COMPLETE CYBERBLOCKZ COURSE

> FOR CAREER & FREELANCING — 2026 <

ETHICAL HACKING
100+ HRS
ONLINE · TELUGU

CTF MASTERCLASS
40 HRS
ONLINE · TELUGU

BUG BOUNTY
60 HRS
ONLINE · TELUGU

200+	19+	10+	9+
TOTAL HOURS	EH MODULES	CTF TOPICS	BB TOPICS

// Instructor: Pranay from CyberBlockz | Online Training | 2026 Edition

> COMPLETE COURSE OVERVIEW

// CyberBlockz offers a complete end-to-end cybersecurity training path designed for beginners through professionals. Master Ethical Hacking, compete in CTF challenges, and earn through Bug Bounty programs — all in one structured program.

[TRACK 01] ETHICAL HACKING COURSE

100+ Hours | 19 Modules | Beginner to Advanced

- Master Networking, Linux & Lab Setup from scratch
- Learn Footprinting, Scanning, Enumeration & Recon
- Vulnerability Assessment, System & Web App Hacking
- Malware, Social Engineering, DoS & Session Hijacking
- Wireless Networks, Cryptography & Firewall Config
- Industry-Recognized Certification upon completion

[TRACK 02] CAPTURE THE FLAG MASTERCLASS

40 Hours | 9 Modules | Intermediate to Expert

- Understand CTF formats: Jeopardy, Attack-Defense, Hybrid
- Set up professional CTF lab environments and tooling
- CTF solving phases, privilege escalation & proxying
- Design and host your own CTF challenges from scratch
- Research latest CVEs and real-world vulnerability studies
- Earn via CTF freelancing — submit and sell challenges

[TRACK 03] BUG BOUNTY COURSE

60 Hours | 9 Modules | Intermediate to Expert

- OWASP Top 10: Injection, XSS, CSRF, SSRF, Broken Auth
- Advanced: Parameter Tampering, LFI/RFI, SSRF, CSRF
- BurpSuite Pro, Nikto, OWASP ZAP & Nessus hands-on
- Write professional vulnerability reports for bounties
- Real-world case studies of successful bounty hunters
- Web patch management & responsible disclosure practices

> WHO CAN LEARN & WHY CYBERBLOCKZ?

[WHO CAN LEARN]

01 [COLLEGE STUDENT]

Start shaping your career right from college by learning in-demand ethical hacking & cybersecurity skills.

02 [GRADUATE]

Upskill yourself, prepare for a bright future and kickstart a career in cybersecurity with certifications.

03 [COLLEGE DROPOUT]

Not sure which career is right? Learn ethical hacking with us to instantly land your first job in the field.

04 [CAREER SWITCHER]

Switch to ethical hacking — one of the most demanded and highly-paid skills globally in 2026.

[WHY CYBERBLOCKZ ONLY]

■ TRUSTED 1.5L+ LEARNERS
#1 choice in Telangana — training quality & support that stands out.

■ 100% PRACTICAL ORIENTED
Regular assignments, assessments and real hands-on projects always.

■ FLEXIBLE ONLINE LEARNING
Weekend batches for working professionals, flexible timings.

■ EXPERT TRAINERS (6+ YRS)
Industry trainers with 6+ years of real-world cybersecurity experience.

■ JOB ASSISTANCE
Resume building, interview prep & direct company interviews arranged.

■ INDUSTRY CERTIFICATION
Nationally & internationally valid certificate to share on your resume.

■ HANDS-ON LIVE PROJECTS
Practice on real websites with premium tools — not dummy environments.

■ COMPREHENSIVE CURRICULUM
India's most comprehensive curriculum covering all depths practically.

```
root@cyberblockz:~/track01
$ ./start_track.sh --track=01 --name="ETHICAL HACKING"
> Duration: 100+ HRS  |  Modules: 19
> Language: Telugu  |  Mode: Online
> Setting up ETHICAL HACKING environment...
[READY] Track 01: ETHICAL HACKING — 2026
```

TRACK 01

ETHICAL HACKING

// The foundation of all cybersecurity skills. Master networking, system hacking, web app attacks, wireless networks, cryptography and more — from scratch to advanced.

