EduGroupe
Accompagner pour réussir

Sécurité systèmes et réseaux - mise en oeuvre

Référence : **SECSSR** Durée : **5 jours (35 heures)** Certification : **Aucune**

Opcommerce

CONNAISSANCES PRÉALABLE

- Aucun prérequis

PROFIL DES STAGIAIRES

- Toute personne en charge de la sécurité d'un système d'information ou intervenant sur le réseau ou la mise en place de serveurs d'entreprises

OBJECTIFS

- Savoir concevoir et réaliser une architecture de sécurité adaptée
- Pouvoir mettre en oeuvre les principaux moyens de sécurisation des réseaux
- Disposer d'une première approche sur la sécurisation des serveurs
- Découvrir en quoi la cryptographie est utile pour sécuriser les échanges d'informations

CERTIFICATION PRÉPARÉE

- Aucune

MÉTHODES PÉDAGOGIQUES

- Pédagogie active et ancrée dans le réel : Alternance d'apports théoriques courts et de travaux pratiques ; Approche par l'expérimentation ; Études de cas concrètes ; Évaluation continue
- Formats et adaptation selon le contexte : Présentiel (inter Paris, Lyon, Nantes, Rennes, Toulouse, Pau / intra partout en France) ; Distanciel synchrone (classe virtuelle) ; Distanciel asynchrone (complément e-learning) ; Inter / Intra
- Dimension innovante : Laboratoire virtualisé dynamique ; Challenge final Capture the Flag ; Visualisation en temps réel du trafic réseau et des alertes IDS ; Intégration de la cryptographie appliquée ; Kit numérique post-formation
- Moyens pédagogiques et techniques mobilisés : Plateforme de laboratoire composée de machines virtuelles ; Réseau isolé en présentiel ou accès VPN sécurisé en distanciel ; Supports numériques complets ; Plateforme en ligne pour quiz et dépôt de ressources

FORMATEUR

- Consultant-formateur expert en cybersécurité systèmes et réseaux, certifié CEH / ISO 27001 / Fortinet, garantissant un transfert de compétences immédiatement applicable

MÉTHODES D'ÉVALUATION DES ACQUIS

- Avant la formation : test de positionnement ou de validation des prérequis
- Pendant la formation : évaluations formatives sous diverses formes
- Fin de formation : évaluation sommative sous forme de quiz général ou étude de cas ; évaluation satisfaction
- Après la formation : Evaluation à froid, un mois après la session de formation
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

1. Jour 1 — L'environnement et les fondamentaux de la sécurité (7h)

2. Matin (3 h 30) - Introduction à la sécurité des systèmes et réseaux

- Définitions, enjeux, typologies de menaces et d'acteurs
- Les objectifs fondamentaux de la SSI (DICP : Disponibilité, Intégrité, Confidentialité, Preuve)
- Rappels sur les couches réseau (TCP/IP) et les points de vulnérabilité
- 💡 *Quiz interactif sur les notions SSI de base*
- 💡 *Brainstorming collectif : cartographier les points faibles de son SI*

3. Après-midi (3 h 30) - Architecture de sécurité – principes et bonnes pratiques

- Approche Defense in Depth, modèle Zero Trust, segmentation logique et physique
- Cloisonnement et filtrage réseau, DMZ, VLAN, pare-feu et reverse proxy
- Intégration de la sécurité dès la conception (Security by Design)
- 💡 *Atelier pratique : conception d'un schéma d'architecture sécurisée pour une PME (exercice en binôme)*
- 💡 *Étude de cas : analyse d'un incident dû à une mauvaise segmentation réseau*

4. Jour 2 — Les attaques : comprendre pour mieux se protéger (7h)

5. Matin (3 h 30) - Panorama des attaques réseau

- Scans, sniffing, spoofing, DoS/DDoS, ARP poisoning, MITM
- Attaques sur protocoles (DNS, DHCP, HTTPS, SMTP…)
- Exploitation de failles serveurs : injection, escalade, ransomware
- 💡 *Lab pratique : démonstration et observation de trafic malveillant via Wireshark et Scapy*

6. Après-midi (3 h 30) - Attaques systèmes et post-exploitation

- Vulnérabilités OS, mauvaises configurations, comptes privilégiés, services non sécurisés
- Exemple : exploitation d'un service vulnérable dans un environnement isolé
- 💡 *Simulation d'un pentest simple (scan + analyse de vulnérabilités)*
- 💡 *Debrief technique : comment détecter et bloquer l'attaque observée*

7. Jour 3 — Les protections et contre-mesures (7h)

8. Matin (3 h 30) - Sécurisation des réseaux

- Pare-feu stateful / applicatifs, proxies, IDS/IPS, NAC, VLAN, ACLs
- VPN, tunneling, chiffrement des flux, authentification forte
- 💡 *Mise en œuvre d'un pare-feu logiciel (pfSense ou iptables)*
- 💡 *Configuration d'un VPN site-à-site et test de connectivité sécurisée*

9. Après-midi (3 h 30) - Sécurisation des systèmes et serveurs

- Durcissement OS (Windows Server / Linux)
- Gestion des comptes, des droits, des logs et du patching
- Supervision et surveillance des journaux de sécurité
- 💡 *Vérification et durcissement d'un serveur selon une checklist CIS*
- 💡 *Mise en œuvre d'un système de détection d'intrusion (IDS open source)*

10. Jour 4 — Monitoring, détection et prévention (7h)

11. Matin (3 h 30) - Supervision de la sécurité

- Outils de monitoring : SIEM, Syslog, Wazuh, ELK
- Corrélation d'événements, détection d'anomalies, gestion d'alertes
- Journaux de sécurité : audit, rotation, conservation
- 💡 *Mise en place d'un tableau de bord de supervision basique (Wazuh ou ELK Stack)*

12. Après-midi (3 h 30) - Prévention et réponse à incident

- Stratégies de prévention : patch management, durcissement, sensibilisation
- Processus de gestion d'incident : détection, confinement, éradication, restauration
- Communication et plan de reprise d'activité (PRA / PCA)
- 💡 *Jeu de rôle : simulation d'une cellule de crise suite à une attaque réseau*

13. Jour 5 — Architectures sécurisées et cryptographie (7h)

14. Matin (3 h 30) - Exemples d'architectures sécurisées

- Architecture de référence SSI : PME, multi-sites, Cloud hybride
- Sécurité des accès distants, Zero Trust et segmentation micro-service
- Exemples concrets d'intégration : EDR, pare-feu nouvelle génération, ZTNA
- 💡 *Atelier collectif : création d'une architecture cible et justification des choix techniques*

15. Après-midi (3 h 30) - Sécurité des échanges et cryptographie

- Principes : chiffrement symétrique/asymétrique, hachage, signature, certificats
- Protocoles sécurisés : TLS/SSL, SSH, IPsec, S/MIME, PGP
- Gestion du cycle de vie des clés et des certificats
- 💡 *Génération de clés, chiffrement et signature de fichiers, configuration d'un tunnel SSH et d'un certificat TLS*
- 💡 *Évaluation finale : QCM + restitution orale des architectures conçues*

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible .