AYI NEDJIMI Consultants

Pentest industriel méthodologie et outils spécifiques OT

Catégorie : Sécurité Industrielle OT/ICS Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Guide complet du pentest industriel : méthodologie adaptée aux environnements OT, outils spécifiques ICS, précautions de sécurité et cadre juridique.

Résumé exécutif

Le test d'intrusion en environnement industriel exige une méthodologie radicalement différente du pentest IT classique en raison des risques physiques directs sur les processus de production. Les contraintes de disponibilité permanente, le risque d'impact physique sur les équipements et le personnel, et la fragilité des automates face aux scans réseau agressifs imposent des précautions spécifiques à chaque phase de l'évaluation de sécurité. Ce guide détaille la méthodologie complète de pentest OT depuis la définition des règles d'engagement jusqu'à la restitution des résultats, les outils spécialisés ICS comme ISF et Redpoint, les techniques d'évaluation non destructives permettant d'identifier les vulnérabilités critiques sans compromettre la sûreté des installations industrielles en production, et les plateformes de simulation pour les tests les plus intrusifs.

Le test d'intrusion industriel constitue l'un des exercices les plus délicats de la cybersécurité. Contrairement aux environnements IT où un crash de serveur se résout par un redémarrage, une action maladroite sur un automate programmable peut provoquer l'arrêt d'une chaîne de production, endommager des équipements coûteux, générer des situations dangereuses pour le personnel ou causer des pollutions environnementales. Cette réalité impose une discipline méthodologique stricte que tout pentester intervenant en environnement OT doit maîtriser avant de toucher au moindre packet sur un réseau industriel. Les incidents documentés de pentesters IT ayant provoqué des arrêts de production par des scans agressifs sur des automates anciens rappellent que les systèmes OT ne tolèrent pas les mêmes approches que les serveurs web ou les postes de travail. La méthodologie de pentest industriel combine des techniques de reconnaissance passive, des tests ciblés sur des environnements de pré-production ou des simulateurs, et des évaluations en production soigneusement encadrées par des règles d'engagement validées conjointement avec les équipes d'exploitation OT et les responsables sûreté de l'installation.

Règles d'engagement spécifiques au pentest OT

Les **règles d'engagement** (Rules of Engagement, RoE) d'un pentest industriel dépassent largement le cadre contractuel d'un pentest IT standard. Elles doivent définir explicitement les systèmes exclus du périmètre (systèmes instrumentés de sécurité, automates pilotant des processus critiques en cours de production), les horaires d'intervention autorisés (alignés sur les

fenêtres de maintenance), les actions interdites (scans de ports agressifs sur les automates, tentatives de fuzzing sur les protocoles temps réel), et les procédures d'escalade en cas d'incident.

Un *référent OT* doit être présent physiquement sur le site pendant toute la durée des tests en production. Ce référent, disposant de la connaissance du processus industriel et de l'autorité pour arrêter les tests immédiatement, constitue le filet de sécurité humain indispensable. Les automates Siemens S7-300/400 anciens, par exemple, peuvent redémarrer suite à un simple scan Nmap avec certaines options de fingerprinting TCP. Les protocoles de communication OT comme Modbus ne gèrent pas les trames malformées de manière prévisible : un paquet inattendu peut provoquer un état indéterminé de l'automate. Ces spécificités exigent une planification minutieuse documentée dans la méthodologie de pentest infrastructure adaptée au contexte industriel.

En 2017, lors d'un audit de sécurité mandaté sur une station de traitement des eaux, un scanner de vulnérabilités IT déployé sans précaution sur le réseau OT a provoqué le redémarrage simultané de plusieurs automates contrôlant les pompes de dosage de chlore. L'incident, qui aurait pu avoir des conséquences sanitaires graves si les systèmes de sécurité physique n'avaient pas fonctionné, illustre la nécessité absolue d'utiliser des outils et méthodologies adaptés aux environnements industriels, comme l'a rappelé l'incident de la station de traitement d'eau d'Oldsmar en Floride en 2021 où un attaquant a tenté de modifier la concentration de soude caustique à des niveaux dangereux via un accès TeamViewer non sécurisé.

Comment réaliser la reconnaissance en environnement OT ?

La phase de reconnaissance en environnement OT privilégie les **techniques passives** qui ne génèrent aucun trafic vers les systèmes cibles. La capture et l'analyse du trafic réseau via des TAP ou des ports miroir révèlent les protocoles utilisés, les adresses des automates, les structures de communication et les versions de firmware sans aucun risque. L'outil **Wireshark** avec les dissectors industriels (Modbus, DNP3, S7comm, EtherNet/IP, OPC UA) constitue l'outil de base pour cette analyse passive.

