SecuEyes

FULL COURSE SYLLABUS

SECUEYES ACADEMY

Full Course Syllabus

Every module and topic across all 8 courses: 7 taught live in Telugu (74 live classes) and 1 self-paced SOC Analyst course.

8	74	65	382
Courses	Live classes	Modules	Topics & lessons

01 Networking · 02 Kali Linux · 03 Ethical Hacking · 04 Web App Pentesting · 05 Secure Code Review · 06 Android App Pentesting · 07 Cybersecurity Auditing · 08 SOC Analyst

Start with a free live demo

Every weekend (IST)

Sat 6–7 PM · Sun 11 AM–12 PM · Sun 7–8 PM

+91 81250 59380 · Call or WhatsApp

contact@secueyes.in

secueyes.in

CERTIFIED & RECOGNISED

Ministry of MSME, Govt. of India

CONTENTS

What's inside

Tap a course to jump to it.

01	**Networking** Live	3 classes
02	**Kali Linux & Lab Setup** Live	2 classes
03	**Ethical Hacking** Live	14 classes
04	**Web Application Penetration Testing** Live	19 classes
05	**Secure Code Review** Live	17 classes
06	**Android Application Penetration Testing** Live	16 classes
07	**Cybersecurity Auditing** Live	3 classes
08	**SOC Analyst** Pre-recorded · self-paced	59 lessons
?	**FAQ & contact** Common questions, demo timings and how to reach us	

HOW THE PROGRAM WORKS

7 live courses

Taught live in Telugu, in order: 74 classes

1 recorded course

SOC Analyst: pre-recorded lessons you can watch any time, at your own pace

Online or classroom

Live online classes with a real-time instructor, or in the classroom in Hyderabad

A certificate per course

Earn one for every course you complete, including SOC Analyst

CERTIFIED & RECOGNISED

SecuEyes

YOUR INSTRUCTOR

Taught by a hacker who investigates cybercrime.



Every class is taught by **Chaitanya Eshwar Prasad**. He doesn't teach from slides: he teaches what he does every week, investigating real cybercrime cases and finding real vulnerabilities.

He started exploring technology in 7th class and was hunting security bugs by 10th. Today he supports cybercrime investigations as a forensic investigator, holds national records for his work, and has taught thousands of students on campus and through his Telugu YouTube channel.

7+	100+	33K+	9+
Years in cybersecurity	Bugs reported & secured	YouTube learners	Campuses as guest speaker

Anisetti Chaitanya Eshwar Prasad
Founder & Lead Instructor, Secueyes

SECURITY RESEARCH · HACKED & REPORTED

Google · YouTube · PayPal · Lenovo · Nokia · Epic Games · Unreal Engine · Rakuten · Kik · CoWIN · MCA, Govt of India · Govt of Telangana

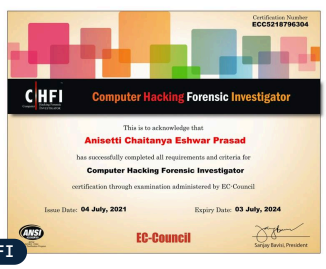
INVITED AS GUEST SPEAKER · UNIVERSITIES & COLLEGES

KL University · Anurag University · GRIET · VNRVJIET · KPRIT · ACE Engineering College · KL SAC · SJB Institute of Technology · Rishi MS Institute for Women

EC-COUNCIL CERTIFICATIONS



CEH



CHFI



CSA

01

Live · Course 01 of 08

Networking

How networks really work: the OSI and TCP/IP models, addressing, subnetting, DNS and ports.

