Ethical_Hacking - Hackveda (Talk to Live Mentor)

Become a Certfied Information System Security Expert - (Beginner - Expert)

Skill level: Beginner - Expert

Training fee: INR 56999 only (Topics covered: 684)

Chief Trainer: Mr. Devanshu Shukla

Training Duration: 114 days (3 hrs per day) | 171 days (2 hrs per day) | 342 days (1 hr per day)

Presentation or Examination will be conducted within 114 days from date of training completion.

* Please note examination will be conducted after completion of training.

Maximum examination attempts: 03

Minimum passing marks for certification and placement: 90%

Query Membership: 01 year (Online / Offline)

Spoken Language: English / Hindi

Venue: Hackveda, H-3/60, III Floor, Sector-18, Rohini, Delhi-110089

Contact person: Mr. Yash Sharma, Software Engineer, Hackveda

Contact phone: 011-27297608, +91-9654825370, +91-9891799066

Registration link: Register Now

Hackveda One2One Support Available:
Training session video will be recorded and delivered to students via our Digital Learning platform Hackveda One2One for any time, any where learning and practice.

Join the training at Hackveda 'TODAY' !

Course contents

Cybersecurity Analyst+: The OSI Model

Cybersecurity Analyst+: Network Hardware

Cybersecurity Analyst+: IPv4

Cybersecurity Analyst+: IPv6

Cybersecurity Analyst+: TCP and UDP

Cybersecurity Analyst+: Use Common Windows TCP/IP Utilities

Cybersecurity Analyst+: Use Common Linux TCP/IP Utilities

Cybersecurity Analyst+: Configure and Scan for Open Ports

Cybersecurity Analyst+: Network Services

Cybersecurity Analyst+: Wired and Wireless Networks

Cybersecurity Analyst+: Use Common Wireless Tools

Cybersecurity Analyst+: Internal and External Networks

Cybersecurity Analyst+: Cloud Concepts

Cybersecurity Analyst+: Cloud Service Models

Cybersecurity Analyst+: Virtualization

Cybersecurity Analyst+: Cloud Security Options

Cybersecurity Analyst+: Topology, Service Discovery, and OS Fingerprinting

Cybersecurity Analyst+: Reviewing Logs

Cybersecurity Analyst+: Packet Capturing

Cybersecurity Analyst+: Capture FTP and HTTP Traffic

Cybersecurity Analyst+: Network Infrastructure Discovery

Cybersecurity Analyst+: Email and DNS Harvesting

Cybersecurity Analyst+: Social Engineering and Phishing

Cybersecurity Analyst+: Acceptable Use Policy

Cybersecurity Analyst+: Data Ownership and Retention Policy

Cybersecurity Analyst+: Data Classification Policy

Cybersecurity Analyst+: Password Policy

Cybersecurity Analyst+: Network Architecture and Reconnaissanse

Cybersecurity Analyst+: Threat Overview

Cybersecurity Analyst+: Threat Classification

Cybersecurity Analyst+: Personally Identifiable Information

Cybersecurity Analyst+: Payment Card Information

Cybersecurity Analyst+: Intellectual Property

Cybersecurity Analyst+: Data Loss Prevention

Cybersecurity Analyst+: Prevent Data Storage on Unencrypted Media

Cybersecurity Analyst+: Scope of Impact

Cybersecurity Analyst+: Stakeholders

Cybersecurity Analyst+: Role-based Responsibilities

Cybersecurity Analyst+: Incident Communication

Cybersecurity Analyst+: Host Symptoms and Response Actions

Cybersecurity Analyst+: Network Symptoms and Response Actions

Cybersecurity Analyst+: Application Symptoms and Response Actions

Cybersecurity Analyst+: Incident Containment

Cybersecurity Analyst+: Incident Eradication

Cybersecurity Analyst+: Lessons Learned

Cybersecurity Analyst+: OEM Documentation

Cybersecurity Analyst+: Network Documentation

Cybersecurity Analyst+: Incident Response Plan / Call List

Cybersecurity Analyst+: Incident Documentation

Cybersecurity Analyst+: Chain of Custody Form

Cybersecurity Analyst+: Change Control Processes

Cybersecurity Analyst+: Types of Reports

Cybersecurity Analyst+: Service Level Agreement

Cybersecurity Analyst+: Memorandum of Understanding

Cybersecurity Analyst+: Asset Inventory

Cybersecurity Analyst+: Identify and Respond to Threats

Cybersecurity Analyst+: SDLC Phases

Cybersecurity Analyst+: Secure Coding

Cybersecurity Analyst+: Security Testing

Cybersecurity Analyst+: Host Hardening

Cybersecurity Analyst+: Patching Overview

Cybersecurity Analyst+: Use SCCM to Deploy Patches

Cybersecurity Analyst+: File System Permissions

Cybersecurity Analyst+: Network Access Control

Cybersecurity Analyst+: VLANs

Cybersecurity Analyst+: Determining Resource Access

Cybersecurity Analyst+: Honeypots

Cybersecurity Analyst+: Jump Box

Cybersecurity Analyst+: IT Security Governance

Cybersecurity Analyst+: Regulatory Compliance

Cybersecurity Analyst+: NIST

Cybersecurity Analyst+: ISO

Cybersecurity Analyst+: TOGAF

Cybersecurity Analyst+: SABSA

Cybersecurity Analyst+: ITIL

Cybersecurity Analyst+: Physical Controls

Cybersecurity Analyst+: Logical Controls

Cybersecurity Analyst+: Configure Router ACL Rules

Cybersecurity Analyst+: Administrative Controls

Cybersecurity Analyst+: Compensating Controls

Cybersecurity Analyst+: Continuous Monitoring of Controls

Cybersecurity Analyst+: Hardware Trust

Cybersecurity Analyst+: Penetration Testing

Cybersecurity Analyst+: Mitigations and Security Control types

Cybersecurity Analyst+: Cryptography Primer

Cybersecurity Analyst+: Symmetric Cryptography

Cybersecurity Analyst+: Asymmetric Cryptography

Cybersecurity Analyst+: Public Key Infrastructure

Cybersecurity Analyst+: Request a PKI Certificate from a Windows CA

Cybersecurity Analyst+: Use Windows EFS File Encryption

Cybersecurity Analyst+: Fingerprinting, Hashing

Cybersecurity Analyst+: File Hashing in Linux

Cybersecurity Analyst+: File Hashing in Windows

Cybersecurity Analyst+: Authentication

Cybersecurity Analyst+: Configure Multifactor Authentication for VPN Clients

Cybersecurity Analyst+: Authorization

Cybersecurity Analyst+: RADIUS, TACACS+

Cybersecurity Analyst+: User Provisioning and Deprovisioning

Cybersecurity Analyst+: Identity Federation

Cybersecurity Analyst+: Server Vulnerabilities

Cybersecurity Analyst+: Endpoint Vulnerabilities

Cybersecurity Analyst+: Network Vulnerabilities

Cybersecurity Analyst+: Mobile Device Vulnerabilities

Cybersecurity Analyst+: Vulnerability Scanning Overview

Cybersecurity Analyst+: Vulnerability Scanning Settings

Cybersecurity Analyst+: SCAP

Cybersecurity Analyst+: Scan for Vulnerabilities using Nessus

Cybersecurity Analyst+: Common Vulnerability Scanning Tools

Cybersecurity Analyst+: Scan for Vulnerabilities using Microsoft Baseline Security Analyzer

