Sécurité systèmes et réseaux - Mise en oeuvre

Protéger efficacement matériel et données

★★★★★ **4,5/5 (24 avis)**

Présentiel ou en classe à distance

5 jours (35 h)
+ certificat optionnel

Prix inter : 3.390,00 € HT
Forfait intra : 8.890,00 € HT

Réf.: SR211



La protection des données de l'établissement passe par une politique de sécurité capable de résister à toutes menaces extérieures. Loin d'être un domaine spécifique, la sécurité doit être prise en compte aussi bien pour les équipements réseaux que pour les systèmes. Même s'il n'est pas un expert, l'administrateur ne doit pas ignorer les risques encourus et doit être capable de mettre en oeuvre une architecture de sécurité répondant aux exigences de l'entreprise et l'organisation.
Cette formation prépare à la certification Mettre en oeuvre un réseau local TCP/IP.

A qui s'adresse cette formation ?

- 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

- Avoir suivi la formation "Pratique des réseaux" (SR200) et "Soyez autonome avec TCP/IP" (SR230) ou connaissances équivalentes
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

Pendant

1 - L'environnement

- Le périmètre (réseaux, systèmes d'exploitation, applications)
- Les acteurs (hacker, responsable sécurité, auditeur, vendeur et éditeur, sites de sécurité)
- Les risques
- La protection
- La prévention
- La détection

2 - Les attaques

- Les intrusions de niveau 2 : au niveau du commutateur d'accès ou du point d'accès sans-fil
- Les intrusions de niveau 3 (IP) : IP spoofing, déni de service, scanSniffer, man-in-the-middle, les applications stratégiques (DHCP, DNS, SMTP), les applications à risques (HTTP)
- Les attaques logiques : virus, ver, cheval de Troie, spyware, phishing, le craquage de mot de passe
- Les attaques applicatives : sur le système d'exploitation ou sur les applications (buffer overflow)

3 - Les protections

- Au niveau des commutateurs d'accès : port sécurisé sur mac-adresse, utilisation du protocole 802.1x, VLAN Hopping, DHCP Snooping, IP source guard, ARP spoofing, filtre BPDU, root guard
- Au niveau sans-fil : mise en place d'une clé WEP, de WPA, de WPA 2 (802.1i)
- Au niveau IP : les pares-feux applicatifs, spécialisés, sur routeur, state full (inspection des couches au-dessus de 3), les UTM, les proxys
- Protection des attaques logiques : les anti-virus, les anti spyware, le concept NAC
- Protection des attaques applicatives : hardening des plates-formes Microsoft et Unix, validations des applicatifs

4 - Monitoring et prévention

- Sondes IDS
- SysLog Serveur
- Exploitations des logs
- IPS : boîtiers dédiés, fonctionnalité du routeur

5 - Exemples d'architectures

- Exemple d'une entité mono-site
- Connexion des nomades
- Exemple entité multi-site

6 - La sécurité des échanges, la cryptographie

- L'objectif du cryptage et fonctions de base
- Les algorithmes symétriques
- Les algorithmes asymétriques
- Les algorithmes de hashing
- Les méthodes d'authentification (pap, chap, Kerberos)
- Le HMAC et la signature électronique
- Les certificats et la PKI
- Les protocoles SSL IPSEC S/MIME
- Les VPN (réseau privé virtuel) site à site et nomades



Les objectifs de la formation

- 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



Certificat

Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.



Les points forts de la formation

- Une formation très pratique : les participants sont amenés à mettre en oeuvre la sécurité d'un réseau d'entreprise des secteurs privé et public et à travers de nombreux TP.
- Un point précis sur les obligations légales en termes de sécurité.
- Le passage en revue des solutions disponibles sur le marché.
- 85% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.

Evaluation

Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Dates et villes 2027 - Référence SR211

Dernières places disponibles Session garantie

A distance

du 1 févr. au 5 févr.	du 13 sept. au 17 sept.
du 7 juin au 11 juin	du 15 nov. au 19 nov.

Paris

du 1 févr. au 5 févr.	du 13 sept. au 17 sept.
du 7 juin au 11 juin	du 15 nov. au 19 nov.