

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 sûreté 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

- 4 jours soit 28 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
- Labs dans le cloud, accessibles depuis un simple navigateur, sans installation
- Dossier partagé contenant les supports de cours 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 passe un examen ayant pour but de valider les connaissances acquises. Cet examen dure 2 heures et se compose de deux parties d'une heure : un QCM et un examen pratique réalisé sur un environnement de test. Il a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification PENTESTINDUS par HS2.

Programme

Jour 1

Module 1 : Introduction aux SI industriels

- Historique des SI industriels et de l'automatisme
- Vocabulaire
- Modèle CIM et modèle de Purdue
- Architectures classiques
- Composants des SI industriels (PLC, HMI, SCADA, DCS, capteurs, effecteurs, RTU...)
- Panorama de la menace sur les SI industriels et analyse de cas réels d'attaques (Stuxnet, Industroyer, Colonial Pipeline, CyberAv3ngers...)

Module 2 : Vulnérabilités courantes des SI industriels

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

Module 3 : Programmation d'automates programmables industriels (API)

- Présentation des différents langages de la norme IEC 61131-3
- Travaux pratiques : exercices de programmation en ladder logic sur simulateur Schneider TM221

Module 4 : Protocoles de communication industriels

- Présentation des protocoles les plus courants (Modbus/TCP, S7, OPC-UA...)
- OPC-UA : modes de sécurité, certificats et PKI, durcissement, et vulnérabilités récentes des implémentations
- Travaux pratiques : analyse de capture réseau Modbus/TCP, S7 et OPC-UA ; utilisation de mbtget et du module modbusclient de Metasploit sur simulateur Schneider ; bibliothèque Snap7 pour échanger avec un simulateur Siemens ; client graphique OPC-UA et opcua-scan pour interroger un serveur OPC-UA Kepware, puis durcissement de ce serveur

Module 5 : Sécurité des automates

- Découverte d'automates sur le réseau : approches active et passive
- Surface d'attaque des automates (web, FTP, services standards)
- Protocoles propriétaires de programmation et leur exploitation
- Téléchargement de code automate et exécution de code arbitraire
- Fonctionnalités de sécurité offertes par les automates récents
- Démonstrations : récupération d'informations, accès au code et forçage des sorties sur automates Schneider M340

Jour 2

Module 6 : Attaquer le procédé industriel

- Les différentes familles d'attaques cyber-physiques

- Porter atteinte au produit, à l'installation et aux personnes
- Matrice MITRE ATT&CK for ICS : tactiques, techniques et actifs spécifiques aux SI industriels

Module 7 : Introduction à la sûreté de fonctionnement

- Présentation du concept
- Méthodologies d'analyse de sûreté fonctionnelle
- Différentes couches de sûreté, focus sur les Systèmes Instrumentés de Sûreté
- Liens entre sûreté de fonctionnement et cybersécurité

Module 8 : Supervision du procédé : SCADA & DCS

- Rôle et architecture de la supervision
- SCADA et DCS : différences, périmètres et cas d'usage
- Travaux pratiques : programmation d'un SCADA Schneider IGSS connecté à l'automate, de la définition des variables au synoptique

Module 9 : Tests d'intrusion : principes & outillage

- Tests d'intrusion et autres méthodologies d'évaluation de la sécurité des SI industriels
- Différentes étapes d'un test d'intrusion : préparation, OSINT, reconnaissance, analyse de vulnérabilités, exploitation, post-exploitation
- Travaux pratiques : scans nmap et scripts NSE, analyse de vulnérabilités avec Nessus, exploitation avec Metasploit

Module 10 : 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 : reconnaissance d'un Active Directory avec BloodHound, utilisation de mots de passe et de condensats avec NetExec, audit de configuration avec PingCastle...

Module 11 : Attaquer la supervision (SCADA & DCS)

- Accès local au poste de supervision et échappement du mode kiosque
- Élévation de privilèges et récupération des secrets locaux
- Exploitation des fichiers projet de la supervision
- Travaux pratiques : rétro-ingénierie du format de fichier projet d'un SCADA pour en extraire la cartographie des variables du procédé

Module 12 : Les SI industriels modernes

- Industrie 4.0 et IIoT : ce que recouvrent réellement ces termes
- Réseaux de communication longue portée et cellulaires
- Protocoles applicatifs associés et leur sécurité
- Conséquences sur les architectures industrielles et leur surface d'attaque
- Travaux pratiques sur le protocole MQTT

Jour 3

Module 13 : Exercice sous forme de CTF (Capture The Flag)

- Mise en pratique des acquis par la réalisation d'un test d'intrusion complet sur l'environnement représentatif d'une société fictive :
 - 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 procédé industriel
 - Observation en temps réel de l'effet des actions sur le procédé, via une interface de supervision

Jour 4

Module 14 : Principes de sécurisation des SI industriels

- Panel normatif, avec un focus sur la norme IEC 62443
- Architectures et technologies de cloisonnement réseau
- Focus sur les diodes réseau

Module 15 : Sécurité du code automate

- Le référentiel TOP 20 Secure PLC Coding Practices
- Analyse critique des recommandations et de leur applicabilité sur le terrain
- Travaux pratiques : mise en œuvre des principales recommandations sur automate Schneider (validation des entrées, drapeaux d'intégrité, état sûr au redémarrage, durcissement des interfaces)