# Cyber Security Course in Chennai

**Learn Cyber Security in Chennai with Hands-On Labs, Cloud Security and Placement Support.**

Learn to protect networks, applications and cloud infrastructure. Start with networking basics and Kali Linux, then move through threat modelling, network scanning and intrusion detection, application security testing with SAST and DAST tools, the OWASP Top 10, penetration testing with Metasploit and Burp Suite, Splunk SIEM log monitoring and AWS security services.

## Your Trainers

**Ramya** — AWS, DevOps & Cybersecurity Trainer
5+ Years of Industry Experience

## Course Curriculum

### Phase 1: Security Foundations Modules 01–03

*Why security matters, networking fundamentals and Kali Linux.*

#### 01. Introduction to Cyber Security

- Importance of Security – Application Stack
- Okta data breach, Sony Pictures (case studies)
- What is Cybersecurity
- Scopes in Cybersecurity
- Openings for Cybersecurity
- Pre-requisites for cybersecurity
- Future opportunities and salary package
- Our course content discussion
- Difference between Information Security and Cyber Security
- Difference between Cybersecurity and Ethical Hacking
- Types of Hackers
- The Hacking Methodology
- Cyber Security Policies

#### 02. Networking Basics

- Basic terminologies of computer networks
- Types of enterprise computer networks
- Types of computer network architecture
- Network devices
- OSI Model
- Network protocols

- Network topology

### 03. Kali Linux

- Kali Linux setup and tools
- Kali Linux features and usage
- Kali Linux commands

## Phase 2: Threat Modelling & Network Security Modules 04–07

*Threat modelling, network scanning, intrusion detection and traffic analysis.*

### 04. Threat Modelling

- What is Threat Modelling and why we need it
- Bugs and their role in Threat Modelling
- Understanding vulnerabilities
- Prioritization and risk minimization: how to prioritize bugs and minimize risks
- Which projects benefit from Threat Modelling, and when to start
- Teams involved in Threat Modelling
- 6 steps in Threat Modelling
- STRIDE & DREAD frameworks
- Overview of Threat Modelling tools and techniques

### 05. Nmap

- Introduction to Nmap
- Host discovery and ping scanning
- Three-way handshake
- Nmap scan techniques and port specification
- Port states in Nmap
- Service, OS and version detection
- Firewall, IPS and IDS spoofing
- Nmap Script Engine - advanced scanning
- ZenMap

### 06. Snort

- Introduction to Intrusion Detection Systems (IDS)
- Intrusion detection methodology
- Types of intrusion detection and prevention systems
- Snort installation scenarios
- Snort fundamentals and configuration
- Snort rule syntax
- Crafting basic Snort rules
- Detecting known vulnerabilities with Snort rules
- Detecting novel vulnerabilities with Snort rules

### 07. Suricata & Wireshark

- Suricata introduction and installation
- Suricata configuration and rules

- Wireshark introduction
- Wireshark installation and network activity tracking

## Phase 3: Application Security & DevSecOps Modules 08–12

*Code review, SAST/DAST/IAST, security scanning tools in CI/CD and SIEM monitoring.*

### 08. Application Code Review

- Importance of code review
- What is SAST, DAST and IAST
- Integrating GitLab with SAST & DAST tools
- How to use GitLab as a pipeline tool

### 09. SonarCloud

- Benefits of using SonarCloud
- SonarCloud (cloud-based) vs SonarQube
- Code quality improvement and early bug detection
- Security vulnerability and code duplication detection
- Comprehensive code review
- Integration with CI/CD pipelines
- Support for multiple languages
- Customizable quality gates

### 10. OWASP ZAP, Snyk & Trivy

- Benefits of OWASP ZAP and open-source flexibility
- Integrating OWASP ZAP with GitLab
- Detecting vulnerabilities using OWASP ZAP
- Benefits of Snyk: continuous monitoring and compliance
- Dependency monitoring and early detection of vulnerabilities
- Integrating Snyk into the development workflow
- Introduction to Trivy and installation
- OS packages and software dependencies scanning
- Docker image and Git repository scanning
- Infrastructure as Code (IaC) issues and misconfigurations scanning

### 11. Nessus, Checkmarx & Acunetix

- Introduction to Nessus and installation
- Host discovery, penetration testing and vulnerability assessments with Nessus
- Introduction to Checkmarx and installation
- Features, advantages and uses of Checkmarx
- Static Application Security Testing (SAST)
- What Acunetix is and what it can scan
- Setting up Acunetix and scanning techniques
- Integration with DevOps
- Common vulnerabilities detected by Acunetix
- Best practices for secure development

### 12. Splunk SIEM

- Splunk tool setup
- Log monitoring
- Splunk features and usage

## Phase 4: Web Attacks & Penetration Testing Modules 13–18

*Google Dorking, the OWASP Top 10, common attacks, Metasploit, Burp Suite and password security.*

### 13. Google Dorking

- Definition, purpose and applications of Google Dorking
- Anatomy of URLs relevant to Google Dorking
- Examples and breakdown of Google Dorking syntax
- Key principles and ethical considerations
- Google Dorking operators and modifiers: basic & advanced
- Practical aspects of Google Dorking
- Identifying directory listing vulnerabilities
- Techniques to find SQL injection vulnerabilities
- Dorking for web server versions

### 14. OWASP Top 10 & Common Web Attacks

- Broken Access Control
- Cryptographic Failures
- Injections
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery (SSRF)
- Common attacks: SQL injection, DoS & DDoS, Man-in-the-Middle, DNS spoofing, password attacks, brute force, phishing, malware, password spraying and XSS
- Cybersecurity defences

### 15. Penetration Testing

- Definition and understanding of penetration testing
- Risk mitigation, vulnerability discovery and remediation
- Continuous improvement of security posture
- Importance and challenges of penetration testing
- Types: network, white box, black box, grey box, wireless and physical penetration testing
- The penetration testing process: planning, scanning, gaining access, maintaining access, analysis & reporting
- Famous tools: Metasploit, Nmap, Wireshark and Burp Suite

### 16. Metasploit

- Metasploit introduction, definition and history
- Metasploit modules: payload, exploitation, NOPs, auxiliary, evasion, post-exploitation and encoders
- Benefits and architecture of Metasploit
- Basics and components of the Metasploit Framework
- msfconsole and Metasploit location directories
- Basic commands: show, search, use, info, options and set
- Choosing the payload and checking if the exploit will work
- A penetration test walkthrough: target identification, host discovery, port scanning, service detection and vulnerability analysis
- Exploiting vulnerabilities: VSFTPD, Samba SMB and VNC; keeping sessions in the background

### 17. Burp Suite

- Burp Suite introduction, workflow and working process
- Community vs Professional vs Enterprise editions
- Burp Suite pen testing process and features
- Getting started: system requirements, download and install
- Configure network and CA certificate on browser
- Intercepting HTTP traffic and modifying requests
- Setting the target scope and reissuing requests
- Running your first scan and generating a report (Pro only)
- Testing workflow: Intruder, Decoder, Repeater and Comparer
- Target scope and site map; Proxy and HTTP history
- Extensions using BApp and API process flow
- Intercept hands-on

### 18. Password Manager & Brute Force Attacks

- What is a password manager and why use one
- Password manager multi-cloud usage
- Hands-on with password managers: LastPass and 1Password
- Understanding brute force attacks and strategies
- Best practices and case studies
- Continuous improvement and future trends
- Prevention steps for brute force attacks

## Phase 5: AWS Cloud & Security Services Modules 19–23

*Core AWS services, then the AWS security services used to protect them.*

### 19. Cloud Computing, EC2 & S3

- Introduction to cloud and AWS services; AWS history
- Private vs public cloud; IaaS vs SaaS vs PaaS
- Scope and features of AWS
- Launching EC2 servers and hosting a web application
- Elastic Block Store (EBS) use cases and Elastic IP creation
- Amazon Machine Image (AMI) and snapshots from volumes
- S3: creating and deleting buckets; adding, getting and deleting objects

- Static website hosting with S3, S3 permissions and lifecycles

### 20. IAM, ELB & Auto Scaling with WAF

- Creating user accounts in AWS
- Setting up multi-factor authentication (MFA)
- Roles and groups in IAM
- Delegating permissions and creating custom policies
- Account settings
- What is Elastic Load Balancer
- Setting up ELB & Auto Scaling hands-on
- Benefits of ELB & ASG with WAF

### 21. VPC, KMS, RDS & Route 53

- Types of networks in AWS; public vs private
- Creating a VPC, routing tables and security groups
- Internet Gateway and NAT Gateway
- KMS: importance of encryption; symmetric and asymmetric keys hands-on
- RDS: selecting and configuring the engine, creating the database, automatic backups and DB security groups
- Route 53: hosted zones, custom domain hosting and routing policies

### 22. AWS Inspector, Macie & Trusted Advisor

- AWS Inspector: purpose, key concepts, setup and assessment targets
- Rules packages, agents and running scheduled assessments
- Interpreting and fine-tuning assessment results
- Amazon Macie: sensitive data identification, configuration and dashboard
- Macie reports, CloudWatch and S3 integration, data privacy best practices
- Trusted Advisor: check categories, cost optimization and resource usage
- Security, performance, reliability, high availability and fault tolerance checks

### 23. GuardDuty & Secrets Manager

- GuardDuty: threat detection, monitoring and key features
- Enabling GuardDuty, managing detectors and tuning detection settings
- Interpreting findings, investigating and responding to alerts
- Secrets Manager: use cases and managing sensitive information
- Storing database credentials, API keys and access tokens
- Rotating and automating secret rotation
- Access control, permissions and monitoring secret usage

## Projects & Hands-On Labs

**Network Reconnaissance with Nmap**
Discover hosts, scan ports, detect services and operating systems, and run Nmap Script Engine scans against a lab network.

**Intrusion Detection with Snort & Suricata**
Install and configure an IDS, write rules that detect known and novel attacks, and track network activity in Wireshark.

**DevSecOps Pipeline in GitLab**
Add SAST, DAST, dependency and container scanning to a GitLab pipeline, then review and fix the vulnerabilities it reports.

**Penetration Test Walkthrough with Metasploit**
Follow a full pen test: target identification, port scanning, vulnerability analysis and exploiting VSFTPD, Samba SMB and VNC in a lab environment.

**Web Application Testing with Burp Suite**
Intercept and modify HTTP traffic, set the target scope and use Intruder, Repeater, Decoder and Comparer to test a lab web application.

**Securing an AWS Environment**
Set up IAM with MFA, encrypt data with KMS, and enable GuardDuty, Inspector and Macie to detect threats and sensitive data.

## Enrol & Contact

Book a free demo class or a 1-on-1 counselling session.
**Call / WhatsApp:** +91 89399 15577
**Email:** contact@greenstechnologys.com
**Website:** www.greenstechnologys.com
25 centres across Chennai, Bengaluru, Coimbatore, Trichy and Salem, plus live online batches. Curriculum may be updated by the trainer to reflect current industry practice.