Cybersecurity Analyst+: Review Vulnerability Scan Results

Cybersecurity Analyst+: Vulnerability Remediation

Cybersecurity Analyst+: Describe ways of reducing vulnerabilities

Cybersecurity Analyst+: Firewalling Overview

Cybersecurity Analyst+: Firewall Rules

Cybersecurity Analyst+: Packet Filtering Firewalls

Cybersecurity Analyst+: Configure a Packet Filtering Firewall

Cybersecurity Analyst+: Proxy Servers

Cybersecurity Analyst+: Security Appliances

Cybersecurity Analyst+: Web Application Firewall

Cybersecurity Analyst+: Intrusion Detection and Prevention Overview

Cybersecurity Analyst+: Host Intrusion Detection Systems

Cybersecurity Analyst+: Network Intrusion Detection Systems

Cybersecurity Analyst+: Network Intrusion Prevention Systems

Cybersecurity Analyst+: Malware Overview

Cybersecurity Analyst+: Viruses

Cybersecurity Analyst+: Worms

Cybersecurity Analyst+: Spyware, Adware

Cybersecurity Analyst+: Ransomware

Cybersecurity Analyst+: Anti-malware

Cybersecurity Analyst+: User Training and Awareness

Cybersecurity Analyst+: Digital Forensics Overview

Cybersecurity Analyst+: Digital Forensics Hardware

Cybersecurity Analyst+: Digital Forensics Software

Cybersecurity Analyst+: Digital Forensics and Data at Rest

Cybersecurity Analyst+: Common Digital Forensic Tools

Cybersecurity Analyst+: Mobile Device Forensics

Cybersecurity Analyst+: Create a physical memory dump

Cybersecurity Analyst+: View deleted files on a hard disk

Cybersecurity Analyst+: Prevent and investigate security problems

Cybersecurity Analyst+: Hiring and Background Checks

Cybersecurity Analyst+: User On-Boarding and Off-Boarding

Cybersecurity Analyst+: Personnel Management Best Practices

Cybersecurity Analyst+: Threats, Vulnerabilities, and Exploits

Cybersecurity Analyst+: Spoofing

Cybersecurity Analyst+: Packet Forgery using Kali Linux

Cybersecurity Analyst+: Impersonation

Cybersecurity Analyst+: Cross-site Scripting

Cybersecurity Analyst+: Root Kits

Cybersecurity Analyst+: Privilege Escalation

Cybersecurity Analyst+: Common Exploit Tools

Cybersecurity Analyst+: Exploring the Metasploit Suite of Tools

Cybersecurity Analyst+: Exploring the Kali Linux Suite of Tools

Cybersecurity Analyst+: Password Cracking

Cybersecurity Analyst+: Reasons for Monitoring

Cybersecurity Analyst+: Common Monitoring Tools

Cybersecurity Analyst+: Linux OS Monitoring Tools

Cybersecurity Analyst+: Windows OS Monitoring Tools

Cybersecurity Analyst+: Windows Event Log Forwarding

Cybersecurity Analyst+: SIEM

Cybersecurity Analyst+: SCADA and ICS

Cybersecurity Analyst+: Monitoring Network Bandwidth

Cybersecurity Analyst+: Point-in-time Data Analysis

Cybersecurity Analyst+: Data Correlation and Analytics

Cybersecurity Analyst+: Detailed Log Analysis

Cybersecurity Analyst+: Understand exploits and monitoring

Securing User Accounts: Importance of User Account Security

Securing User Accounts: Authenticity

Securing User Accounts: Integrity

Securing User Accounts: Confidentiality

Securing User Accounts: Security Attack Motives

Securing User Accounts: Security Attack Phases

Securing User Accounts: Username Enumeration

Securing User Accounts: CSRF

Securing User Accounts: Web Server Password Cracking

Securing User Accounts: Vulnerability Scanning

Securing User Accounts: Patches and Updates

Securing User Accounts: Network Protocols

Securing User Accounts: Account Protocols

Securing User Accounts: Event Logging

Securing User Accounts: Defense in Depth

Securing User Accounts: Privilege Management

Securing User Accounts: Permissions Categories

Securing User Accounts: Naming Conventions

Securing User Accounts: Limiting Logon Attempts

Securing User Accounts: Setting Account Expiry Dates

Securing User Accounts: Disabling Unused Accounts

Securing User Accounts: Setting Time Restrictions

Securing User Accounts: Setting Machine Restrictions

Securing User Accounts: Determining Appropriate User Account Policies

Securing User Accounts: Authentication and Identification

Securing User Accounts: User Authentication Components

Securing User Accounts: Authentication Types

Securing User Accounts: Authorization

Securing User Accounts: User Logon Process

Securing User Accounts: Authentication Credentials Overview

Securing User Accounts: Password Credentials

Securing User Accounts: Asymmetric Key Credentials

Securing User Accounts: Biometric Credentials

Securing User Accounts: Ticket-based Hybrid Authentication

Securing User Accounts: Registration Basics

Securing User Accounts: Username Best Practices

Securing User Accounts: Account Verification

Securing User Accounts: Using CAPTCHA

Securing User Accounts: Enabling Two-Step Verification

Securing User Accounts: Preventing Username Enumeration

Securing User Accounts: Password Strength Criteria

Securing User Accounts: Password Complexity Requirements

Securing User Accounts: Password Field Security

Securing User Accounts: Password Strength Feedback

Securing User Accounts: Enforcing Password History Policies

Securing User Accounts: Password Age Policies

Securing User Accounts: Protecting against Password Hacking

Securing User Accounts: Securing User Account Registration

Securing User Accounts: Overview of the Logon Feature

Securing User Accounts: Development Best Practices

Securing User Accounts: Using SSL for Logon Security

Securing User Accounts: Managing Simultaneous Sessions

Securing User Accounts: Common Logon Attacks

Securing User Accounts: Logon Fraud Detection and Prevention

Securing User Accounts: Overview of the Logoff Feature

Securing User Accounts: Session Expiry

Securing User Accounts: Remote Logoff

Securing User Accounts: Securing Logoff Against CSRF

Securing User Accounts: Password Storage Best Practices

Securing User Accounts: Password Hashing Best Practices

Securing User Accounts: Overview of Password Reset

Securing User Accounts: Timed Password Reset

Securing User Accounts: Implementing Verification Questions

Securing User Accounts: Password Hints

Securing User Accounts: Account Change Risks

Securing User Accounts: At-risk Account Attributes

Securing User Accounts: Password Verification for Changes

Securing User Accounts: Implementing Account Change Notifications

Securing User Accounts: Confirming Account Changes

Securing User Accounts: Dealing with Compromised Systems

Securing User Accounts: Collecting Attack Evidence

Securing User Accounts: Neutralizing Attacks

Securing User Accounts: Securing Account Access and Mitigating Risk

OWASP Top 10: Introduction to the OWASP Project

OWASP Top 10: Introduction to the OWASP Top 10

OWASP Top 10: A1 Injection In Action

OWASP Top 10: A1 Injection - How It Works

OWASP Top 10: A2 Broken Authentication/Session Management In Action

OWASP Top 10: A2 Broken Authentication/Session - How It Works

OWASP Top 10: A3 Cross Site Scripting In Action

OWASP Top 10: A3 Cross Site Scripting In Action - How It Works

OWASP Top 10: A4 Insecure Direct Object References In Action

OWASP Top 10: A4 Insecure Direct Object References - How It Works

OWASP Top 10: A5 Security Misconfiguration In Action

OWASP Top 10: A5 Security Misconfiguration - How It Works

OWASP Top 10: A6 Sensitive Data Exposure In Action

OWASP Top 10: A6 Sensitive Data Exposure - How It Works

OWASP Top 10: A7 Missing Function Level Access Control In Action

OWASP Top 10: A7 Missing Function Level Access Control - How It Works

OWASP Top 10: A8 Cross Site Request Forgery In Action

OWASP Top 10: A8 Cross Site Request Forgery - How It Works

OWASP Top 10: A9 Using Components with Known Exploits In Action

OWASP Top 10: A9 Using Components with Known Exploits - How It Works

OWASP Top 10: A10 Unvalidated Redirects and Forwards In Action

OWASP Top 10: A10 Unvalidated Redirects and Forwards - How It Works

OWASP Top 10: Authentication versus Authorization

OWASP Top 10: Defense in Depth

OWASP Top 10: Error Message Security

OWASP Top 10: Config File Encryption

OWASP Top 10: Asymmetric Encryption in .NET

OWASP Top 10: NuGet Packages Security

OWASP Top 10: Symmetric Encryption in .NET

OWASP Top 10: Command Injection Mitigation

OWASP Top 10: SQL Server Injection Mitigation

OWASP Top 10: Trusted versus SQL Authentication

OWASP Top 10: Insecure Direct Object Reference Mitigation

OWASP Top 10: Password Hashing

OWASP Top 10: Releasing Resources to Avoid Pool Exhaustion

OWASP Top 10: CORS Preflight Scrutiny

OWASP Top 10: Authorization in Web API

OWASP Top 10: Authorization in WCF

OWASP Top 10: .NET Web Authentication Types

OWASP Top 10: Insecure Web.config Setting Mitigation

OWASP Top 10: SSL and Transport Security

OWASP Top 10: Web Parameter Tampering Mitigation

OWASP Top 10: Content Spoofing Mitigation

OWASP Top 10: Output Encoding

OWASP Top 10: ASP.NET & ASP.NET MVC Validation

OWASP Top 10: Session State in ASP.NET MVC

OWASP Top 10: Password Policies

OWASP Top 10: Multi-factor Authentication

OWASP Top 10: Appropriate Password Management

OWASP Top 10: HttpOnly Cookie Flag

OWASP Top 10: Microsoft Anti-cross Site Scripting Library

OWASP Top 10: Authorization in ASP.NET MVC Controllers

OWASP Top 10: Identify Top 10 Threats

OWASP Top 10: Mitigate Security

OWASP Top 10: Authenticating with External Logins in ASP.NET MVC

IT Security: iPhone Restriction Feature

IT Security: iPhone Privacy Features

IT Security: iPhone Safari Security

IT Security: iPhone Wi-Fi Bluetooth Security

IT Security: iPhone

IT Security: iPad Restriction Feature

IT Security: iPad Privacy Features

IT Security: iPad Safari Security

IT Security: iPad Wi-Fi Bluetooth Security

IT Security: iPad

IT Security: Securing the Cloud

IT Security: Threat Vectors in the Cloud

IT Security: Governance in the Cloud

IT Security: Cloud Encryption and Key Management

IT Security: Virtualization for Security and Security for Virtualization

IT Security: Cloud Security Models and Standards

IT Security: Building Security Policies for Cloud Infrastructure

IT Security: SECaaS

IT Security: Guidelines to Protect Web Services

IT Security: Data Security in the Cloud

IT Security: Big Data Challenges in the Cloud

IT Security: What is Your Cloud Provider Doing to Protect Your Assets

IT Security: Identity Management

IT Security: Mobile and BYOD Security

IT Security: Cloud Visibility

Foundations of Android Security: Understanding the Android Environment

Foundations of Android Security: Installing Android Standalone SDK Tools

Foundations of Android Security: Understanding the Linux Kernel

Foundations of Android Security: Understanding Android Runtime Components

Foundations of Android Security: Getting Familiar with Android Application Services

Foundations of Android Security: Getting Familiar with Activity Lifecycles

Foundations of Android Security: Understanding Android Application Framework

Foundations of Android Security: Overview of Android Software Stack Layers

Foundations of Android Security: Overview of Application User Protection Levels

Foundations of Android Security: Getting Familiar with Code Signing

Foundations of Android Security: Packaging an Android Application

Foundations of Android Security: Updating an Android Application

Foundations of Android Security: Identifying Application-based Permissions

Foundations of Android Security: Installing the Android Studio IDE

Foundations of Android Security: Enabling the ProGuard Tool in Android SDK

Foundations of Android Security: Creating a Signing Key and Certificate

Foundations of Android Security: Using Code Signing to Protect Application from Malware

Foundations of Android Security: Leveraging Linux Security Services to Protect Data

Foundations of Android Security: Understanding Permissions Assignment

Foundations of Android Security: Working with Shared User IDs

Foundations of Android Security: Declaring Application Permissions

Foundations of Android Security: Enforcing Permissions

Foundations of Android Security: Identifying Common Application Security Risks

Foundations of Android Security: Using Untrusted Devices, Applications, and Networks

Foundations of Android Security: Working with Untrusted Systems and Content

Foundations of Android Security: Scanning a Network Using Nmap

Foundations of Android Security: Examining Network Activity with BusyBox

Foundations of Android Security: Analyzing Network Traffic Using Wireshark

Foundations of Android Security: Intercepting Browser Application Traffic

Foundations of Android Security: Penetration Testing Best Practices

Foundations of Android Security: Analyzing Android Device Mount Points

Foundations of Android Security: Examining Android File Systems

Foundations of Android Security: Examining Android Device Directory Structure

Foundations of Android Security: Overview of Storage Options for Application Data

Foundations of Android Security: Exploring the /data/data Directory

Foundations of Android Security: Working with Root Access

Foundations of Android Security: Creating an Android Device Image

Foundations of Android Security: Accessing Application Databases

Foundations of Android Security: Working with Device Administration Policies

Foundations of Android Security: Enforcing Application Permissions

Foundations of Android Security: Analyzing Application Traffic and Data

Foundations of iOS Security: Overview of Apple Store Security

Foundations of iOS Security: Understanding Possible Security Threats

Foundations of iOS Security: Understanding iOS Attack Surface

Foundations of iOS Security: Using Code Signing and Data Execution Prevention

Foundations of iOS Security: Protecting Processes and Code Segments

Foundations of iOS Security: Getting Familiar with the Data Protection API

Foundations of iOS Security: Getting Familiar with File Protection Classes

Foundations of iOS Security: Getting Familiar with Keychain Protection Classes

Foundations of iOS Security: Getting Familiar with Keybags

Foundations of iOS Security: Attacking User Passcodes

Foundations of iOS Security: Overview on iOS Network Security

Foundations of iOS Security: Working with Virtual Private Networks

Foundations of iOS Security: Working with Wi-Fi Networks

Foundations of iOS Security: Working with Bluetooth Connections

Foundations of iOS Security: Working with Single Sign-on Authentication

Foundations of iOS Security: Working with AirDrop Security

Foundations of iOS Security: Overview of Code Signing in iOS

Foundations of iOS Security: Understanding the Mandatory Access Control Framework

