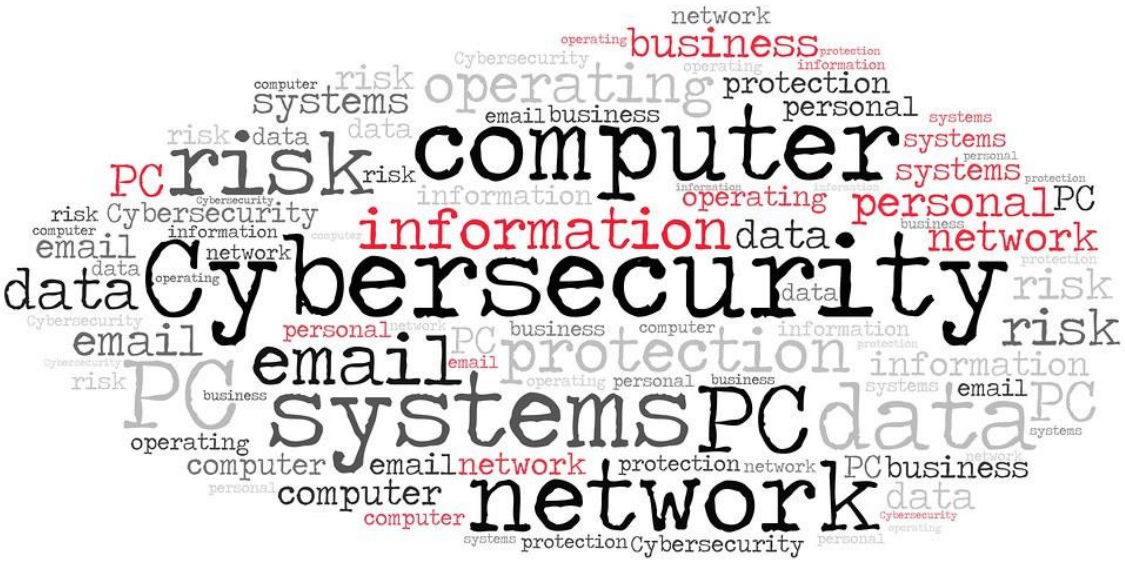
CyberSPAIS
Security Privacy & Assurance of Information Systems

CyberSPAIS Certified Penetration Tester (CCPT)



CyberSPAIS Certified Penetration Tester (CCPT) – Overview

- Who Is Eligible for This Course?
  - Working professionals looking to specialise in
    - Vulnerability Assessment
    - Penetration Testing
    - Red & Blue Teaming
    - Bug Bounty Hunting

- Course Duration
  - 2 Months (80 Hours)

- Potential Job Roles Relevant to The Course
  - Security Analyst, Security Engineer, Vulnerability Analyst, Penetration Tester, Red & Blue Teaming, Bug Bounty Hunter, Security Consultant.

- Course Syllabus
  - Cybersecurity Fundamentals
  - Kali Linux & Penetration Testing
  - Introduction to Anonymity
  - Planning a Penetration Test
  - Reconnaissance & Information Gathering
  - Open-Source Intelligence (OSINT)
  - Scanning & Enumeration
  - Scripting for Penetration Testing
  - Analysing Scan Results
  - Vulnerability Mapping
  - Exploitation & Gaining Access
  - Social Engineering PenTest
  - Wireless PenTest
  - Network PenTest
  - Identity & Access Management (IAM) PenTest
  - System PenTest
  - Active Directory Exploitation
  - Web Application PenTest
  - Cloud PenTest
  - Mobile, IoT & OT PenTest
  - Automating PenTest
  - Persistence
  - Lateral Movement
  - Exfiltration
  - Cleanup & Restoration
  - Penetration Test Reporting
  - Remediation

- Potential Certifications Relevant to The Course
  - CEH, CPENT, CompTIA Pentest+, OSCP

- Why Training @CyberSPAIS?
  - Job Oriented Industry Relevant Curriculum
  - Based On Latest Cyber Security Topics & Trends
  - 100% Assistance for Placements & Internships
  - Industry Experienced & Certified Trainer
  - Concepts Explained with Industry Scenarios
  - Comprehensive Hands-on Sessions & Labs
  - Regular Module Wise Assessments & Evaluations
  - Cybersecurity Projects & Internships
  - Thorough Preparation – Job Interview & Soft Skills
  - Certification Exams

CyberSPAIS Certified Penetration Tester (CCPT) – Syllabus

- Module1: Cybersecurity Fundamentals
  - Importance of Security
  - Security Job Opportunities
  - Information & Cyber Security
  - Terms & Definitions
  - Confidentiality
  - Integrity
  - Availability
  - AAA
  - Identification
  - Authentication
  - Authorization
  - Accounting
  - Non-Repudiation
  - Information Assets
  - Threats
  - Vulnerabilities
  - Attacks
  - Intrusion & Breach
  - Defense In Depth
  - Discuss Data Breach Reports
  - Attacks & Impacts of Cyber Attacks
  - Major Categories of Computer Crime
  - Social Engineering
  - Security Laws & Regulations
  - Security Standards (ISO 27001, PCI DSS Etc.)

