Formation « Tests d'intrusion des systèmes industriels »

Réf : PENTESTINDUS

La vérification de la cybersécurité par les tests d'intrusion est une mesure de sécurité courante (Redteam, Bug Bounty), et qui est dans l'arsenal des bonnes pratiques. Dans le cas des systèmes industriels, le matériel cible est spécifique, le contexte et sa sureté de fonctionnement et sa criticité souvent hors des contextes de tests habituels. Il est donc indispensable de comprendre cet environnement et ces composants pour pouvoir en évaluer le niveau de sécurité.

Objectifs

- 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

Durée & horaires

- 3 jours soit 21 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- 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

Méthode pédagogique

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

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Clé USB contenant les machines virtuelles, les outils utilisés, ainsi que de la documentation complémentaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification PENTESTINDUS par HS2.**

Programme

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'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…

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 sureté fonctionnelle
- Différentes couches de sureté
- 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 :