AT A GLANCE

Language: **Telugu**

Certificate: **On completion**

AFTER THIS COURSE

- Explain how data moves through the OSI and TCP/IP layers
- Read TCP flags and the three-way handshake
- Work out IP ranges, subnets, DNS lookups and common ports

TOOLS YOU'LL USE

OSI model · TCP/IP · Subnetting · DNS · Ports & protocols

SYLLABUS · 3 MODULES · 17 TOPICS

01 Introduction to Networking

5 topics

- Types of networks
- UDP
- TCP/IP
- TCP/IP three-way handshake
- TCP flags: URG, ACK, PUSH, RST, SYN, FIN

02 OSI Model (Open Systems Interconnection)

7 topics

- Application layer
- Presentation layer
- Session layer
- Transport layer
- Network layer
- Data-link layer
- Physical layer

03 Basic Protocols

5 topics

- FTP (File Transfer Protocol)
- Telnet
- SMTP (Simple Mail Transfer Protocol)
- HTTP (HyperText Transfer Protocol)
- HTTPS (HTTP Secure)

02

Live · Course 02 of 08

Kali Linux & Lab Setup

Build your own legal hacking lab and get fluent with Kali Linux, the tool every pentester starts from.

AT A GLANCE

Language
Telugu

Certificate
On completion

Lab
Hacker Lab

AFTER THIS COURSE

- [x] Run Kali Linux and vulnerable targets on your own PC
- [x] Move around Kali with confidence from the terminal
- [x] Manage files, permissions and archives

TOOLS YOU'LL USE

VMware · Kali Linux · Metasploitable · DVWA

SYLLABUS · 2 MODULES · 8 TOPICS

01 Hacker Lab Setup

4 topics

- VMware setup on your PC
- Kali Linux installation in VMware
- Metasploitable: a vulnerable server
- DVWA setup

02 Kali Linux for Hackers

4 topics

- Kali Linux overview
- Kali Linux settings and configuration
- Read, write and extract permissions
- Kali Linux basic commands

03

Live · Course 03 of 08

Ethical Hacking

The full attacker toolkit: recon, scanning, exploitation, system and mobile hacking, sniffing, Wi-Fi, social engineering, passwords and cryptography.

AT A GLANCE

Language
Telugu

Certificate
On completion

Lab
Hacker Lab

AFTER THIS COURSE

- Map a target with OSINT, Nmap and Netcat
- Exploit lab machines with Metasploit and custom payloads
- Understand sniffing, Wi-Fi, DoS and social engineering attacks and how to defend against them

TOOLS YOU'LL USE

Nmap · Netcat · Metasploit · msfvenom · Wireshark · Bettercap · Shodan · theHarvester · Nikto · hping3

SYLLABUS · 15 MODULES · 84 TOPICS

01 Introduction to Ethical Hacking

4 topics

- Types of hackers
- Phases of ethical hacking
- Hacking concepts
- Security researchers, analysts and auditors

02 Information Gathering (Footprinting)

10 topics

- Website footprinting
- Whois
- VirusTotal
- Shodan
- GHDB (Google Hacking Database)
- theHarvester
- Nikto
- Information gathering from social media

02 Information Gathering (Footprinting) (continued)

- Image metadata
- Sublist3r

03 Nmap Scanning

6 topics

- Network scanning
- Server scanning
- Host discovery
- Port discovery
- Service version detection
- OS discovery

04 Netcat

6 topics

- Port scanning (TCP and UDP)
- Chat between two users (initiator and listener)
- Banner grabbing (FTP and SSH)
- File transfer
- Grabbing the HTTP banner
- Windows reverse connection

05 Metasploit

5 topics

- Server enumeration
- Modules: exploit, payload, auxiliary, encoder, evasion, post
- Exploiting the victim machine
- Setting LHOST and RHOST
- Creating a payload with msfvenom

06 Web Server Hacking

4 topics

- Scanning with Nmap
- Finding CVEs with Searchsploit

06 Web Server Hacking (continued)

- Finding exploits in Rapid7
- Exploiting with Metasploit

07 System Hacking

6 topics

- OS bypassing
- Error generation method (password cracking)
- Ngrok configuration
- Windows reverse shell
- Windows machine hacking
- Live screen with VNC

08 Mobile Hacking

6 topics

- Introduction to mobile OS
- Reverse shell with msfvenom
- Binding the reverse shell
- Tunnel forwarding with an open-source tool
- Access over WAN and LAN
- Exploiting mobile platforms