L'outil **Redpoint** (scripts NSE pour Nmap spécifiques OT) permet une reconnaissance semi-passive des dispositifs industriels, mais doit être utilisé avec précaution et uniquement sur autorisation explicite. Les scripts de découverte Modbus interrogent le registre d'identification du dispositif (Device ID, fonction 43) sans modifier aucune valeur. Pour les protocoles Siemens, le script s7-info extrait les informations hardware et firmware du PLC. L'inventaire automatisé via des solutions comme Claroty complète cette reconnaissance par une cartographie exhaustive et non intrusive du réseau OT, alimentant directement la base de connaissances du pentester. L'intégration des résultats de reconnaissance avec les bases de vulnérabilités ICS-CERT permet de corréler chaque dispositif découvert avec les CVE publiées affectant sa version de firmware spécifique, créant une carte de risque protocolaire qui guide la priorisation des tests d'exploitation ultérieurs.

La reconnaissance des configurations réseau, incluant l'identification des VLAN, des règles de pare-feu et des chemins de communication entre zones Purdue, est essentielle pour planifier les scénarios de mouvement latéral qui seront testés dans les phases suivantes du pentest OT. Cette cartographie réseau passive révèle souvent des faiblesses de segmentation invisibles dans la documentation d'architecture théorique du site industriel.

La reconnaissance OSINT spécifique OT utilise des sources comme Shodan, Censys et ZoomEye pour identifier les systèmes industriels exposés sur Internet (HMI publiques, serveurs OPC UA accessibles, ports Modbus ouverts). Les bases de vulnérabilités ICS-CERT et les advisories constructeurs permettent d'identifier les vulnérabilités connues des versions de firmware découvertes lors de la reconnaissance passive. L'intégration avec le framework MITRE ATT&CK for ICS structure les découvertes selon les tactiques et techniques documentées.

Outils spécialisés pour le pentest ICS

L'arsenal d'outils du pentester OT diffère significativement de la boîte à outils IT classique. **ISF** (Industrial Exploitation Framework), inspiré de Metasploit, regroupe des modules d'exploitation spécifiques aux automates et protocoles industriels. **SCADA Shutdown Tool** permet de tester les capacités d'arrêt de processus via les protocoles Modbus et DNP3. **Mbtget** et **pymodbus** offrent une interaction fine avec les automates Modbus pour tester les contrôles d'accès aux registres.

Outil	Protocoles	Usage	Risque OT
Wireshark + dissectors OT	Tous	Analyse passive trafic	Nul (passif)
Redpoint (NSE)	Modbus, S7, BACnet	Reconnaissance active	Faible
ISF	Multi-protocoles	Exploitation	Élevé
Mbtget/pymodbus	Modbus TCP/RTU	Test registres	Moyen
PLCScan	S7, Modbus	Énumération PLC	Faible-Moyen
Codesys exploit tools	Codesys V2/V3	Exploitation runtime	Élevé

Mon avis : Le pentest industriel en production directe devrait être l'exception, pas la règle. La majorité des tests exploitables peuvent être réalisés sur une plateforme de simulation reproduisant l'architecture cible. Les investissements dans des labs OT avec des automates réels et des simulateurs de processus permettent de tester des scénarios offensifs agressifs sans aucun risque opérationnel, tout en développant les compétences des équipes de sécurité.

Pourquoi les simulateurs ICS sont essentiels au pentest ?

Les **simulateurs ICS** permettent de reproduire l'environnement cible dans un lab isolé pour exécuter les tests les plus intrusifs sans risque. *GRFICSv2* (Graphical Realism Framework for Industrial Control Simulations) simule un processus chimique complet avec automates virtuels,

HMI et réseau SCADA. **OpenPLC** fournit un automate programmable open source compatible avec les langages IEC 61131-3 pour créer des environnements de test réalistes. SWaT (Secure Water Treatment) de SUTD offre un dataset et un simulateur de station de traitement des eaux.

La construction d'un lab de pentest OT avec des automates physiques (Siemens S7-1200, Allen-Bradley MicroLogix, Schneider M340) connectés à des simulateurs de processus permet les tests les plus réalistes. L'investissement initial, entre 10 000 et 50 000 euros selon la complexité, est négligeable comparé au coût d'un incident de production causé par un test mal encadré. Ces plateformes servent également à la formation des analystes SOC aux spécificités OT et à la validation des règles de détection décrites dans notre guide sur la détection engineering.

Quelles vulnérabilités rechercher en priorité sur les systèmes OT ?

