Coding MASTERS
Masters in Online Training

Real Time

Cyber Security

5-10 Mini and Major Projects

Why Choose us?

- Mock Interviews
- Resume Building
- 1:1 Career Mentorship
- Industry Ready Curriculum

+91-96669 56556 info@codingmasters.in codingmasters.in

Coding MASTERS
Masters in Online Training

Reviews
DATA ANALYST

devatha vishwajith
3 reviews

★★★★★ 2 years ago

I joined testing course before 3 months and I already got placed in a good company, do trust dinesh sir and wait for you're turn to get placed he is really helpful and always ready to help with you're doubts. I highly recommend to join his classes and start your career in any IT industry.

Prasanthi Bheemireddy
1 review

★★★★★ 2 years ago

I started this course with fear and lot of doubts. Sir made it easier and always supportive. I liked his way of teaching,Because he never rush the class by teaching in fast track. He has really good knowledge in testing.

Raghavendra Kattela
2 reviews

★★★★★ 9 months ago

I had zero knowledge of testing, they had given me briefing from basic to mastering it. I had an opportunity to show case my skills in my same workplace during the transition of the banks in a short term. That's show how they are really into the business. I am glad I have right mentor. Thank you Subbaraju sir.

Kishan Kumar Yadav
1 review

★★★★★ a year ago

I've had the pleasure of attending a training session conducted by Subba raju sir, and I must say it was a truly enlightening experience. Their deep knowledge of the subject matter, combined with their engaging teaching style, made the learning process both enjoyable and highly effective.
Overall, I would highly recommend.

Module 01 — Introduction to Ethical Hacking

Key Topics:

1. Security fundamentals (CIA triad)
2. Information security controls and policies
3. Legal, ethical and regulatory considerations
4. Ethical hacking methodology and scope

Covered Tools:

1. Lab VM (Kali / Ubuntu)
2. Metasploit (overview)
3. OWASP resources
4. Whiteboard / flipchart

Module 02 — Footprinting & Reconnaissance

Key Topics:

1. OSINT techniques
2. Domain / WHOIS / SSL reconnaissance
3. Subdomain discovery and mapping
4. Passive vs active reconnaissance

Covered Tools:

1. TheHarvester
2. Whois
3. DNSenum
4. Chrome / Firefox devtools

Module 03 — Scanning Networks

Key Topics:

1. Port scanning methodologies
2. Service / version detection
3. Vulnerability scanning basics
4. Timing, stealth and evasion options

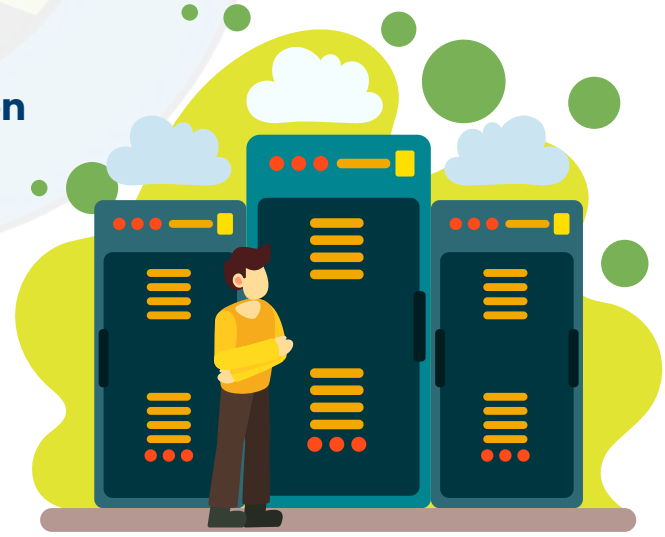
Covered Tools:

1. Nmap
2. Masscan
3. Nessus / OpenVAS
4. Netcat
5. Zenmap
6. Hping3

Module 04 — Enumeration

Key Topics:

1. Network and service enumeration
2. User/group enumeration
3. BGP and NFS enumeration techniques
4. SMB, LDAP, SNMP enumeration



Covered Tools:

1. Enum4linux
2. Nmap scripts
3. SNMPwalk
4. ldapsearch
5. BGP tooling (bgpq3)
6. Smbclient

Module 05 — Vulnerability Analysis

Key Topics:

1. Vulnerability discovery vs validation
2. Using CVE databases & Exploit-DB
3. Prioritization and risk scoring (CVSS)
4. False positives and verification

Covered Tools:

1. Nessus
2. OpenVAS
3. Nexpose
4. Burp Scanner (for web)
5. CVE search engines
6. Exploit-DB

Module 06 — System Hacking

Key Topics:

1. Windows and Linux privilege escalation
2. Password attacks and cracking
3. Persistence mechanisms
4. Covering tracks and steganography basics

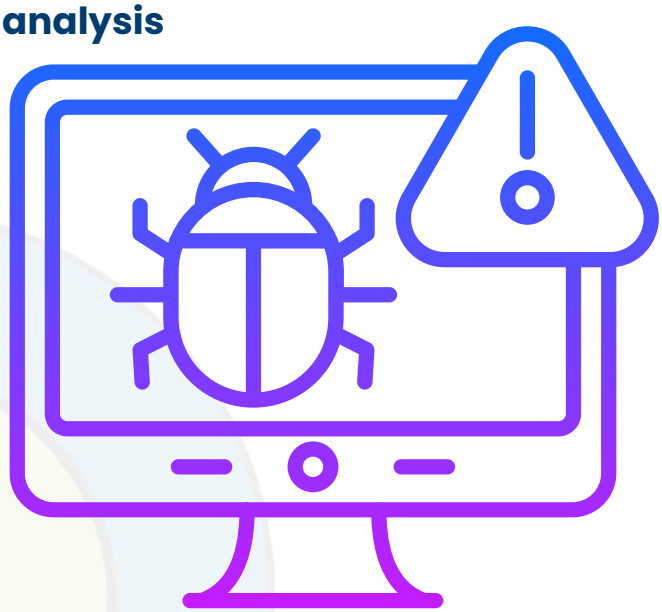
Covered Tools:

1. Metasploit
2. Mimikatz
3. John the Ripper
4. Hashcat
5. PowerSploit
6. Empire
7. Steghide / Stegsolve

Module 07 — Malware Threats

Key Topics:

1. Malware types (trojan, worm, RAT, fileless)
2. APT lifecycle and indicators
3. Sandboxing and static / dynamic analysis
4. Reverse engineering basics



Covered Tools:

1. IDA Free
2. REMnux tools
3. YARA
4. VirusTotal
5. Strings
6. PEStudio

Module 08 — Sniffing

Key Topics:

1. Packet capture fundamentals
2. Promiscuous mode and switch vs hub behavior
3. Protocol analysis (HTTP, DNS, TLS)
4. Traffic injection / man-in-the-middle basics

Covered Tools:

1. Wireshark
2. Tcpdump
3. Ettercap
4. BetterCAP
5. Tshark
6. Mitmproxy

Module 09 — Social Engineering

Key Topics:

1. Phishing frameworks
2. Vishing and SMShing methods
3. Spear-phishing crafting
4. Human risk assessment and countermeasures

Covered Tools:

1. GoPhish
2. Social-Engineer Toolkit (SET)
3. Maltego (OSINT)
4. Email platforms

Module 10 — Denial-of-Service (DoS)

Key Topics:

1. DoS vs DDoS fundamentals
2. Protocol-based attacks (TCP / UDP / ICMP)
3. Application layer DoS
4. Mitigation and rate-limiting strategies

Covered Tools:

1. Hping3
2. LOIC (lab-only)
3. Mausezahn
4. Stress testing tools (in isolated lab)
5. Cloud-based DDoS simulation tools

Module 11 — Session Hijacking

Key Topics:

1. Session tokens and cookies
2. Cross-site scripting/session fixation
3. Cookie theft and replay attacks
4. Secure session management practices

Covered Tools:

1. Burp Suite
2. OWASP ZAP
3. Browser devtools
4. CookieCadger
5. Mitmproxy

Module 12—Evading IDS, Firewalls & Honeypots

Key Topics:

1. IDS/IPS evasion techniques
2. Firewall rule analysis and bypass
3. Honeypot fingerprinting
4. Encryption and tunneling evasions

Covered Tools:

1. Snort / Suricata (for testing)
2. Scapy
3. Nmap evasion flags
4. Proxychains
5. Stunnel
6. SSH tunneling

Module 13 — Hacking Web Servers

Key Topics:

1. Server misconfigurations
2. Path traversal & file inclusion
3. HTTP / HTTPS misconfigurations
4. Server-side exploit chains

Covered Tools:

1. Nikto
2. Nmap
3. Dirbuster / ffuf
4. Burp Suite
5. Server log analysis tools
6. OpenVAS

Module 14 — Hacking Web Applications

Key Topics:

1. OWASP Top 10 deep-dive
2. Input validation flaws
3. Authentication/authorization weaknesses
4. Secure coding and remediation

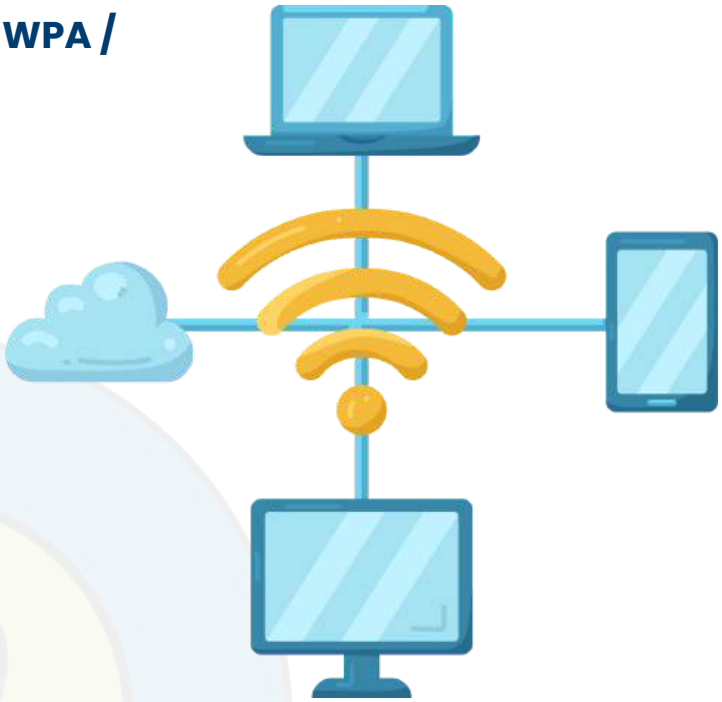
Covered Tools:

1. Burp Suite
2. OWASP ZAP
3. SQLMap
4. Wfuzz
5. WebGoat
6. Juice Shop (vulnerable apps)

Module 15 — Hacking Wireless Networks

Key Topics:

1. Wi-Fi encryption protocols (WEP / WPA / WPA2 / WPA3)
2. Handshake capture and cracking
3. Rogue AP and Evil Twin attacks
4. Bluetooth / 802.11 attacks basics



Covered Tools:

1. Aircrack-ng suite
2. Kismet
3. Wireshark
4. Reaver
5. Hostapd (for AP emulation)

Module 16 — Hacking Mobile Platforms

Key Topics:

1. Android/iOS attack surfaces
2. Mobile app reverse engineering
3. Insecure storage and communication
4. Mobile device management (MDM) security

Covered Tools:

1. Android Studio + adb
2. Frida
3. Apktool
4. MobSF
5. Burp Suite for mobile
6. iOS debug tools (ideviceinstaller)

Module 17 — IoT Hacking

Key Topics:

1. IoT architecture and common weaknesses
2. Firmware analysis
3. Protocol attacks (MQTT, CoAP)
4. OT / ICS basics and safety considerations

Covered Tools:

1. Binwalk
2. Firmadyne
3. radare2
4. Shodan
5. MQTT tools
6. IoT-specific toolkits
7. ModSecurity (for web interfaces)

Module 18 — Cloud Computing

Key Topics:

1. Cloud shared responsibility model
2. IAM misconfigurations
3. Serverless and container threats
4. Cloud logging and monitoring

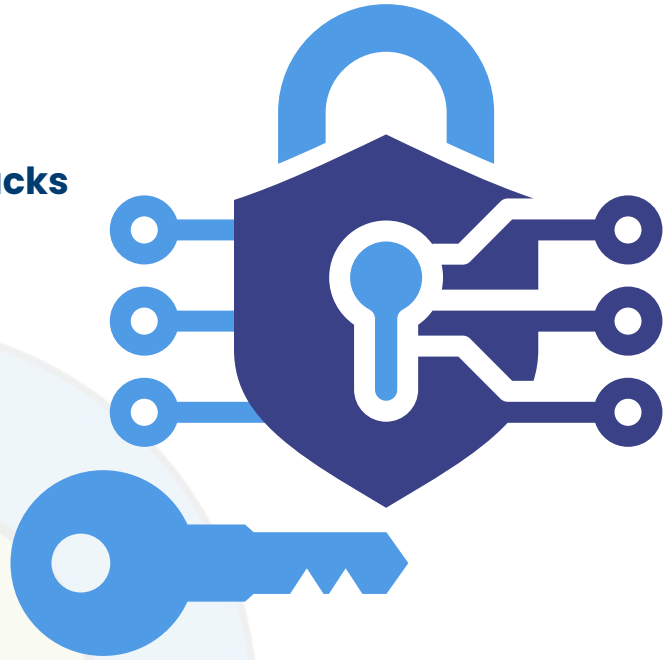
Covered Tools:

1. AWS CLI / Azure CLI / GCP SDK
2. ScoutSuite
3. Prowler
4. Kubectl
5. Kube-bench
6. Trivy
7. CloudSploit

Module 19 — Cryptography

Key Topics:

1. Symmetric vs Asymmetric Crypto
2. TLS / SSL internals
3. PKI and Certificate Management
4. Common Crypto Mistakes and Attacks



Covered Tools:

1. OpenSSL
2. Wireshark (TLS inspection)
3. Hashcat
4. GnuPG
5. Keytool
6. PKI labs

Final Project & Assessment

1. Capstone project: Realistic penetration test on an isolated lab environment (web + network + cloud components)
2. Deliverables: Written report (findings, risk rating, remediation steps), presentation, demo of exploit chains (lab-safe)
3. Assessment: Practical exam + viva + report evaluation

Coding MASTERS
Masters in Online Training

MODULE 11

Ready for job

Build a strong resume, practice interviews, and get placement support to kickstart your career confidently.

LEARN THE SKILLS BUILD REAL PROJECTS. GET INTERVIEW READY

- RESUME BUILDING
- MOCK INTERVIEWS
- Q&A SESSIONS
- HR INTERVIEW QUESTIONS
- PLACEMENT ASSISTANCE

Contact Us

Bhavya Krishna Residency,
Flat No: 404, OPP: Siddartha Degree College, Ameerpet Rd,Nagarjuna Nagar colony
Yella Reddy Guda,
HYDERABAD-500073

Phone Number:
+91-96669 56556

Website:
codingmasters.in

Our Recent Placed Students

At **Coding Masters**, our faculty team comprises talented and experienced professionals with several decades of real-world industry experience. Our teaching style is tailored to meet **industry requirements**, ensuring no wasted effort or opportunity for learners. We are dedicated to empowering aspiring professionals with the skills they need to excel in the ever-evolving tech landscape. Known for offering the best **AI Powered Data Analytics training in Hyderabad**, Coding Masters blends innovation, hands-on learning, and industry
relevance.

Our mission is to bridge the gap between **academic knowledge and industry** expectations by providing high-quality training in **AI Powered Data Anlytics** and more. Guided by experts like **Subba Raju Sir**, every student receives personalized mentorship and a transformative learning experience.