VERSION IT

VERSION IT

Since 2001

24th ANNIVERSARY

CYBER SECURITY

Best Training And Placement Institute

Amrutha Arcade, SAP St, Behind Maitrivanam,
1st Left, Srinivasa Nagar, Ameerpet,
Hyderabad, Telangana 500082

+91 9848015399
+91 9391237284

www.versionit.co.in

VERSION IT

About Version IT

Version IT is not a mere software training institute, a team of IT professionals developed it as the best knowledge centre for hundreds of career-building conscious young people. Our training academy is the best training institute in Hyderabad offering various software courses with aptly placement orientation. We proudly announce that we achieved 100% placements in every batch we have taken up in the past two decades. Version IT Academy's strength is our academic excellence with which we have been placed in the top position among the software training institute in Hyderabad.

Corporate Training

Class Room Training

Online Training

Why Choose Us!

VERSION IT

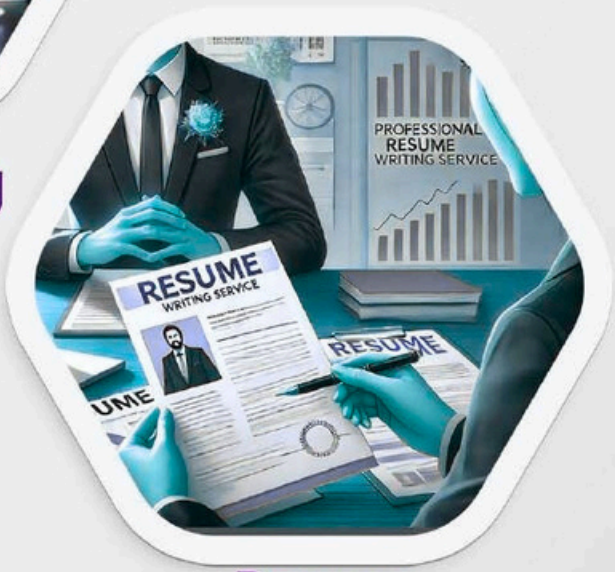
Training By Certified Instuctors

Mock Interviews

Weekly Assignments

Project Training

Interview Cracking tips



Resume Preparation

VERSION IT

Cyber Security - Course Curriculum

Module 1: Introduction to Cybersecurity

- What is Cybersecurity?
- Threats, vulnerabilities, and risks
- Types of cyber attacks (malware, phishing, DDoS, ransomware)
- Cybersecurity domains (network, application, endpoint, cloud, etc.)
- Security goals: Confidentiality, Integrity, Availability (CIA Triad)
- Cybersecurity frameworks: NIST, ISO/IEC 27001

Module 2: Ethical Hacking Fundamentals

- Who are hackers? Black Hat, White Hat, Grey Hat
- Principles of ethical hacking
- Legal considerations and compliance (Computer Fraud and Abuse Act, GDPR, HIPAA)
- Penetration testing lifecycle
- Bug bounty programs and responsible disclosure

Module 3: Lab – 1 Setting Up the Lab Environment & Configuration

- Installing and configuring VMware/VirtualBox for a controlled testing environment
- Installing Kali Linux and setting up essential tools (Metasploit, Nmap, Burp Suite)
- Configuring a target machine (e.g., Metasploitable) for penetration testing practice

Module 4: Networking and Security Basics

- OSI & TCP/IP models
- IP addressing, DNS, DHCP, NAT
- Ports and protocols (TCP, UDP, ICMP)
- Network scanning basics
- Wireshark & packet analysis

Module 5: Lab – 2 Networking Setup & Packet Analysis

- Configure a virtual network with multiple machines (attacker, target, defender)
- Perform basic ping tests, and use traceroute to understand network topology
- Analyze network traffic using Wireshark to capture TCP/IP packets and identify protocols and ports