Foundations of iOS Security: Understanding Provisioning

Foundations of iOS Security: Getting Familiar with Application Signing

Foundations of iOS Security: Listing Application Entitlements

Foundations of iOS Security: Collecting and Verifying Signing Information

Foundations of iOS Security: Enforcing Signatures on Processes

Foundations of iOS Security: Preventing Changes on Signed Pages

Foundations of iOS Security: Understanding Dynamic Code Signing

Foundations of iOS Security: Overview of iOS Sandbox

Foundations of iOS Security: Understanding Sandboxing and Runtime Security

Foundations of iOS Security: Understanding Sandboxing with Extensions

Foundations of iOS Security: Understanding How Sandboxing Impacts the App Store

Foundations of iOS Security: Working with Mobile Configuration Profiles

Foundations of iOS Security: Working with the Apple Configurator

Foundations of iOS Security: Creating a Configuration Profile

Foundations of iOS Security: Updating and Removing Configuration Profiles

Foundations of iOS Security: Setting Up the OS X Server Profile Manager

Foundations of iOS Security: Enrolling Devices using Profile Manager Web Portal

Foundations of iOS Security: Enrolling Devices by Downloading Enrollment Profiles

Foundations of iOS Security: Overview of Fuzzing iOS Applications

Foundations of iOS Security: Carrying Out a Fuzz Test

Foundations of iOS Security: Fuzzing MobileSafari

Foundations of iOS Security: Exploiting Bug Classes

Foundations of iOS Security: Understanding the iOS System Allocator

Foundations of iOS Security: Understanding TCMalloc

Foundations of iOS Security: Overview of Return-Oriented Programming

Foundations of iOS Security: Understanding the ARM Systems Call Convention

Foundations of iOS Security: Understanding the iOS ARM Calling Convention

Foundations of iOS Security: Displaying iOS Signing Info and Entitlements

Foundations of iOS Security: Working with Profiles

Securing Mobile Devices in the Enterprise: Mobile Device Overview

Securing Mobile Devices in the Enterprise: The Mobile Security Landscape

Securing Mobile Devices in the Enterprise: Overview of Security

Securing Mobile Devices in the Enterprise: Identifying Risks

Securing Mobile Devices in the Enterprise: Sensitive Mobile Assets

Securing Mobile Devices in the Enterprise: Sensitive Usage of Mobile Devices

Securing Mobile Devices in the Enterprise: Sensitive Data Storage and Transport

Securing Mobile Devices in the Enterprise: Weak Server-side Controls

Securing Mobile Devices in the Enterprise: Insecure Data Storage

Securing Mobile Devices in the Enterprise: Insufficient Transport Layer Protection

Securing Mobile Devices in the Enterprise: Unintended Data Leakage

Securing Mobile Devices in the Enterprise: Poor Authorization and Authentication

Securing Mobile Devices in the Enterprise: Broken Cryptography

Securing Mobile Devices in the Enterprise: Client-side Injection

Securing Mobile Devices in the Enterprise: Security Decisions via Untrusted Inputs

Securing Mobile Devices in the Enterprise: Improper Session Handling

Securing Mobile Devices in the Enterprise: Lack of Binary Protections

Securing Mobile Devices in the Enterprise: Technical Impacts of Exploits

Securing Mobile Devices in the Enterprise: Business Impacts of Exploits

Securing Mobile Devices in the Enterprise: Secure Device Data-handling Requirements

Securing Mobile Devices in the Enterprise: Device Authorization and Authentication Requirements

Securing Mobile Devices in the Enterprise: Device Sensor, Jailbreak, & MDM System Requirements

Securing Mobile Devices in the Enterprise: Secure Device Connectivity and App Requirements

Securing Mobile Devices in the Enterprise: Secure Device User Requirements

Securing Mobile Devices in the Enterprise: Assessing Mobile Threats

Securing Mobile Devices in the Enterprise: Cryptography Usage

Securing Mobile Devices in the Enterprise: Cryptography One-way Functions

Securing Mobile Devices in the Enterprise: Hashing Overview

Securing Mobile Devices in the Enterprise: Performing Hashing

Securing Mobile Devices in the Enterprise: Symmetric Encryption Overview

Securing Mobile Devices in the Enterprise: Asymmetric Encryption Overview

Securing Mobile Devices in the Enterprise: Performing Encryption

Securing Mobile Devices in the Enterprise: Digital Signing Overview

Securing Mobile Devices in the Enterprise: Performing Digital Signing

Securing Mobile Devices in the Enterprise: Key Distribution

Securing Mobile Devices in the Enterprise: Digital Certificates Overview

Securing Mobile Devices in the Enterprise: Creating Certificates

Securing Mobile Devices in the Enterprise: Back-end Security Requirements

Securing Mobile Devices in the Enterprise: Application Hardening

Securing Mobile Devices in the Enterprise: Secure App Deployment

Securing Mobile Devices in the Enterprise: Protecting the Transport Layer

Securing Mobile Devices in the Enterprise: Infrastructure Security Requirements

Securing Mobile Devices in the Enterprise: Building a Demilitarized Zone

Securing Mobile Devices in the Enterprise: Reverse Proxy Features

Securing Mobile Devices in the Enterprise: Securing Directory Services and CA

Securing Mobile Devices in the Enterprise: Securing E-mail Services

Securing Mobile Devices in the Enterprise: Rights Management Systems

Securing Mobile Devices in the Enterprise: Protecting Data at Rest and in Transit

Securing Mobile Devices in the Enterprise: Mobile Device Management Systems

Securing Mobile Devices in the Enterprise - Exercise: Securing Back-end Systems

Securing Mobile Devices in the Enterprise: Requirements for the Mobile Enterprise

Securing Mobile Devices in the Enterprise: Mobile Device Ownership Models

Securing Mobile Devices in the Enterprise: Unmanaged Devices in a Small Organization

