

CSG-CSP

BECOME

CSG - CERTIFIED SECURITY PROFESSIONAL

6

MONTHS

PROGRAM

**ETHICAL
HACKING**

**CYBER
SECURITY**

WITH A.I

ENROLL NOW, HIRED TOMORROW



**CYBERSECURITY
GHOST**



Course Description

- This 6-month industry-aligned program is designed with practical cybersecurity skills, hands-on projects and internship experience, preparing them to confidently enter the cybersecurity job market

-
- This program leads to the industry-aligned **CSGCSP** Certification, awarded after successful completion of training, real-world projects, and final assessment

**CSGCSP - CYBERSECURITYGHOST
CERTIFIED SECURITY PROFESSIONAL**



CYBERSECURITY
GHOST

6 MONTHS PROGRAM IN

CYBERSECURITY WITH A.I

- **MODULE 1: WINDOWS ESSENTIALS & SECURITY**

- WINDOWS OS INTRODUCTION: SHELL & KERNEL
- USERS & PERMISSIONS, DISK MANAGEMENT
- TASK MANAGEMENT & EVENT VIEWER
- NETWORK SHARING & WINDOWS REGISTRY BASICS
- POLICY EDITOR OVERVIEW & ACCESS CONTROL
- VIRTUALIZATION BASICS (VMWARE / VIRTUALBOX)

- **MODULE 2: LINUX ESSENTIALS & SECURITY**

- LINUX OS HISTORY, ARCHITECTURE & FILE SYSTEM
- USERS & FILE PERMISSIONS + SPECIAL PERMISSIONS
- SYSTEM MONITORING & PROCESS MANAGEMENT
- CONFIGURING & SECURING SERVICES (SSH, FTP, HTTP)
- LOGS & ENVIRONMENT VARIABLES

- IP TABLE & BASIC FIREWALL RULES
-
- BASH SCRIPTING: LOOPS, CONDITIONALS, FILE HANDLING
-
- PACKAGE MANAGEMENT & SOFTWARE INSTALLATION

- **MODULE 3: NETWORKING**

-
- NETWORKING ESSENTIALS: INTERNET VS INTRANET,
-
- NETWORK TYPES, TOPOLOGIES
-
- OSI & TCP/IP MODEL
-
- IP & MAC ADDRESS, IPV4/IPV6, PACKET STRUCTURE
-
- NETWORK COMPONENTS & DEVICES (ROUTER, SWITCH, FIREWALL, PROXY)
-
- NETWORK PROTOCOLS & PORTS: TCP, UDP, DNS, DHCP, HTTP, HTTPS, TELNET, SSH
-
- ADVANCED CONCEPTS: NAT, PAT, ACL, VLAN, TRUNKING, STP, VPN & TUNNELING
-
- CISCO PACKET TRACER

- **MODULE 4: PYTHON FOR HACKERS**

- PYTHON BASICS: VARIABLES, LOOPS,
-
- FUNCTIONS, FILE I/O
-
- SOCKETS & NETWORK REQUESTS
-
- AUTOMATION SCRIPTS FOR RECON: PORT SCANNER,
-
- BANNER GRABBER, LOG PARSER



CSG-CSP ETHICAL HACKING WITH A.I

- Module 1** – Introduction
- Module 2** – Footprinting and Reconnaissance
- Module 3** – Scanning Networks
- Module 4** – Enumeration
- Module 5** – Vulnerability Analysis
- Module 6** – System Hacking
- Module 7** – Malware Threats
- Module 8** - Sniffing
- Module 9** – Social Engineering
- Module 10** – Denial of Service
- Module 11** – Session Hijacking
- Module 12** – Evading IDS, Firewalls
- Module 13** – Hacking Web Servers
- Module 14** – Hacking Web Applications
- Module 15** – SQL Injection
- Module 16** – Hacking Wireless Networks
- Module 17** – Hacking Mobile Platforms
- Module 18** – Hacking IoT and OT Hacking
- Module 19** – Cloud Computing
- Module 20** – Cryptography
- Module 21** – Defending A.I
- Module 22** – LLM Attacks



ADVANCE PENETRATION TESTING

CSG-CSP

- **Module 1: Python for Pentesters**

- Subnet Scanning
- Port Scanning
- Banner Grabbing
- Host Enumeration
- Nmap Automation
- Python Scripts for Recon Reports



