Formation Tests d'intrusion des systèmes industriels

Objectif

A l'issue de la formation, vous serez capable de :

- Comprendre le fonctionnement des SI industriels et leurs spécificités.
- Découvrir les outils et les méthodologies pour les tests d'intrusion sur SI industriel.
- Mettre en pratique ses connaissances sur un environnement industriel représentatif.

Programme

Introduction aux SI industriels

- Historique des SI industriels et de l'automatisme
- Vocabulaire
- Modèle CIM
- Architectures classiques
- Composants des SI industriels (PLC,HMI,SCADA,DCS,capteurs,effecteurs, RTU…)

Tests d'intrusion : principes & outillage

- Tests d'intrusion et autres méthodologies d'évaluation de la sécurité des SI industriels
- Différentes étapes et outil d'un test d'intrusion classique (notamment reconnaissance, exploitation, post-exploitation)
- Travaux pratiques : scans nmap, exploitation simple avec Metasploit

Sécurité des systèmes Windows et Active Directory

- Introduction aux environnements Windows et AD
    - Méthodes d'authentifications, format et stockage des mots de passe et secrets
    - Faiblesses classiques de ces environnements
    - Travaux pratiques : recherche d'informations dans un AD avec Powerview, utilisation de mots de passe et condensats avec crackmapexec…

Vulnérabilités courantes en environnement industriel

- Segmentation réseau
- Sécurité dans les protocoles
- Supervision Sécurité
- Sensibilisation
- Gestion des tiers
- Correctifs de sécurité

Protocoles de communication industriels

229 rue de Solferino, 59000 Lille – Tél.: +33 6 67 61 38 59– SIRET : 93995807000012 – www.activformation.fr – contact@activformation.fr
Numéro de déclaration d'activité : 32591326259 Code NAF :8559A

- Présentation des protocoles les plus courants (modbus tcp, S7, OPC…)
- Travaux pratiques : analyse de capture réseau Modbus/TCP, S7 et OPC-UA

Introduction à la sureté de fonctionnement

- Présentation du concept
- Méthodologies d'analyse de sureté fonctionnelle
- Différentes couches de sureté
- Travaux pratiques : ébauche d'analyse HAZOP sur un exemple simple

Programmation d'automates programmables industriels (API)

- Présentation des différents langages
- Travaux pratiques : Exercices de programmation en ladder logic sur simulateur Schneider TM221 et SCADA Schneider IGSS

Tests d'intrusion sur API

- Outils de communication pour les protocoles industriels
- Surface d'attaque des automates (web, ftp, http)
- Présentation d'attaques avancées sur les API (protocoles propriétaires, …)
- Travaux pratiques :
    - Utilisation de mbtget pour envoi de requêtes modbus sur simulateur Schneider, bibliothèque Snap 7 pour échanger avec simulateur Siemens, opcua-gui pour échanger avec SCADA Schneider IGSS

Principes de sécurisation des SI industriels

- Panel normatif
- Architectures et technologies de cloisonnement réseau
- Focus sur les diodes réseau
- Autres points d'attention particuliers

Étude de cas (laboratoire cyberange)

- Analyse d'une Étude de cas présentant une description d'une société fictive, des schémas réseau, ainsi que des règles de pare-feu.
- Travail collaboratif pour identifier vulnérabilités, risques, et élaboration de plan d'action

Exercice sous forme de CTF (Capture The Flag)

- Mise en pratique des acquis par la réalisation d'un test d'intrusion sur un environnement représentatif
    - Compromission d'un environnement bureautique
    - Découverte de liens réseau et rebond vers le SI industriel
    - Attaques sur les automates et la supervision pour impacter un processus physique *(train miniature et bras robotisés)*
    - Visuels de la maquette

Evaluation et fin de session

229 rue de Solferino, 59000 Lille – Tél.: +33 6 67 61 38 59– SIRET : 93995807000012 – www.activformation.fr – contact@activformation.fr
Numéro de déclaration d'activité : 32591326259 Code NAF :8559A

- Validation des acquis via QCM et mise en simulation

Public

- Ingénieur en charge de la sécurité ou du contrôle de SI industriels ,
- Consultants, auditeurs et pentesteurs voulant monter en compétence sur les SI industriels
- Ingenieur SI voulant se former à la sécurité d'un point de vue attaque et par la pratique.

Pré-requis :

- Aucun pré requis n'est nécessaire.

Durée de la formation

4 jours (28 heures) en présentiel ou télé-présentiel

Conditions d'accès à la formation

- Vérification des prérequis.
- Inscription par mail ou par téléphone.
- Pour les formations à distance posséder un ordinateur connecté à Internet et Teams installé.

Délais d'accès

1 semaine maximum après la signature de la convention. Sauf obligations réglementaire, il est possible de réduire ce délai.

Sessions

✓ Nous consulter

Méthode pédagogique

✓ Selon la formation et le public nous choisissons la méthode et le support le plus adapté. Nous tenons une rigueur particulière pour respecter au moins ces points :

- Transmission de savoir sous forme d'exposés étayés par des diaporamas, des films, des photos, des exercices, des études de cas.
- Remise d'un support de formation
- Questions réponses.
- Validation des compétences par une attestation de fin de formation

229 rue de Solferino, 59000 Lille – Tél.: +33 6 67 61 38 59– SIRET : 93995807000012 – www.activformation.fr – contact@activformation.fr
Numéro de déclaration d'activité : 32591326259 Code NAF :8559A

Modalités d'évaluation

- ✓ L'évaluation se fera en fonction du sujet traité tout au long de la formation et à la fin de la formation selon l'une des modalités suivantes : Mise en situation, jeux de rôle, exercices pratiques, QCM.

Profil des formateurs ou formatrices

- ✓ 35 à 60 ans, diplômé(e) et expérimenté(e) dans le domaine.

Taux de réussite

- Le taux de réussite dans nos formations est calculé à partir des questionnaires d'évaluation fin de formation. Il permet de mesurer la progression pédagogique.
  L'organisme de formation Activformation étant nouveau. Ce taux n'est pas significatif ce jour.

Certification

- Nous consulter.

Prix de la formation

- Nous consulter

Accessibilité

Nous portons un intérêt particulier aux personnes handicapées. Le handicap est différent d'une personne à une autre et les moyens d'adaptation des formations de ce public sont aussi diversifiés. Nous invitons les personnes handicapées à nous contacter directement par téléphone ou via le formulaire pour partager avec nous leur projet de formation. Un conseiller proposera la solution la plus adaptée.

229 rue de Solferino, 59000 Lille – Tél.: +33 6 67 61 38 59– SIRET : 93995807000012 – www.activformation.fr – contact@activformation.fr
Numéro de déclaration d'activité : 32591326259 Code NAF :8559A