CERTIFIED CYBER WARRIOR PROGRAM (CCWP)– FOUNDATION

Detailed Academic Curriculum & Syllabus

Global Cyber Security Foundations Program

Program Overview

Program Name

Certified Cyber Warrior Program (CCWP) – Foundation

Program Duration

6 Months

Program Level

Beginner to Intermediate Foundation Level

Training Modes

- Online Live Training
- Offline Classroom Training
- Hybrid Learning Support

Program Objective

The CCWP Foundation Program is designed to build strong cybersecurity foundations and prepare students for real-world cybersecurity careers through:

- Practical Training
- Enterprise-Oriented Learning
- Hands-on Labs
- Investigations
- Projects
- Professional Reporting
- Interview Preparation

The Program follows:

- International Cyber Security Standards
- Structured Learning Progression
- Industry-Oriented Methodologies
- Enterprise Security Workflows

Practical Learning Structure

Component	Weightage
Practical Labs	50%
Theory Sessions	30%
Projects & Assessments	20%

Program Learning Outcomes

After completing CCWP Foundation, students will be able to:

Technical Skills

- Understand enterprise IT infrastructure
- Linux Administration
- Bash Scripting
- Networking Fundamentals
- Packet Analysis
- Network Security
- Web Application Security
- API Security Fundamentals
- Python Programming
- Security Automation
- Windows Security Basics
- Active Directory Fundamentals
- SOC Operations
- SIEM Monitoring
- Log Analysis
- Threat Intelligence
- Incident Response
- Cloud Security Fundamentals
- AWS Basics
- Azure Basics

- Docker Fundamentals
- Kubernetes Awareness
- Container Security Awareness
- DevSecOps Awareness
- Threat Hunting Fundamentals
- Detection Engineering Awareness
- Security Monitoring
- Authentication & Access Control
- Vulnerability Assessment
- Penetration Testing Fundamental
- Security Documentation
- Technical Reporting

Professional Skills

- Analytical Thinking
- Investigation Methodology
- Technical Communication
- Professional Reporting
- Resume Building
- LinkedIn Optimization
- GitHub Portfolio Development
- Interview Preparation
- Team Collaboration

- Cybersecurity Ethics
- Documentation Standards
- Security Operations Workflow Understanding

Practical Skills

- Security Investigations
- Packet Capturing & Analysis
- Web Security Testing
- SIEM Monitoring
- Phishing Investigation
- Incident Investigation
- IOC Analysis
- Root Cause Analysis
- Cloud Security Assessments
- Linux Hardening
- Active Directory Configuration
- Security Log Analysis
- API Testing
- Python Security Automation
- Security Reporting
- Threat Analysis
- Security Documentation

Certification Alignment

This curriculum aligns with concepts from:

- CompTIA A+
- Network +
- Linux +
- Security +
- Google Cybersecurity Certificate
- Microsoft SC-900
- CeH
- Microsoft AZ-900
- AWS Cloud Practitioner
- OWASP Top 10
- PNPT
- CompTIA Security +
- SC-200 Concepts
- Certified Ethical Hacker (CeH)
- eJPT Fundamentals
- BTL-1 (Blue Team Foundation)
- NIST Cybersecurity Framework Basics
- CIS Controls Awareness
- DevSecOps Awareness Concepts
- Docker & Kubernetes Security Awareness

Training Methodology

The program follows:

- Theory Sessions
- Live Demonstrations
- Guided Labs
- Practical Exercises
- Assignments
- Case Studies
- Mini Projects
- Capstone Projects
- Assessments
- Mock Interviews

Recommended Practice

Students are encouraged to spend:

- 2–3 hours daily in labs
- practical investigation practice
- project building
- documentation

What Makes CCWP Different?

