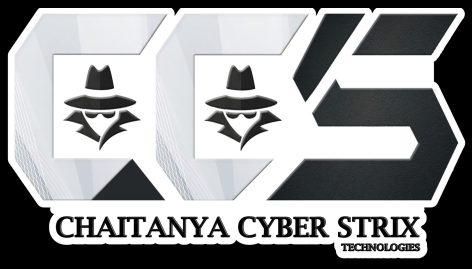
CYBERSECURITY- THE FUTURE

ETHICAL HACKING

WEB APPLICATION PENTESTING



CHAITANYA CYBER STRIX
TECHNOLOGIES

ETHICAL HACKING

&

WEB APPLICATION PENETRATION TESTING

ONLINE TRAINING

OFFLINE TRAINING

WORKSHOPS

BECOME A BUG HUNTER

CERTIFIED ETHICAL HACKER TRAINERS WITH OVER 5+ YEARS OF EXPERIENCE

2 MONTHS COURSE PROGRAM & 2 CERTIFICATES + INTERNSHIP

Contact us

+91 81251 30203

www.chaitanyacyberstrix.com

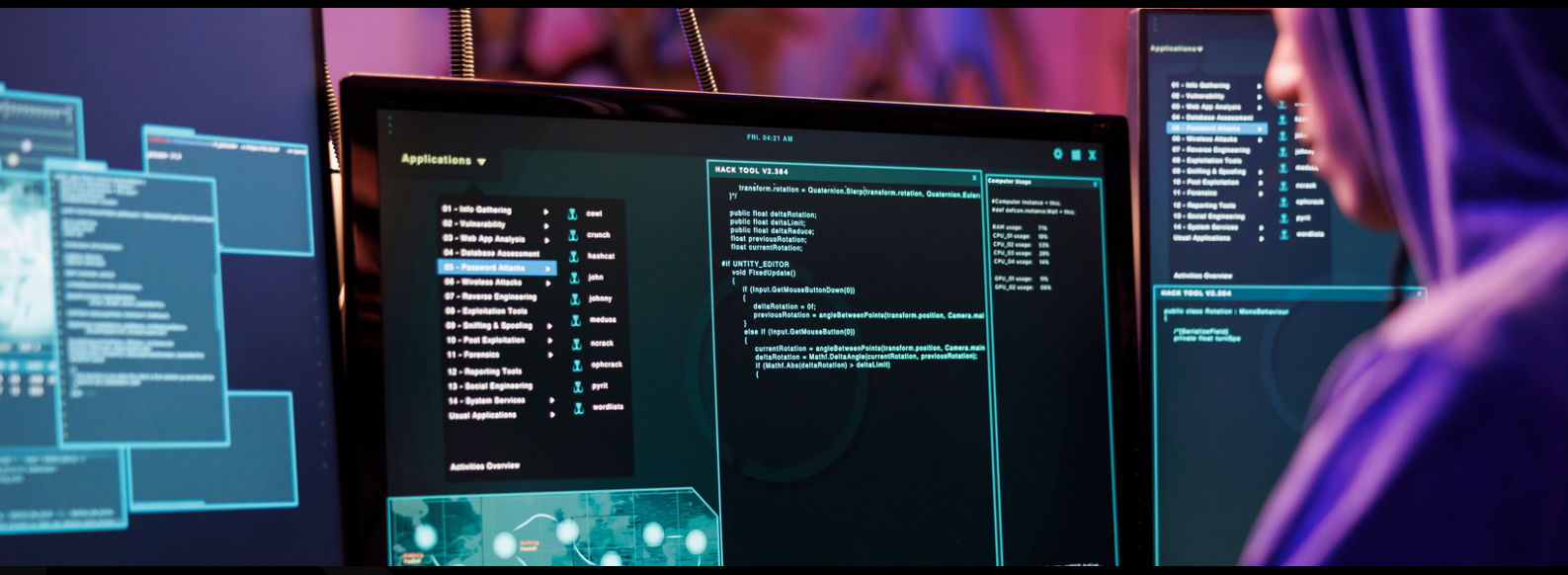
contact@chaitanyacyberstrix.com

COURSE CONTENT

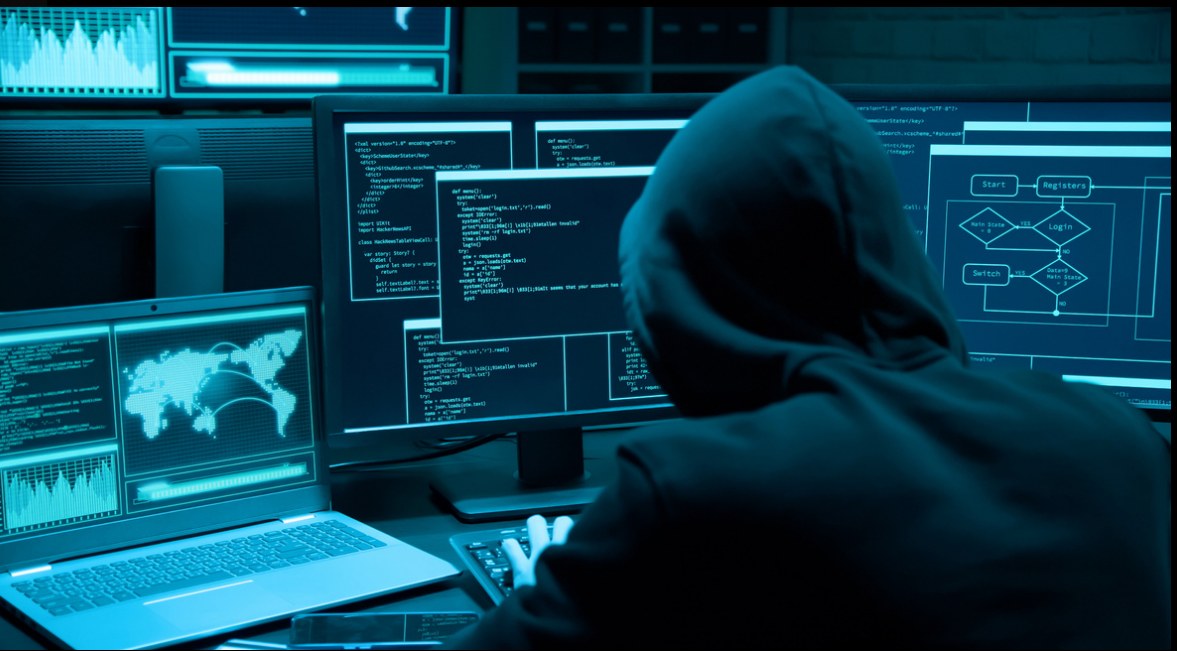
- Networking
- Ethical Hacking
- Web Application Pentesting
- Bug Bounty Hunting

It's not Bookish Hacking.
It’s Actual Hacking.

When it comes to the world of hacking, theoretical knowledge can only take you so far. In a landscape that is constantly evolving and changing, practical, real-world experience is essential. It signifies a hands-on, experiential approach to hacking, where the understanding of vulnerabilities and security breaches isn’t merely academic, but grounded in real-world scenarios and practical application. This tagline asserts the importance of lived experience in the field of hacking, conveying a message of expertise and proficiency that goes beyond mere book knowledge.



DRIVING PROGRESSION, EMPOWERING SECURITY.



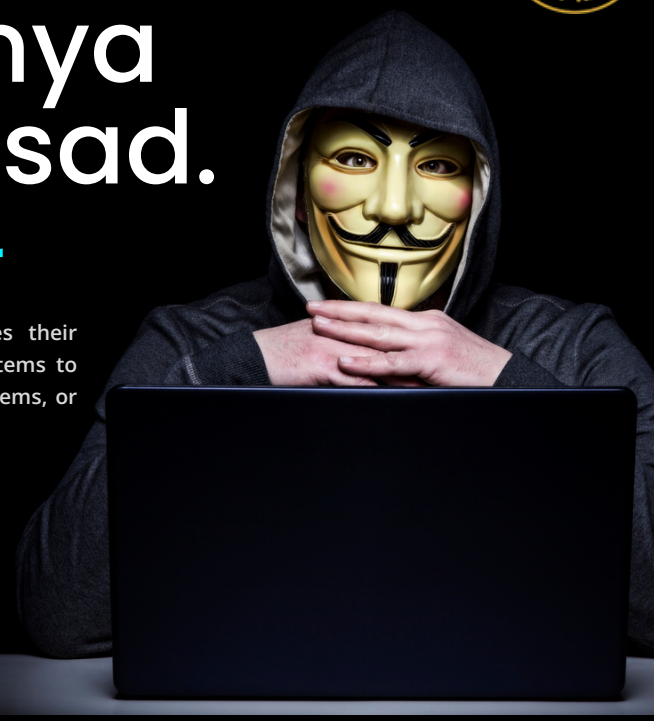
Hey there,

I'm Chaitanya Eshwar Prasad.

