Catalogue de Formation
29/07/2020

KAÏNA-COM
CATALOGUE DE FORMATION

Fondamentaux de la cybersécurité, y compris démonstration et formation pratique

Fournir un aperçu de l'environnement de la "Cybersécurité" moderne et faire de la formation pratique

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 – Fondamentaux de la cybersécurité, y compris démonstartion et formation pratique

Référence

KSE012

Niveau

☒ Débutant
☒ Intermédiaire
☐ Expert

Nombre de Jours

Programme de formation (24 H) :

- 24 heures (4 heures/jour)

Lieu de la formation

☐ I: e-learning, Formation individuelle (Formation en ligne)
☒ V: v-learning, classe virtuelle
☐ C: c-learning, cours présentiel

KAÏNA-COM
LE CARRÉ HAUSSMANN II,
6 Allée de la Connaissance
77127 Lieusaint - France

Prérequis

- Connaissance de base des réseaux IP.
- Un niveau d'anglais business moyen est requis car la formation sera dispensée en anglais.

Public

Cadre de haut niveau, ingénieur avant-vente, responsable informatique, QA (Assurance Qualité) et Support technique.

Ce sujet continue à la page suivante

KSE012 – Fondamentaux de la cybersécurité, y compris démonstartion et formation pratique, Suite

Objectifs

L'objectif principal du cours de cybersécurité est de couvrir les sujets fondamentaux de la cybersécurité, de fournir un aperçu de l'environnement de la sécurité moderne, le paysage de la cyber-menace et la mentalité des attaquants, y compris la façon dont les attaquants travaillent, quels outils utilisent-ils ?, quelles vulnérabilités ciblent-ils ? Et ce qu'ils recherchent vraiment.
Les participants de ce cours peuvent faire partie des équipes d'AQ (assurance qualité), des équipes de validation et des équipes de développement.

Ce sujet continue à la page suivante

KSE012 – Fondamentaux de la cybersécurité, y compris démonstartion et formation pratique, Suite

Contenu du cours

Contenu du cours :

Table 1: KSE012 - Contenu du cours (Part#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

Ce sujet continue à la page suivante

KSE012 – Fondamentaux de la cybersécurité, y compris démonstartion et formation pratique, Suite

Contenu du cours, Suite

Table 2: KSE012 - Contenu du cours (Part#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

Ce sujet continue à la page suivante

KSE012 – Fondamentaux de la cybersécurité, y compris démonstartion et formation pratique, Suite

Contenu du cours, Suite

Table 2: KSE012 - Contenu du cours (Part#2), Suite

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 - Contenu du cours (Part#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

Ce sujet continue à la page suivante

KSE012 – Fondamentaux de la cybersécurité, y compris démonstartion et formation pratique, Suite

Contenu du cours, Suite

Table 4: KSE012 - Contenu du cours (Part#3), Suite

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