Securing Mobile Devices in the Enterprise: Unmanaged Company-owned Devices

Securing Mobile Devices in the Enterprise: Unmanaged Device User Policies

Securing Mobile Devices in the Enterprise: Configuring Unmanaged Android Devices

Securing Mobile Devices in the Enterprise: Configuring Unmanaged iOS Devices

Securing Mobile Devices in the Enterprise: Configuring Unmanaged Windows Phone Devices

Securing Mobile Devices in the Enterprise: Secure Cloud Storage

Securing Mobile Devices in the Enterprise: Encrypting Cloud Data

Securing Mobile Devices in the Enterprise: Exchange ActiveSync Functionality

Securing Mobile Devices in the Enterprise: Managing Devices with Exchange ActiveSync

Securing Mobile Devices in the Enterprise: Short-lived Session Keys

Securing Mobile Devices in the Enterprise: Configuring Perfect Forward Secrecy

Securing Mobile Devices in the Enterprise: Virtual Private Networking Overview

Securing Mobile Devices in the Enterprise: Configuring Virtual Private Networks

Securing Mobile Devices in the Enterprise: BYOD Containers

Securing Mobile Devices in the Enterprise: BYOD Container Usage Scenarios

Securing Mobile Devices in the Enterprise: Configuring BYOD Containers

Securing Mobile Devices in the Enterprise: Application Wrapper Overview

Securing Mobile Devices in the Enterprise: Mitigating Malicious App Functionality

Securing Mobile Devices in the Enterprise: Mitigating Code Vulnerabilities in Apps

Securing Mobile Devices in the Enterprise: Microsoft Azure Rights Management Overview

Securing Mobile Devices in the Enterprise: Protecting Content with Microsoft Azure RMS

Securing Mobile Devices in the Enterprise - Exercise: Mitigating Threat for BYOD and COD Devices

Securing Mobile Devices in the Enterprise: Enterprise Mobile Device Security Challenges

Securing Mobile Devices in the Enterprise: Enterprise Mobile Device Security Model Solution

Securing Mobile Devices in the Enterprise: Creating a Microsoft Intune Account

Securing Mobile Devices in the Enterprise: Navigating Microsoft Intune

Securing Mobile Devices in the Enterprise: Enrolling Devices in Microsoft Intune

Securing Mobile Devices in the Enterprise: Targeting Devices in Microsoft Intune

Securing Mobile Devices in the Enterprise: Enforcing Configurations in Microsoft Intune

Securing Mobile Devices in the Enterprise: Handling Certificates in Microsoft Intune

Securing Mobile Devices in the Enterprise: Deploy Enterprise Profiles in Microsoft Intune

Securing Mobile Devices in the Enterprise: Distribute Apps in Microsoft Intune

Securing Mobile Devices in the Enterprise: Protect Data in Microsoft Intune

Securing Mobile Devices in the Enterprise: System Center Configuration Manager Overview

Securing Mobile Devices in the Enterprise: Configuring the Microsoft Intune Connector Role

Securing Mobile Devices in the Enterprise: Preparing for Windows Mobile Device Enrollment

Securing Mobile Devices in the Enterprise: Preparing for iOS Mobile Device Enrollment

Securing Mobile Devices in the Enterprise - Exercise: Configuring Intune

Certified Cloud Security Professional (CCSP): Cloud Computing Definitions

Certified Cloud Security Professional (CCSP): Cloud Computing Participants

Certified Cloud Security Professional (CCSP): Cloud Computing Characteristics

Certified Cloud Security Professional (CCSP): Cloud Computing Infrastructure

Certified Cloud Security Professional (CCSP): Cloud Computing Activities

Certified Cloud Security Professional (CCSP): Cloud Computing Service Capabilities

Certified Cloud Security Professional (CCSP): Cloud Service Types (the Cloud Stack)

Certified Cloud Security Professional (CCSP): Cloud Deployment Models

Certified Cloud Security Professional (CCSP): Cloud Cross-cutting Aspects

Certified Cloud Security Professional (CCSP)

Certified Cloud Security Professional (CCSP): Asset Access Control

Certified Cloud Security Professional (CCSP): Asset Removal and Storage Media Sanitization

Certified Cloud Security Professional (CCSP): Cloud Network Security

Certified Cloud Security Professional (CCSP): Securing the Virtualized Environment

Certified Cloud Security Professional (CCSP): Infrastructure and Data Threats

Certified Cloud Security Professional (CCSP): Platform-specific Security

Certified Cloud Security Professional (CCSP): Cloud - Data Life Cycle

Certified Cloud Security Professional (CCSP): Cloud Service Continuity

Certified Cloud Security Professional (CCSP): Cloud Service Investment

Certified Cloud Security Professional (CCSP): Cloud Functional Security

Certified Cloud Security Professional (CCSP): Cloud Service Certification Assessment

Certified Cloud Security Professional (CCSP): Product Certification

Certified Cloud Security Professional (CCSP): Architectural Security

Certified Cloud Security Professional (CCSP): Data Lifecycle Stages

Certified Cloud Security Professional (CCSP): Data Asset Security and Associated Technologies

Certified Cloud Security Professional (CCSP): Storage Types

Certified Cloud Security Professional (CCSP): Storage Type Threat

Certified Cloud Security Professional (CCSP): Storage Type Threat Mitigation

Certified Cloud Security Professional (CCSP): Encryption of Data Assets

Certified Cloud Security Professional (CCSP): Key Management

Certified Cloud Security Professional (CCSP): Masking of Data

Certified Cloud Security Professional (CCSP): Tokenization of Data

Certified Cloud Security Professional (CCSP): Emerging Data Protection Technologies

Certified Cloud Security Professional (CCSP): Personally Identifiable Information (PII) Law