Les vulnérabilités les plus fréquemment découvertes lors des pentests OT se regroupent en catégories récurrentes. Les **identifiants par défaut** non modifiés constituent la vulnérabilité numéro un : mots de passe constructeur sur les automates, comptes admin par défaut sur les HMI, clés communautaires SNMP « public/private » sur les commutateurs industriels. L'exploitation de ces identifiants donne un accès immédiat aux systèmes critiques sans aucune technique avancée nécessaire.

Les *services réseau non nécessaires* exposés sur les automates (serveurs web de diagnostic, services FTP pour le transfert de programmes, Telnet pour la maintenance) élargissent considérablement la surface d'attaque. La majorité de ces services, activés par défaut en usine, ne sont jamais désactivés après la mise en service. Les **firmwares obsolètes** contenant des vulnérabilités publiquement documentées (CVE) constituent un autre axe d'exploitation majeur, aggravé par l'absence de processus de mise à jour systématique en environnement OT. L'approche de threat hunting permet d'identifier ces expositions avant qu'un attaquant ne les exploite.

Les faiblesses de segmentation réseau, testées par des tentatives de mouvement latéral entre zones Purdue, révèlent souvent des chemins d'accès non prévus entre les niveaux IT et OT. La capacité à atteindre un automate critique depuis le réseau bureautique, en traversant les pare-feu par des services autorisés détournés, constitue le scénario de compromission le plus réaliste et le plus redouté. Les résultats de ces tests alimentent directement les recommandations d'architecture de segmentation réseau et Zero Trust.

Avez-vous déjà vérifié si les mots de passe constructeur par défaut sont encore actifs sur vos automates en production ?

Faut-il certifier les pentesters OT différemment ?

Les certifications classiques de pentest (OSCP, CEH) ne couvrent pas les compétences spécifiques requises pour intervenir en environnement industriel. La certification **GICSP** (Global Industrial Cyber Security Professional) du SANS Institute valide une connaissance des systèmes de contrôle industriels et de leurs vulnérabilités. La certification **ICS 515** de Dragos et SANS couvre spécifiquement la visibilité et la détection en environnement ICS.

Au-delà des certifications, l'expérience pratique sur des systèmes industriels réels est irremplaçable. Un pentester OT efficace doit comprendre le fonctionnement des processus industriels qu'il teste, lire un schéma P&ID (Piping and Instrumentation Diagram), interpréter les programmes automate en Ladder ou Structured Text, et anticiper les conséquences physiques de ses actions sur le processus. Cette double compétence cybersécurité et automatisme industriel est rare et précieuse, justifiant des investissements significatifs en formation croisée. L'intégration des résultats du pentest OT dans la stratégie de réponse aux incidents garantit que les vulnérabilités découvertes alimentent des scénarios de réponse réalistes et testés.

Sources et références : CISA ICS · ANSSI

Comment documenter et restituer un pentest OT ?

La restitution d'un pentest industriel doit s'adresser simultanément aux équipes de sécurité IT, aux responsables OT et à la direction. Le rapport technique détaille chaque vulnérabilité découverte avec son contexte d'exploitation spécifique OT : quel automate est affecté, quel processus physique est potentiellement impacté, quelle commande protocolaire permet l'exploitation. Les captures réseau Wireshark illustrant les attaques réussies sur les protocoles industriels apportent la preuve technique nécessaire à la compréhension des risques par les équipes automatisme.

Le rapport managérial traduit les découvertes techniques en **risques métier** compréhensibles par la direction : impact potentiel sur la production en heures d'arrêt, risques de sûreté pour le personnel, conséquences environnementales et exposition réglementaire. La matrice de risque combine la probabilité d'exploitation (facilité technique, accessibilité réseau) avec la gravité des conséquences industrielles. Les recommandations de remédiation sont priorisées selon un calendrier réaliste aligné sur les fenêtres de maintenance planifiées du site, distinguant les actions immédiates (mesures compensatoires réseau) des actions planifiées (mises à jour firmware, modification d'architecture). Cette documentation alimente directement les stratégies de continuité d'activité et de résilience industrielle face aux menaces cyber identifiées lors des tests.

À retenir : Le pentest industriel requiert une méthodologie spécifique intégrant des règles d'engagement strictes, une prédominance des techniques passives et semi-passives, l'utilisation de simulateurs pour les tests destructifs, et une expertise combinée en cybersécurité et en systèmes de contrôle. La présence permanente d'un référent OT qualifié sur site pendant l'intégralité des tests en production reste absolument non négociable pour garantir la sûreté des installations industrielles critiques.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr