Information Security Foundation

Hands-On | 42 Hours, 7 Days | Hack2Secure's 'Information Security Associate' Exam Attempt

Online LAB Access | Laptop Required | Aligned with Industry Security Best Practices & Requirements

Hack2Secure's Workshop on 'Information Security Foundation' provides hands-on exposure on Core InfoSec Concepts, using Simulated Lab Environment, required for understanding and analysis of different Information Security Risk and Attack vectors. Scoped around Web, Network and Cloud Security practices, these intensive practical oriented sessions provide deep-dive on required practical tips and tricks to evaluate, test and assess different Security flaws.

Key Take Away

- Information Security Concepts & Definitions
  - Core Security Concepts
  - Security Design Principles
- Basic Network Concepts
- Network Packet Crafting & Protocol Analysis
  - TCP, IP, UDP, DNS
- SSL/TLS Protocol, IPSec, VLAN
- HTTP Protocol: Versions, Methods & Analysis
- OWASP Web Security Testing Framework
- Injection Attacks, Cross Site Scripting
- "Network & Web Security Analysis": Steps
- Network & Web Application Firewalls
- Buffer Overflow Attack
- Cloud Computing Concepts & Security Risk
- Big Data Security
- Wireshark, NMap, Netcat, Scapy
- Web Proxy Servers: Burp Suite & ZAP
- Google Hacking

What You Will Receive

- **Instructor Led Classroom Sessions**
- **Soft Deliverables**
  - Program Slides & Lab Guides
  - Reference Documents
- **Online Lab Access** [30 Days]
- **Hack2Secure's ISA Cert Attempt Voucher**
  - 1 Attempt, 6 months Validity
  - Globally Proctored and Delivered by Pearson VUE
- Access to **Self-Paced Online Sessions**
- **Training Completion Certificate**

For more details
www.hack2secure.com/isf

Who Should Attend

- Students
  - Looking to pursue career in Information Security domain
- Professional
  - Looking to explore their skills in Information Security domain
  - Looking to address InfoSec concerns in business and explore adoptable measures to ensure Security as a process
- Research & Development Teams, Consultants
- Security Team/Office
- Management Team
  - Managers, Leads
  - Project Assurance Team
  - CxO, Directors, VPs

Detailed Curriculum

Module#1: InfoSec Concepts -1

- Information Security: Intro
  - Current State & Career Scope
  - Introducing different domains in InfoSec
- Core Security Concepts: C.I.A. Triad
  - Ensuring Confidentiality
    - About, How to Ensure
    - Symm & Asymm Encryption, PKI
    - Common Attacks, Case Studies
  - Ensuring Integrity
    - About, How to Ensure
    - Hashing, Digital Signatures
    - Common Attacks, Case Studies
  - Ensuring Availability
    - About, How to Ensure
    - DoS/DDoS Attack, Case Studies
- Core Security Concepts: A.A.A.
  - About Authentication
    - Types, Deployment methods
    - Common Attack, Case Studies
    - Password Security Best Practices
    - Brute Force & Dictionary Attack
    - Authentication Servers: Overview
      - Kerberos, LDAP
      - Active Directory
  - About Authorization
    - About, How to Ensure
    - Access Control: Types
    - Common Attacks, Case Studies
  - About Accountability
    - About, How to Ensure
    - Common Attacks, Case Studies
- Core Security Concepts: Best Practices
- Secure Design Principles
  - About. Best Practices. Case Studies

Module#2: InfoSec Concepts – 2

- Security Definitions & Terminology
  - Risk, Threats & Vulnerabilities
  - Policies, Procedures & Practices
  - Standards & Compliances
  - Security Testing: Black, Grey & White Box
  - Vulnerability Assessment & Penetration Testing
- Introducing different InfoSec Resources
- Introducing Malwares
  - Virus, Worms, Trojans
  - Adware, Spyware, Rootkits, Keyloggers
  - Rogue Software, Ransomware, Hijacker

Module#3: Basic Network Concepts

- Network Types & Devices
- Network Communication Models
- OSI Model: About, Usage, Layers
- Network Protocols
  - TCP
    - About, Header, 3 Way Handshake
    - Flooding Attack
  - IP
    - About, Header
    - Classes & Sub-netting
    - Hijacking Attack
  - UDP: About, Header, Usage
  - DNS
    - About, Usage, Working
    - Common Attacks

Module#4: Network Security – 1

- Network Sniffing
  - About, How it works
  - Wireshark: Usage
  - Protocol Analysis: TCP, IP, DNS
- Network Packet Crafting
  - Scapy & Hping
    - TCP, IP Packets & Analysis
    - Crafting Attack Packets

Module#5: Network Security – 2

- SSL/TLS Protocol
  - Handshake Process, Case Studies
  - Testing Methods & Best Practices
- IPSec Protocols: About, Working
- VLAN: About, Usage

Module#6: Web Security Foundation

- Why to Security Applications
- HTTP Protocol
  - Versions, Working, Request Types
  - Header Analysis, Cookies
- Introducing Web Services
  - About, Testing Requirements
- Secure Web Communication: Best Practices
- Introducing OWASP Security Testing Framework
- Web Proxy Servers
  - Burp Suite, Zed Attack Proxy (ZAP)
    - Usage, Features
    - Request-Response Analysis
    - Automating Security Attacks

Detailed Curriculum

Module#7: Common Web Security Attacks

- SQL Injection: Types, Root Cause
- Cross Site Scripting (XSS): Types, Root Cause
- Session Fixation & Hijacking Attack
- Privilege Escalation, Directory Traversal Attack
- Cross Site Request Forgery
  - About, Root Cause, Myths, Best Practices
- Client Side Attacks

Module#8: Web & Network Security Testing

- Reconnaissance: Information Gathering
  - Why, Active & Passive Methods
  - Website Mirroring
  - Recon-NG, TheHarvester, Shodan
  - Exploring Google Search, GHDB
- Enumeration & Fingerprinting
  - Netcat
  - Spidering, Crawling
  - Directory Browsing
- Mapping & Scanning
  - Nmap, Nessus Vulnerability Scanner
  - Nikto, W3af

Module#9: Buffer Overflow Attacks

- About Buffer overflow
- Types: Heap & Stack Overflow
- Defensive Best Practices

Module#10: Firewalls

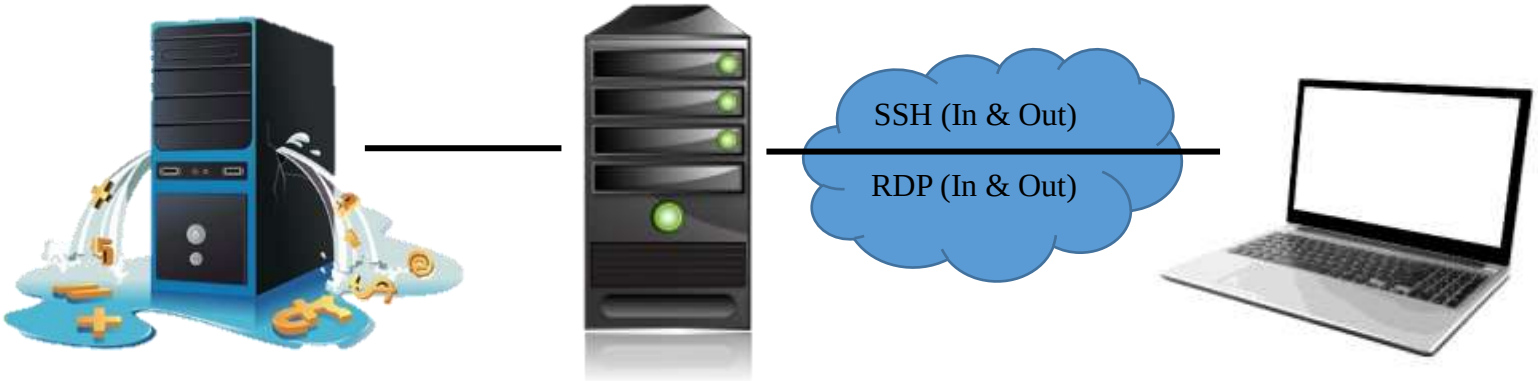
- Network Security Devices
  - Firewalls
    - About, Types, Usage, Limitations
  - Intrusion Detection & Prevention Systems (IDS & IPS)
- Web Application Defenses
  - Filtering & Firewall
  - Web Application Firewall (WAF): Types

