CHAITANYA CYBER STRIX
TECHNOLOGIES

Become a Bug Bounty Hunter

ETHICAL HACKING

&

WEB APPLICATION PENETRATION TESTING

ONLINE TRAINING

OFFLINE TRAINING

WORKSHOPS

EC-Council Accredited Training Center

CompTIA AUTHORIZED PARTNER

6 MONTHS ONLINE INTERNSHIP AND TWO CERTIFICATES

CONTACT US

+91 81251 30203

www.chaitanyacyberstrix.com

H.No : 10-15/59/1, Surya Nagar Colony, Vajpaypee Road, R.L Nagar, Medchal, Hyderabad, Telangana, India, 501301

COURSE CONTENT

- Networking
- Ethical Hacking
- Web Application Pentesting
- Bug Bounty Hunting

COURSE PREREQUISITES

No Coding Required.
Basic knowledge of Computer Systems.
One year in an information security role or equivalent experience is recommended.
Ability to read and understand python code will help, although it is not mandatory.

CLASSROOM TRAINING

When it comes to quality instruction in a classroom training experience a more stimulating learning environment with our optimized mix of lecture, hands-on practice, when you have doubts our instructors are available to clear and ensure you comprehend the course and knowledge.

ONLINE TRAINING

We are providing training through Online LIVE with a real time live instructor. The live instructor teaches the course and provides the opportunity for students to ask live questions via voice or instant message during the live training event with practicals

WORKSHOPS

We conduct workshops and seminars in Information Security. Ethical Hacking & Information Security Workshop will teach you how to protect yourself from the cyber attacks and make yourself come to know how to secure your organization from hackers.

NETWORKING

Networking

- **Introduction to Networking**
- Types of Networks
- UDP
- TCP/IP
- TCP/IP Three Way Handshake
- TCP Flags

1. URG
2. ACK
3. PUSH
4. RST
5. SYN
6. FIN

- **OSI Model (Open System Interconnection)**

1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Data-Link Layer
7. Physical Layer

- **Basic Protocols**

1. FTP (File Transfer Protocol)
2. Telnet
3. SMTP (Simple Mail Transfer Protocol)
4. HTTP (Hyper Text Transfer Protocol)
5. HTTPS (Hyper Text Transfer Protocol Secure)

ETHICAL HACKING

Hacker Lab Setup

- VMware Setup in PC
- Kali Linux Installation in VMware
- Metasploitable – Vulnerable Web Server
- DVWA Setup

Kali Linux for Hackers

- Kali Linux Overview
- Kali Linux Settings and Configuration
- Kali Linux Read, Write and Extract Permissions
- Kali Linux Basic Commands

Introduction to Ethical Hacking

- Types of Hackers
- Ethical Hacking Phases
- Hacking Concepts
- Security Researchers, Analysts, Auditors etc...

Information Gathering (Footprinting)

- Website Foot-printing
- Who is
- Virus total
- Shodan
- GHDB (Google Hacking Data Base)
- The Harvester tool
- Nikto Tool
- Information Gathering from Social Media
- VOIP and VPN Footprinting
- Maltego - Advanced tool
- Image Metadata

ETHICAL HACKING

Enumeration

- NetBIOS Enumeration
- SNMP Enumeration
- SMB Enumeration
- Telnet Enumeration
- SMTP Enumeration

NMAP Scanning (Network Scanning)

- Network Scanning with NMAP
- Server Scanning with NMAP
- Host Discovery
- Port Discovery
- Service Version Detection
- OS Discovery

Net Cat (Powerful tool for pentesters)

- Port Scanning with Netcat (TCP and UDP)
- Chatting between two users (Initiator and listener)
- Banner grabbing (FTP and SSH) with Netcat
- File Transfer with Netcat
- Grabbing the HTTP Banner
- Windows Reverse Connection

Metasploit (Pentester Tool)

- Server Enumeration with Metasploit
- Detail Explanation of Modules

1. Exploit Module
2. Payload Module
3. Auxiliaries Module

ETHICAL HACKING

5.Encoder Module
6.Evasions Module
7Nops Module
8.Post Module

- Exploiting the Victim Machine
- Setting up Lhost, Rhost for getting access
- Creating a payload using msfvenom

Web Server Hacking

- Scanning with NMAP
- Using Searchsploit tool for finding CVE
- Finding the exploit in Rapid7
- Using Pen testing tool (Metasploit)

System Hacking

- OS Bypassing
- Error Generation Method (Cracking Password)
- Ngrok configuration
- Windows Reverse Shell
- Windows Machine Hacking
- Getting the live screen with VNC

Mobile Hacking

- Introduction to Mobile OS
- Creating reverse shell with msfvenom
- Binding the reverse shell
- Tunnel forwarding with open-source tool
- Getting Access in WAN connection
- Getting Access in LAN connection
- Exploiting the Mobile Platforms

ETHICAL HACKING

Malware

- Introduction to Malwares
- Types of Malware
- Virus
- Worms
- Trojans
- Crypters for hiding the malwares

Sniffing

- Introduction to Sniffing
- Introduction to Wireshark tool
- Analyzing the data packets from Wireshark
- Introduction to Bettercap
- MAC address spoofing
- Performing MAC flooding attack
- Man-in-the-Middle Attack – ARP Poisoning

DOS/DDOS (Distributed Denial-of-Service Attack)

- Introduction to Denial-of-Service attack
- Introduction to Distributed Denial-of-Service attack
- Introduction to Botnets
- Syn Flooding (DOS) attack
- Perform a DOS attack using Hping3
- Perform a DDOS attack using HOIC
- Perform a DDOS attack using LOIC

Wireless Hacking

- Wireless Encryptions
- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)

ETHICAL HACKING

- WPA2 (Wi-Fi Protected Access)
- Hacking Wi-Fi Networks
- Wi-Fi Deauther Attack
- Brute forcing the WI-Fi Networks
- Introduction to Service Defined Radio

Social Engineering

- Introduction to Social Engineering
- Types of Social Engineering
- Human-based Social Engineering
- Computer based Social Engineering
- Insider Attacks
- External Attacks

Password Cracking

- Hack Windows Password using CMD
- Hack Linux Password
- Crack SSH Password
- Crack Telnet Password

Cryptography

- Types of Cryptography
- Symmetric Key
- Asymmetric key
- Encryption Algorithms
- Cryptography Tools (MD5 and MD6 HashCalc)
- Generate Hashes with HashCalc
- Calculate MD5 Hashes using MD5 Calculator
- Decoding and Encoding
- Hide plain text in files (Steganography)

WEB APPLICATION PENETRATION TESTING

- XSS (Cross site Scripting)
- Local File Inclusion
- IDOR (Insecure Direct Object Reference)
- Path Traversal
- ColdFusion Vulnerability
- Breach Attack Vulnerability
- Heart Bleed Vulnerability
- Missing HSTS
- Poodle Attack Vulnerability
- Host Header Attack
- HTML Injection
- OS Command Injection
- SQL Injection
- (CSRF) Cross Site Request Forgery
- Insecure CORS configuration
- No Rate Limit
- Parameter Tampering
- XXE (XML External Entity)
- Open Redirection
- File Upload Vulnerability
- Credential Stuffing
- Improper Administrative Login
- Insecure Login Forms
- Insecure Logout Management
- Session Hijacking
- Session ID Exposure in URL
- SSRF (Server-Side Request Forgery)
- Broken Authentication and Session Management
- Clickjacking
- Remote Code Execution