Certified Cloud Security Professional (CCSP): Data Discovery Implementation

Certified Cloud Security Professional (CCSP): Sensitive Data Classification

Certified Cloud Security Professional (CCSP): Data Controls and Application

Certified Cloud Security Professional (CCSP): Data Rights Objects and Management

Certified Cloud Security Professional (CCSP): Data Retention Policy

Certified Cloud Security Professional (CCSP): Data Deletion

Certified Cloud Security Professional (CCSP): Data Archiving

Certified Cloud Security Professional (CCSP): Event Sources

Certified Cloud Security Professional (CCSP): Event Logging, Storage, and Analysis

Certified Cloud Security Professional (CCSP): Chain of Custody and Non-repudiation

Certified Cloud Security Professional (CCSP): Data Asset Security

Certified Cloud Security Professional (CCSP): Physical Architecture

Certified Cloud Security Professional (CCSP): Network and Communications Service

Certified Cloud Security Professional (CCSP): Compute Service

Certified Cloud Security Professional (CCSP): Virtualized Infrastructure

Certified Cloud Security Professional (CCSP): Storage Service

Certified Cloud Security Professional (CCSP): Risk

Certified Cloud Security Professional (CCSP): Threat and Attack

Certified Cloud Security Professional (CCSP): Virtualization Vulnerabilities

Certified Cloud Security Professional (CCSP): Defence

Certified Cloud Security Professional (CCSP): DataCenter Protection

Certified Cloud Security Professional (CCSP): Protection

Certified Cloud Security Professional (CCSP): Protecting Access

Certified Cloud Security Professional (CCSP): Auditing

Certified Cloud Security Professional (CCSP): Cloud Environment BC and DR

Certified Cloud Security Professional (CCSP): Business Requirements and Risk

Certified Cloud Security Professional (CCSP): Strategy and Planning

Certified Cloud Security Professional (CCSP): Implementation

Certified Cloud Security Professional (CCSP): Specify infrastructural security

Certified Cloud Security Professional (CCSP): Training and Awareness

Certified Cloud Security Professional (CCSP): Common Dangers and Potential Pitfalls

Certified Cloud Security Professional (CCSP): Published Security Issues

Certified Cloud Security Professional (CCSP): Cloud Application Development

Certified Cloud Security Professional (CCSP): Functional Testing

Certified Cloud Security Professional (CCSP): Cloud Application Security Testing

Certified Cloud Security Professional (CCSP): APIs

Certified Cloud Security Professional (CCSP): Supply-Chain & Community

Certified Cloud Security Professional (CCSP): Architecture

Certified Cloud Security Professional (CCSP): Business Requirements

Certified Cloud Security Professional (CCSP): Application Management

Certified Cloud Security Professional (CCSP): Known Common Vulnerabilities

Certified Cloud Security Professional (CCSP): Risks

Certified Cloud Security Professional (CCSP): Threat Modeling and QoS

Certified Cloud Security Professional (CCSP): Security Devices

Certified Cloud Security Professional (CCSP): Cryptography

Certified Cloud Security Professional (CCSP): Isolation

Certified Cloud Security Professional (CCSP): Virtualization

Certified Cloud Security Professional (CCSP): Federation and Identity Provision

Certified Cloud Security Professional (CCSP): Single Sign-On/Off (SSO)

Certified Cloud Security Professional (CCSP): Multi-Factor Authentication

Certified Cloud Security Professional (CCSP): Specify Application Security

Certified Cloud Security Professional (CCSP): Logical Aspect Design and Risk Assessment

Certified Cloud Security Professional (CCSP): Physical and Environmental Design

Certified Cloud Security Professional (CCSP): Hardware Configuration and Security

Certified Cloud Security Professional (CCSP): Hardware and Virtualization Configuration

Certified Cloud Security Professional (CCSP): Access Control

Certified Cloud Security Professional (CCSP):Operating System Security

Certified Cloud Security Professional (CCSP): Host Management

Certified Cloud Security Professional (CCSP): Remote Access

Certified Cloud Security Professional (CCSP): Operating System Baseline

Certified Cloud Security Professional (CCSP): Operating System

Certified Cloud Security Professional (CCSP): Performance Monitoring

Certified Cloud Security Professional (CCSP): Hardware Monitoring

Certified Cloud Security Professional (CCSP): Host Configuration

Certified Cloud Security Professional (CCSP): Network Security Management

Certified Cloud Security Professional (CCSP): Event Logging

Certified Cloud Security Professional (CCSP): Virtualized Infrastructure Construction

Certified Cloud Security Professional (CCSP): Guest Operating System Installation

Certified Cloud Security Professional (CCSP): Regulatory Control and Standards Adoption

Certified Cloud Security Professional (CCSP): Physical and Logical Risk Management

Certified Cloud Security Professional (CCSP): Forensic Data Collection and Management

Certified Cloud Security Professional (CCSP): Communications Management

Certified Cloud Security Professional (CCSP): Operations Security

Certified Cloud Security Professional (CCSP): International Legislation Conflict

Certified Cloud Security Professional (CCSP): Legal Risks

Certified Cloud Security Professional (CCSP): Legal Control

Certified Cloud Security Professional (CCSP): eDiscovery

Certified Cloud Security Professional (CCSP): Forensic Requirement

Certified Cloud Security Professional (CCSP): Defining and Categorizing PII

Certified Cloud Security Professional (CCSP): International Regulation variations

Certified Cloud Security Professional (CCSP): Audit Controls - Internal and External

Certified Cloud Security Professional (CCSP): Audit Requirements, Scope, and Reporting

Certified Cloud Security Professional (CCSP): Virtualization - Auditing Challenges

