

** Cette fiche à été générée sur formation-cn.fr le 24/10/2020 à 02:10 **

Ref : DNDAPENTESTINDUS

Durée : 3 Jours

Tarif : 2 220 €HT

Formation Tests d'intrusion des systèmes industriels

Objectifs de la formation Tests d'intrusion des systèmes industriels:

- 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 de la formation Test d'intrusion des systèmes industriels:

Module 1 : 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...)

Module 2 : 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

Module 3 : Sécurité des systèmes Windows et Active Directory

- Introduction aux environnements Windows et AD
- Méthodes d'authentications, 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...

Module 4 : Vulnérabilités courantes en environnement industriel

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

Module 5 : Protocoles de communication industriels

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

Module 6 : Introduction à la sureté de fonctionnement

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

Module 7 : 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

Module 8 : 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

Module 9 : Principes de sécurisation des SI industriels

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

Module 10 : Étude de cas

- 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

Module 11 : 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

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 , Automaticien voulant se former à la sécurité d'un point de vue attaque et par la pratique.

Pré-requis

Bonne connaissance générale en informatique et en réseaux, par exemple une certification SECUCYBER d'HS2 ou CISSP d'(ISC)². Maîtrise d'un interpréteur de commande (Bash, Powershell, etc). Utilisation de machines virtuelles. Une expérience en test d'intrusion est un plus. Aucune connaissance des systèmes industriels n'est nécessaire.

Méthodes pédagogiques

Cours magistral. Démonstrations. Travaux pratiques avec un ordinateur par stagiaire, avec mise en œuvre sur plusieurs automates et exercice sous forme de concours (CTF).