Information Security Training

Course: **00087**
Filter: **Beginner**
Duration: **20 hours**
Category:: **Software Application Security**
Price: **3000,00 €**

About Course

In this Information Security Training course, you will gain the foundational knowledge and skills to analyze and assess network risks and then select and deploy appropriate countermeasures.

What you'll learn

- Evaluate methods for strong authentication.
- Search for possible vulnerabilities in operating systems.
- Search for possible vulnerabilities in operating systems.
- Reduce your organization’s exposure to dangers in enterprise-wide and virtual private networks (VPNs).
- Analyze your exposure to security threats.
- Protect your organization's systems and data.
- Deploy firewalls and data encryption to minimize threats.
- Assess alternative user and host authentication mechanisms.
- Manage risks originating from inside the organization and from the internet.
- Leverage continued support with after-course one-on-one instructor coaching and computing sandbox.

Pre-requisites

- None

Curriculum

Module 1: Building A Secure Organization

- Real threats that impact cybersecurity
- Hackers, internal and external
- Eavesdropping
- Spoofing
- Sniffing
- Trojan horses
- Viruses
- Wiretaps
- A cyber security policy: the foundation of your protection
- Defining your information assurance objectives
- Assessing your exposure

Module 2: A Cryptography Primer

- Securing data with symmetric encryption
- Choosing your algorithm: DES, AES, Rc4, and others
- Assessing key length and key distribution
- Solving key distribution issues with asymmetric encryption
- Generating keys
- Encrypting with RSA
- Explore PGP and GnuPG
- Evaluating Web of Trust and PKI
- Ensuring integrity with hashes
- Hashing with Md5 and SHA
- Protecting data in transit
- Building the digital signature

Module 3: Verifying User and Host Identity

- Assessing traditional static password schemes

- Creating a strong password policy to prevent password guessing and cracking
- Protecting against social engineering attacks
- Encrypting passwords to mitigate the impact of password sniffing
- Evaluating strong authentication methods
- Preventing password replay using one-time and tokenized passwords
- Employing biometrics as part of multi-factor authentication
- Authenticating hosts
- Distrusting IP (Internet Protocol) addresses
- Mitigating address-spoofing issues and implementing countermeasures
- Implementing solutions for wireless networks

Module 4: Preventing System Intrusions

- Discovering system vulnerabilities
- Searching for operating system vulnerabilities
- Discovering file permission issues
- Limiting access via physical security
- Encrypting files for confidentiality
- Encrypting with application-specific tools
- Recovering encrypted data
- Hardening the operating system
- Locking down user accounts
- Securing administrator's permissions
- Protecting against viruses

Module 5: Guarding Against Network Intrusions

- Scanning for vulnerabilities
- Searching for rogue servers
- Profiling systems and services
- Reducing Denial of Service (DoS) attacks
- Securing DNS (Domain Name System)
- Limiting the impact of common attacks
- Deploying firewalls to control network traffic
- Preventing intrusions with filters
- Implementing a cyber security policy

- Deploying personal firewalls
- Protecting web services and applications
- Validating user input
- Controlling information leakage

Module 6: Ensuring Network Confidentiality

- Threats from the LAN
- Sniffing the network
- Mitigating threats from connected hosts
- Partitioning the network to prevent data leakage
- Identifying wireless LAN vulnerabilities
- Confidentiality on external connections
- Ensuring confidentiality with encryption