- SOC + VAPT + Cloud in One Program
- Real-World Case Studies
- Enterprise-Oriented Training
- Practical-First Learning
- Portfolio-Focused Approach
- Modern Cloud & Container Awareness

Domain	Skills
Linux	Administration, Hardening, SSH
Networking	Packet Analysis, Protocols
SOC	SIEM, Alert Analysis
Web Security	OWASP, Burp Suite
Cloud	IAM, S3 Security
Programming	Python Automation
Investigation	IOC Analysis, Threat Hunting
Reporting	VAPT & SOC Reporting

Students Graduate With

- GitHub Portfolio
- Python Security Tools
- VAPT Reports
- SOC Investigation Reports
- Cloud Assessment Reports
- Mini SOC Deployment
- Linux Hardening Project
- Threat Investigation Reports
- Web Security Assessment Reports

Program Standards

CCWP follows:

- enterprise security workflows
- ethical cybersecurity practices
- international learning methodologies
- practical-first training
- portfolio-based learning
- investigation-driven learning
- industry-oriented reporting practices

CAREER OUTCOMES

After completing CCWP Foundation, students become prepared for roles such as:

- SOC Analyst L1
- Junior Security Analyst
- Cybersecurity Intern
- Junior Penetration Tester
- Cyber Security Associate
- Junior VAPT Analyst
- Security Operations Intern
- IT Support + Security Roles
- Security Support Engineer
- Cloud Security Intern
- Junior Incident Response Analyst
- SIEM Monitoring Analyst
- Threat Intelligence Intern

Module Structure

Module	Duration
Module 1 – IT & Computer Fundamentals	2 Weeks
Module 2 – Linux Administration & Security	4 Weeks
Module 3 – Networking & Network Security	5 Weeks
Module 4 – Cyber Security Fundamentals	3 Weeks
Module 5 – Python Programming for Cybersecurity	4 Weeks
Module 6 – Web Application Security Fundamentals & VAPT	5 Weeks
Module 7 – Windows Security & Active Directory Basics	4 Weeks
Module 8 – SOC Operations & Blue Team Foundations	4 Weeks
Module 9 – Cloud Security Foundations	3 Weeks
Module 10 – Professional Development & Career Preparation	2 Weeks
MODULE 11 — Cyber Security Case Studies & Real-World Incident Analysis	2 Weeks
Module 12 – Capstone Projects & Final Assessment	2 Weeks

MODULE 1 – IT & Computer Fundamentals

Objective

Build strong IT fundamentals required for cybersecurity learning.

Topics Covered :

Introduction to IT

- IT Industry Overview
- Enterprise Infrastructure Basics
- Cybersecurity Domains
- Career Paths in Cybersecurity
- Hardware & Software

Computer Hardware Fundamentals

- CPU Architecture
- RAM & Memory
- Storage Devices
- Motherboard Components
- BIOS & UEFI
- Peripheral Devices

Operating System Fundamentals

- Windows Overview
- Linux Overview
- Mac OS & Mobile OS Overview
- Processes & Memory Concepts

File Systems

- NTFS
- FAT32
- EXT4
- Partitioning Concepts
- File Management

Virtualization

- Virtual Machines
- Hypervisors
- Snapshots
- Lab Environments
- Lab Building

Internet Fundamentals

- Working Of Internet
- Client-Server Architecture
- Domains & Hosting
- ISPs
- Web Infrastructure

Cloud Computing Basics

- Cloud Fundamentals
- IaaS / SaaS / PaaS
- Public vs Private Cloud

Practical Labs

- Install VirtualBox/VMware
- Create Windows VM
- Create Linux VM
- Configure Virtual Networks
- Snapshot Management

Mini Project

Personal Cybersecurity Lab Setup

Students build:

- Windows VM
- Kali Linux VM
- Ubuntu VM
- Testing Network Environment

Skills Gained

- IT Infrastructure Understanding
- Virtualization Skills
- Operating System Basics
- Lab Building

MODULE 2 – Linux Administration & Security

Objective

Develop Linux administration & Linux security skills.

Topics Covered :

Linux Fundamentals

- Linux History
- Linux Distributions
- Linux Architecture
- File System Structure

Linux Terminal & Bash

- Navigation
- File Operations
- Linux Commands
- Searching
- Editing Files
- Pipes & Redirection

Users & Permissions

- Users & Groups
- chmod & chown
- sudo privileges

Linux Administration

- Apt Package Management
- Services & Processes
- systemctl
- Cron Jobs

Networking Commands

- ping
- netstat
- ss
- traceroute
- nslookup & dig

SSH Administration

- Secure Remote Access
- SSH Hardening
- Key Authentication

Bash Scripting

- Variables
- Conditions
- Loops
- Automation Scripts

Linux Security

- Firewall Basics
- UFW
- Fail2ban
- Password Policies
- Linux Hardening

Log Management

- auth.log
- syslog
- journalctl

Practical Labs

- Linux Installation
- User Management
- Permission Management
- Firewall Configuration
- SSH Hardening
- Bash Scripting
- Log Analysis

Mini Project

Linux Security Hardening Project

Students:

- secure Linux server
- configure firewall
- implement hardening
- create security documentation

Skills Gained

- Linux Administration
- Bash Scripting
- Linux Security
- SSH Management
- Log Analysis

MODULE 3 – Networking & Network Security

Objective

Build strong networking and network security foundations.

Topics Covered :

Networking Fundamentals

- Data Communication Basics
- Types of Network
- TCP/IP Model
- OSI Model
- Packets & Frames
- Routing & Switching

IP Addressing

- IPv4
- IPv6
- Public vs Private Ips
- NAT
- DHCP & APIPA
- Subnetting
- CIDR
- Subnetting Numericals

Core Protocols

- Protocols
- Ports
- Ports Services
- Port Forwarding
- DNS
- ARP
- DHCP
- HTTP/HTTPS
- FTP
- SSH
- SMTP
- ICMP
- Telnet & RDP

Network Infrastructure & Devices

- Routers , Gateways
- Switches , Hub , Bridge
- Firewalls / IDS / IPS
- Access Points
- Proxies

Network Topologies

- Network Arangement
- Network Topologies
- Importance of Topologies

Enterprise Networking

- VLAN Basics
- VPN Concepts
- NAT Working
- Load Balancers
- Enterprise Architecture

Wireless Networking

- Wi-Fi Standards
- WPA/WPA2/WPA3
- Wireless Security
- Wifi Attacks

Packet Analysis

- Wireshark
- ARP Spoofing
- Packet Inspection
- Traffic Analysis / Malware Analysis

Network Scanning

- Nmap
- Host Discovery
- Network Scanning
- Service Detection
- Enumeration Basics
- Firewall / IDS / IPS Evasion

Network Security

- Firewall Rules
- IPS / IDS Setup
- Network Segmentation
- Secure Network Design

Practical Labs

- Wireshark Labs
- Packet Capture Analysis / Malware Analysis
- Nmap Scanning
- Firewall Configuration
- IPS / IDS Setup
- Wifi Attacks / Wifi Attacks Methodology
- Wireshark – Nmap (Attack & Defense)

Mini Project

Suspicious Traffic Investigation

Students analyze malicious traffic and create investigation reports.

Skills Gained

- Networking Fundamentals
- Subnetting
- Packet Analysis
- Network Monitoring
- Wireshark Usage
- Wireshark / Nmap
- Firewall / IDS / IPS
- Wifi Attacks
- Network Security Basics

MODULE 4 – Cyber Security Fundamentals

Objective

Build strong cybersecurity concepts and security operations understanding.

Topics Covered :

Security Fundamentals

- Cyber Security Fundamentals
- CIA Triad
- Threats
- Vulnerabilities
- Risks

Security Principles

- Defense in Depth
- Least Privilege
- Zero Trust

Types of Cyber Attacks

- Malwares
- Phishing & Social Engineering Toolkit
- DNS Spoofing / Advance Phishing
- Credential Attacks / Insider Threats

Malware Fundamentals

- Virus
- Worm
- Trojan
- Spyware
- Rootkits
- Botnets
- Ransomwares

Authentication & Authorization

- MFA
- Password Security
- Identity Management

Cryptography Basics

- Cryptography Concepts
- Importance of Cryptography
- Encryption
- Hashing
- AES
- RSA
- SSL/TLS
- PKI

Security Frameworks

- MITRE ATT&CK
- Cyber Kill Chain
- NIST Basics
- CIS Controls

Risk Management & Compliance

- Risk Assessment
- Security Policies
- GDPR
- ISO 27001 Basics

Security Operations Basics

- Logs
- Alerts
- Incident Response
- Vulnerability Management

Practical Labs

- Password Auditing
- Malware Demonstrations
- Phishing , Social Engineering Attacks , DNS Spoofing
- Credentials Attacks and More

Mini Project

Security Risk Assessment

Students perform risk analysis and create professional reports.

Skills Gained

- Security Concepts
- Risk Assessment
- Cryptography Basics
- Incident Response Basics
- Malwares
- Social Engineering Attacks
- Security Framework Fundamentals
- Security Operations Fundamentals

MODULE 5 – Python Programming for Cybersecurity

Objective

Teach automation & scripting for cybersecurity tasks.

Topics Covered :

Python Fundamentals

- Variables
- Data Types
- Functions
- Conditions
- Loops

Data Handling

- Strings
- Lists
- Dictionaries
- File Handling

Regex & Parsing

- Pattern Matching
- Log Parsing
- IOC Extraction

APIs & Automation

- Requests Library
- REST APIs
- JSON Handling

Socket Programming Basics

- TCP Communication
- Client-Server Concepts

Security Automation

- Log Analysis
- Whois Automation
- Threat Intelligence Parsing

Secure Coding Basics

- Input Validation
- Exception Handling

Practical Labs

- Port Scanner
- Whois Tool
- Log Analyzer
- API Integration
- Socket Programming

Mini Project

Python Security Automation Tool

Students build automation utilities for security operations.

Skills Gained

- Programming Knowledge
- Python Scripting
- Security Automation
- API Usage
- Log Parsing
- Tool Development Basics

MODULE 6 – Web Application Security Fundamentals and Vulnerability Assessment & Penetration Testing (VAPT)

Objective

Develop web application security testing skills.

Topics Covered :

Web Fundamentals

- Web Architecture
- Frontend vs Backend
- Static & Dynamic Websites
- Client-Server Communication
- Request and Response Lifecycle
- Web Servers
- Browsers
- DNS Resolution
- DNS Records
- Hosting Basics
- Html Basics
- Css Basics
- Javascript Basics
- APIs
- JSON
- AJAX & PHP Concepts

HTTP & HTTPS

- HTTP Methods
- GET / POST / PUT / Delete / Patch
- Headers
- Request Headers / Response Headers / Security Headers
- Status Codes
- Certificates
- TLS/SSL
- Secure Communication
- Https Importance

Authentication & Session Security

- Login Mechanisms
- Sessions
- Cookies
- Tokens
- Session Management
- Session IDs
- Session Security
- Session Timeout
- Session Hijacking Concepts
- Access Control
- Authorization
- RBAC
- IDOR Cencepts
- Authentication Security & MFA

Introduction Web Application Security Testing

- Web Security Testing Methodology
- Importance of Web Security and Penetration Testing
- Phases of Penetration Testing
- Types of Penetration Testing
- Footprinting & Reconnaissance
- Information Gathering
- Passive Information Gathering
- OSINT
- Doxing
- Google Hacking Database (GHDB)
- Active Information Gathering
- Information Gathering Tools
- Network Information Gathering
- Image Footprinting
- Mobile Number Footprinting
- Mapping
- Vulnerability Introduction
- Vulnerability Assessment
- VAPT Methodology
- Validation
- Reporting Format
- Reporting

Advanced API Security Awareness

- JWT Authentication Basics
- 0Auth Basics
- API Tokens
- API Rate Limiting
- API Abuse Concepts
- Broken Authentication in APIs
- API Authorization Concepts

