
SYNNEFO
SOLUTIONS
ADVANCED
CYBER
SECURITY
PROFESSIONAL
[ A C S P ]

# THE ADVANTAGE

**CYBER SECURITY • ETHICAL HACKING**
**VAPT • SOC SKILLS**

Synnefo Solutions is an IT company–based academy offering industry-driven training with real-world labs and mentorship.

- 100% Job Guaranteed
- Synnefo SmartSpace: Kerala's First LaaS
- Intensive Internship
- Realtime projects

## Class mode details

Course duration:
**10 months**

Includes a 4 month internship program

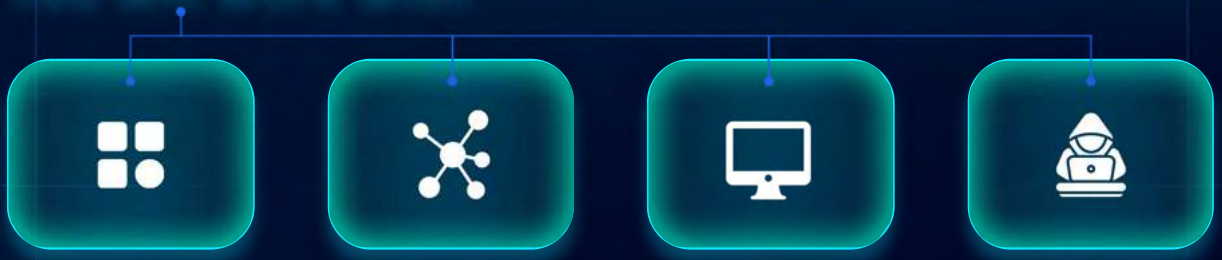
- ONLINE
- OFFLINE
- HYBRID

# ABOUT THE COURSE

## Course Overview

Cyber Security & Ethical Hacking (VAPT) helps you think like an attacker and defend like a professional through practical, real-world training.

## You will work with




## What You Will Learn

Using tools like Kali Linux, Burp Suite, Nmap & Metasploit, you'll practice scanning, exploitation, privilege escalation, and VAPT reporting — just like real industry teams

## Suitable for:

Beginners • Students • Developers
IT Support • Network Admins
Security Enthusiasts

# FEATURES MODULE OVERVIEW

## Training Features

- Real-time projects
- Hands-on lab access
- Doubt-clearing sessions
- Recorded classes (Online/Hybrid)
- Industry experienced trainers

## Key Modules

- Cybersecurity Foundations
- Ethical Hacking Principles
- Vulnerability Assessment & VAPT
- Penetration Testing Practices
- Linux & Security Lab Setup
- Cryptography & Secure Systems
- Web Application Security & Exploitation
- Wireless, Cloud & IoT Security
- Network & Directory Services Security
- Android & Mobile Security
- SOC & Incident Response
- Security Tools & Professional Reporting
- Career & Industry Readiness

# CAREERS

## Career Opportunities

- VAPT Analyst
- Junior Penetration Tester
- Security Analyst
- SOC Analyst (L1/L2)
- Cybersecurity Intern
- Web App Security Tester
- Network Security Engineer
- Application Security Engineer
- Cyber Defense Analyst
- Penetration Tester
- Freelance Ethical Hacker

## Certifications

- Course Completion Certificate
- NACTET Certificate
- Internship Certificate

# ABOUT US

Synnefo is an ISO 9001:2015 certified, IT company–based academy offering 100% job-guaranteed programs, supported by 50+ recruitment partners and NACTET affiliation. With 5000+ students trained, we deliver industry-driven learning through live projects and internships.

Students gain hands-on exposure in real-time lab facilities with integrated NOC, SOC, and Data Center environments, along with an exclusive SDLC Hub. Our programs are further strengthened by soft-skill training, mock interviews, international testing centers, and lifetime placement support, ensuring complete career readiness.

ENQUIRE NOW

Start your cybersecurity journey with guaranteed job support.


+91 7736013411

Near Maharajas
Metro Station, Ernakulam

www.synnefo.in


SYNNEFO SOLUTIONS

# ADVANCED CYBER SECURITY PROFESSIONAL

## COURSE MODULES

# CYBER SECURITY FOUNDATIONS

## Introduction to CyberSecurity

- Evolution of cybersecurity field
- The Confidentiality, Integrity, and Availability (CIA) Triad
- Security standards and frameworks
- Why cybersecurity continues to grow

## Introduction to Hacking

- Hacking is an art of exploitation
- The five phases of effective hacking
- Types of hackers based on their intent
- How businesses protect their operations from attacks
- Bright side of hacking
- Offensive Security and Defensive Security
- Role of an ethical hacker
- Route to be an effective white hat