100+ HRS	19 MODULES	2026	LIVE
DURATION	CURRICULUM	EDITION	PROJECTS

> ETHICAL HACKING CURRICULUM

01 NETWORKING CONCEPTS

- What is Computer Networking & How it Works
- Types of Networks and What is IP Address
- IPv4 vs IPv6 / Types of IP Address
- Introduction to MAC Address
- Role of Ports in Networking
- Introduction to Router and its Elements
- What is OSI Model and How does it Work
- What is TCP/IP Model and How does it Work
- OSI vs TCP/IP Model Comparison
- Network Protocols and Types of Protocols
- How TCP Works / TCP vs UDP
- Domain Name, DNS and DNS Records
- HTML Request & Response / Request Methods
- Capturing & Analysing Packets (Wireshark)

02 INTRODUCTION TO ETHICAL HACKING

- What is Ethical Hacking? Types of Hackers
- Types of Attacks on a System
- Cybersecurity Laws & Regulations
- What is Linux & Cool Features of Linux
- Basic File System of Linux
- Basic Linux Commands (Practical)
- Advanced Linux Commands (Practical)

03 SETTING UP ETHICAL HACKING LAB

- Installing Kali Linux in VirtualBox
- Configuring Kali Linux
- Downloading a Good Wordlist
- Installing Burp Suite Pro
- Installing Nessus
- Other Tools with their Modules

04 FOOTPRINTING AND RECONNAISSANCE

- What are Footprinting and Reconnaissance
- Types of Footprinting & Reconnaissance
- Footprinting Through Search Engines
- Advanced Google Hacking Techniques
- Footprinting Through Social Networking Sites
- Website Footprinting (Netcraft, Wappalyzer)
- Email Footprinting (Email Tracker Pro)
- DNS Footprinting (DNSenum, DNS Lookup)
- MX Lookup, NS Lookup
- WHOIS Footprinting
- Footprinting Through OSINT Framework

05 SCANNING NETWORKS

- What is Network Scanning
- Network Scanning Methodology
- Types of Network Scans
- Checking for Live Systems and Buffer Size
- Checking for Open Ports
- Checking for Services on Ports
- Checking for Software with Versions
- OS Fingerprinting & Banner Grabbing
- Countermeasures
- Saving XML Report for Metasploit & Conversion
- Tools: Ping, Nmap, Zenmap, Masscan, hping3

06 ENUMERATION

- What is Enumeration & Types
- Default Ports Overview
- How to Enumerate NetBIOS
- How to Enumerate SNMP
- How to Enumerate SMTP
- How to Enumerate NFS
- How to Enumerate DNS
- How to Enumerate All Services
- Countermeasures
- Tools: Nmap, MSF, Armitage, NetCat

> ETHICAL HACKING CURRICULUM

07 VULNERABILITY ASSESSMENT

- What is Vulnerability Assessment
- Classification of Vulnerability
- Vulnerability Assessment Lifecycle
- Vulnerability Assessment Solutions
- Vulnerability Scoring Systems
- Scanning for Vulnerability in Nmap Scans
- MSF, Exploit DB, Armitage
- Vulnerability Scanning — ZAP (OWASP)

08 BEING ANONYMOUS

- Layers of Internet: Deep/Dark/Surface/Hidden Web
- Changing User Agent (Random User Agent Switcher)
- Changing MAC Address (Macchanger)
- Auto Run Shell Script (MAC Changer)
- Changing Wi-Fi MAC Address
- Configuring Proxy (Manual and Tor Proxy)
- Configuring VPN (Free VPN)
- Who is Best for IP Anonymity
- Anonymous Configuration in Linux
- Accessing Dark Web (Tor Browser)
- Creating Dark Web Website (Tor Server)

09 SYSTEM HACKING

- What is System Hacking & Methodology
- Cracking Windows Password (Pwdump, ophcrack)
- Creating a Good Password List (crunch)
- Escalate Privileges in Linux
- Escalate Privileges in Windows OS
- System Hacking via URL (Camera, Location, etc.)
- URL Masking
- System Hacking via Open Ports (Nmap, NetCat)
- MSF, Armitage, Exploit DB
- System Hacking using NetCat
- What is Steganography & Types
- Steganography Practical (Open Stego)

10 MALWARE THREATS

- What is Malware & Examples
- What is a Trojan
- What are Viruses and Worms
- Types of Malware Analysis
- Static Malware Analysis
- Dynamic Malware Analysis
- How to Create RAT Trojan (HTTP, RAT)
- Creating Payloads (MSF)
- Creating Undetectable Payloads

11 SNIFFING

- What is Sniffing
- How an Attacker Hacks the Network Using Sniffers
- Active Scanning Techniques
- Types of Sniffing Protocols Vulnerable to Sniffing
- Flooding Setup DHCP Rouge (MITM Attack)
- Sniffing with Wireshark
- Tools: Wireshark, TCPDUMP

12 SOCIAL ENGINEERING

- What is Social Engineering & Types
- Human-Based Social Engineering
- Computer-Based Social Engineering
- Mobile-Based Social Engineering
- Social Engineering using SET (Social Engineering Toolkit)

