Catalogue de Formation
21/05/2020

KAÏNA-COM

CATALOGUE DE FORMATION

Principes fondamentaux de la cybersécurité, y compris démonstration et formation pratique (Cyber Security Fundamentals including Demo and Hands-on training)

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

KBP002 – Cyber Fundamentals including Demo and Hands-on training

Référence	KBP002
Niveau	☒ Débutant ☒ Intermédiaire ☐ Expert
Nombre de Jours	Programme de formation (80 H) : • 20 x 4h par 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
Prix	5.500,00 € HT
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

KBP002 – Cyber Fundamentals including Demo and Hands-on training, 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

KBP002 – Cyber Fundamentals including Demo and Hands-on training, Suite

Contenu du cours

Contenu du cours :

Table 1: KBP002 - Contenu du cours (Meeting#1)

Chapter	Description
Introduction to Cyber Security	- Hacking History - Cyber Attacks Trends - Cloud Security Challenges - External and Internal threats - Threats and attacks - Security Criteria's - Threat Taxonomy Models summary
Basics of Networking	- Network Definitions and Topology - LAN, WAN, MAN - Synchronized and Unsynchronized modes - Network speed – bit rate - Bandwidth and the Noise factor - Errors handling - Utilization and coding efficiency
OSI layer model	- The need for Standards - Layers model and protocols - OSI Model - OSI Layers responsibilities
Summary including Q&A	- Summary including Q&A

Ce sujet continue à la page suivante

KBP002 – Cyber Fundamentals including Demo and Hands-on training, Suite

Contenu du cours, Suite

Table 2: KBP002 - Contenu du cours (Meeting#2)

Chapter	Description
The physical layer and vulnerabilities	• Twisted Pair, Coax, Fiber Optic, Satellite, Microwave
Data Link Layer (IEEE Ethernet) – the 2nd Layer	• Ethernet Common Topologies • CSMA (Carrier Sense Multiple Access) Protocol • Ethernet Frame Structure • MAC Addresses • MAC Spoofing for attacks
The 3rd Layer and IP vulnerabilities	• Network Layer (IP) • IP Header Structure • MTU and Fragmentation process • ARP and DHCP security issues • DOS attacks including fragmented packets
Summary including Q&A	• Summary including Q&A

Ce sujet continue à la page suivante

KBP002 – Cyber Fundamentals including Demo and Hands-on training, Suite

Contenu du cours, Suite

Table 3: KBP002 - Contenu du cours (Meeting#3)

Chapter	Description
The 4th Layer-Transportation Layers	• UDP • TCP • SCTP
Inspection and interception Tool – Hands-on	• Introduction to Wireshark • Getting Started • Capturing Packets • Color Coding • Sessions Filtering methods
Internet working	• HUB, Switch and Router • Routing techniques and Algorithms • Challenges - High availability and LB
Summary including Q&A	• Summary including Q&A

Table 4: KBP002 - Contenu du cours (Meeting#4)

NAT – Topology hiding	• NAT types / NAT challenges • Universal Plug and Play (UPNP) • Simple Traversal of UP through NAT (STUN) • Traversal Using Relay NATs (TURN)
Inspection and interception Tool – Hands-on	• Inspecting Packets • Network Topology studying • MAC Addresses and manufacturers • 3rd layer and IP Addresses analysis • Open ports at 4th Layer Analysis
Applications Evolution and security issues	• HTTP, Telnet, FTP, Email • Media Applications – VoIP • Collaboration
Summary including Q&A	• Summary including Q&A

Ce sujet continue à la page suivante

KBP002 – Cyber Fundamentals including Demo and Hands-on training, Suite

Contenu du cours, Suite

Table 5: KBP002 - Contenu du cours (Meeting#5)

Chapter	Description
Networking Issues	• Quality of Service • Class of Service • Related DoS attacks
Basics of Security Management	• Security Layers • Defending concept according OSI Layers • Security modules and functionalities • Server Hardening
MiTM challenge and confidentiality solutions	• What is TLS • What is IPsec • Applications over TLS and IPsec
Summary including Q&A	• Summary including Q&A

Ce sujet continue à la page suivante

KBP002 – Cyber Fundamentals including Demo and Hands-on training, Suite

Contenu du cours, Suite

Table 6: KBP002 - Contenu du cours (Meeting#6)

Chapter	Description
Inspection and interception Tool – Hands-on	• Call flow analysis • Traffic analysis and eavesdropping • Numbers Harvesting • Conferences eavesdropping • Password capture
Offensive security: Kali Linux	• What is Kali Linux? • Some Kali Facts • Installing Kali Linux • Tools Categories • Kali Desktop • Kali Top Tools • Kali Linux Alternatives
Basic Linux commands	• Basic Linux commands
Summary including Q&A	• Summary including Q&A

Ce sujet continue à la page suivante

KBP002 – Cyber Fundamentals including Demo and Hands-on training, Suite

Contenu du cours, Suite

Table 7: KBP002 - Contenu du cours (Meeting#7)

Chapter	Description
Virtual Machines	• VMWare • Virtual Box
Virtual Machines – Hands-on Part 1	• Virtual machine installation • Setting the VM • Configuration process
Kali Linux – Hands-on Part 2	• Download and install Kali Linux on VM • Setting and preparations • Networking and interconnection tests
Summary including Q&A	• Summary including Q&A

Table 8: KBP002 - Contenu du cours (Meeting#8)

Chapter	Description
Network and Vulnerabilities Scanning	• Basic Scanning Techniques • Discovery Option • Operation System Detection • Nmap Script Engine • Nmap GUI • Vulnerabilities Information Sources • Vulnerabilities Scanners
NMAP – Hands-on	• Download and installation process • NMAP - Networks Scanning for Topology analysis and network Mapping • Findings
Summary including Q&A	• Summary including Q&A

Ce sujet continue à la page suivante

KBP002 – Cyber Fundamentals including Demo and Hands-on training, Suite

Contenu du cours, Suite

Table 9: KBP002 - Contenu du cours (Meeting#9)

Chapter	Description
OpenVAS for vulnerabilities scanning	• What is OpenVAS tool? • How to use it? • GUI and setting process
OpenVAS - Hands-on	• OpenVAS - Hands-on
Summary including Q&A	• Summary including Q&A

Table 10: KBP002 - Contenu du cours (Meeting#10)

Chapter	Description
Advanced Reconnaissance Tools	• NCAT – Swiss Army Knife • Maltego
NCAT	• Hands-on
Maltego	• Hands-on
Summary including Q&A	• Summary including Q&A

Ce sujet continue à la page suivante

KBP002 – Cyber Fundamentals including Demo and Hands-on training, Suite

Contenu du cours, Suite

Table 11: KBP002 - Contenu du cours (Meeting#11)

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
Firewall - Hands-on Session	• FW Rules setting • Denial of Service and DDoS attacks • Port scanning and vulnerabilities • Blocking scenarios
Summary including Q&A	• Summary including Q&A

Ce sujet continue à la page suivante

KBP002 – Cyber Fundamentals including Demo and Hands-on training, Suite

Contenu du cours, Suite

Table 12: KBP002 - Contenu du cours (Meeting#12)

Chapter	Description
Introduction to Cryptography	• The History of Cryptography • Symmetric and Asymmetric encryption keys
Symmetric Cryptography	• The concept • Caesar cipher • Mono-Alphabetic cipher • Poly-Alphabetic cipher • DES and AES encryption methods
Asymmetric Cryptography	• The concept • Private and Public keys • RSA encryption method
Summary including Q&A	• Summary including Q&A

Ce sujet continue à la page suivante

KBP002 – Cyber Fundamentals including Demo and Hands-on training, Suite

Contenu du cours, Suite

Table 13: KBP002 - Contenu du cours (Meeting#13)

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 Testing3 • Vulnerabilities • What do we test? • Pen Testing Phases • Types of Testing • Areas of Penetration Tests • References
Network Penetration	• DEMO Session
Summary including Q&A	• Summary including Q&A

Ce sujet continue à la page suivante

KBP002 – Cyber Fundamentals including Demo and Hands-on training, Suite

Contenu du cours, Suite

Table 14: KBP002 - Contenu du cours (Meeting#14)

Chapter	Description
Wireless Network penetration	• John the Ripper/Crunch • Brute-force search • Brute-force attack • Password cracking/ WPA2 crack
Wireless Network penetration	• Demo
Cloud Security	• What is Cloud Computing? • Major Cloud Service Models • The SPI Cloud Model • Is it Possible to Secure the Cloud? • Cloud Risk Management
Summary including Q&A	• Summary including Q&A

Table 15: KBP002 - Contenu du cours (Meeting#15)

Chapter	Description
Web Application	• WEB Site vulnerabilities • OWASP Top-10 vulnerabilities
WAF – WEB Application Firewall	• WAF – WEB Application Firewall
SQL Injection	• Demo and Hands-on
Summary including Q&A	• Summary including Q&A

Ce sujet continue à la page suivante

KBP002 – Cyber Fundamentals including Demo and Hands-on training, Suite

Contenu du cours, Suite

Table 16: KBP002 - Contenu du cours (Meeting#16)

Chapter	Description
IDS/IPS and events detections	• IDS/IPS definitions • Architecture aspects –sensors locations • Rules and behavior analysis
SIEM for Security Information and Event Management	• SIEM for Security Information and Event Management
SEIM	• Demo
Summary including Q&A	• Summary including Q&A

Table 17: KBP002 - Contenu du cours (Meeting#17)

Chapter	Description
Computer forensics	• What is the Purpose of Computer Forensics? • Typical Investigations • Computer Forensic Capabilities • Private Computer Forensic Organizations
Business Continuity Management	• Business Continuity Management
Computer forensics	• Demo
Summary including Q&A	• Summary including Q&A

Ce sujet continue à la page suivante

KBP002 – Cyber Fundamentals including Demo and Hands-on training, Suite

Contenu du cours, Suite

Table 18: KBP002 - Contenu du cours (Meeting#18)

Chapter	Description
Cyber Security in the Organization	• Regulations, standards • Responsibilities • Organization policy
Measuring Cyber Risks	• Risk assessment • Probability and Impact • Risk Calculation
Elevating data security in the organization	• Improvement process • Creating workplan
Case Study	• Case Study
Summary including Q&A	• Summary including Q&A

Table 19: KBP002 - Contenu du cours (Meeting#19)

Chapter	Description
Introduction to AI	• What is AI • AI history • Types of AI • What can we (telecom industry) do with it
Neural networks	• NN networks theory / how it works • Available analytics tools • Real life examples / case study • What can we do with it?
Statistic / Social AI	• The crowd is smarter than the Bishop • How it works • Real life examples / case study • What can we do with it?

Ce sujet continue à la page suivante

KBP002 – Cyber Fundamentals including Demo and Hands-on training, Suite

Contenu du cours, Suite

Table 20: KBP002 - Contenu du cours (Meeting#20)

Chapter	Description
NLP- Natural language processing	• What is NLP and how it relates to AI • Natural Language Understanding (NLU) • Natural Language Generation (NLG) • Real life examples / case study • What can we do with it
Future of CRM/CEM	• What will be the interface? • Shortening (and focusing) the session • Predication for CEM • AI for CEM
The End	• Q&A • Couse's Evaluation