Hacking et Sécurité

Programme *(Mis à jour le 21/11/2024)*

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.
- Ateliers et Travaux pratiques

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.
- Ateliers et Travaux pratiques

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.
- Ateliers et Travaux pratiques

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.
- Ateliers et Travaux pratiques

Référence

THIS3298

Durée

5 jours / 35 heures

Prix HT / stagiaire

3550€

Objectifs pédagogiques

- Comprendre 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

Niveau requis

- Bonnes connaissances en sécurité SI, réseaux, systèmes (en particulier Linux) et en programmation

Public concerné

- Administrateurs, développeurs et de manière générale à tous ceux qui veulent renforcer leur connaissance sur les vulnérabilités des systèmes d'informations
- Responsables, architectes sécurité, techniciens et administrateurs systèmes et réseaux.

Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

Conditions d'accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

Moyens pédagogiques et techniques

Salles de formation (les personnes en situation de handicap peuvent avoir des besoins spécifiques pour suivre la formation. N'hésitez pas à nous contacter pour en discuter) équipée d'un ordinateur de dernière génération par stagiaire, réseau haut débit et vidéo-projection UHD
Documents supports de formation projetés
Apports théoriques, étude de cas concrets et exercices
Mise à disposition en ligne de documents supports à la suite de la formation

Dispositif de suivi de l'éxécution de l'évaluation des résultats de la formation

Feuilles d'émargement (signature électronique privilégiée)
Evaluations formatives et des acquis sous forme de questions orales et/ou écrites (QCM)