HACKING SECURITE
Expertise

Plan de cours N° : 1172
Durée : 4 jours (28h)

PARTICIPANTS / PRE-REQUIS
Toute personne souhaitant se sensibiliser aux risques d'attaque informatique et obtenir les outils pour assurer la sécurité informatique.

Connaissance des réseaux, routeurs, annuaires (Active Directory), langage de script.

OBJECTIFS PEDAGOGIQUES
Analyser les différentes étapes de la kill chain selon Lockheed Martin et leur application dans les attaques réelles. Maîtriser les frameworks PRE-ATT&CK et ATT&CK pour identifier et contrer les menaces. Utiliser les outils techniques pour les attaques sur les réseaux d'entreprise, y compris les outils de reconnaissance et de contrôle. Détailler les méthodes d'authentification et d'autorisation, et gérer les mots de passe dans Active Directory.. Identifier les vecteurs et phases d'infection des malwares, et mettre en place des techniques de protection efficaces. Identifier les méthodes de reconnaissance et d'exploitation des IoT, et comprendre les principes de la sécurité périmétrique et du Zero Trust.

MOYENS PEDAGOGIQUES
Tour de table au début de chaque formation pour définir les objectifs de chaque participant,
Alternance entre apports théoriques (en moyenne 30%) et exercices pratiques (en moyenne 70%),
Utilisation de cas concrets issus de l'expérience professionnelle de nos formateurs,
Remise d'un support de cours,
Assistance post-formation d'une durée de 1 an sur le contenu de la formation via notre adresse mail dédiée formateurs@atp-formation.com

MOYENS PERMETTANT LE SUIVI DE L'EXECUTION ET DES RESULTATS
Positionnement préalable oral ou écrit,
Evaluation des acquis tout au long de la formation par des exercices de synthèse,
Attestation de stage remise à chaque apprenant, avec son niveau d'acquisition pour chaque objectif pédagogique,
Feuille de présence signée par demi-journée,
Questionnaire de satisfaction pour évaluer la qualité de l'enseignement,
En option : passage certification possible selon les thématiques.

MOYENS TECHNIQUES EN PRESENTIEL
Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs récents et performants, d'un vidéo projecteur et d'un tableau blanc.

MOYENS TECHNIQUES DES CLASSES A DISTANCE
Grâce à un logiciel comme Teams, suivez une formation en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
Nous vous conseillons très fortement l'utilisation de votre webcam et de disposer d'un double écran.
Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par téléphone au 04.76.41.14.20.

ORGANISATION
Les cours ont lieu de 9h00-12h30 13h30-17h00 (adaptable à la demande).

PROFIL FORMATEUR
Nous recrutons méticuleusement nos formateurs selon 3 critères: expertise, pédagogie et agilité.

ACCESSIBILITE
Les personnes atteintes de handicap souhaitant suivre nos formations sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités d'organisation.

MISE A JOUR
18/07/2024

HACKING SECURITE
Expertise

Plan de cours N° : 1172
Durée : 4 jours (28h)

Explication des différentes étapes de la kill chain selon Lockheed Martin
- Les étapes institutionnelles
- Liens avec la réatlité des attaques

Présentation des frameworks MITRE
- Le framework PRE-ATT&CK
- Le framework ATT&CK

Schéma d'attaque de type APT ou Malware
- Les différentes étapes techniques d'une attaque sur un réseau d'entreprise
- Illustration par l'exemple

Exploration de l'outillage technique pour une attaque d'entreprise
- Les outils de reconnaissance externe
- Les outils de prise de possession du poste de travail
- Les outils de reconnaissance interne
- Les outils d'exploitations et de contrôle

Méthodes d'authentification et d'autorisation des annuaires
- Fonctionnement des protocoles d'authentification
- Fonctionnement des autorisations et compréhension du contrôle d'accès

Gestion des mots de passe dans les annuaires Active Directory
- Stockage des mots de passe
- Changement de mots de passe
- Politique de gestion des mots de passe

Focus sur le protocole KERBEROS

Focus sur le fonctionnement de la sécurité dans Active Directory
- Quels sont les points faibles ?
- Comment découvrir et exploiter les points faibles ?

Chemins d'attaque sur Active Directory par APT et Malwares

Introduction aux malwares
- Les vecteurs d'infection
- les phases d'infection

Techniques liées aux malwares
- Les formats de fichers
- Les API des windows
- Techniques de hooking

Quelles méthodes de protection ?
- Anti-phising
- Les anti virus et EDR

Usage des SIEMs dans la sécurité

Quelle place pour la sécurité périmétrique ?

Attaques sur les réseaux wifi

Attaques sur les applications web
- Les différentes méthodes d'attaque
- Quels points de contrôle ?

Sécurité des IoT et méthode de compromission
- Introduction à l'IoT

Sécurité des IoT et méthode de compromission
- Méthode de reconnaissance et d'exploitation sur les IoT

Introduction au Zero Trust