- **Module 2: Web Security**

- OWASP Top 10
- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Server-Side Request Forgery (SSRF)
- Server-Side Template Injection (SSTI)
- Deserialization Attacks
- JWT Attacks
- Web server side attacks
- Web client side attacks
- Python Automation for Web Scanning

- **Module 3: Exploitation & Post-Exploitation**

- Metasploit Basics
- Manual Exploits
- Reverse Shells
- Session Hijacking
- Windows Privilege Escalation
- Linux Privilege Escalation
- Persistence Techniques

- **Module 4: Network Pivoting & C2 Framework**

- Lateral Movement Techniques
- Tunneling Techniques
- Port Forwarding
- C2 Frameworks
- Post-Exploitation
- Active Directory Attacks

- **Module 5: Mobile App Security**

- OWASP Mobile Top 10 Vulnerabilities
- Authentication Flaws
- Insecure Storage
- Weak Cryptography
- Reverse Engineering APK
- Vulnerable App Exploitation



**CYBERSECURITY
GHOST**

- **Capstone Projects**
- Enterprise Simulation: Recon → Scan → Exploit → Post-Exploitation → Pivot → AD Attack → Report
- Web + Network Combined PenTest
- Python Automation Scripts Showcase

HAVING QUERIES ?

CHAT WITH US/
CALL US

 **+91 6395041992**

 **@CYBERSECURITYGHOST**

 **@CYBERSECURITYGHOST**

CONNECT WITH THE INSTRUCTOR AND FOUNDER :

 **TRISHANTRAJORA**





MODERN ATTACK SURFACES & A.I SECURITY

- **Module 1: Compliance & Frameworks**
- NIST Cybersecurity Framework
- MITRE ATT&CK for Red & Blue Teams
- PCI-DSS & ISO 27001 Awareness
- Real-World Reporting & Documentation Standards

- **Module 2: Cloud Security**
- AWS Basics
- Azure Basics
- IAM Misconfigurations
- S3 Bucket Exposure
- Exposed Secrets
- Aws3 Attack and Defence
- Enumerate Users/Roles/Permissions
- Exploit API Misconfigurations
- Vulnerable Cloud Lab Deployment
- Python Automation for Cloud Scanning

- **Module 3: Container Security**

- Intro to containerisation
- Intro to Docker
- Kubernetes
- Container vulnerabilities
- Container Hardening
- Privilege Escalation in Containers
- Docker Escape Techniques

- **Module 4: AI Security**

- Fundamentals of AI Security
- Applications of AI in InfoSec
- Introduction to Red Teaming AI & ML Systems
- Prompt Injection Attacks
- LLM Output Manipulation Attacks
- AI Data Pipeline Attacks
- Attacking AI Applications & Systems
- Adversarial Simulations & Security Testing

Practice & Consolidation

- Web + Network + AD + Cloud + Container
- Python Scripts for Recon, Scanning, Report Automation
- Mock Pentest Simulation: End-to-End Workflow



CSG-CSP

CAPSTONE PROJECTS AND PLACEMENTS

- **Capstone Project 1 – Enterprise Simulation**
- Recon → Scan → Exploit → Post-Exploitation → Pivot → AD Attack → Cloud/Container → Report
- Deliverables: Full Report, Screenshots, Python Automation Scripts
-
- **Capstone Project 2 – Web + Cloud + Container Pentest**
- Web Application Vulnerabilities
- Cloud Misconfigurations
- Container Exploits
- Full End-to-End Pentest Report
- Automation Scripts
- Workflow Documentation



CSG-CSP MENTORSHIP

- **Placements - Job/Internship / Real-World Lab Work**
- Enterprise Scenario Labs
- Vulnerability Discovery
- Reporting
- Projects
- GitHub Portfolio Creation
- Workflow Showcase
- Resumes
- SOME SECRETS TO GET INTO CYBERSECURITY
- AS FRESHER
- JOBS/INDUSTRY INTERNSHIPS

ENROLL TODAY, HIRED TOMORROW
YOUR CYBERSECURITY CAREER STARTS HERE



**CYBERSECURITY
GHOST**

For Any Query About Course : [+91 6395041992\[whatsapp/call\]](https://wa.me/916395041992)
Email : csgtrainings@gmail.com



+91 6395041992



[@CYBERSECURITYGHOST](https://www.youtube.com/@CYBERSECURITYGHOST)



[@CYBERSECURITYGHOST](https://www.instagram.com/@CYBERSECURITYGHOST)



[TRISHANTRAJORA](#)