kaïna-COM ACADEMY

PILAT EUROPE
Leading a new era of human resources

Boost Program

SUMMER EDITION 2020

Cyber Security Package: 007

- Don’t Let the Hackers In
- Cyber Fundamentals including Hands-on training

Training Catalogue
02/07/2020

KAÏNA-COM
TRAINING CATALOGUE

Don’t Let the Hackers In

Nos locaux
KAÏNA-COM France
LE CARRÉ HAUSSMANN II
6 Allée de la Connaissance
77 127 Lieusaint

Contact
+33(0)9 50 20 91 64

E-mail
info@kaina-com.fr

Site Internet
www.kaina-com.fr

KSE003 – Don't Let the Hackers In

Reference	KSE003
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	Understanding computer software and architecture.
Audience	Anyone who needs to learn about anti-hacking techniques.

Continued on next page

KSE003 – Don't Let the Hackers In, Continued

Objective

Computer and information security is of utmost importance in today's technological (and political?) environment. The threats imposed by viruses, Trojan horses and other software malware is well known, as is the problem of the hackers – both those programmers who breaks into computer systems because of the challenge imposed and those who break in for criminal or terrorist purposes – to steal, change or destroy information.
In this "anti-hacker" course, participants learn about the basic threats hackers pose and what is needed in order to protect computer systems from them.

Continued on next page

KSE003 – Don't Let the Hackers In, Continued

Course Contents

Course Contents :

Table 1: KSE003 - Course Contents

Chapter	Description
Introduction	• What's there to worry about
Organizational Threats	• Users • Host • Server • Perimeter
Defense Methodologies	• Defense in depth • IATF • ISSE • Technology environment defined
Defense Tools	• Users • Host • Server • Perimeter
Security Assessment Demonstration	• Concepts • Tools
The End	• Summary • Q&A • Evaluation

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

Nos locaux
KAÏNA-COM France
LE CARRÉ HAUSSMANN II
6 Allée de la Connaissance
77 127 Lieusaint

Contact
+33(0)9 50 20 91 64

E-mail
info@kaina-com.fr

Site Internet
www.kaina-com.fr

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