- Module 2: Kali Linux & Penetration Testing
  - Introduction to Linux
  - Linux File Hierarchy
  - Linux Shell
  - Basic Linux Commands
  - About Kali Linux
  - Creating a Virtual Lab
  - Installing Kali Linux
  - Installing Metasploitable
  - Configuring Kali Linux
  - Package Management

- Module 3: Introduction to Anonymity
  - Anonymity
  - TOR Browser
  - Nmap Proxy Chains
  - Installing VPN in Kali Linux
  - WhoAMI Anonymity Tool

- Module 4: Planning a Penetration Test
  - Penetration Testing Overview
  - Pre-Engagement Activities
  - Regulations & Standards
  - Types of Penetration Testing
  - Types of Agreements
  - Legal & Ethical Considerations
  - Rules of Engagement
  - Defining Scope
  - Shared Responsibility Model
  - Preparing for Cloud PenTest
  - Penetration Testing Frameworks

- Module 5: Reconnaissance & Information Gathering
  - Passive Reconnaissance
  - Network Sniffing
  - Active Reconnaissance
  - Port & Protocol Scanning
  - HTML Scraping
  - Banner Grabbing
  - Discuss Tools

- Module 6: Open-Source Intelligence (OSINT)
  - Social Media & Job Boards
  - Information Disclosure
  - Cryptographic Flaws

- DNS Lookups
- Certificate Transparency Logs
- Search Engine Analysis (Google Dorking)
- Cryptographic Flaws
- Discuss OSINT Tools

- Module 7: Scanning & Enumeration
  - OS & Service Discovery
  - Enumerating Protocols
  - Enumerating DNS
  - Enumerating Directories
  - Enumerating Hosts
  - Enumerating Users
  - Enumerating Email
  - Enumerating Permissions
  - Enumerating Wireless
  - Enumerating Web
  - Attack Mapping
  - Nmap & Nmap Scripting Engine (NSE)

- Module 8: Scripting for Penetration Testing
  - Scripting Basics
  - Bash Fundamentals
  - Bash Scripting
  - PowerShell Fundamentals
  - PowerShell Scripting
  - Python Fundamentals
  - Python Scripting

- Module 9: Analysing Scan Results
  - Analysing Scan Results
  - False Positive & False Negative
  - Validating Scan Results
  - Using CVE & CVSS
  - Exploit Prediction Scoring System
  - Target Prioritization
  - Common Target Criteria
  - Scripting for Validation
  - Capability Selection

- Module 10: Vulnerability Mapping
  - Application Scanning
  - Software Analysis
  - Host Scanning
  - Network Scanning

- Mobile Scanning
- Container Scanning
- Cloud Scanning
- ICS Scanning
- Wireless Scanning
- Static Code Analysis
- Discuss Tools

- Module 11: Exploitation & Gaining Access
  - What is Exploitation?
  - Reverse Shells & Bind Shells
  - Metasploit Framework
  - Msfconsole Commands
  - Creating Payloads using Msfvenom
  - Creating Payloads using Veil
  - FatRat Payload Creation
  - Hexeditor & Antiviruses

- Module 12: Social Engineering PenTest
  - Methods of Influence
  - Phishing Campaigns
  - Social Engineering Toolkit (SET)
  - Gophish
  - Impersonation
  - Surveillance
  - Water Hole
  - Evilginx
  - Tailgating & Piggybacking
  - Browser Exploitation Framework (BeEF)
  - Discuss Tools

- Module 13: Wireless PenTest
  - Wireless Attacks & Security
  - Wireless Signal Exploitation
  - Aircrack-ng
  - Wireless Hacking
  - WPS PIN Attacks
  - Captive Portal Attacks
  - Evil Twin
  - Kismet
  - Wi-Fi Fuzzing

- Module 14: Network PenTest
  - Network Attacks
  - Stress Testing

- Bypassing Segmentation
- MAC Spoofing
- NAC Bypass
- Session-Based Attacks
- Service Exploitation
- Packet Crafting
- Netcat
- Default Credentials
- LLMNR/NBT-NS Poisoning
- ARP Poisoning
- Metasploit
- Discuss Tools

- Module 15: Identity & Access Management (IAM) PenTest
  - Authentication Attacks
  - Password Attacks
  - Password Cracking Tools
  - Credential Attacks
  - Credential Passing Attacks
  - Directory Service Attacks
  - CrackMapExec (CME)
  - SAML Attacks
  - OpenID Connect Attacks
  - Hash Attacks
  - Discuss Tools

- Module 16: System PenTest
  - Host Attacks
  - Privilege Escalation
  - Credential Harvesting
  - Misconfiguration Exploitation
  - Unquoted Service Paths
  - Disabling Security Software
  - Payload Obfuscation
  - User Controlled Access Bypass
  - Shell & Kiosk Escapes
  - Library & Process Injection
  - Log Tampering
  - Discuss Tools

- Module 17: Active Directory Exploitation
  - Enumerating Active Directory
  - Exploiting Active Directory
  - Post Exploitation
  - Escalating Privileges

- Module 18: Web Application PenTest
  - Web Application Vulnerabilities
  - Race Conditions
  - Buffer Overflow
  - Authentication Flaws
  - Insecure References
  - Improper Error Handling
  - Improper Header
  - Code Signing
  - Vulnerable Components
  - Software Composition
  - Directory Traversal
  - Cross-Site Scripting
  - Request Forgeries
  - Injection Attacks
  - File Inclusions
  - Code Execution
  - Session Hijacking
  - Abusing API
  - Discuss Tools
- Module 19: Cloud PenTest
  - Cloud Attacks
  - IAM Misconfigurations
  - Logging Information Exposure
  - Resource Misconfiguration
  - Metadata Service Attacks
  - Image & Artifact tampering
  - Supply Chain Attack
  - Container Exploits
  - Trust Relationship Abuse
  - Third Party Integration Exploits
  - Cloud Security Testing
  - Cloud Audits
  - Discuss Tools
- Module 20: Mobile, IoT & OT PenTest
  - Mobile Attacks
  - Bluetooth Attacks
  - NFC & RFID Attacks
  - AI Attacks
  - OT System & Attacks
  - Testing OT Systems
  - Discuss Tools

- Module 21: Automating PenTest
  - Automated Attacks
  - Attacks with Bash
  - Empire/PowerSploit
  - PowerView
  - PowerUpSQL
  - AD Search
  - Impacket
  - Scapy
  - Caldera
  - Infection Monkey
  - Atomic RedTeam

- Module 22: Persistence
  - Persistence
  - Command & Control
  - Automating Persistence
  - Remote Shells
  - Backdoor
  - Remote Access Trojans
  - Account Credentials
  - Browser Based Persistence
  - Security Control Tampering
  - Discuss Tools

- Module 23: Lateral Movement
  - Pivoting & Relaying
  - Using Proxy Chains
  - Enumeration
  - Service Discovery
  - Protocol Discovery
  - Remote Access Discovery
  - Printer Discovery
  - Discovering Internal Website
  - Discuss Tools

- Module 24: Exfiltration
  - Covert Channels
  - Steganography
  - DNS Tunnelling
  - ICMP Tunnelling
  - HTTPS Tunnelling
  - Alternate Data Streams
  - Exfiltrating Data

- Module 25: Cleanup & Restoration
  - Persistence Removal
  - Revert Configuration Changes
  - Credentials Removal
  - Removing Testing Tools
  - Decommission Testing Infrastructure
  - Artifact Preservation
  - Secure Data Destruction

- Module 26: Penetration Test Reporting
  - Executive Summary Process
  - Root Cause Analysis
  - Report Components
  - Risk Scoring
  - Definitions In Report
  - Limits & Assumptions
  - Special Considerations
  - Report Analysis

- Module 27: Remediation
  - System Hardening
  - Input Sanitization
  - Network Controls
  - Authentication Recommendations
  - Encryption Recommendations
  - Patch Management
  - Process Level Remediation
  - Administrative Controls
  - Physical Controls
  - Operational Controls
  - Implementing Recommendations

- Tools Covered
  - Wayback Machine, theHarvester, Hunter.io, OSINT Tools, WHOIS, Recon-ng, nslookup, dig, DNSdumpster, Amass, Shodan, Censys.io, tcpdump, Wireshark, Aircrack-ng, Nmap, Nikto, OpenVAS, Trivy, BloodHound, PowerSploit, Grype, Kube-Hunter, TruffleHog, SET Toolkit, Gophish, Evilginx, Kismet, Netcat, Metasploit, OWASP ZAP, Empire, PowerView, PowerUpSQL, Impacket, Scapy, Caldera, sshuttle, Covenant

- Assessments
- Student Project
- Final Exam
- Interview Preparation

- Issue Course Certificate
- Placement Evaluation & Assistance
