Hacking et sécurité, niveau 1

Cours Pratique de 5 jours
Réf : HAC - Prix 2022 : 3 390€ HT

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.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

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

LE PROGRAMME

dernière mise à jour : 06/2019

1) Le Hacking et la sécurité

- Formes d'attaques, modes opératoires, acteurs, enjeux.
- Audits et tests d'intrusion, place dans un SMSI.

2) 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.

3) 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. Détection du filtrage.

4) Les attaques Web

- OWASP : organisation, chapitres, Top10, manuels, outils.
- Découverte de l'infrastructure et des technologies associées, forces et faiblesses.

PARTICIPANTS

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" (réf. FRW).

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- 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 œuvre de différentes attaques Web en conditions réelles côté serveur et côté client.

5) 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.

LES DATES

BREST
2022 : 03 oct.

AIX-EN-PROVENCE
2022 : 05 sept., 21 nov.

BRUXELLES
2022 : 05 sept., 14 nov.

GRENOBLE
2022 : 19 sept., 21 nov.

LUXEMBOURG
2022 : 05 sept., 14 nov.

NANCY
2022 : 21 nov.

ORLÉANS
2022 : 05 sept., 14 nov.

RENNES
2022 : 03 oct., 14 nov.

STRASBOURG
2022 : 03 oct., 14 nov.

TOURS
2022 : 05 sept., 14 nov.

MARSEILLE
2022 : 21 nov.

ANGERS
2022 : 17 oct.

DIJON
2022 : 21 nov.

LILLE
2022 : 05 sept., 14 nov.

LYON
2022 : 19 sept., 21 nov.

NANTES
2022 : 03 oct., 14 nov.

PARIS LA DÉFENSE
2022 : 05 sept., 17 oct., 14 nov., 05 déc.

ROUEN
2022 : 17 oct.

TOULON
2022 : 21 nov.

METZ
2022 : 21 nov.

CLERMONT-FERRAND
2022 : 21 nov.

BORDEAUX
2022 : 17 oct., 05 déc.

GENÈVE
2022 : 05 sept., 14 nov.

LIMOGES
2022 : 17 oct.

MONTPELLIER
2022 : 05 sept., 21 nov.

NIORT
2022 : 17 oct.

REIMS
2022 : 17 oct.

SOPHIA-ANTIPOLIS
2022 : 05 sept., 21 nov.

TOULOUSE
2022 : 17 oct., 05 déc.

MULHOUSE
2022 : 03 oct.

CLASSE A DISTANCE
2022 : 05 sept., 17 oct., 21 oct., 14 nov., 05 déc.