



SkillsDA®
Center for advance training

**Get Skilled
Be Employable**

CYBER SECURITY PROFESSIONAL PROGRAM

ISO 9001: 2015 Certified Training Center



In this Module program, you will learn:

Introduction

SkillsDA is an ISO 9001:2015 Cyber Security Training Centre situated in Chennai providing hands-on training on the Unique Cyberange Smart City Simulator thus ensuring its trainees are really skilled and Job Ready to fill the huge requirement of Cyber Security Specialists in a rapidly expanding digital world.



How to select and use the right frameworks to enhance cybersecurity decision-making in your organization



How to assess risk, improve defenses, and reduce vulnerabilities in your organization



How to speak the language of cybersecurity to enable informed conversations with your technology teams and colleagues, and ensure your organization is as cybersecure as possible

CS-Defensive & CS-Offensive Program

Module - 1 of CS- Defensive/Offensive

Fundamentals of Information technology

1. Fundamentals of Operating System
2. Introduction to Networking
3. Fundamentals of Programming
4. Fundamentals of Cloud Computing & Big Data Concepts



PROGRAM

CS-Defensive Program

Module - 2

Simple log Analysis & Tools

Module - 3

Security Operation Center (SOC)

1. Overview of the SOC Infrastructure
2. Modern Security Architecture Principles
3. Frameworks and Enterprise Security Architecture
4. Security Architecture-Key Techniques/Practices
5. SOCs/Security Architecture-Key Infrastructure Devices
6. Defensible Network Security Architecture Principles
7. Network Security Monitoring
8. SOCs and Defensible Endpoint Security Architecture
9. Automation and Continuous Security Monitoring
10. Hands On-Detecting Malware via Windows event logs

Module - 4

Process & Compliance

1. Introduction to ISO 27001 – Information Security Management System
2. Importance of Regulatory & Compliance Processes
3. Industry best practices for SOC & Security

CS-Offensive Program

Module - 2

Vulnerability Assessment

1. Network Vulnerability Assessment
2. System Vulnerability Assessment
3. Web & Mobile Application Vulnerability Assessment

Module - 3

Penetration Testing

1. Information Gathering
2. Network Exploitation
3. System Exploitation
4. Web & Mobile Application Exploitation
5. Client Side Attacks
6. Post Exploitation Attacks

Module - 4

Industrial system hacking

1. Introduction
2. Cyber Attack Vectors
3. Scenario: Discovery of Sensitive Devices
4. Scenario: Network Hacking via IoT
5. Scenario: Hacking Smart Devices
6. Scenario: Ransomware attacks
7. Scenario: Turbine Overpowered
8. Scenario: DoS & DDoS
9. Case Studies

LAB SYLLABUS



Defensive - Lab Syllabus

Phase I : Defending Corporate Networks

SOC Auditing

- Lab - 1 - Information Gathering Exercises
- Lab - 2 - Port Scanning & Vulnerability Scanning Exercises
- Lab - 3 - Network Exploitation Exercises.
- Lab - 4 - System Exploitation Exercises
- Lab - 5 - Web Application Exercise

SOC Operations

- Lab - 6 - Log Monitoring & Log Analysis
- Lab - 7 - Intrusion Detection & Prevention Exercises
- Lab - 8 - Network Security and Firewall Audit
- Lab - 9 - Vulnerability Assessment and Security Policy Audit

Advanced SOC Operations

- Lab - 10 - Securing Networks and Systems
- Lab - 11 - Malware Detection and Analysis
- Lab - 12 - Lateral Movement detection
- Lab - 13 - Incident Response and Procedures
- Lab - 14 - Forensic Procedures and First Steps
- Lab - 15 - Alerting and Notifications

Phase II : Defending Industrial Systems

Securing Systems

- Lab 1 - IoT Device Log Configurations
- Lab 2 - Ingesting SCADA system Logs
- Lab 3 - Parsing Special Device Logs
- Lab 4 - Industry Specific Attacks
- Lab 5 - Logic Attacks
- Lab 6 - Common Protocol Attacks
- Lab 7 - ICS Security
- Lab 8 - Firmware Attacks
- Lab 9 - Physical Attacks
- Lab 10 - Intrusion and sniffing





Offensive - Lab Syllabus

Penetration Testing

- Lab - 1 - Information Gathering Exercises
- Lab - 2 - Port Scanning & Vulnerability Scanning Exercises
- Lab - 3 - Network Exploitation Exercises.
- Lab - 4 - System Exploitation Exercises
- Lab - 5 - Web Application Exercise

Finding Targets And Gathering Information

- 01: Finding the IP address of the city's Municipal Corporation office.
- 02: Finding the SCADA master control device controlling Billboards.
- 03: Finding the NOC center for traffic light and accident relief system
- 04: Finding the City's Central Fire Alarm Management System
- 05: Finding the SCADA PLC master control of the DAM Project

Network, Port Recon And Cctv Hacking

- 06: Scanning the network for IP Cams.
- 07: Gain access to the city's central surveillance system
- 08: Move the camera away from the buildings 1,3 and 5

Traffic Controller Lights And Manipulating Systems

- 09: Establish connection to Traffic Controller System
- 10: Gain access to Modbus Relay Switching Program
- 11: Manipulate the program to gain access from external network

Network Exploitation And Banking System

- 12: Find the gateway to central bank system
- 13: Gain access to the bank's security system
- 14: Manipulate the bank's alarm system

Scada Switching, Hacking Railway Networks

- 15: Find the Northern Railway Networks system
- 16: Obtain access to NRN Network
- 17: Gain access to switching system
- 18: Switching tracks - controlling Modbus Relay

Automobile, Wifi And Hospital Hacking

- 19: DDOS'ing alarm systems
- 20: Hacking ECU causing total vehicle immobilization
- 21: Taking over Wi-Fi network at the local coffee shop
- 22: Manipulating medical records of patients admitted in hospital

Secure Power Grid And Defend Networks

- 23: Writing Firewall Rules for city's Power Grid
- 24: Snort Configuration for detecting attacks
- 25: SCADA Security for city's power grid
- 26: Setting Up Honeypots for defending networks
- 27: Policy Management to minimize risk

Forensic Operations Of System And Network












- 28: GSM interception and handling PCAP Files
- 29: Handling file system images
- 30: Log analysis of attack on a telecom system

Deliverables

-  120 hours class room training
-  30 hours Simulator training
-  200+ virtual labs
-  E-Learning platform
-  Soft Skill Training
-  NSD Certification
-  Internship & projects
-  Placement Support

At the End of the Course the
trainee will be able to be a
Professional in Cyber Security

Applicable Job Roles

- Threat Hunter 
- Pen Tester 
- L1 SOC Engineer 
- L2 SOC Engineer 
- SOC Analyst / SOC Engineer 
- Security Engineer 
- Security Administrator 
- Security Researcher 
- Security Architect 
- Cyber Security Consultant 
- Information Security Auditor 

 <https://www.facebook.com/skillsda.chennai/>

 twitter.com/skillsda

 [instagram.com/skillsda](https://www.instagram.com/skillsda)

 <https://www.linkedin.com/company/skillsda>

 SkillsDA - Cyber Security

SkillsDA®
Center for advance training

INGU's Knowledge Academy Pvt Ltd .

Plot No.193, Nehru Nagar 1st Main Road, OMR Road Kottivakkam, Chennai – 600096 , INDIA

Mobile : +91 9090589696 | Fixed-line : +91 44 4859 9696 | Email : info@skillsda.com | Website : www.skillsda.com