Formation Détection d'intrusions

comment gérer les incidents de sécurité

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

Cette formation à la fois théorique et pratique présente les techniques d'attaque les plus évoluées à ce jour et montre comment y faire face. A partir d'attaques réalisées sur cibles identifiées (serveurs Web, clients, réseaux, firewall, bases de données...), le participant apprendra à déclencher la riposte adaptée (filtrage d'anti-trojan, filtrage d'URL mal formée, détection de spam et détection d'intrusion en temps réel avec sonde IDS).

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

Objectifs

| Identifier les techniques d'analyse et de détection
| Déployer différents outils de détection d'intrusion
| Mettre en oeuvre les solutions de prévention et de détection d'intrusions
| Gérer un incident d'intrusion
| Utiliser le cadre juridique

Public

| Responsables, architectes sécurité.
| Techniciens et administrateurs systèmes et réseaux.

Prérequis

| Bonnes connaissances des réseaux TCP/IP.
| Connaissances de base en sécurité informatique.

Programme de la formation

Le monde de la sécurité informatique
| Définitions "officielles" : le hacker, le hacking.
| La communauté des hackers dans le monde, les "gurus", les "script kiddies".
| L'état d'esprit et la culture du hacker.
| Les conférences et les sites majeurs de la sécurité.
| Travaux pratiques : Navigation Underground. Savoir localiser les informations utiles.

TCP/IP pour firewalls et détection d'intrusions
| IP, TCP et UDP sous un autre angle.
| Zoom sur ARP et ICMP.
| Le routage forcé de paquets IP (source routing).
| La fragmentation IP et les règles de réassemblage.
| De l'utilité d'un filtrage sérieux.
| Sécuriser ses serveurs : un impératif.
| Les parades par technologies : du routeur filtrant au firewall stateful inspection ; du proxy au reverse proxy.
| Panorama rapide des solutions et des produits.
| Travaux pratiques : Visualisation et analyse d'un trafic classique. Utilisation de différents sniffers.

Comprendre les attaques sur TCP/IP
| Le "Spoofing" IP.

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 16 au 19 juillet 2024

PARIS
du 9 au 12 juillet 2024

AIX-EN-PROVENCE
du 16 au 19 juillet 2024

BORDEAUX
du 16 au 19 juillet 2024

LILLE
du 16 au 19 juillet 2024

LYON
du 16 au 19 juillet 2024

NANTES
du 16 au 19 juillet 2024

SOPHIA-ANTIPOLIS
du 16 au 19 juillet 2024

STRASBOURG
du 16 au 19 juillet 2024

TOULOUSE
du 16 au 19 juillet 2024

VOIR TOUTES LES DATES

| Attaques par déni de service.
| Prédiction des numéros de séquence TCP.
| Vol de session TCP : Hijacking (Hunt, Juggernaut).
| Attaques sur SNMP.
| Attaque par TCP Spoofing (Mitnick) : démystification.
| Travaux pratiques : Injection de paquets fabriqués sur le réseau. Utilisation au choix des participants d'outils graphiques, de Perl, de C ou de scripts dédiés.
Hijacking d'une connexion telnet.

Intelligence Gathering : l'art du camouflage
| Chercher les traces : interrogation des bases Whois, les serveurs DNS, les moteurs de recherche.
| Identification des serveurs.
| Comprendre le contexte : analyser les résultats, déterminer les règles de filtrage, cas spécifiques.
| Travaux pratiques : Recherche par techniques non intrusives d'informations sur une cible potentielle (au choix des participants). Utilisation d'outils de scans de réseaux.

Protéger ses données
| Systèmes à mot de passe "en clair", par challenge, crypté.
| Le point sur l'authentification sous Windows.
| Rappels sur SSH et SSL (HTTPS).
| Sniffing d'un réseau switché : ARP poisonning.
| Attaques sur les données cryptées : "Man in the Middle" sur SSH et SSL, "Keystoke Analysis" sur SSH.
| Détection de sniffer : outils et méthodes avancées.
| Attaques sur mots de passe.
| Travaux pratiques : Décryptage et vol de session SSH : attaque "Man in the Middle". Cassage de mots de passe avec LophtCrack (Windows) et John The Ripper (Unix).

Détecter les trojans et les backdoors
| Etat de l'art des backdoors sous Windows et Unix.
| Mise en place de backdoors et de trojans.
| Le téléchargement de scripts sur les clients, exploitation de bugs des navigateurs.
| Les "Covert Channels" : application client-serveur utilisant ICMP.
| Exemple de communication avec les Agents de Déni de Service distribués.
| Travaux pratiques : Analyse de Loki, client-serveur utilisant ICMP. Accéder à des informations privées avec son navigateur.

Défendre les services en ligne
| Prise de contrôle d'un serveur : recherche et exploitation de vulnérabilités.
| Exemples de mise en place de "backdoors" et suppression des traces.
| Comment contourner un firewall (netcat et rebonds) ?
| La recherche du déni de service.
| Les dénis de service distribués (DDoS).
| Les attaques par débordement (buffer overflow).
| Exploitation de failles dans le code source. Techniques similaires : "Format String", "Heap Overflow".
| Vulnérabilités dans les applications Web.
| Vol d'informations dans une base de données.
| Les RootKits.
| Travaux pratiques : Exploitation du bug utilisé par le ver "Code Red". Obtention d'un shell root par différents types de buffer overflow. Test d'un déni de service (Jolt2, Ssping). Utilisation de netcat pour contourner un firewall. Utilisation des techniques de "SQL Injection" pour casser une authentification Web.

Comment gérer un incident ?
| Les signes d'une intrusion réussie dans un SI.
| Qu'ont obtenu les hackers ? Jusqu'où sont-ils allés ?
| Comment réagir face à une intrusion réussie ?
| Quels serveurs sont concernés ?
| Savoir retrouver le point d'entrée et le combler.
| La boîte à outils Unix/Windows pour la recherche de preuves.
| Nettoyage et remise en production de serveurs compromis.

Conclusion : quel cadre juridique ?
| La réponse adéquate aux hackers.
| La loi française en matière de hacking.
| Le rôle de l'Etat, les organismes officiels.
| Qu'attendre de l'Office Central de Lutte contre la Criminalité (OCLCTIC) ?
| La recherche des preuves et des auteurs.
| Et dans un contexte international ?

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

| Le test intrusif ou le hacking domestiqué ?
| Rester dans un cadre légal, choisir le prestataire, être sûr du résultat.

Méthode pédagogique

Des architectures sécurisées et "normalement " protégées (firewall multi-DMZ, applications sécurisées) seront la cible des attaques.

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.