Certified Cloud Security Professional (CCSP): Audit Reporting and Standards

Certified Cloud Security Professional (CCSP): Gap Analysis and Planning

Certified Cloud Security Professional (CCSP): Information Management Systems and Control 1

Certified Cloud Security Professional (CCSP): Information Management Controls

Certified Cloud Security Professional (CCSP): Cloud Server Provider (CSP) Risk Management

Certified Cloud Security Professional (CCSP): Data Ownership and Responsibility

Certified Cloud Security Professional (CCSP): Risk Management

Certified Cloud Security Professional (CCSP): Risk Frameworks

Certified Cloud Security Professional (CCSP): Risk Management Metrics

Certified Cloud Security Professional (CCSP): Cloud - Risk Assessment

Certified Cloud Security Professional (CCSP): Contract and Vendor Management and Assessment

Certified Cloud Security Professional (CCSP): Supply-chain Management

Certified Cloud Security Professional (CCSP): Compliance Assurance

Advanced Architecting on Amazon Web Services: AWS Availability Levels

Advanced Architecting on Amazon Web Services: AWS Components for High Availability

Advanced Architecting on Amazon Web Services: Traditional DR

Advanced Architecting on Amazon Web Services: Recovery Time Objective

Advanced Architecting on Amazon Web Services: Recovery Point Objective

Advanced Architecting on Amazon Web Services: RTO and RPO Examples

Advanced Architecting on Amazon Web Services: Backup and Restore with AWS

Advanced Architecting on Amazon Web Services: AWS Pilot Light

Advanced Architecting on Amazon Web Services: Warm Standby DR Solutions

Advanced Architecting on Amazon Web Services: Multi-Site DR Solutions

Cryptography Fundamentals: Introducing Cryptography

Cryptography Fundamentals: Identifying Historical Use of Cryptography

Cryptography Fundamentals: Describing Cryptographic Terminology

Cryptography Fundamentals: Defining Why Cryptography is Difficult

Cryptography Fundamentals: Identifying the Current State of Cryptography

Cryptography Fundamentals: Describing Export Controls and Limits on Cryptography

Cryptography Fundamentals: Describing How Cryptography Provides Confidentiality

Cryptography Fundamentals: Recognizing the Need for Data Integrity

Cryptography Fundamentals: Defining Cryptography Authentication

Cryptography Fundamentals: Applying Non-repudiation to Cryptography

Cryptography Fundamentals: Using a One-time Pad

Cryptography Fundamentals: Describing Substitution Ciphers

Cryptography Fundamentals: Using Symmetric Algorithms

Cryptography Fundamentals: Working with Asymmetric Algorithms

Cryptography Fundamentals: Hiding Data Using Steganography

Cryptography Fundamentals: Using One-way Hashes

Cryptography Fundamentals: Describing Digital Signatures

Cryptography Fundamentals: Distinguishing between Block and Key Sizes

Cryptography Fundamentals: Using Padding

Cryptography Fundamentals: Formatting the Output

Cryptography Fundamentals: Using Nonces and the Initialization Vector

Cryptography Fundamentals: Identifying and Using Entropy

Cryptography Fundamentals: Creating or Generating Keys

Cryptography Fundamentals: Identify the Cryptographic Algorithm to Use

Cryptography Fundamentals: Describing Electronic Codebook (ECB)

Cryptography Fundamentals: Using Cipher Block Chaining (CBC)

Cryptography Fundamentals: Using Propagating Cipher Block Chaining (PCBC)

Cryptography Fundamentals: Using Cipher Feedback (CFB)

Cryptography Fundamentals: Using Output Feedback (OFB)

Cryptography Fundamentals: Describing Counter (CTR)

Cryptography Fundamentals: Using the AES Block Algorithm

Cryptography Fundamentals: Applying the DES/3DES Block Algorithm

Cryptography Fundamentals: Describing the Blowfish Block Algorithm

Cryptography Fundamentals: Describing the RC4 Streaming Algorithm

Cryptography Fundamentals: Describing the ElGamal Algorithm

Cryptography Fundamentals: Defining the RSA Algorithm

Cryptography Fundamentals: Describing MD5, SHA1, and SHA3

Cryptography Fundamentals: Using SHA2

Cryptography Fundamentals: Describing HMAC

Cryptography Fundamentals: Describing Key Management

Cryptography Fundamentals: Describing Key Exchange

Cryptography Fundamentals: Describing Key Escrow

Cryptography Fundamentals: Identifying Secure Communications Over HTTPS

Cryptography Fundamentals: Working with the Secure Shell (SSH)

Cryptography Fundamentals: Using GPG with E-mail

Cryptography Fundamentals: Working with Disk Encryption

Cryptography Fundamentals: Identifying Algorithm and Key Strengths

How to Join

1.) Register your name online at Register Now

2.) Deposit your training fee via IMPS / NEFT / PAYTM / Google Tez / Phone Pe or Cash Deposit at Training Centre

3.) Send snapshot / transaction number via Whatsapp to +91-9654825370 or Email us at admin@hackveda.in

4.) Bill will be generated and sent to your Email ID, Hackveda One2One account details will also be sent via sms and email. You can also collect Hackveda One2One account details from training centre.

Bank Details for IMPS / Paytm to Bank / NEFT / ATM - Cash Deposit

Name: Devanshu Shukla

Account Number: 55142333064

Bank Name: State Bank of India

Branch: Rama Market, Pitampura

IFS Code: SBIN0050403

Pay via PayTM / Google Tez / Phone Pe

9654825370

Optional Pre-requisites

Laptop & Charger, 4GB+ Pendrive, Headphones

Training Centres

Hackveda - H-3/60, III Floor, Sector-18, Rohini, Delhi - 110089