Formation Sécurité systèmes et réseaux, niveau 1

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

Ce stage pratique vous montrera comment mettre en oeuvre les principaux moyens de sécurisation des systèmes et des réseaux. Après avoir étudié quelques menaces pesant sur le système d'information, vous apprendrez le rôle des divers équipements de sécurité dans la protection de l'entreprise afin d'être en mesure de concevoir une architecture de sécurité et de réaliser sa mise en oeuvre.

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

Objectifs

| Connaître les failles et les menaces des systèmes d'information
| Maîtriser le rôle des divers équipements de sécurité
| Concevoir et réaliser une architecture de sécurité adaptée
| Mettre en oeuvre les principaux moyens de sécurisation des réseaux
| Utiliser des outils de détection de vulnérabilités : scanners, sondes IDS
| Sécuriser un système Windows et Linux

Public

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

Prérequis

| Bonnes connaissances en réseaux et systèmes.

Programme de la formation

Risques et menaces
| Introduction à la sécurité.
| Etat des lieux de la sécurité informatique.
| Le vocabulaire de la sécurité informatique.
| Attaques "couches basses".
| Forces et faiblesses du protocole TCP/IP.
| Illustration des attaques de type ARP et IP Spoofing, TCP-SYNflood, SMURF, etc.
| Déni de service et déni de service distribué.
| Attaques applicatives.
| Intelligence gathering.
| HTTP, un protocole particulièrement exposé (SQL injection, Cross Site Scripting, etc.).
| DNS : attaque Dan Kaminsky.
| Travaux pratiques : Installation et utilisation de l'analyseur réseau Wireshark. Mise en oeuvre d'une attaque applicative.

Architectures de sécurité
| Quelles architectures pour quels besoins ?
| Plan d'adressage sécurisé : RFC 1918.
| Translation d'adresses (FTP comme exemple).
| Le rôle des zones démilitarisées (DMZ).
| Exemples d'architectures.
| Sécurisation de l'architecture par la virtualisation.
| Firewall : pierre angulaire de la sécurité.
| Actions et limites des firewalls réseaux traditionnels.

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
- du 28 au 31 mai 2024
- du 16 au 19 juillet 2024

PARIS
- du 21 au 24 mai 2024
- du 9 au 12 juillet 2024

AIX-EN-PROVENCE
- du 28 au 31 mai 2024
- du 10 au 13 septembre 2024

BORDEAUX
- du 28 au 31 mai 2024
- du 10 au 13 septembre 2024

GRENOBLE
- du 28 au 31 mai 2024
- du 10 au 13 septembre 2024

LILLE
- du 28 au 31 mai 2024
- du 10 au 13 septembre 2024

LYON
- du 28 au 31 mai 2024
- du 10 au 13 septembre 2024

NANTES
- du 28 au 31 mai 2024
- du 10 au 13 septembre 2024

VOIR TOUTES LES DATES

| Evolution technologique des firewalls (Appliance, VPN, IPS, UTM...).
| Les firewalls et les environnements virtuels.
| Proxy serveur et relais applicatif.
| Proxy ou firewall : concurrence ou complémentarité ?
| Reverse proxy, filtrage de contenu, cache et authentification.
| Relais SMTP, une obligation ?
| Travaux pratiques : Mise en oeuvre d'un proxy Cache/Authentification.

Sécurité des données
| Cryptographie.
| Chiffrements symétrique et asymétrique. Fonctions de hachage.
| Services cryptographiques.
| Authentification de l'utilisateur.
| L'importance de l'authentification réciproque.
| Certificats X509. Signature électronique. Radius. LDAP.
| Vers, virus, trojans, malwares et keyloggers.
| Tendances actuelles. L'offre antivirale, complémentarité des éléments. EICAR, un "virus" à connaître.
| Travaux pratiques : Déploiement d'un relais SMTP et d'un proxy HTTP/FTP Antivirus. Mise en oeuvre d'un certificat serveur.

Sécurité des échanges
| Sécurité Wi-Fi.
| Risques inhérents aux réseaux sans fil.
| Les limites du WEP. Le protocole WPA et WPA2.
| Les types d'attaques.
| Attaque Man in the Middle avec le rogue AP.
| Le protocole IPSec.
| Présentation du protocole.
| Modes tunnel et transport. ESP et AH.
| Analyse du protocole et des technologies associées (SA, IKE, ISAKMP, ESP, AH...).
| Les protocoles SSL/TLS.
| Présentation du protocole. Détails de la négociation.
| Analyse des principales vulnérabilités.
| Attaques sslstrip et sslsnif.
| Le protocole SSH. Présentation et fonctionnalités.
| Différences avec SSL.
| Travaux pratiques : Réalisation d'une attaque Man in the Middle sur une session SSL. Mise en oeuvre d'IPSec mode transport/PSK.

Sécuriser un système, le "Hardening"
| Présentation.
| Insuffisance des installations par défaut.
| Critères d'évaluation (TCSEC, ITSEC et critères communs).
| Sécurisation de Windows.
| Gestion des comptes et des autorisations.
| Contrôle des services.
| Configuration réseau et audit.
| Sécurisation de Linux.
| Configuration du noyau.
| Système de fichiers.
| Gestion des services et du réseau.
| Travaux pratiques : Exemple de sécurisation d'un système Windows et Linux.

Audit et sécurité au quotidien
| Les outils et techniques disponibles.
| Tests d'intrusion : outils et moyens.
| Détection des vulnérabilités (scanners, sondes IDS, etc.).
| Les outils de détection temps réel IDS-IPS, agent, sonde ou coupure.
| Réagir efficacement en toutes circonstances.
| Supervision et administration.
| Impacts organisationnels.
| Veille technologique.

Etude de cas
| Etude préalable.
| Analyse du besoin.
| Elaborer une architecture.
| Définir le plan d'action.

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

| Déploiement.
| Démarche pour installer les éléments.
| Mise en oeuvre de la politique de filtrage.
| Travaux pratiques : Elaboration d'une maîtrise de flux.

Méthode pédagogique

Mise en oeuvre d'une solution de proxy HTTP sous Windows ou Linux, d'une solution antivirale sur les flux réseaux. Conception et mise en oeuvre d'une architecture multi-firewalls, multi-DMZ. Mise en oeuvre des techniques fondamentales de sécurisation du système d'exploitation.

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.