Hacking et sécurité avec CyberRange

Cours Pratique de 5 jours - 35h
Réf : HCR - Prix 2024 : 3 530CHF HT

Cette formation avancée vous apprendra les techniques indispensables pour mesurer le niveau de sécurité de votre système d'information. À 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

TRAVAUX PRATIQUES

La CyberRange d'Airbus CyberSecurity est utilisée pour réaliser et jouer des scénarios réalistes comprenant de véritables cyber-attaques.

LE PROGRAMME

dernière mise à jour : 02/2020

1) Le hacking et la sécurité

- Formes d'attaques.
- Modes opératoires.
- Acteurs, enjeux.

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.
- Les scénarios et outils disponibles sur CyberRange.

Travaux pratiques : Écouter le réseau avec des sniffers. Utiliser scapy (ligne de commande, script python) : injections, interception, lecture de pcap, scan, DoS, man-in-the-middle (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.
- Les scénarios et les outils disponibles sur CyberRange.

Travaux pratiques : Utilisation de l'outil nmap et détection du filtrage sur la plateforme CyberRange.

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 cours "Sécurité systèmes et réseaux" (réf. SCR).

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.

4) 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.
- Les scénarios disponibles sur CyberRange.

Travaux pratiques : Mise en œuvre de différentes attaques web en conditions réelles côté serveur et côté client avec CyberRange.

5) Les attaques applicatives

- Metasploit : architecture, fonctionnalités, interfaces, workspaces.
- Écriture d'exploit, génération de shellcodes.

LES DATES

CLASSE À DISTANCE
2024 : 01 juil., 07 oct., 16 déc.