Formation Hacking et sécurité, niveau 1

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

Cette formation avancée vous apprendra les techniques indispensables pour mesurer le niveau de sécurité de votre Système d'Information. A la suite de ces attaques, vous apprendrez à déclencher la riposte appropriée et à élever le niveau de sécurité de votre réseau.

Référence	HAC
Durée	5 jours (35h)
Tarif	3 530 €HT
Repas	repas inclus

Objectifs

| Définir les techniques des pirates informatiques et pouvoir contrer leurs attaques
| Mesurer le niveau de sécurité de votre Système d'Information
| Réaliser un test de pénétration
| Définir l'impact et la portée d'une vulnérabilité

Public

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

Prérequis

| Bonnes connaissances en sécurité SI, réseaux, systèmes (en particulier Linux) et en programmation.
| Ou connaissances équivalentes à celles du stage "Sécurité systèmes et réseaux, niveau 1".

Programme de la formation

Le Hacking et la sécurité
| Formes d'attaques, modes opératoires, acteurs, enjeux.
| Audits et tests d'intrusion, place dans un SMSI.

Sniffing, interception, analyse, injection réseau
| Anatomie d'un paquet, tcpdump, Wireshark, tshark.
| Détournement et interception de communications (Man-in-the-Middle, attaques de VLAN, les pots de miel).
| Paquets : Sniffing, lecture/analyse à partir d'un pcap, extraction des donnés utiles, représentations graphiques.
| Scapy : architecture, capacités, utilisation.
| Travaux pratiques : Ecouter le réseau avec des sniffers. Réaliser un mini intercepteur de paquets en C. Utiliser scapy (ligne de commande, script python) : injections, interception, lecture de pcap, scan, DoS, MitM.

La reconnaissance, le scanning et l'énumération
| L'intelligence gathering, le hot reading, l'exploitation du darknet, l'Ingénierie Sociale.
| Reconnaissance de service, de système, de topologie et d'architectures.
| Types de scans, détection du filtrage, firewalking, fuzzing.
| Le camouflage par usurpation et par rebond, l'identification de chemins avec traceroute, le source routing.
| L'évasion d'IDS et d'IPS : fragmentations, covert channels.
| Nmap : scan et d'exportation des résultats, les options.
| Les autres scanners : Nessus, OpenVAS.
| Travaux pratiques : Utilisation de l'outil nmap, écriture d'un script NSE en LUA.

SESSIONS PROGRAMMÉES

PARIS

du 4 au 8 novembre 2024*
du 6 au 10 janvier 2025
du 3 au 7 février 2025
du 7 au 11 avril 2025
du 12 au 16 mai 2025
du 7 au 11 juillet 2025
du 22 au 26 septembre 2025
du 13 au 17 octobre 2025
du 1er au 5 décembre 2025

VOIR TOUTES LES DATES

(*) session confirmée

Détection du filtrage.

Les attaques Web
| OWASP : organisation, chapitres, Top10, manuels, outils.
| Découverte de l'infrastructure et des technologies associées, forces et faiblesses.
| Côté client : clickjacking, CSRF, vol de cookies, XSS, composants (flash, java). Nouveaux vecteurs.
| Côté serveur : authentification, vol de sessions, injections (SQL, LDAP, fichiers, commandes).
| Inclusion de fichiers locaux et distants, attaques et vecteurs cryptographiques.
| Évasion et contournement des protections : exemple des techniques de contournement de WAF.
| Outils Burp Suite, ZAP, Sqlmap, BeEF.
| Travaux pratiques : Mise en oeuvre de différentes attaques Web en conditions réelles côté serveur et côté client.

Les attaques applicatives et post-exploitation
| Attaque des authentifications Microsoft, PassTheHash.
| Du C à l'assembleur au code machine. Les shellcodes.
| L'encodage de shellcodes, suppression des NULL bytes.
| Les Rootkits. Exploitations de processus: Buffer Overflow, ROP, Dangling Pointers.
| Protections et contournement: Flag GS, ASLR, PIE, RELRO, Safe SEH, DEP. Shellcodes avec adresses hardcodées/LSD.
| Metasploit : architecture, fonctionnalités, interfaces, workspaces, écriture d'exploit, génération de Shellcodes.
| Travaux pratiques : Metasploit : exploitation, utilisation de la base de données. Msfvenom : génération de Shellcodes, piégeage de fichiers. Buffer overflow sous Windows ou Linux, exploitation avec shellcode Meterpreter.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

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.

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.