09 Malware

4 topics

- Types of malware
- Viruses
- Worms
- Trojans

10 Sniffing

7 topics

- Introduction to sniffing
- Wireshark
- Analysing packets in Wireshark

10 Sniffing (continued)

- Bettercap
- MAC address spoofing
- MAC flooding
- Man-in-the-middle: ARP poisoning

11 DoS / DDoS

5 topics

- Denial-of-service attacks
- Distributed denial-of-service attacks
- Botnets
- SYN flooding with hping3
- HOIC and LOIC in the lab

12 Wireless Hacking

6 topics

- Wireless encryption
- WEP, WPA and WPA2
- Hacking Wi-Fi networks
- Wi-Fi deauth attack
- Brute-forcing Wi-Fi networks
- Introduction to software-defined radio

13 Social Engineering

5 topics

- Introduction and types
- Human-based social engineering
- Computer-based social engineering
- Insider attacks
- External attacks

14 Password Cracking

4 topics

- Windows passwords from CMD
- Linux passwords
- SSH passwords
- Telnet passwords

15 Cryptography

6 topics

- Types of cryptography
- Symmetric and asymmetric keys
- Encryption algorithms
- Hash tools: MD5 and HashCalc
- Decoding and encoding
- Hiding text in files (steganography)

04

Live · Course 04 of 08

Web Application Penetration Testing

Hunt real web vulnerabilities with Burp Suite: the OWASP Top 10, XSS, SQL injection, CSRF, SSRF, command injection, file inclusion, XXE and access control.

AT A GLANCE

Language
Telugu

Certificate
On completion

Lab
ACEP Tech Electronics

AFTER THIS COURSE

- [x] Test a web app end to end with Burp Suite
- [x] Find and exploit the OWASP Top 10 and 20+ more bug classes
- [x] Write findings the way bug bounty programs and clients expect

TOOLS YOU'LL USE

Burp Suite · sqlmap · Burp Collaborator · DVWA · bWAPP · OWASP WebGoat

SYLLABUS · 12 MODULES · 82 TOPICS

01 Introduction to WAPT

7 topics

- What is web application penetration testing
- Vulnerability assessment vs penetration testing
- Bug hunting methodology
- Web application vs website
- DBMS architecture
- URL structure
- Lab setup: DVWA, bWAPP, OWASP WebGoat

02 OWASP Top 10 (2021)

10 topics

- A01 Broken Access Control
- A02 Cryptographic Failures
- A03 Injection
- A04 Insecure Design

02 OWASP Top 10 (2021) (continued)

- A05 Security Misconfiguration
- A06 Vulnerable and Outdated Components
- A07 Identification and Authentication Failures
- A08 Software and Data Integrity Failures
- A09 Security Logging and Monitoring Failures
- A10 Server-Side Request Forgery

03 Burp Suite

4 topics

- Proxy configuration
- Repeater
- Web crawling
- Target scanning

04 Cross-Site Scripting (XSS)

6 topics

- JavaScript event handlers
- Reflected XSS
- Stored XSS
- DOM-based XSS
- Cookie theft with XSS
- XSS exploitation

05 SQL Injection

7 topics

- Error-based
- Union-based
- Blind: boolean-based and time-based
- Manual injection
- Automated scanning
- Admin panel bypass
- sqlmap

06 Cryptographic Failures

5 topics

- ColdFusion vulnerability
- BREACH attack
- Heartbleed
- Missing HSTS
- POODLE attack

07 Broken Authentication & Sessions

6 topics

- Credential stuffing
- Improper admin login
- Insecure login forms
- Insecure logout
- Session hijacking
- Session ID exposed in the URL

08 CSRF

4 topics

- Change email
- Change address
- Add to cart
- CSRF exploitation

09 SSRF

4 topics

- SSRF stock checker
- SSRF to an internal API
- Blind SSRF
- Burp Collaborator

10 Shell, Command Execution & File Inclusion

5 topics

- File upload vulnerabilities
- Remote code execution

10 Shell, Command Execution & File Inclusion (continued)

- OS command injection
- Local file inclusion (LFI)
- Remote file inclusion (RFI)

11 XXE (XML External Entity)

7 topics

- Introduction to XML and entities
- Document Type Definitions (DTD)
- XXE injection
- Billion laughs (DoS)
- XXE through file upload
- XXE to remote code execution
- XSS via XXE