Certified Ethical Hacker

A Entrepreneur and Hacker is someone who uses their programming skills and knowledge of computer systems to gain unauthorized access to computer networks, systems, or data.

www.chaitanyaeshwarprasad.com



10 + Years of experience

50 + Completed projects

400 + Bug Bounty Rewards

Chaitanya Eshwar Prasad, a passionate cybersecurity professional and entrepreneur based in Hyderabad, Telangana, India . I'm a India Book of Records 2023 holder. With a deep interest in information technology and networks, I'm constantly seeking to evolve my skills and knowledge to stay ahead of the curve. I've been passionate about cybersecurity since the 7th grade, and I started my own company in the 10th grade. I believe that my early exposure to the world of technology has given me a unique perspective and valuable skills that I bring to every project.

I'm proud to be the Founder Director and CEO of Chaitanya Cyber Strix Technologies Pvt. Ltd., a company dedicated to providing top-notch cybersecurity services, the co-founder of Shasra Engineering and Construction Private Limited Company.

As a self-learner, I've earned several certifications in cybersecurity, including Certified Ethical Hacker v11 (CEH), Computer Hacking Forensic Investigator v9 (CHFI), Certified SOC Analyst (CSA), and more. I've also honed my skills in Web App Penetration Tester, Android Penetration Tester, IoT Penetration Tester, API Penetration Tester, Thick Client Penetration Tester, Network Penetration Tester, ISO 27001 Lead Auditor, Cloud Security, SIEM Tool, SDR, and Automotive Security.

In addition to my technical expertise, I'm also a PHP programmer, pencil sketch artist, graphic designer, professional badminton player, and digital marketer. At work, I'm expressive, innovative, and capable, always striving to provide the best solutions for my clients. I'm excited to continue learning, growing, and making a difference in cybersecurity. Let's connect and collaborate!

COURSE PREREQUISITES

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

CLASSROOM TRAINING

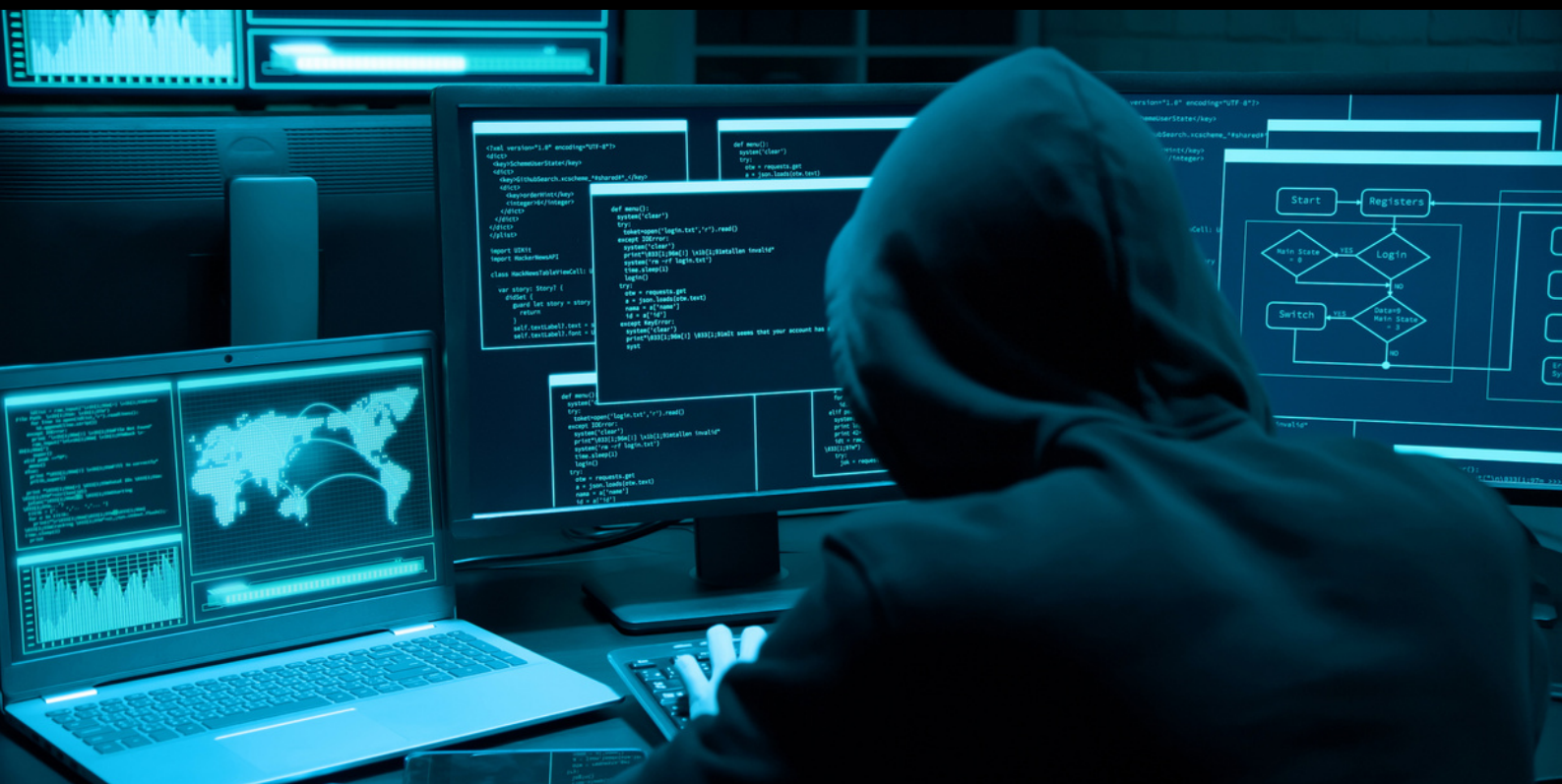
When it comes to quality instruction in a classroom training experience a more stimulating learning environment with our optimized mix of lecture, hands-on practice, when you have doubts our instructors are available to clear and ensure you comprehend the course and knowledge.

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.



What is this Course about ?

Ethical Hacking & WAPT

Ethical hacking is the practice of testing computer systems, networks, or web applications for security vulnerabilities with the permission of the system owner. It involves simulating real-world cyber attacks to identify weaknesses that malicious actors could exploit.

Ethical hackers use various tools and techniques to assess security posture and recommend measures to mitigate risks. Web application testing specifically focuses on evaluating the security of web-based applications, including websites and web services. It aims to uncover vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms. Through thorough testing, ethical hackers help organizations enhance their cybersecurity defenses, protect sensitive data, and prevent unauthorized access. This proactive approach to security helps organizations stay ahead of potential threats and ensures the integrity and confidentiality of their digital assets.

Modules Covered - EH & WAPT Course

Basics of Networking

SNIFFING

Wireless Hacking

KALI LINUX

OSI Model

Hacker Lab

BUG BOUNTY

ETHICAL HACKING

Cryptography

NMAP SCANNING

OWASP TOP 10

FOOT PRINTING

PROTOCOLS

Mobile Hacking

Social Engineering

NET CAT

METASPLOIT

Malware

System Hacking

DOS/ DOS Attack

Webserver Hacking

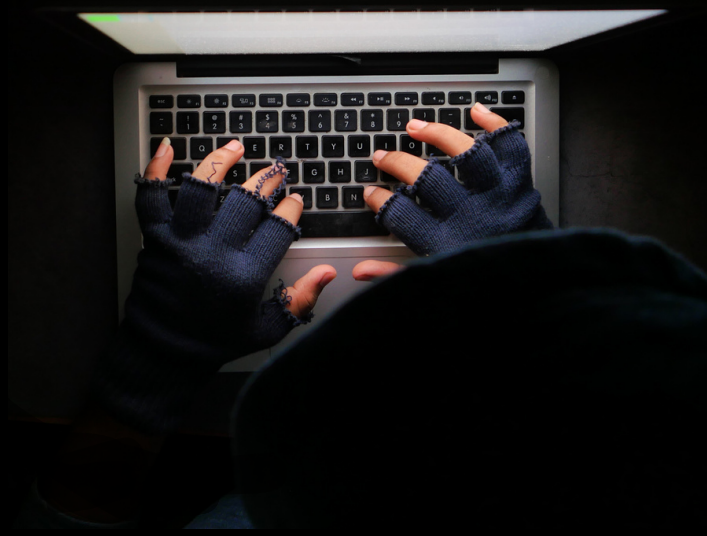
SQL Injection

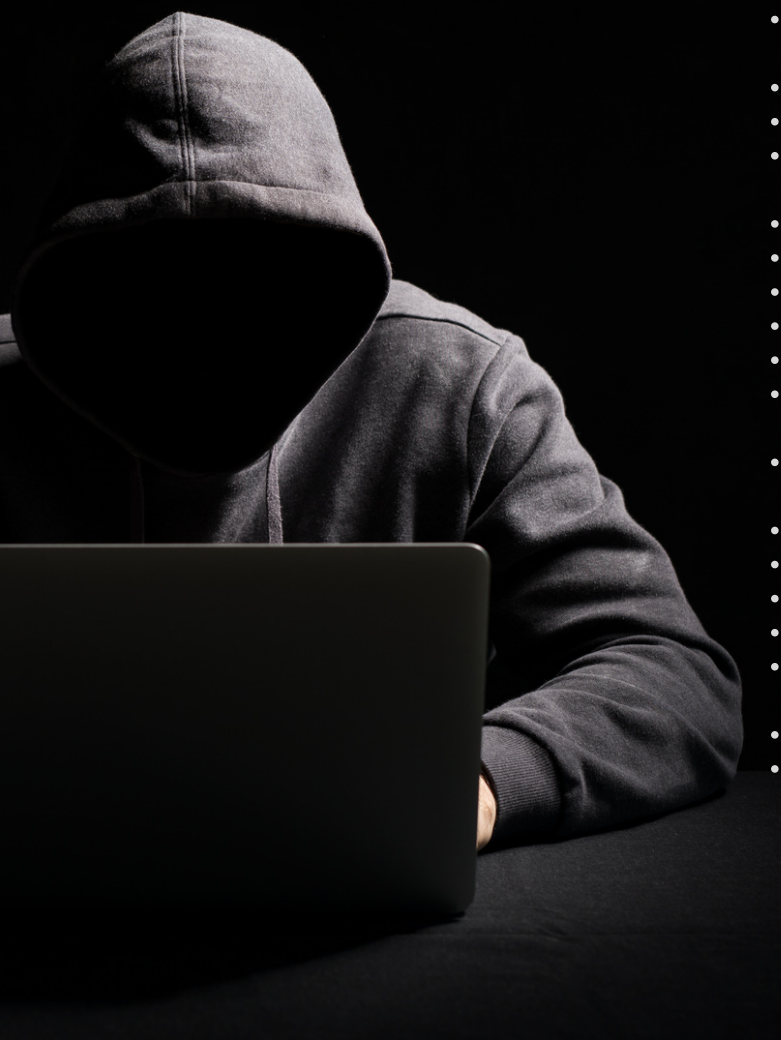
Pen Testing

CHAITANYA CYBER STRIX

What will you learn?

- 10+ hacking tools such as Metasploit, Aircrack-ng, SQLmap, etc.
- 30+ hands-on real-life hacking examples.
- No prior knowledge required
- Hack & secure WiFi & wired networks.
- Hack servers.
- Create backdoors & Hack Windows.
- Start from 0 up to a high-intermediate level.
- Discover & exploit web application vulnerabilities to hack websites.
- Learn Network Hacking / Penetration Testing.
- Learn about the different hacking fields & hackers.
- Install a hacking lab & needed software (on Windows, OS X and Linux).
- Discover vulnerabilities & exploit them to hack into servers.
- Hack secure systems using client-side & social engineering.
- Secure systems from all the attacks shown.
- Install & use Kali Linux - a hacking operating system.
- Linux basics.
- Linux commands
- How to use the Linux terminal.
- Network basics & how devices interact inside a network.
- Run attacks on networks without knowing its key.
- Control Wi-Fi connections without knowing the password.
- Create a fake Wi-Fi network with internet connection & spy on clients.
- Crack WEP/WPA/WPA2 encryptions.
- ARP Spoofing / ARP Poisoning.





- Sniff network traffic & analyse it to extract important info such as: passwords, cookies, urls, videos, images ..etc.
- Intercept network traffic & modify it on the fly.
- Discover devices connected to the same network.
- Inject Javascript in pages loaded by clients connected to the same network.
- Redirect DNS requests to any destination (DNS spoofing).
- Secure networks from the discussed attacks.
- Edit router settings for maximum security.
- Discover suspicious activities in networks.
- How to prevent MITM attacks.
- Discover open ports, installed services and vulnerabilities on computer systems.
- Exploit buffer over flows & code execution vulnerabilities to gain control over systems.
- Hack systems using client side attacks.
- Hack Windows using fake updates.
- Backdoor normal programs.
- Backdoor any file type such as pictures, pdf's ...etc.
- Gather information about people, such as emails, social media accounts, emails and friends.
- Hack secure systems using social engineering.
- And many More ...

CHAITANYA CYBER STRIX
TECHNOLOGIES

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)

CHAITANYA CYBER STRIX
TECHNOLOGIES

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

CHAITANYA CYBER STRIX

ETHICAL HACKING

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**
4. **Encoder Module**
5. **Evasions Module**
6. **Post Module**

Exploiting the Victim Machine

Setting up Lhost, Rhost for getting access

Creating a payload using msfvenom

CHAITANYA CYBER STRIX
TECHNOLOGIES

ETHICAL HACKING

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

Malware

- Types of Malware
- Virus
- Worms
- Trojans

CHAITANYA CYBER STRIX

ETHICAL HACKING

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

CHAITANYA CYBER STRIX

ETHICAL HACKING

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)

CHAITANYA CYBER STRIX

WEB APPLICATION PENETRATION TESTING

Introduction about WAPT

- What is Web Application Penetration Testing
- Vulnerability Assessments
- Penetration Testing
- DVTA Setup
- Bwapp Setup
- Bug Hunting Methodology

OWASP TOP 10 2021

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication
- A8:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures
- A10:2021-Server-Side Request Forgery

Cryptography

- Types of Cryptography
- Symmetric Key
- Asymmetric key
- Encryption Algorithms
- Decoding and Encoding
- Hide plain text in files (Steganography)

CHAITANYA CYBER STRIX
TECHNOLOGIES

WEB APPLICATION PENETRATION TESTING

Burpsuite

- Repeater
- Web Crawling
- Proxy Configuration
- Target Scanning

XSS (Cross-Site Scripting)

- Reflected XSS
- Stored XSS
- DOM based XSS
- XSS via XXE
- XSS through file uploading
- SSRF to XSS

SQL Injection

- Error Based SQL Injection
- Union Based SQL Injection
- Blind SQL Injection
  1. Boolean Based SQL Injection
  2. Time Based SQL Injection
- Manual Injection
- Automated Scanning
- SQLMap Tool

File Inclusions

- Local File Inclusion
- Remote File Inclusion

CHAITANYA CYBER STRIX
TECHNOLOGIES

WEB APPLICATION PENETRATION TESTING

Cryptographic Failures

- ColdFusion Vulnerability
- Breach Attack Vulnerability
- Heart Bleed Vulnerability
- Missing HSTS
- Poodle Attack Vulnerability

Broken Authentication and Session Management

- Credential Stuffing
- Improper Administrative Login
- Insecure Login Forms
- Insecure Logout Management
- Session Hijacking
- Session ID Exposure in URL

CSRF (Cross Site Request Forgery)

- Cookies
- Session ID's
- Same Origin Policy
- CSRF Exploitation

SSRF (Server-Side Request Forgery)

- Ngrok Configuration
- Blind SSRF
- Burp Collaborator
- SSRF Exploitation
- SSRF to XSS

CHAITANYA CYBER STRIX
TECHNOLOGIES

WEB APPLICATION PENETRATION TESTING

Shell & Command Executions

- File Upload Vulnerability
- Remote Code Execution
- OS Command Injection

XXE (XML External Entity)

- Introduction to XML
- Introduction to XXE Injection
- What is an Entity?
- What is the Document Type Definition (DTD)?
- XXE Billion Laugh Attack-DOS
- XXE Using File Upload
- XXE to Remote code Execution
- XSS via XXE

Additional Vulnerabilities

- IDOR (Insecure Direct Object Reference)
- Host Header Attack
- HTTP Request Smuggling
- HTML Injection
- Open Redirection
- Path Traversal
- Directory Traversal
- Insecure CORS configuration
- Clickjacking
- No Rate Limit
- Parameter or Data Tampering