13 DOS & DDOS ATTACKS

- What is DoS Attack / What is DDoS Attack
- Basic Categories of DoS/DDoS Attacks
- Vectors DoS in Networking (hping3, MSF)
- DoS in Websites / DoS Using Programs
- CPU and Memory Utilization Commands

> ETHICAL HACKING CURRICULUM

14 SESSION HIJACKING

- What is Session Hijacking
- Why is Session Hijacking Successful
- Session Hijacking Process
- Types of Session Hijacking
- Performing Session Hijacking (Burp Suite, Ettercap)

15 HACKING WEB SERVERS & WEB APPS

- What is Web Server & Web Server Attacks
- Web Server Attack Methodology
- Web Application Concepts
- Web Application Hacking Methodology

16 HACKING WIRELESS NETWORKS

- What is Wireless Networking
- Types of Wireless Encryption
- Complete Hacking WEP (Wi-Fi) Basic to Advanced
- WPA/WPA2 (Air Packages)

18 CRYPTOGRAPHY

- What is Cryptography
- Difference: Encoding vs Hashing vs Cryptography
- Types of Cryptography & How it Works
- Cryptography Tools
- Hashing Tools
- Encoding Tools

19 SYSTEM SECURITY (Firewall, WAF, Antivirus)

- All About Firewalls
- GUI Windows Firewall Configuration
- GUI Linux Firewall Configuration
- WAF in Linux Config – MOD

root@cyberblockz:~/track02

```
$ ./start_track.sh --track=02 --name="CTF MASTERCLASS"
> Duration: 40 HRS  |  Modules: 9
> Language: Telugu  |  Mode: Online
> Setting up CTF MASTERCLASS environment...
[READY] Track 02: CTF MASTERCLASS — 2026
```

TRACK 02

CTF MASTERCLASS

// Take your hacking skills competitive. Learn to solve, build and monetise Capture The Flag challenges across Jeopardy, Attack-Defense & Hybrid formats.

40 HRS	9 MODULES	2026	LIVE
DURATION	CURRICULUM	EDITION	PROJECTS

> CTF MASTERCLASS CURRICULUM

01 INTRODUCTION TO CTF'S PROGRAMS

- What is CTF (Capture The Flag)?
- Types of CTFs: Jeopardy, Attack-Defense, Hybrid
- Overview of popular CTF platforms

02 IDENTIFYING SERVICES & UTILIZATION

- Understanding Common Ports and Services
- How to use those services in real time
- Configuration files and important commands
- Writing and using Automation Scripts

03 CTF LAB SETUP

- Setting up Virtual Environments
- Installation of required files and tools
- Installation of Assessment Lab environments

04 CTF SOLVING TECHNIQUES

- Phases of Solving a CTF Challenge
- Initial Phase Hacking Techniques
- Understanding the OS Level Structure
- Privilege Escalation Techniques
- Reverse Proxy & Port Forwarding Techniques

05 CTF CREATION TECHNIQUES

- Choosing the Right Operating System
- Basic Design Principles for CTF Challenges
- User Level Configurations
- Checking and Eliminating Rabbit Holes
- Hosting CTF Challenges in Real Time

06 RESEARCH FOR LATEST VULNERABILITIES

- Real-world Case Studies of Bugs
- Platforms to Find the Latest Vulnerabilities

07 HOW TO EARN VIA CTF'S (FREELANCING)

- Platforms to Submit and Monetize CTF Challenges
- Finding and Approaching Clients to Sell CTFs

08 LABS & PRACTICAL ASSESSMENTS

- Hands-on Practice with Vulnerable Applications
- Live Capture the Flag (CTF) Challenges

09 PREREQUISITES

- Advanced Networking Skills
- Knowledge of Kali Linux Operating System
- Familiarity with Top 10 OWASP Vulnerabilities
- Basic Knowledge of Cybersecurity Tools

root@cyberblockz:~/track03

```
$ ./start_track.sh --track=03 --name="BUG BOUNTY COURSE"
> Duration: 60 HRS  |  Modules: 9
> Language: Telugu  |  Mode: Online
> Setting up BUG BOUNTY COURSE environment...
[READY] Track 03: BUG BOUNTY COURSE — 2026
```

TRACK 03

BUG BOUNTY COURSE

// Turn your skills into income. Master web vulnerabilities, professional bug reporting, and earn through real-world bug bounty programs globally.

60 HRS	9 MODULES	2026	LIVE
DURATION	CURRICULUM	EDITION	PROJECTS

> BUG BOUNTY CURRICULUM

01 INTRODUCTION TO BUG BOUNTY PROGRAMS

- What is Bug Bounty and How it Works
- Overview of Penetration Testing
- Ethical Hacking and its Legal Implications

02 OWASP TOP 10 VULNERABILITIES

- 1. Injection (SQL Injection, Command Injection)
- 2. Broken Authentication
- 3. Sensitive Data Exposure
- 4. Security Misconfiguration
- 5. Cross-Site Scripting (XSS)
- 6. Broken Access Control

03 ADVANCED VULNERABILITIES

- 1. Parameter Tampering
- 2. Local and Remote File Inclusion (LFI/RFI)
- 3. Server-Side Request Forgery (SSRF)
- 4. Cross-Site Request Forgery (CSRF)

04 BUG BOUNTY HEAVY TOOLS

- BurpSuite Pro — Hands-on labs for testing vulnerabilities
- Nikto — Web vulnerability scanning
- OWASP ZAP — Automation strategies
- Nessus — Automation for penetration testing

05 REPORTING BUGS & GUIDELINES

- How to Write Clear and Detailed Bug Reports
- Vulnerability Disclosure Best Practices

06 CASE STUDIES

- Real-world case studies of successful bug bounty hunters
- Analysis of high-severity vulnerabilities found

07 WEB PATCH MANAGEMENT

- Importance of Patch Management in Web Security
- Techniques to Effectively Manage Patches

08 LABS & PRACTICAL ASSESSMENTS

- Hands-on Practice with Vulnerable Applications
- Capture the Flag (CTF) Challenges

09 PREREQUISITES

- Basic Networking Skills
- Knowledge of Kali Linux Operating System

> CAREER & FREELANCING PATHWAYS

[CAREER OPPORTUNITIES]

PENETRATION TESTER
■4L–■18L/yr

Test systems for vulnerabilities on behalf of orga
High demand across IT, banking, government sectors

SECURITY ANALYST
■3.5L–■15L/yr

Monitor, detect and respond to cyber threats in real
Work in SOCs, MSSPs or in-house security teams.

BUG BOUNTY HUNTER
$100–$50,000/bug

Find and report vulnerabilities in company prograr
Earn payouts from HackerOne, Bugcrowd, Intigriti.

CTF CHALLENGE CREATOR
■5K–■50K/challenge

Design & sell CTF challenges to platforms and enterpr
Freelance through Upwork, Fiverr, direct clients.

CYBERSECURITY CONSULTANT
■6L–■30L/yr

Provide expert advisory to businesses on security
High-paying freelance or full-time consulting role

ETHICAL HACKING TRAINER
■4L–■20L/yr

Teach ethical hacking at academies, colleges or onlir
Build your own training brand using CyberBlockz skil

[FREELANCING INCOME STREAMS]

- ■ **Bug Bounty Programs** HackerOne, Bugcrowd, Intigriti, YesWeHack, Open Bug Bounty
- ■ **CTF Platforms** CTFtime, HackTheBox, TryHackMe, PicoCTF, Root-Me
- ■ **Freelance Marketplaces** Upwork, Fiverr, Freelancer, Toptal, PeoplePerHour
- ■ **Direct Consulting** LinkedIn outreach, referrals, personal brand building
- ■ **Content Creation** YouTube, blogs, online courses — monetise your expertise

> STUDENT TESTIMONIALS

VENKATA SAI
★★★★★
Perfect course for beginners. Everything explained clearly with examples. Even without background knowledge, you can easily follow.

NAVEEN KUMAR
★★★★★
The course was amazing. Teaching style is excellent making tough concepts feel simple. Truly grateful for the effort put into teaching.

THONDAMANATI CHARAN
★★★★★
So happy I joined. Missed a few live classes but they provided recordings and cleared all doubts in the very next class.

MOHAMMED ABBAS
★★★★★
Fantastic for beginners and professionals alike. Hands-on labs and real-world scenarios made learning practical and engaging.

RAJESH KORRAI
★★★★★
Thank you trainer Pranay and Cyber Blockz for the enhanced training. Content covers beginner to pro. Highly recommend!

GOPALA KRUSHNA
★★★★★
Trainer makes content easy to learn and answers all questions. Learned many complex concepts. Recommend to anyone interested.

START YOUR COMPLETE CYBERSECURITY JOURNEY WITH CYBERBLOCKZ

> 200+ Hours | 3 Tracks | Career & Freelancing

// Ethical Hacking + CTF Masterclass + Bug Bounty — 2026 Edition

[TOTAL DURATION]	200+ Hours across 3 complete tracks
[FEES]	WhatsApp us — varied discounts available
[DEMO CLASS]	WhatsApp to Book 1-Day Free Demo Class
[PHONE]	+91 8074557618

[CONTACT US]

[EMAIL]	pranay@cyberblockz.org
[PHONE]	+91 8074557618
[INSTAGRAM]	@cyberblockz_official
[YOUTUBE]	@cyberblockz
[WEBSITE]	live.cyberblockz.org