12 Additional Vulnerabilities

17 topics

- IDOR
- Host header attacks
- HTTP request smuggling
- HTML injection
- Open redirection
- Path and directory traversal
- Insecure CORS
- Clickjacking
- Missing rate limits
- Parameter tampering
- JWT attacks
- Negative quantity
- Race conditions (coupons)
- Mass assignment
- OTP bypass

12 Additional Vulnerabilities (continued)

- Insecure deserialization
- SSTI

05

Live · Course 05 of 08

Secure Code Review

Read code like an attacker and fix it like a defender: input validation, authentication, authorization, cryptography, error handling, sessions and common web flaws.

AT A GLANCE

Language	Certificate
Telugu	On completion

AFTER THIS COURSE

- [x] Spot vulnerabilities by reading backend code
- [x] Recommend the exact code fix, not just the finding
- [x] Fit code review into the development lifecycle

TOOLS YOU'LL USE

Static analysis tools · OWASP Top 10 · CWE · Secure coding standards

SYLLABUS · 11 MODULES · 48 TOPICS

01 Understanding Backend Code Issues

4 topics

- Authentication bypass and the reason behind it
- Fixing code to prevent authentication bypass
- Direct object reference issues and fixes in code
- Backend directory leaks and keeping them safe

02 Fundamentals of Software Security

3 topics

- Basics of secure software development
- Common security principles and best practices
- The OWASP Top 10 from a developer's view

03 Code Review Methodology

3 topics

- Establishing a structured review process
- Techniques for reviewing code effectively
- Code review in the software development lifecycle

04 Secure Coding Guidelines & Standards

3 topics

- Coding standards and secure coding guidelines
- Industry standards such as CWE
- Applying secure coding practices

05 Static Analysis Tools

3 topics

- Introduction to static analysis for code review
- Configuring popular code analysis tools
- Analysing results to find real vulnerabilities

06 Basic Code Review Testing

6 topics

- Input validation
- Authentication
- Authorization
- Cryptography
- Error handling
- Session management

07 Secure Authentication & Authorization

3 topics

- Reviewing authentication and authorization mechanisms
- Common authentication vulnerabilities
- Secure session management and access control

08 Secure Data Handling

3 topics

- Secure storage and encryption
- Input validation and sanitisation
- Preventing sensitive data exposure

09 Error Handling, Logging & Configuration

4 topics

- Error handling vulnerabilities
- Secure logging practices
- Secure configuration management
- Common misconfigurations and their impact

10 Challenges & Remediation

3 topics

- Practical code review exercises
- Recommending remediation
- Communicating findings and mitigations

11 Common Vulnerabilities in Code

13 topics

- CSRF
- Cookie hijacking
- Error handling
- IDOR
- LDAP injection
- LFI and RFI
- Directory and path traversal
- Open redirection
- SQL injection
- SSRF
- Password storage
- Session hijacking
- XSS

06

Live · Course 06 of 08

Android Application Penetration Testing

Break Android apps the professional way: OWASP Mobile Top 10, static and dynamic analysis, SSL pinning bypass, validation, retesting and report writing.

AT A GLANCE

Language
Telugu

Certificate
On completion

Lab
Android App Sec Lab

AFTER THIS COURSE

- [x] Decompile and analyse any APK
- [x] Find insecure storage, deep links, logging and network flaws
- [x] Bypass SSL pinning with Frida and write a full VAPT report

TOOLS YOU'LL USE

Android Studio · ADB · JADX-GUI · MobSF · Burp Suite · Frida · Objection

SYLLABUS · 9 MODULES · 45 TOPICS

01 Introduction to Android VAPT

6 topics

- What is Android application penetration testing
- Vulnerability assessment vs penetration testing
- Mobile bug hunting methodology
- Native app vs web app
- Android app architecture: APK, DEX, Manifest
- App components

02 Lab Setup

6 topics

- Android Studio + emulator (AOSP API 29)
- JADX-GUI
- MobSF
- Burp Suite
- Frida + Objection
- Build and install the ACEP Tech Academy app

