace Searches
    - Searching and Seizing Computers with a Warrant
    - The Electronic Communications Privacy Act
    - Electronic Surveillance in Communications Networks
    - Evidence

23. Digital Evidence
    - Digital Data
    - Definition of Digital Evidence
    - Increasing Awareness of Digital Evidence
    - Challenging Aspects of Digital Evidence
    - The Role of Digital Evidence
    - Characteristics of Digital Evidence
    - Types of Digital Data
    - Digital Evidence Examination Process
    - Evidence Assessment
    - Evidence Acquisition
    - Evidence Preservation
    - Evidence Examination and Analysis
    - Evidence Documentation and Reporting
    - Electronic Crime and Digital Evidence Consideration by Crime Category

24. First Responder Procedures

- Electronic Evidence
- First Responder Toolkit
- First Response Basics
- Securing and Evaluating Electronic Crime Scene
- Conducting Preliminary Interviews
- Documenting Electronic Crime Scene
- Collecting and Preserving Electronic Evidence
- Packaging and Transporting Electronic Evidence
- Reporting the Crime Scene
- Note Taking Checklist
- First Responder Common Mistakes

25. Understanding hard disks and file systems

- Hard Disk Drive Overview
- Hard Disk Interfaces
- Disk Platter
- Tracks
- Sector
- Cluster
- Bad Sector
- Hard Disk Data Addressing
- Disk Capacity Calculation
- Measuring the Performance of the Hard Disk
- Disk Partitions and Boot Process
- Understanding File Systems
- RAID Storage System
- File System Analysis Using The Sleuth Kit (TSK)

26. Data acquisition and duplication

- Data Acquisition and Duplication Concepts
- Data Acquisition Types
- Disk Acquisition Tool Requirements
- Validation Methods
- RAID Data Acquisition
- Acquisition Best Practices
- Data Acquisition Software Tools
- Data Acquisition Hardware Tools

27. Defeating anti-forensics techniques

- Encryption
- Steganography
- Tunneling

- Onion Routing
- Obfuscation
- Spoofing

28. Windows Forensics

- Collecting Volatile Information
- Collecting Non-volatile Information
- Windows Memory Analysis
- Windows Registry Analysis
- Cache, Cookie, and History Analysis
- MD5 Calculation
- Windows File Analysis
- Metadata Investigation
- Text Based Logs
- Other Audit Events
- Forensic Analysis of Event Logs
- Windows Password Issues
- Forensic Tools

29. Linux Forensics

- Collecting Volatile Information
- Collecting Non-volatile Information
- Linux Memory Analysis
- Cache, Cookie, and History Analysis
- Linux File Analysis
- Metadata Investigation
- Text Based Logs

30. Data and partitions recovery

- Recovering the Deleted Files
- Recycle Bin in Windows
- File Recovery in Linux
- File Recovery Tools for Windows
- File Recovery Tools for Linux
- Recovering the Deleted Partitions
- Partition Recovery Tools

31. Forensics investigation using Access Data FTK and Autopsy

- Overview of Forensic Toolkit (FTK)
- Software Requirement
- Configuration Option
- Database Installation
- FTK Application Installation

- FTK Examiner User Interface
- Starting with FTK
- FTK Interface Tabs
- Adding and Processing Static, Live, and Remote Evidence
- Using and Managing Filters
- Using Index Search and Live Search
- Decrypting EFS and other Encrypted Files
- Installation Autopsy
- Import data in Autopsy
- Analyze data in Autopsy
- Working with Reports

32. Steganography and image file forensics

- What is Steganography?
- How Steganography Works
- Legal Use of Steganography
- Unethical Use of Steganography
- Steganography Techniques
- Image Steganography
- Audio Steganography
- Video Steganography
- Document Steganography: wbStego
- Steganalysis
- Image Files
- Data Compression
- Locating and Recovering Image Files
- Image File Forensics Tools

33. Log Capturing and Event Correlation

- Computer Security Logs
- Operating System Logs
- Application Logs
- Security Software Logs
- Router Log Files
- Honeypot Logs
- Linux Process Accounting
- Logon Event in Window
- Windows Log File
- IIS Logs
- DHCP Logs
- Log Management
- Centralized Logging and Syslogs
- Time Synchronization

- Event Correlation
- Log Capturing and Analysis Tools

34. Network forensics
    - Network Forensics Analysis Mechanism
    - Intrusion Detection Systems (IDS) and their Placement
    - Firewall
    - Honeypot
    - Network Attacks
    - Log Injection Attacks
    - Investigating and Analyzing Logs
    - Investigating Network Traffic
    - Traffic Capturing and Analysis Tools
    - Documenting the Evidence Gathered on a Network

35. Investigating wireless attacks
    - Wireless Technologies
    - Types of Wireless Networks
    - WEP vs. WPA vs. WPA2
    - Wireless Attacks
    - Investigating Wireless Attacks
    - Features of a Good Wireless Forensics Tool
    - Wireless Forensics Tools
    - Traffic Capturing and Analysis Tools

36. Investigating web attacks
    - Identifying possible vulnerable points
    - Check access logs
    - Detect malicious payloads
    - Find relevant exploits

37. Database forensics
    - Gather database files
    - Importing files in database viewer
    - Analyze data modification
    - Find suspicious or malicious files
    - Detect unauthorized users

38. Investigating email crimes
    - Email Terminology
    - Importance of Electronic Records Management
    - Email Crimes
    - Email Headers
    - Steps to Investigate

- Investigating Email Crime and Violation
- Examine Email Headers
- Analyzing Email Headers
- Trace Email Origin
- Acquire Email Archives
- Recover Deleted Emails
- Email Forensics Tools
- Laws and Acts against Email Crimes

39. Mobile forensics
    - Hardware Characteristics of Mobile Devices
    - Software Characteristics of Mobile Devices
    - Components of Cellular Network
    - Mobile Operating Systems
    - Mobile Forensics
    - Mobile Forensic Process
    - Mobile Forensics Software Tools
    - Mobile Forensics Hardware Tools

40. Forensics report writing and presentation

Course Curriculum (Non IT Professionals)

Cybersecurity Awareness Training

1. Threats Overview
    - Malware
    - Phishing
    - Latest Threats

2. Email Protection
3. Password Policy
4. Web Protection
5. Social Engineering
6. Mobile Device Security
7. Personal Online Account Safety
8. Protecting Computer Resources
9. Safe Usage of Internet
10. Backup & Disaster Recovery
11. Cloud Accounts Security
12. Best Practices for Remote Employees