## Introduction to Vulnerability

- Loopholes everywhere
- Root cause of a weakness
- Severity levels for security issues
- Vulnerability exploitation and remediation process

## Introduction to VAPT

- Systematic review of security weaknesses
- Simulated cyber attack against the system
- Pros and cons of VAPT
- Internal and external pentesting

# PENETRATION TESTING BASICS

## Introduction to Pentesting

- Importance of Non-Disclosure Agreement
- Scope determination
- Reconnaissance phase
- Vulnerability Assessment and Penetration Testing
- Reporting
- Remediation
- Retest

## Introduction to Virtual Machines

- Advantages of a virtual machine
- Installation and con guration
- Linux designed for hackers
- Troubleshooting VM

## Introduction to Cryptography

- Birth of secure communication
- Encryption & Decryption vs Encoding & Decoding
- Symmetric and Asymmetric encryption
- Cryptography-based vulnerabilities

## Introduction to Steganography

- Deep dive into steganography
- Common ways to hide messages
- Metadata and related attacks
- Extracting information from files

## Types of Pentesting

- Web Application
- Network / Infrastructure
- Mobile Application
- API
- Client Application
- Wireless
- Cloud
- IoT
- AI / ML

# ADDITIONAL INTRODUCTORY MODULES

## Introduction to Wireless Pentesting

- What is wireless security
- Common wireless technologies (Wi-Fi, Bluetooth, NFC)
- Wireless attack surface
- Why wireless networks are targeted
- Importance of secure wireless configuration

## Introduction to Cloud Pentesting

- What is cloud computing
- Shared Responsibility Model
- Why cloud environments are targeted
- Common cloud security mistakes
- Traditional vs cloud pentesting

## Introduction to IoT Pentesting

- What is IoT and connected devices
- IoT architecture and components
- Why IoT devices are vulnerable
- Common IoT security weaknesses
- Risks of insecure IoT deployments

# WEB APPLICATION PENTESTING BASICS

## Web Pentesting & Methodology

- Web application architecture
- Pentesting methodologies
- Web application architecture
- Pentesting methodologies

## OWASP

- Open Worldwide Application Security Project
- OWASP as preferred methodology
- OWASP Top 10

## Introduction to API

- API overview
- API calls
- API documentation
- Common API vulnerabilities

## Setting Up Testing Environment

- Pentesting browsers
- Browser extensions
- Proxy servers
- Proxy setup and configuration

## Introduction to Burp Suite

- Proxy fundamentals
- Installation
- CA certificate setup
- Burp Suite deep dive

## Subdomain Enumeration

- Importance of subdomains
- Assetfinder
- Subdomain brute forcing
- Bash automation

## Information Gathering

- OSINT
- Fuzzing
- Search engine hacking
- Wayback URLs
- Social media leakage

## Request and Response

- HTTP status codes
- Request methods
- Headers
- Header-based vulnerabilities

# WEB APPLICATION PENTESTING PRACTICAL

## Online Platforms

- PortSwigger Labs
- TryHackMe
- Hack The Box
- Miscellaneous platforms

## Injection Vulnerabilities

- Injection concepts
- Parameter testing
- Exploitation workflow
- Mitigations

## Authentication & Authorization

- Authentication vs Authorization
- Authentication vulnerabilities
- Bypass techniques
- Mitigations

## Access Control Vulnerabilities

- Access control levels
- IDOR
- Bypass techniques
- Mitigations

## Session Management

- Cookies vs Tokens
- Session vulnerabilities
- Mitigations

## Enumeration & Rate Limiting

- Enumeration techniques
- Rate limiting issues
- Bruteforce attacks
- Bypass techniques

## Sensitive Data Exposure

- Information leakage
- Cryptographic issues
- Directory listing
- Mitigations

## Credential Vulnerabilities

- Default credentials
- Weak credentials
- Credential reuse
- Mitigations

## Reset Password Vulnerabilities

- Account takeover
- Token leakage
- Guessable tokens
- Mitigations

## Business Logic Vulnerabilities

- Logic aws
- Identi cation
- Exploitation
- Mitigations

## Vulnerable Components

- CVE & CWE
- GitHub & ExploitDB
- Outdated components
- Mitigations

## Account Takeover

- ATO techniques
- Protection bypass
- Request manipulation
- Mitigations

## Subdomain Takeover

- DNS basics
- Vulnerable services
- Exploitation
- Mitigations

## Common Web Application Vulnerabilities

- Open Redirection
- TLS/SSL issues
- SPF spoofing
- Directory Traversal
- LFI / RFI
- Clickjacking
- CSRF
- SSRF
- CORS miscon guration
- DoS
- File upload
- GraphQL vulnerabilities
- OAuth miscon guration
- Race conditions
- AI/ML issues
- Prototype Pollution
- Dependency Confusion
- Miscellaneous

## Tools & Scanners

- Automated scanners
- Common pentesting tools
- Script automation

## Web Conclusion

- Bug bounty introduction
- Pentest report writing
- Bug hunter vs pentester
- Web challenge

# NETWORK PENTESTING

## Introduction to Network Pentesting

- Network fundamentals
- Network types
- Pre-engagement considerations

## Network Scope

- Scope identification
- Static vs Dynamic IP
- IP scanning automation

## Scanning Using Nmap

- Nmap basics
- Advanced scanning
- NSE scripts
- Automation

## Nessus

- Installation
- Essentials vs Professional
- Pros and cons

## Common Network Vulnerabilities

- Credential issues
- Miscon gurations
- Outdated services
- Cryptography issues

## Metasploit Framework

- msfconsole
- Exploit modules
- Auxiliary modules
- Limitations

## Privilege Escalation

- Linux PrivEsc
- Windows PrivEsc

## Post Exploitation

- Red Teaming
- Linux POS
- Windows POS

## Network Conclusion

- Network pentest report
- Mitigations
- CTF

# SOC (SECURITY OPERATIONS CENTER)

## Security Operations & Analyst Roles

- SOC essentials
- SOC roles & responsibilities
- Defensive technologies
- Monitoring & detection
- Ticketing lifecycle
- Alert handling
- Practical ticket challenge

## Cybersecurity Foundations

- Cybersecurity risk & defensive strategy
- Cyber risk in organizations
- Framework-based security approaches

## Log & Event Management

- Log fundamentals
- Log formats
- Fields & separators
- Windows event logs
- Log analysis exercises

## SIEM – Wazuh

- SIEM fundamentals
- Wazuh architecture
- Detection work ow
- Search queries
- Dashboards
- Alert response labs

## Network Security Monitoring

- Network detection
- Indicators of compromise
- Web log analysis
- Tra c analysis challenges

## Host-Based Detection & EDR

- Host monitoring
- Endpoint detection
- EDR concepts
- Detection labs

## Threat Techniques & Attack Vectors

- Windows execution
- Persistence
- Spear-phishing (link & attachment)
- Detection challenges

## Windows Authentication

- Local authentication
- Domain authentication
- Credential flow
- Authentication challenges

# ANDROID PENTESTING

## Introduction to Android Pentesting

- Birth of Android
- Pros and cons of Android
- Scope determination
- Dalvik Executable (DEX)
- Smali code
- AndroidManifest.xml
- Activities
- Application signatures

## OWASP Top 10 Mobile

- Introduction to OWASP Mobile
- Common mobile vulnerabilities
- Categorizing mobile vulnerabilities

## Introduction to Static Analysis

- Deep dive into static analysis
- Decompiling using apktool
- jadx-gui
- Visual Studio Code for review

## Introduction to MobSF

- MobSF installation and con guration
- Automation using MobSF
- Pros and cons of MobSF
- Static analysis using MobSF

## Lab Setup

- Genymotion installation and con guration
- Android Studio installation and con guration
- Setting up proxy inside mobile device
- Automation using pen-andro

## Android Debug Bridge (ADB)

- Introduction to ADB
- Con guring Android devices using ADB
- Common ADB commands and usage
- Attacks using ADB

## Rooting

- User hierarchy in Android
- Rooting emulators
- Rooting physical devices
- Pros and cons of rooting

## Frameworks and Modules (Part 1)

- Deep dive into frameworks
- Installation and con guration of Magisk
- Installation and con guration of Xposed Framework
- Bypassing protection mechanisms using frameworks

## Frameworks and Modules (Part 2)

- Deep dive into frameworks
- Installation and con guration of Magisk
- Installation and con guration of LSPosed Framework
- Frida installation and con guration

## SSL Pinning

- Importance of SSL pinning
- Different SSL pinning techniques
- Ways to bypass SSL pinning
- Mitigations

## Common Android Vulnerabilities

- Algorithm-based vulnerabilities
- Root detection
- Emulator detection
- Hardcoded sensitive information
- Server communication issues
- Improper storage of sensitive data
- Web application issues on mobile
- Session management aws
- Third-party SDK risks
- Miscellaneous vulnerabilities

## Reverse Engineering

- Deep dive into reverse engineering
- Decompiling Android applications
- Identifying loopholes in source code
- Modifying source code
- Recompiling applications
- Generating signatures
- Signing APKs using apktool
- Troubleshooting common issues

# ACTIVE DIRECTORY

## Active Directory

- Cybersecurity career paths
- Resume & CV building
- Interview preparation
- Mock interviews

# OFFENSIVE SECURITY OVERALL CONCLUSION

## Career Guidance

- Cybersecurity career paths
- Resume & CV building
- Interview preparation
- Mock interviews