CATALOGUE FORMATIONS 2019

SENSIBILISATION

AW1.01 – SENSIBILISATION UTILISATEURS

- N/A
- 2 heures
- FR/EN

Les mesures de sécurité les plus complexes peuvent généralement être déjouées en attaquant le maillon le plus faible de la sécurité de votre système d'information : l'utilisateur. Cette formation, basée sur des démonstrations et exemples concrets, vise à donner les bons réflexes aux utilisateurs (social engineering, code malveillant, réseaux sociaux, utilisateurs nomades, équipements mobiles, attaques de type MiTM, …) .

AW1.02 – SENSIBILISATION DEVELOPPEURS (OWASP TOP 10)

- Connaissances en programmation (développeurs)
- 1/2 journée
- FR

Découvrez le TOP10 des risques OWASP, les conseils et solutions pour les réduire, ainsi qu'une série d'exemples et conseils adaptés aux langages utilisés par vos équipes (PHP, Java, C, ...).

FORENSICS

FOR1.01 – RÉPONSE À INCIDENTS – NIV. 1

- N/A
- 1 journée
- FR

Cette formation vise à présenter les méthodes et outils à utiliser afin d'investiguer un incident de sécurité. Les thèmes abordés inclus l'acquisition de disques durs, la récupération d'informations, la création de chronologies d'événements. Cette formation intensive est essentiellement pratique avec de nombreux labs basés sur des outils gratuits. Elle introduit toutes les notions de base indispensables à la compréhension du forensic de systèmes Windows.

FOR2.01 – POLITIQUE DE GESTION D'INCIDENTS

- N/A
- 1/2 journée
- FR

La réponse à incidents ne se joue pas uniquement sur des outils et des techniques. Une grande partie se réalise en amont en préparant les procédures et en connaissant les actions à réaliser. Cette formation a pour but de présenter les bonnes pratiques concernant la gestion d'incident ainsi que des recommandations face à différents scénarios.

FOR1.02 – RÉPONSE À INCIDENTS – NIV. 2

- *FOR1.01 - Réponse à incidents – Niv.1* (ou connaissances équivalentes)
- 1 journée
- FR

Cette formation vise à présenter les méthodes et outils à utiliser afin d'investiguer un incident de sécurité. Elle fait suite à la formation Niveau 1 et aborde des techniques avancées telles que la résurrection de systèmes Windows à partir d'images de disques durs et l'analyse de la mémoire vive. Cette formation intensive est essentiellement pratique avec de nombreux labs basés sur des outils gratuits et commerciaux. Elle est axée sur des études de cas complètes et sur une approche professionnelle du forensic de systèmes Windows.

SCRT Information Security
LE TRÉSI 6
1028 PRÉVERENGES
INFO@SCRT.CH
T +41 21 802 64 01
F +41 21 802 64 02
WWW.SCRT.CH

HACKING

HA1.01 – ATTAQUE D'APPLICATIONS WEB – PARTIE 1

- N/A
- 1 journée
- FR

Ce cours a pour but de préparer le participant à pouvoir non seulement tester la sécurité d'une application Web, mais également de corriger les failles les plus couramment rencontrées. La méthodologie d'analyse d'un site Web est développée en se concentrant tout d'abord sur l'identification des systèmes et des points d'entrées, puis sur l'exploitation de failles comme les injections SQL ou le Cross-Site Scripting. Il s'agit avant tout d'un cours pratique où les participants peuvent exploiter les failles discutées afin de bien comprendre leur fonctionnement et ainsi protéger au mieux leurs propres applications.

HA1.02 – ATTAQUE D'APPLICATIONS WEB – PARTIE 2

- *HA1.01 – Attaque d'applications web – Niv. 1* (ou connaissances équivalentes)
- 1 journée
- FR

Ce cours est une suite logique du cours «*HA1.01 – Attaque d'applications web – Niv. 1*». Il reprend certains concepts en les poussant plus loin pour montrer que l'exploitation d'une faille permet souvent non seulement de compromettre une application, mais dans certains cas, toute l'infrastructure l'hébergeant. Le cours analyse autant des attaques côté serveur, tels que les XML eXternal Entites, les Local File Inclusion ou autres problèmes de chiffrement faible, que des attaques côté client visant à contourner la «Same Origin Policy» du navigateur.

HA2.01 – ATTAQUE D'ENVIRONNEMENTS WINDOWS AVEC METASPLOIT

- N/A
- 1 journée
- FR

Cette formation présente les caractéristiques du modèle de sécurité des systèmes Windows ainsi que les attaques les plus courantes contre les environnements d'entreprise. Des démonstrations et des exercices permettent aux participants de mieux comprendre le fonctionnement de ces attaque et – par extension – comment s'en protéger efficacement.

HA3.01 – EXPLOITATION DE CORRUPTION MEMOIRE SUR LINUX

- Bonnes connaissances en systèmes Linux. Bases de programmation en langages C et assembleur (x86).
- 1 journée
- FR

Cette formation permet d'obtenir de solides bases en exploitation de corruption mémoire sur un système Linux 32bits. Elle commence par une introduction de l'assembleur x86 et le développement de *shellcode* et se termine par la création de chaînes ROP en passant par les format string et les buffer overflows.

HA4.01 – ATTAQUE D'APPLICATION MOBILE

- N/A
- 1 journée
- FR

Ce cours a pour but de partager des expériences et des connaissances dans les audits d'applications mobiles sous Android et iOS. Cette formation présente des processus et des techniques de vérification aidant un participant à préparer un environnement de test idéal pour évaluer la sécurité d'une application. Entre autres, elle présente plusieurs méthodologies pour des tests de sécurité passant de l'analyse locale à l'inspection du trafic réseau d'une application. Ce cours fournit également plusieurs exemples d'automatisation de tâches fastidieuses qui interviennent dans la majorité des audits de sécurité mobile (contournement *root/jailbreak detection* ou *certificate pinning*).

INFRASTRUCTURE

IN1.01 - FORTINET (FORTIGATE)

- N/A
- 1 journée
- FR

Déploiement et administration d'équipements FortiGate de Fortinet. Cette formation fournit une base pour la préparation au premier niveau de certification Fortinet : FCNSA (Fortinet Certified Network Security Administrator).

IN1.02 - FORTIGATE AVANCÉ

- IN1.01 – Fortinet (ou connaissances équivalentes)
- 1 journée
- FR

Cette formation présente certaines fonctionnalités avancées des équipements FortiGate de Fortinet. Ce cours pratique met notamment l'accent sur les domaines tels que IPSec, Routage avancé (dynamique), IPv6, HA.

IN3.01 – PKI MICROSOFT

- Administration Windows
- 1 journée
- FR

Cette formation présente les fondamentaux de la mise en place d'une infrastructure PKI dans un environnement Microsoft Windows. Après avoir revu les bases concernant les certificats, la formation s'orientera sur la configuration et l'utilisation d'une PKI au travers de plusieurs cas concrets (Mise en place d'une PKI, la génération de certificats, l'authentification client et machine, l'administration,...). La pratique ne sera pas oubliée avec des démonstrations et des exercices dans des environnements virtualisés pour illustrer le tout.

IN4.01 – LOG MANAGEMENT

- N/A
- 1 journée
- FR

Cette formation présente les fondamentaux du log management et de son intégration. Elle regroupe les analyses forensiques, les mises en conformité avec les normes ISO27001, PCI-DSS, HIPAA ainsi que l'exploitation de logs pour le monitoring de service, le troubleshooting et la détection d'intrusion.

IN5.01 - SÉCURISATION LINUX 1

- Connaissances de base des systèmes Linux
- 1 journée
- FR

Basé sur les distributions GNU/Linux des familles RedHat et Debian. L'objectif de cette formation est de présenter un tour d'horizon des techniques de sécurisation existantes, des bonnes pratiques et des évolutions de celles-ci dans ces deux catégories d'OS Linux. L'usage de SELinux et des autres sous-systèmes MAC (Mandatory Access Control) est rapidement survolé, l'accent est mis sur les outils traditionnels et sur systemd.

IN5.02 - SÉCURISATION LINUX 2

- Connaissance avancée des systèmes Linux (LPIC-2)
- 1 journée
- FR

Basé sur la distribution CentOS7 (dérivée de RedHat). Cette formation présente le fonctionnement et l'utilisation du mode targeted de SELinux, notamment création et usage de policies custom. Sont aussi traités l'usage des cgroups et des conteneurs LXC, ainsi que le verrouillage des accès par firewalling. Un survol rapide présente le mode mls de SELinux et ses objectifs.