03 OWASP Mobile Top 10 (2024)

10 topics

- M1 Improper Credential Usage
- M2 Inadequate Supply Chain Security
- M3 Insecure Authentication/Authorization
- M4 Insufficient Input/Output Validation
- M5 Insecure Communication
- M6 Inadequate Privacy Controls
- M7 Insufficient Binary Protections
- M8 Security Misconfiguration
- M9 Insecure Data Storage
- M10 Insufficient Cryptography

04 Static Analysis

5 topics

- Decompiling the APK with JADX
- Reading AndroidManifest.xml
- Automated scanning with MobSF
- Hardcoded credentials
- Hardcoded API keys

05 Dynamic Analysis (ADB)

4 topics

- SQL injection login bypass
- Insecure deep links
- Sensitive data in Logcat
- Unauthenticated debug mode

06 Local Storage Attacks

3 topics

- Plaintext password storage
- World-readable external storage
- Unprotected certificate export

07 Manifest & Configuration

4 topics

- Exported broadcast receivers
- allowBackup
- Cleartext traffic
- Debuggable build + unencrypted database

08 Network Security Testing

4 topics

- Burp Suite interception
- Insecure WebView SSL bypass
- SSL/TLS certificate pinning
- Bypassing SSL pinning with Frida & Objection

09 Reporting

3 topics

- Vulnerability validation and retesting
- Remediation guidance
- Writing a full VAPT report

07

Live · Course 07 of 08

Cybersecurity Auditing

Run a complete compliance audit: HIPAA, ISO/IEC 27001:2022 and PCI DSS assessments, evidence, risk management and reporting.

AT A GLANCE

Language
Telugu

Certificate
On completion

Lab
Security Auditing workspace

AFTER THIS COURSE

- [x] Assess controls against HIPAA, ISO 27001 and PCI DSS
- [x] Score and track risks with likelihood × impact
- [x] Deliver audit reports with linked evidence

TOOLS YOU'LL USE

ISO/IEC 27001:2022 · PCI DSS · HIPAA · Risk heat map

SYLLABUS · 8 MODULES · 39 TOPICS

01 Orientation & Navigation

5 topics

- Product picker and module selection
- Dashboard navigation
- HIPAA, ISO 27001 and PCI DSS modules
- Compliance percentage and statistics
- Requirements and controls navigation

02 Requirements & Controls Assessment

7 topics

- Requirement and control identification
- Compliance status assessment
- Assessment notes
- Search and status filters
- HIPAA and PCI DSS partial compliance
- ISO 27001 control assessment
- Real-time dashboard updates

03 Evidence Management

4 topics

- Evidence upload and description
- Linking evidence to requirements and controls
- PDF, Office, image, text and archive files
- Evidence download, deletion and verification

04 Risk Management

5 topics

- Likelihood × impact risk scoring
- High, medium and low classification
- Risk description and ownership
- Mitigation strategy and status tracking
- ISO 27001 risk heat map

05 Framework-Specific Tracking

4 topics

- HIPAA PHI and business associate tracking
- PCI DSS cardholder data and service provider tracking
- Access pattern and disposal procedure tracking
- Contract and compliance status tracking

06 Reports & Exports

5 topics

- Compliance summary and risk assessment reports
- Evidence documentation reports
- Requirement and control report tables
- Report preview and analytics
- HTML, CSV and JSON export

07 Full Audit Workflow

6 topics

- Requirements and controls assessment
- Supporting evidence collection
- Risk identification and mitigation tracking

07 Full Audit Workflow (continued)

- Final compliance report
- Audit activity attribution
- End-to-end audit cycle

08 Framework Coverage

3 topics

- HIPAA: 40 requirements
- ISO/IEC 27001:2022: 93 Annex A controls
- PCI DSS: 36 requirements

08

Recorded · Course 08 of 08

SOC Analyst

Get job-ready for a Security Operations Centre: SIEM and Splunk log investigation, phishing email analysis, digital forensics and incident response. Pre-recorded, so you learn at your own pace, with a certificate when you finish.