Module#11: Cloud: Concepts & Security

- Introducing the Cloud
  - About, Terminologies, Models
- Primary Security Concerns
  - OWASP
    - Top10 Cloud Security Risk
  - Cloud Security Alliance
    - The Treacherous
  - Case Studies, Best Practices
- Big Data
  - Data Discovery Techniques
  - Security Challenges & Best Practices

Online Lab Layout

Cloud Based | Independent Setup for Each Participant | Accessible for 30 Days



Vulnerable Web Server (Target Machine)

Linux Machine (Client/Attacker)

Candidate Machine

Information Security Associate

Evaluate your InfoSec Essential Knowledge & Skills

Hack2Secure

Information Security Associate

Globally Available | Proctored | 180 mins. | 90 MCQ | Passing Grade: 60% | Exam Language: English

Hack2Secure Information Security Associate (ISA) Certificate program evaluates individual's conceptual and implementation level skills in Industry recommended Information Security practices. This program ensures candidate's awareness on Web, Network and Cloud Security Challenges, Threats, Standards and Best Practices. It walks through building blocks of different Information Security domains and ensures Security measures and strategies are addressed from core level.

Benefits

- Validates your awareness and knowledge in Information Security Systems and Domains.
- Get Global Recognition and Credibility
- Ensures Real Time skills required to handle Information Security Risk
- Demonstrate Knowledge of Industry Standards and Best Practices
- Ensures effective skills to measure and implement Security Controls

To Schedule Exam
"Information Security Associate"
www.pearsonvue.com/hack2secure

Attempt to Hack2Secure's ISA Exam is **included** as part of Information Security Foundation Training Program from Hack2Secure

1 Attempt | 6 months Voucher Validity

Proctored & Delivered globally at Pearson VUE Authorized Test Centres

Pearson | VUE

About Hack2Secure

Hack2Secure excels in "Information Security" Domain and offers customised IT Security programs, including Training, Services and Solutions. Our programs are designed by industry experts and tailored as per specific needs. We help students, professionals and companies with knowledge, tools and guidance required to be at forefront of a vital and rapidly changing IT industry.

Hack2Secure
INSPIRE • INDUCE • INNOVATE

InfoSec Training

Vendor Independent, Customizable, Across Domains

Hack2Secure excels in delivering intensive, immersion security training sessions designed to master practical steps necessary for defending systems against the dangerous security threats. Our wide range of fully customizable training courses allow individual to master different aspects of Information Security as per their industry requirement and convenience.

- Delivered Training to more than 15k+ Professionals Globally
- Customizable Security Training Programs, aligned with Business Requirements

InfoSec Certification

- Globally delivered and Proctored Security Certification programs with **PearsonVUE**
- Vendor Independent Programs based on Industry Security Standards and Practices

InfoSec Services

Hack2Secure offers IT Security Professional Services to provide ways to stay ahead of Security Threats through adaptive and proactive Security methods like

- Secure Software Development Lifecycle
- Secure Application Design & Threat Modeling
- Application Security Testing
- Risk Assessment, Consulting

skype hack2secure

+91 (80) 49 58 32 99
+91 (80) 49 58 33 99

Hack2Secure featured as:

25 FASTEST GROWING CYBER SECURITY COMPANIES IN INDIA
Source: The CEO Magazine, India

10 BEST SECURITY COMPANIES in INDIA: 2017
Source: Silicon Review Magazine, India

EXCELLENCE IN SECURITY TRAINING PROGRAMMES
Source: GDS Review Magazine