kaïna-COM
ACADEMY

PILAT EUROPE
Leading a new era of human resources

Boost Program

SUMMER EDITION 2020

Cyber Security Package: Shield

- ✓ Cyber Fundamentals including Hands-on training
- ✓ Building Secure Applications

WWW.KAINA-COM.FR

Training Catalogue
02/07/2020

KAÏNA-COM

TRAINING CATALOGUE

Cyber Security Fundamentals including Hands-on

Hands-on course to provide insights into the modern security environment, the cyber threat landscape and attacker mentality

KSE012 – Cyber Security Fundamentals including Hands-on

Reference	KSE012
Experience	☒ Beginner ☒ Intermediate ☐ Advanced
Duration	Training Program: • 24 hours (4 hours/day)
Training Method	☐ I: i-learning, individual training (web-based training) ☒ V: v-learning, virtual class ☐ C: c-learning, classroom training **KAÏNA-COM** LE CARRÉ HAUSSMANN II, 6 Allée de la Connaissance 77127 Lieusaint - France
Prerequisite	Basic Knowledge of IP Networking
Audience	High level Managers, Presale Managers, IT Managers, QA and Technical Support.

Continued on next page

KSE012 – Cyber Security Fundamentals including Hands-on, Continued

Objective

The main goal of the Cyber security course is to cover some fundamentals cyber security topic, to provide insights into the modern security environment, the cyber threat landscape and attacker mentality, including how attackers work, what tools they use, what vulnerabilities they target and what they're really after.

Continued on next page

KSE012 – Cyber Security Fundamentals including Hands-on, Continued

Course Contents

Course Contents :

Table 1: KSE012 - Course Contents (Day#1)

Chapter	Description
Introduction to Cyber Security	• Hacking History • Cyber Attacks Trends • External and Internal threats • Hackers Types • Threats and attacks • Security Criteria's • Threat Taxonomy Models summary
Basics of Security Management	• Security Layers • Defending concept according OSI Layers • Security modules and functionalities • NAT- Network Address Translation • Firewalls Types • Network Access Control (NAC) • IDS and IPS • Encryption protocols: IPSec, TLS and SRTP • Replay Attacks Protection • Server Hardening
TCP/IP vulnerabilities	• Network Layer (IP) services – 3rd Layer • IP Header Structure • MTU and Fragmentation process • IP Addressing – issues and solutions – ARP, DHCP, NAT • Transportation Layers: TCP, UDP, SCTP
Introduction to Cryptography	• Public and Private keys • Symmetric and Asymmetric encryption keys • DES and Triple DES • AES and RSA methods

Continued on next page

KSE012 – Cyber Security Fundamentals including Hands-on, Continued

Course Contents, continued

Table 2: KSE012 - Course Contents (Day#2)

Chapter	Description
Firewall	• PFF, Proxy GW, Stateful Inspection • Management menu • Rules and policy
IPTables Firewall	• What is IPTables? • Chains and Chain Policy • Creating Rules and Rules Examples • Connection States • User Defined Chains • Logging Events/Packets • Advanced Examples • Managing IPTables Firewall
Network and Vulnerabilities Scanning	• Basic Scanning Techniques • Discovery Option • Operation System Detection • Nmap Script Engine • Nmap GUI • Vulnerabilities Information Sources • Vulnerabilities Scanners
Kali Linux	• What is Kali Linux? • Some Kali Facts • Installing Kali Linux • Tools Categories • Kali Desktop • Kali Top Tools • Kali Linux Alternatives
Network Scanning – Hands-on Session	• NMAP – Networks Scanning for Topology analysis and network Mapping • OpenVAS for vulnerabilities scanning and analysis

Continued on next page

KSE012 – Cyber Security Fundamentals including Hands-on, Continued

Course Contents, continued

Chapter	Description
Services inspection – Hands-on	• Numbers Harvesting • Conferences eavesdropping • Password capture
Firewall – Hands-on Session	• FW Rules setting • Denial of Service and DDoS attacks • Port scanning and vulnerabilities • Blocking scenarios

Table 3: KSE012 - Course Contents (Day#3)

Chapter	Description
Certificates and Authentication process	• Certificates and X.509 ITU-T Standard • HTTP digest authentication • Authentication scheme for a trusted domain • Authentication Challenges
Penetration Testing	• What is Penetration Testing? • Reasons for Pen Testing • Hackers and Pen Testing • Vulnerabilities • What do we test • Pen Testing Phases • Types of Testing • Areas of Penetration Tests • References
Network Penetration	• Hands-on Session
Wireless Network penetration- Hand-on Session	• John the Ripper/Crunch • Brute-force search • Brute-force attack • Password cracking/ WPA2 crack

Continued on next page

KSE012 – Cyber Security Fundamentals including Hands-on, Continued

Course Contents, continued

Chapter	Description
Security Summary	• Policy enforcement • Organization Security personal and hierarchic • Chief Information Security Officer – CISO • Penetration Tester / Hacker • Forensics • Information Security Administrator: ISAD • Information Security Auditor • Application Development Security Expert • InfoSec Systems Project Manager • InfoSec Incident Expert • Physical InfoSec Expert • Behavior Analysis Expert and To-Do-List
The End	• Summary • Q&A • Evaluation

Training Catalogue
02/07/2020

KAÏNA-COM
TRAINING CATALOGUE

Building Secure Applications - Advanced

KSE011 – Building Secure Applications - Advanced

Reference	KSE011
Experience	☒ Beginner ☒ Intermediate □ Advanced
Duration	Training Program: • 32 hours (4 hours/day)
Training Method	□ I: i-learning, individual training (web-based training) ☒ V: v-learning, virtual class □ C: c-learning, classroom training KAÏNA-COM LE CARRÉ HAUSSMANN II, 6 Allée de la Connaissance 77127 Lieusaint - France
Prerequisite	Experience and comprehension of application development
Audience	Application developers and Everyone who seeks to better understand how to build Secure Applications.

Continued on next page

KSE011 – Building Secure Applications - Advanced, Continued

Objective	Most of the focus when dealing with security has been on securing the network infrastructure (firewalls, VPNs etc.) and the server OS (e.g. patch management systems). However, in the last few years the focus has shifted to the application layer. This is because infrastructure (network and OS) security has improved significantly while applications have remained vulnerable. The application layer has become the main target of attack, while secure applications have become synonymous with higher quality. The course covers the different aspects of application security including authentication, authorization, auditing, confidentiality and data-integrity, as well as the different technologies addressing these requirements. It includes the risk analysis model and explains how to use it to analyze the risks associated with application vulnerabilities. Participants learn how to build secure applications: starting from including security in the application development life cycle and continuing to secure coding practices and security testing tools.

Continued on next page

KSE011 – Building Secure Applications - Advanced, Continued

Course Contents

Course Contents :

Table 1: KSE011 - Course Contents

Chapter	Description
Introduction	• The risks caused by unsecure applications: application vulnerabilities and associated threats • Examples of application layer attacks and associated risks • Security infrastructure and how it helps to protect the application
Encryption and hash functions	• Ensure data confidentiality and data integrity • Symmetric encryption – Stream encryption algorithms – Block encryption algorithms • Asymmetric encryption • Message hash functions and HMAC • Digital signatures and digital certificates • How to secure the data • Crypto++ examples • Confidentiality best practices
Authentication and Identity Management	• Passwords including password management • Challenge-resp authentication and tokens • One-time passwords (OTP) and OTP tokens • Smart cards and public key technology • Password storage and management • Brute force and dictionary attacks • Biometric authentication • Two factor authentication • Ticket based authentication • Digital certificates • PKI / PAM / RADIUS / ID Management

Continued on next page

KSE011 – Building Secure Applications - Advanced, Continued

Course Contents, continued

Chapter	Description
Application Layer Vulnerabilities	• Coding vulnerabilities – Input validation – Injection attacks – Application layer DoS • Business logic vulnerabilities
Input Validation	• Server side validation • Client side validation • Input validation using positive security logic • Input validation using negative security logic • Canonicalization and evasion • Injection attacks and countermeasures
Authorization and Access Control	• The principle of least privileges • Access control matrix • Discretionary Access Control (DAC) • Mandatory Access Control (MAC) • Role Based Access Control (RBAC) • Distributed enforcement model with centralized management
Auditing and Logging	• The need • Central logging • Auditing and log analysis

Continued on next page

KSE011 – Building Secure Applications - Advanced, Continued

Course Contents, continued

Chapter	Description
Risk Analysis and Threats	• Vulnerability, threat and risk • Risk analysis and risk mitigation • Security risks • Identifying threats • STRIDE threat model and threat modeling • DREAD and risk management • Responding to threats (risk mitigation)
SDLC – Secure Development Life Cycle	• The Methodology • Integrating security requirements • Secure design • Secure coding • Security testing • Security in deployment, support and maintenance • Security policy management
Secure Design	• Guidelines to designing secure applications • Reducing the attack surface • Identifying trusts and secrets
Threat Modeling and SDLC Tools	• Microsoft threat analysis and modeling tool • Pattern and practice check lists • Creating a threat model

Continued on next page

KSE011 – Building Secure Applications - Advanced, Continued

Course Contents, continued

Chapter	Description
Application Layer Vulnerabilities	• Business logic vulnerabilities • Coding vulnerabilities • Web application vulnerabilities – Injection attacks – Buffer overflow – XSS, cross site scripting – XSRF, cross site request forgery – Application layer DoS and DDoS
Web Services Security Standards	• XML encryption • XML digital signatures • SAML • XCAML • Web service security
Secure Communication Protocols	• SSL • IPSec
The End	• Summary • Q&A • Course's Evaluation