Basics of Metasploit Basics

- Introduction to Metasploit Framework
- Auxiliaries
- Payloads
- Exploits
- Evaders
- Exploitation Techniques
- Vulnerability Exploitation
- Enumeration Techniques
- SMTP Enumeration & Exploitation
- FTP Enumeration & Exploitation
- SMB Enumeration & Exploitation
- RDP Enumeration & Exploitation
- Telnet Enumeration & Exploitation
- Post Exploitation Techniques
- Reporting & Documentation

Introduction to Burp Suite

- Introduction to Burpsuite
- Browser – Proxy Configuration
- Burpsuite Configuration & Setup
- Repeater
- Intruder
- Decoder
- Comparer
- Burpsuite Advance (Extensions , Filters)

OWASP Top 10

- Broken Access Control
- IDOR
- Forced Browsing
- Privilege Escalation Concepts
- Cryptographic Failure
- SQL Injection Basics
- Command Injection Concepts
- LDAP Injection Basics
- Cross Site Scripting (XSS)
- Reflected XSS
- Stored XSS
- DoM XSS
- CSRF Concepts
- Token Protection
- Security Misconfigurations & Outdated Components

API Security Basics

- REST APIs
- JSON APIs
- Authentication Concepts
- Rate Limiting
- API Misconfiguration

Secure Development Concepts

- Input Validation
- Output Encoding
- Secure Authentication
- Error Handling
- Security Headers
- CSP
- HSTS
- X-Frame Options
- Secure Cookies
- Logging & Monitoring
- Security Logging
- Web Monitoring Basics

Practical Labs

- Http Analysis
- DVWA Labs
- OWASP Juice Shop
- Burp Suite Labs
- SQL Injection Testing
- XSS Testing
- Authentication Testing
- FTP , SMB , SMTP , RDP , Telnet Exploitation
- Password Testing
- API Testing & Security Header Testing

Mini Project

Web Application Security Assessment

Students perform web security assessments and create VAPT reports.

Skills Gained

- Web Security Testing
- Burp Suite Usage
- Metasploit Framework Basics
- Exploitation Techniques
- VAPT
- API Testing
- Information Gathering
- Web Security / Penetration Testing

MODULE 7 – Windows Security & Active Directory Basics

Objective

Understand Windows enterprise environments and Active Directory fundamentals.

Topics Covered

Windows Fundamentals

- Windows Architecture
- User Mode vs Kernel Mode
- NTFS
- Permissions
- File Attributes
- Registry Structure
- Security Implications
- Processes & Services

Users & Authentication

- Users & Groups
- Authentication vs Authorization
- NTLM Basics
- Kerberos Basics
- Password Complexity
- Account Lockout
- MFA Concepts

Windows Exploitation

- Remote Access Trojan (RAT)
- Windows Payloads
- What is FUD Payloads
- Exploiting Windows 7
- Exploiting Windows 10 / 11

Active Directory Fundamentals

- What is Active Directory
- Domain Controllers
- Organizational Units
- Group Policies
- GPO Concepts
- Security Policies
- User Restrictions
- Enterprise Authentication
- Active Directory Structure
- Trusts and Relationships

PowerShell Basics

- Commands
- Administration Tasks
- Security Monitoring
- Scripting Introduction

Windows Administration & Security

- Windows Services Management
- Startup Process
- Security Logs
- Application Logs
- System Logs
- Windows Hardening
- Firewall
- Defender
- User Restrictions
- Patch Management

Windows Security Monitoring

- Failed Login Monitoring
- Suspicious Processes
- MRT
- Common Persistence Mechanisms

Enterprise Attack Awareness

- Pass-the-Hash Awareness
- Kerberoasting Awareness
- Lateral Movement Concepts
- Privilege Escalation Awareness

Practical Labs

- Windows Administration and Hardening
- AD Setup
- Event Log Analysis
- PowerShell Practice
- User Enumeration & Exploitation
- Remote Access Trojans
- Process Monitoring
- Group Policy Configuration

Mini Project

Active Directory Enterprise Lab

Students deploy and secure mini AD environment.