AT A GLANCE

Format
Pre-recorded videos

Language
Telugu

Lessons
59 · 5 modules

Pace
Self-paced, anytime

Certificate
On completion

AFTER THIS COURSE

- Investigate alerts and logs in Splunk the way a SOC analyst does
- Analyse phishing emails, headers, links and attachments
- Handle evidence and incidents from identification to recovery

TOOLS YOU'LL USE

Splunk · SIEM · SOAR · Windows Event IDs · SPF · DKIM · DMARC · Threat intelligence

SYLLABUS · 5 MODULES · 59 LESSONS

01 SOC Fundamentals

7 lessons

THEORY

- What is a SOC?
- SOC workflow
- What is SIEM?
- What is threat intelligence?
- What is SOAR?
- What is digital forensics?
- What is incident response?

02 Log Analysis & Investigation

18 lessons

SPLUNK FUNDAMENTALS (THEORY)

- Introduction to Splunk
- Splunk architecture & workflow

SPLUNK HANDS-ON (PRACTICAL)

- Splunk demo & your first search
- Understanding Windows Event IDs
- Investigating failed login attempts
- Analysing successful login events
- Process creation monitoring
- New user account creation detection
- Linux SSH log analysis
- Firewall log analysis
- DNS log analysis
- Email log analysis & phishing detection
- Brute-force attack investigation (end to end)
- Password spraying detection
- Suspicious PowerShell detection
- Privilege escalation detection
- Malware infection investigation
- Data exfiltration investigation

03 Email Phishing Analysis

12 lessons

THEORY

- Introduction to email phishing
- Email authentication
- Email header analysis
- SPF (Sender Policy Framework)
- DKIM (DomainKeys Identified Mail)
- DMARC (Domain-based Message Authentication, Reporting & Conformance)

03 Email Phishing Analysis (continued)

PRACTICAL

- Phishing email analysis
- Email header analysis
- SPF, DKIM & DMARC verification
- Sender domain analysis
- URL analysis
- Attachment analysis

04 Digital Forensics

14 lessons

THEORY

- Introduction to digital forensics
- The digital forensics process
- Identify
- Preserve
- Collect
- Examine
- Analyse
- Report

PRACTICAL

- Evidence identification
- Evidence preservation
- Evidence collection
- Evidence examination
- Evidence analysis
- Forensics report preparation

05 Incident Response

8 lessons

THEORY

- Introduction to incident response
- The incident response lifecycle

PRACTICAL

- Incident response workflow
- Incident identification
- Containment techniques
- Malware eradication
- System recovery
- Incident documentation & lessons learned

FAQ

Questions, answered.

Do I need prior experience?	No. The program starts from networking basics. Basic computer knowledge is enough to begin; a year in IT or security helps, and being able to read PHP code is useful for Secure Code Review but not required.
How long is the program?	74 live classes across 7 courses.
What language are classes in?	All classes are taught in Telugu.
Online or classroom?	Both. Join live online classes with a real-time instructor, or learn in the classroom. We also run workshops for colleges and teams.
Do I get a certificate?	Yes, one for each course you complete, including the recorded SOC Analyst course.
What are the fees?	Fees, batch dates and the full schedule are shared in the free live demo, so you can decide with all the details in front of you.
What do I need to start?	A laptop or PC that can run a virtual machine. We set up Kali Linux and your practice lab together in the Kali Linux & Lab Setup classes.
Is the SOC Analyst course live?	No. SOC Analyst is our pre-recorded course: watch the lessons whenever you like and learn at your own pace. The other seven courses are taught live.
Is this legal?	Yes. Every attack is practised only in our own lab machines and intentionally vulnerable apps, never on systems you do not own or have permission to test.
Will you help me find a job?	We give employment guidance and placement assistance, freelancing direction and student support. Hiring decisions are always made by employers.

Ready to take the first step?

Free live demo: Saturday 6:00 – 7:00 PM · Sunday 11:00 AM – 12:00 PM · Sunday 7:00 – 8:00 PM (IST).

+91 81250 59380 · Call or WhatsApp

contact@secueyes.in

secueyes.in

Scan to visit