Formation Sécurité systèmes et réseaux, niveau 2

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Ce stage avancé vous permettra de mesurer le niveau de sécurité de votre système d'information au moyen d'outils de détection d'intrusions, de détection de vulnérabilités, d'audit... Il vous apportera la connaissance de solutions avancées pour maintenir et faire évoluer dans le temps le niveau de sécurité souhaité au regard de vos besoins. Les travaux pratiques proposés permettront d'acquérir les compétences nécessaires à l'installation, la configuration et l'administration des applications les plus utilisées dans le domaine de la sécurité.

Référence	SEA
Durée	4 jours (28h)
Tarif	2 790 €HT
Repas	repas inclus

Objectifs

| Mesurer le niveau de sécurité de votre système d'information
| Utiliser des outils de détection d'intrusions, de détection de vulnérabilités et d'audit
| Renforcer la sécurité de votre système d'information
| Mettre en oeuvre une architecture AAA (Authentication, Autorization, Accounting)
| Mettre en oeuvre SSL/TLS

Public

| Responsable, architecte sécurité.
| Techniciens et administrateurs systèmes et réseaux.

Prérequis

| Bonnes connaissances de TCP/IP et de la sécurité des réseaux d'entreprise.
| Ou connaissances équivalentes à celles apportées par le stage "Sécurité systèmes et réseaux, niveau 1" (FRW).

Programme de la formation

Rappels
| Le protocole TCP/IP.
| La translation d'adresses.
| L'architecture des réseaux.
| Le firewall : avantages et limites.
| Les proxys, reverse-proxy : la protection applicative.
| Les zones démilitarisées (DMZ).

Les outils d'attaque
| Paradigmes de la sécurité et classification des attaques.
| Principes des attaques : spoofing, flooding, injection, capture, etc.
| Librairies : Libnet, Libpcap, Winpcap, Libbpf, Nasl, lua.
| Outils : Scapy, Hping, Ettercap, Metasploit, Dsnif, Arpspoof, Smurf.
| Travaux pratiques : Analyse de protocoles avec Wireshark. Utilisation de Scapy et Arpspoof.

La cryptographie, application
| Les services de sécurité.
| Principes et algorithmes cryptographique (DES, 3DES, AES, RC4, RSA, DSA, ECC).
| Certificats et profils spécifiques pour les divers serveurs et clients (X509).
| Protocole IPSEC et réseaux privés virtuels (VPN).

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 9 au 12 juillet 2024
PARIS
du 2 au 5 juillet 2024
AIX-EN-PROVENCE
du 9 au 12 juillet 2024
BORDEAUX
du 9 au 12 juillet 2024
LILLE
du 9 au 12 juillet 2024
LYON
du 9 au 12 juillet 2024
NANTES
du 9 au 12 juillet 2024
SOPHIA-ANTIPOLIS
du 9 au 12 juillet 2024
STRASBOURG
du 9 au 12 juillet 2024
TOULOUSE
du 9 au 12 juillet 2024

VOIR TOUTES LES DATES

| Protocoles SSL/TLS et VPN-SSL. Problématiques de compression des données.
| Travaux pratiques : Prise en main d'openssl et mise en oeuvre d'OpenPGP.
Génération de certificats X509 v3.

Architecture AAA (Authentication, Autorization, Accounting)
| Le réseau AAA : authentification, autorisation et traçabilité.
| One Time Password : OTP, HOTP, Google Authentificator, SSO (Protocole Kerberos).
| La place de l'annuaire LDAP dans les solutions d'authentification.
| Les module PAM et SASL.
| Architecture et protocole Radius (Authentication, Autorization, Accounting).
| Les attaques possibles.
| Comment se protéger.
| Travaux pratiques : Attaque d'un serveur AAA.

Détecter les intrusions
| Les principes de fonctionnement et méthodes de détection.
| Les acteurs du marché, panorama des systèmes et applications concernés.
| Les scanners réseaux (nmap) et applicatifs (web applications).
| Les IDS (Intrusion Detection System).
| Les avantages de ces technologies, leurs limites.
| Comment les placer dans l'architecture d'entreprise.
| Panorama du marché, étude détaillé de SNORT.
| Travaux pratiques : Installation, configuration et mise oeuvre de SNORT, écriture de signature d'attaques.

Vérifier l'intégrité d'un système
| Les principes de fonctionnement.
| Quels sont les produits disponibles.
| Présentation de Tripwire ou AIDE (Advanced Intrusion Detection Environment).
| L'audit de vulnérabilités.
| Principes et méthodes et organismes de gestion des vulnérabilités.
| Site de référence et panorama des outils d'audit.
| Définition d'une politique de sécurité.
| Etude et mise en oeuvre de Nessus (état, fonctionnement, évolution).
| Travaux pratiques : Audit de vulnérabilités du réseau et serveurs à l'aide de Nessus et Nmap. Audit de vulnérabilités d'un site Web.

Gérer les événements de sécurité.
| Traitement des informations remontées par les différents équipements de sécurité.
| La consolidation et la corrélation.
| Présentation de SIM (Security Information Management).
| Gestion et protocole SNMP : forces et faiblesses de sécurité.
| Solution de sécurité de SNMP.
| Travaux pratiques : Montage d'attaque SNMP.

La sécurité des réseaux Wi-Fi
| Comment sécuriser un réseau Wi-Fi ?
| Les faiblesses intrinsèques des réseaux Wi-Fi.
| Le SSID Broadcast, le MAC Filtering, quel apport ?
| Le WEP a-t-il encore un intérêt ?
| Le protocole WPA, première solution acceptable.
| Implémentation WPA en mode clé partagée, est-ce suffisant ?
| WPA, Radius et serveur AAA, l'implémentation d'entreprise.
| Les normes 802.11i et WPA2, quelle solution est la plus aboutie aujourd'hui ?
| Travaux pratiques : Configuration des outils pour la capture de trafic, scan de réseaux et analyse de trafic WIFI, injection de trafic, craquage de clés WIFI. Configuration d'un AP (Point d'acces) et mise oeuvre de solutions de sécurité.

La sécurité de la téléphonie sur IP
| Les concepts de la voix sur IP. Présentation des applications.
| L'architecture d'un système VoIP.
| Le protocole SIP, standard ouvert de voix sur IP.
| Les faiblesses du protocole SIP.
| Les problématiques du NAT.
| Les attaques sur la téléphonie sur IP.
| Quelles sont les solutions de sécurité ?

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

La sécurité de la messagerie
| Architecture et fonctionnement de la messagerie.
| Les protocoles et accès à la messagerie (POP, IMAP, Webmail, SMTP, etc.).
| Problèmes et classifications des attaques sur la messagerie (spam, fishing, usurpation de l'identité, etc.).
| Les acteurs de lutte contre le SPAM.
| Les méthodes, architectures et outils de lutte contre le SPAM.
| Outils de collecte des adresses de messagerie.
| Les solutions mises en oeuvre contre le SPAM.

Méthode pédagogique

De très nombreux outils seront déployés par les participants. Sonde IDS SNORT, scan de vulnérabilité avec NESSUS, analyse et scan des réseaux avec ETHEREAL et NMAP. Sécurisation d'un réseau Wi-Fi.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.