Module 6: Reconnaissance and Footprinting

- Passive vs active reconnaissance
- WHOIS, nslookup, Shodan
- Google hacking and OSINT tools
- Social engineering basics

Module 7: Lab – 3 Reconnaissance and OSINT

- Use Nmap for network mapping and service discovery on a target network
- Perform a WHOIS lookup, DNS enumeration, and search for subdomains
- Conduct Google Dorking for OSINT and perform Maltego data collection
- Engage in a simulated social engineering attack using phishing techniques

Module 8: Scanning and Enumeration

- Portscanningwith Nmap Banner
- grabbing and version detection
- Identifying services and vulnerabilities
- SMB, SNMP, NetBIOS enumeration

Module 9: Lab – 4 Network Scanning & Enumeration

- Conduct port scanning and service detection using Nmap on a target network
- Use Nessus to perform a vulnerability assessment of a target machine
- Perform SMB enumeration and SNMP enumeration on a network of machines

Module 10: Gaining and Maintaining Access

- Exploitationbasics (Metasploit framework) Password
- attacks (Brute-force, Dictionary, Rainbow tables) Privilege
- escalation (Linux & Windows) Maintaining access and
- clearing tracks

Module 11: Lab – 5 Exploitation & Metasploit

- UseMetasploit toexploit vulnerabilitiesin acontrolled labenvironment
- Develop custom exploits using Metasploit and execute them in a controlled setup

Module 12: Web Application Hacking

- OWASPTop10 (XSS, SQLi,CSRF,SSRF,etc.)
- Burp Suite intro
- Input validation and parameter tampering
- Exploiting authentication flaws

Module 13: Lab – 6 Web Application Penetration Testing

- UseBurp Suite to interceptHTTP requestsand test forvulnerabilitieslikeSQL injection and XSS
- Conduct a SQL injection attack on a vulnerable web application
- Perform Cross-Site Scripting (XSS)
- Implement session hijacking techniques in a vulnerable application

Module 14: Malware and Exploit Analysis

- Types ofmalware (viruses, worms,trojans,RATs)
- Static and dynamic malware analysis
- Exploit development basics
- Antivirus evasion and encoding

Module 15: Defensive Security

- Introduction to Defensive Security
- Blue Team vs Red Team vs Purple Team
- Security controls (preventive, detective, corrective)
- Firewall, IDS/IPS, SIEM tools (Splunk)
- Endpoint security: Antivirus, EDR (Endpoint Detection and Response)

Module 16: Lab – 7 Defensive Security

- Configure and test anIntrusionDetectionSystem(IDS) using tools like Snort
- Implement and test firewall rules

Module 17: SOC (Security Operations Center) Overview

- What is a SOC?

- SOC tiers: Tier 1 (monitoring), Tier 2 (analysis), Tier 3 (threat hunting)
- Role of SIEM (Security Information and Event Management)
- Common SOC tools: ELK Stack, Splunk, AlienVault
- Log sources: firewall, endpoint, proxy, authentication systems

Module 18: SOC Functions

- Threat monitoring and incident detection
- Event triage and escalation
- Incident response and containment
- Forensics and root cause analysis
- Reporting and compliance

Module 19: Threat Intelligence and Response

- Threat intelligence lifecycle
- IOC vs IOA
- Cyber kill chain and MITRE ATT&CK
- Incident response lifecycle (Preparation, Detection, Containment, Eradication, Recovery)
- Forensic acquisition tools (FTK Imager, Autopsy)

Module 20: Lab – 8 Incident Response

- Perform incident response simulations to handle security breaches and gather forensic data

Module 21: Capture the Flag (CTF) Challenge

- Introduction to CTF competitions and platforms (e.g., Hack The Box, TryHackMe)
- Hands-on challenges: Solving real-world cybersecurity puzzles in a simulated environment
- Practical application of penetration testing and defense strategies learned throughout the course

Module 22: Lab – 9 Capture the Flag

- Participate in a CTF competition to solve real-world puzzles

Our Alumni Work At

VERSION IT

+91 9848015399 +91 9391237284

www.versionit.co.in

VERSION IT

Our Other Courses

Development Technologies

- Java Full stack
- Python Full stack
- .Net Full stack
- MERN
- MEAN
- React

Cloud Technologies

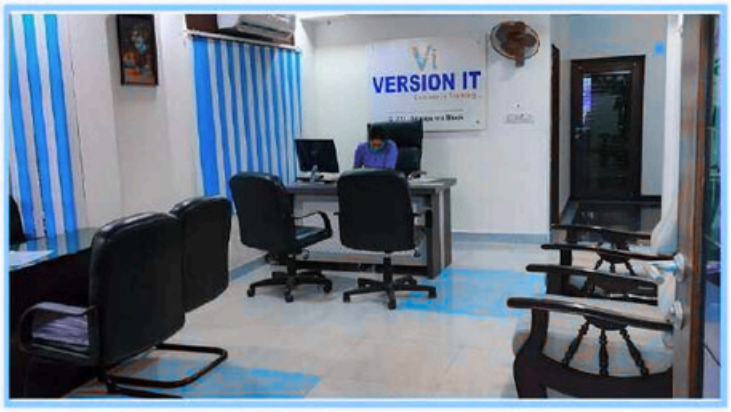
- aws
- Azure
- GCP
- Dev Ops
- Salesforce
- servicenow

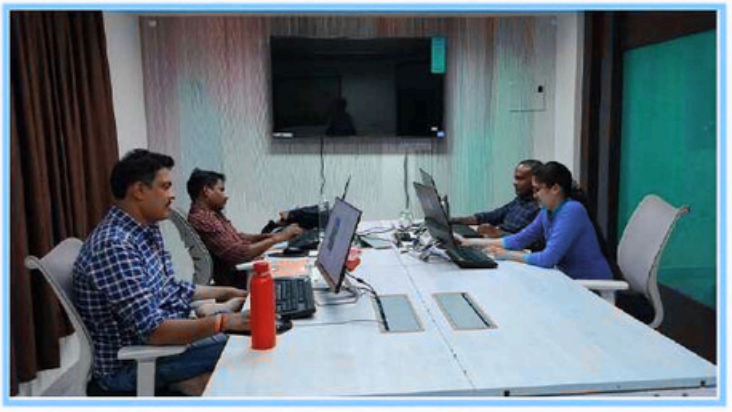
Triending Technologies

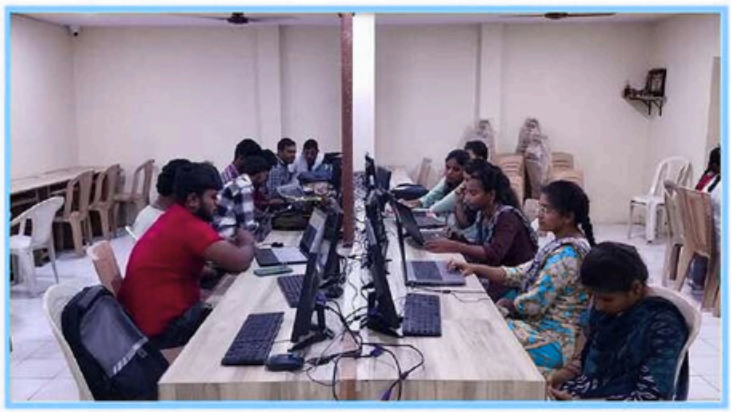
- Data Science
- Data Analytics
- Cyber Security
- Azure Data Engineer
- Aws Data Engineer
- GCP Data Engineer

Our Infrastructure

VERSION IT







Our Branches

Address

Amrutha Arcade, SAP St, Behind Maitrivanam, 1st Left, Srinivasa Nagar, Ameerpet, Hyderabad, Telangana 500082

+91 9848015399 +91 9391237284

www.versionit.co.in