Skills Gained

- Windows Administration
- Active Directory Basics
- PowerShell Fundamentals
- Windows Security Monitoring
- Spyware Information
- Windows Exploitation

MODULE 8 – SOC Operations & Blue Team Foundations

Objective

Build practical SOC & Blue Team skills.

Topics Covered :

SOC Fundamentals

- Purpose of SOC
- SOC Types
- SOC Roles & Responsibilities
- SOC Analyst L1 & L2
- Incident Responder
- Threat Hunter
- Detection Engineer
- SOC Workflow
- Alert Generation
- Triage
- Investigation
- Escalation
- Response & Documentation

Security Logging

- Windows Logs
- Linux Logs
- Network Logs
- Web Logs

SIEM Fundamentals

- Introduction to SIEM and SIEM Architecture
- Log Collection
- Correlation
- Dashboard
- Alerting
- SIEM Use Cases
- Brute Force Detection
- Malware Alerts
- Suspicious Network Activity

Introduction to Wazuh

- Wazuh Architecture
- Agents
- Monitoring Dashboard

Introduction to Splunk

- Search Basics
- Dashboards
- Alerting Concepts

ELK Stack Basics

- Elastic Search
- Logstash
- Kibana

Threat Intelligence Fundamentals

- Threat Intelligence
- IOC Concepts
- Threat Feeds
- File Hashes
- URLs
- MITRE ATT&CK Basics
- Techniques
- Mapping Attacks
- Threat Hunting Basics
- Hunting Concepts
- Behavioral Analysis
- IOC Searching

Phishing & Email Analysis

- Email Headers
- SPF
- DKIM
- DMARC
- URL Analysis
- Attachment Analysis

Malware Analysis Fundamentals

- Malware Analysis Basics
- Sandboxing
- Antivirus & EDR Basics

Incident Response Lifecycle

- Preparation
- Identification
- Detection
- Containment
- Recovery
- Alert Triage
- False Positives
- Prioritizations
- Investigation workflow
- Evidence Collection
- Timeline Analysis
- Sigma Rules
- Detection Mapping
- Documentation & Ticketing

Practical Labs

- SIEM Setup
- Windows Logs Analysis
- Linux Logs Analysis
- Wazuh Setup
- Splunk Basics
- Phishing investigation
- Threat Intelligence
- IOC Investigation
- MITRE ATT&CK Mapping

Tools :

- Wazuh
- Splunk
- ELK Stack
- Virus Total
- AbuseIPDB
- Any.Run
- CyberChef

Mini Project

Mini SOC Deployment

Students deploy SIEM and investigate security incidents.

Skills Gained

- SOC Operations
- SIEM Monitoring
- SOC Analysis
- Wazuh
- Splunk
- ELK Stack
- Virustotal
- AbuseIPDB
- Any.Run
- CyberChef
- MITRE ATT&CK
- Incident Investigation
- Threat Intelligence Operation

MODULE 9 – Cloud Security Foundations

Objective

Understand cloud technologies and cloud security basics.

Topics Covered :

Cloud Fundamentals

- Cloud Computing
- Evolution of Cloud
- Benefits of Cloud
- IaaS/PaaS/SaaS
- Public vs Private Cloud
- Hybrid Cloud
- Multi Cloud

AWS Fundamentals

- AWS Global Infrastructure
- IAM
- EC2
- S3
- VPC Basics
- Security Groups

Container Fundamentals

- What are Containers
- Containers vs Virtual Machines
- Benefits of Containers
- Modern Cloud Infrastructure

Docker Fundamentals

- Docker Architecture
- Docker Images
- Docker Containers
- Docker Hub
- Docker Lifecycle

Basic Docker Commands

- Pull Images
- Run Containers
- Stop Containers
- Remove Containers
- Inspect Containers

Kubernetes Awareness

- What is Kubernetes
- Container Orchestration
- Kubernetes Architecture
- Pods
- Nodes
- Deployments
- Services
- Scaling Concepts

Container Security Basics

- Insecure Images
- Exposed Containers
- Weak Configurations
- Container Monitoring Basics

Kubernetes Security Awareness

- RBAC Concepts
- Secrets Management Awareness
- Least Privilege
- Cluster Security Awareness

AWS IAM

- Users
- Groups
- Roles
- Policies
- MFA

S3 Security

- Bucket
- Public Access Point
- Encryption

AWS Monitoring Basics

- CloudTrail
- CloudWatch

Azure Fundamental

- Introduction to Azure
- Azure Architecture
- Resource Groups
- Azure Identity Basics
- Roles & permissions

Cloud Security Concepts

- Shared Responsibility Model
- Cloud Provider Responsibility
- Customer Responsibility
- Cloud Risks
- Misconfiguration
- Weak IAM
- Exposed Storage
- IAM Security
- Cloud Networking Basics
- Cloud Firewalls
- Credential Exposure
- Logging & Monitoring

Cloud Security Best Practices

- Secure Configuration
- Hardening
- Secure Defaults
- Data Protection
- Encryption
- Backup Concepts
- Secure Storage
- Cloud Governance
- Governance Concepts

DevSecOps Fundamentals

- What is DevSecOps
- DevOps vs DevSecOps
- Secure Development Lifecycle (SDLC)
- CI/CD Basics
- Security in CI/CD Pipelines

Secure Development Awareness

- Shift Left Security
- Code Review Concepts
- Security Testing in Development

Practical Labs

- AWS Setup
- S3 Security
- IAM Setup
- Cloud Monitoring
- Azure Basics
- Secure Storage Configuration
- Cloud Security Assessment
- Docker Installation
- Run Containers
- Container Inspection
- Kubernetes Architecture Demo

Mini Project

Cloud Security Assessment

Students secure cloud infrastructure and create security reports.

Skills Gained

- Cloud Fundamentals
- AWS Basics
- Azure Basics
- IAM Security
- Cloud Monitoring
- Cloud Security Basics
- Cloud Monitoring

MODULE 10 – Professional Development & Career Preparation

Objective

Prepare students for placements and professional cybersecurity careers.

Topics Covered :

Career Development

- Cybersecurity Career Paths
- Industry Roles
- Salary Trends
- National and International Markets
- Freelancing
- Remote Work

Resume Building

- Resume Structure
- ATS-Friendly Resume
- Technical Resume Structure

LinkedIn & Branding

- LinkedIn Optimization
- Professional Networking

Git & GitHub

- Git Basics
- Repository Management
- Documentation

Reporting

- VAPT Reports
- SOC Reports
- Technical Documentation

Interview Preparation

- HR Interviews
- Technical Interviews
- Mock Interviews

Workplace Professionalism

- Communication Skills
- Team Collaboration
- Cybersecurity Ethics

Practical Labs

- Resume Building
- GitHub Portfolio
- Reporting Practice
- Mock Interviews

MODULE 11 — Cyber Security Case Studies & Real-World Incident Analysis

Objective

Students learn how real cyber attacks happen, how organizations respond, and how security teams investigate incidents.

Topics Covered

- Introduction to Cybersecurity Case Studies
- Importance of Real-World Incident Analysis
- Cyber Attack Lifecycle Analysis
- Investigation Methodology
- Root Cause Analysis
- Evidence Collection Concepts
- Incident Timeline Analysis
- Threat Actor Methodologies
- Enterprise Security Failures

Ransomware & Malware Case Studies

- Ransomware Attack Lifecycle
- WannaCry Case Study
- Colonial Pipeline Incident
- Healthcare Ransomware Incidents
- Malware Delivery Mechanisms
- Persistence Concepts
- Business Impact Analysis
- Recovery & Response Concepts

Phishing & Social Engineering Case Studies

- Business Email Compromise (BEC)
- CEO Fraud
- Credential Phishing Campaigns
- Fake Login Pages
- Email Spoofing
- Human Manipulation Techniques
- Social Engineering Failures
- Enterprise Awareness Failures

Web Application Breach Case Studies

- SQL Injection Breaches
- Cross-Site Scripting Incidents
- Authentication Failure Cases
- Session Management Failures
- API Security Breaches
- Token Exposure Cases
- Authorization Failure Cases
- Insecure Configuration Incidents

Cloud Security Case Studies

- Public Cloud Misconfigurations
- Exposed S3 Bucket Cases
- IAM Misconfiguration Incidents
- Cloud Credential Exposure
- GitHub Secret Exposure Cases
- Insecure Container Deployments
- Kubernetes Misconfiguration Cases
- Cloud Logging Failures

SOC & Incident Response Case Studies

- SOC Investigation Workflow
- Alert Triage Methodology
- SIEM Investigation Cases
- IOC Analysis
- Log Correlation
- False Positive Analysis
- Threat Hunting Case Studies
- Detection Engineering Awareness

Insider Threat & Enterprise Security Cases

- Insider Threat Incidents
- Privilege Misuse Cases
- Access Control Failures
- Weak Segmentation Cases
- Security Misconfiguration Incidents

Nation-State & Advanced Threat Awareness

- APT Awareness
- Supply Chain Attack Cases
- Critical Infrastructure Incidents
- Telecom & Energy Sector Incidents
- Large-Scale Data Breaches
- Persistence & Lateral Movement Awareness

Practical Labs

- Phishing Investigation
- Malware Timeline Analysis
- SIEM Investigation
- Cloud Breach Analysis
- Web Application Breach Investigation
- IOC Investigation
- Alert Correlation Exercises
- Root Cause Analysis Practice

Mini Project

Real-World Security Incident Investigation

Students must:

- investigate real cyber incident
- identify attack chain
- analyze security failures
- map MITRE ATT&CK techniques

MODULE 12 – Capstone Projects & Final Assessment

Objective

Validate technical, practical, and professional skills through real-world projects.

Mandatory Capstone Projects

Linux Hardening Project

- Secure Linux environment
- Implement hardening controls

Network Investigation Project

- Analyze suspicious traffic
- Investigate malicious activity

Python Security Tool

- Build automation utility
- Create documentation

Web Application Assessment

- Identify vulnerabilities
- Generate VAPT report

Mini SOC Deployment

- Configure SIEM
- Investigate incidents

Cloud Security Assessment

- Secure IAM
- Assess cloud risks

Active Directory Lab

- Configure enterprise environment
- Implement policies

Final Assessment Structure :

Assessment Type	Weightage
Theory Exams	20%
Practical Labs	40%
Projects	25%
Reporting & Documentation	10%
Viva & Interviews	5%

Final Program Outcome

After completing CCWP Foundation, students will graduate with:

- Practical Cyber Security Skills
- Real-World Lab Experience
- Portfolio Projects
- Professional Reporting Abilities
- Interview Preparation
- Enterprise Technology Exposure
- Industry-Oriented Skillsets

The program is designed to create:

- Ethical Cyber Security Professionals
- Industry-Ready Analysts
- Practical Security Learners
- Certified Cyber Warriors
- Globally Employable Cyber Security Talent.

Program Highlights

- Practical-First Training
- SOC + VAPT + Cloud Learning
- Real-World Case Studies
- Portfolio-Based Learning
- Enterprise Security Workflows
- Modern Cloud & Container Awareness
- Professional Reporting
- Interview Preparation

CCWP Foundation is an enterprise-oriented, practical, globally aligned cybersecurity foundation program designed to prepare students for modern cybersecurity careers through hands-on labs, real-world investigations, cloud security awareness, SOC operations training, security case studies, and professional development.

The program combines:

- Cybersecurity Fundamentals
- Enterprise Technologies
- Cloud Infrastructure Awareness
- Security Operations
- Networking
- Windows System / Linux Administration
- Modern Web Security
- Python Automation
- Professional Reporting
- Real-World Case Study Analysis

to create skilled, ethical, and job-ready cybersecurity professionals.