“Ça fait quoi si j’appuie là ?” Retour d’expérience de tests d’intrusion sur systèmes industriels

Claire Vacherot
claire.vacherot@orangecyberdefense.com

Orange Cyberdefense

Résumé. Il est de notoriété publique que les systèmes d’information industriels (OT) sont souvent moins bien couverts par les démarches de cybersécurité, malgré les impacts dévastateurs que des attaques les ciblant peuvent avoir. Heureusement, la situation a évolué depuis quelques années et la cybersécurité OT est en pleine expansion, avec des mesures qui sont spécifiques à ces systèmes, ou empruntées à l’IT mais adaptées au contexte industriel. Les tests d’intrusion font partie de ces mesures. Vu les spécificités et contraintes de ces systèmes, il n’est pas possible d’appliquer telles quelles les mêmes méthodes de test qu’on emploie habituellement sur l’IT. Comment peut-on procéder dans ce cas ? Dans cet article, nous partagerons notre méthodologie et nos retours d’expérience pour répondre à cette question. Nous verrons qu’il est nécessaire d’adapter sa méthodologie pour tester des environnements industriels, et donc de prendre des précautions particulières et de bannir certains types de test qui pourraient mettre en péril le fonctionnement des procédés industriels. Ce sera aussi l’occasion d’aborder les situations et problèmes de sécurité les plus fréquemment relevés durant nos missions d’audit. Ceux-ci sont pour la plupart liés aux différences de cycle de vie des composants et de maturité sur les questions de cybersécurité. Outre les mesures de durcissement proposées habituellement sur l’IT, qui ne sont d’ailleurs pas toujours applicables selon les contextes opérationnels, nous mettrons l’accent sur le cloisonnement réseau comme solution intéressante pour palier à certaines menaces qui ciblent ces systèmes critiques.

1 Introduction

L’an dernier ont été publiés les détails du malware FrostyGoop [13] utilisé notamment en 2024 en Ukraine contre les systèmes de distribution d’énergie. Celui-ci rejoint la liste croissante des menaces de cybersécurité qui ciblent directement les systèmes industriels. Aussi appelés OT (Operation Technology), ces systèmes constituent le pendant opérationnel de l’IT (Information Technology) puisqu’il n’est pas question de la gestion de la donnée informatique mais du contrôle de procédés physiques et mécaniques. De fait, on les trouve par exemple dans les secteurs de l’industrie,

de l'énergie, du transport ou encore dans la gestion technique d'infrastructures. À l'origine, les systèmes industriels étaient déconnectés du monde de l'informatique bureautique et fonctionnaient de manière autonome. Ils ont été progressivement interconnectés avec l'IT et ont commencé à utiliser certains de ses standards en plus des leurs, pour simplifier les procédures de supervision, de fonctionnement et de maintenance.

Cependant, alors même que, dans les industries, la notion de sûreté appliquée à ces systèmes est très présente, la cybersécurité y était secondaire jusqu'à récemment. Bien qu'il y ait eu de nettes améliorations ces dix dernières années, l'OT reste peu considéré et peu couvert par les mesures de cybersécurité. Cela implique finalement que le niveau de sensibilisation et les mesures techniques qui existent pour sécuriser ces systèmes sont généralement moins avancés que ce que l'on trouve sur l'IT, et ce alors que les attaques se sont perfectionnées. Heureusement, on voit apparaître régulièrement de nouvelles mesures et techniques de sécurisation dédiées à ces systèmes, ou empruntées à l'IT mais adaptées au monde industriel. Les tests d'intrusion sont l'une de ces mesures. Cependant, vu les spécificités et contraintes de ces systèmes, il n'est pas possible d'appliquer telles quelles les mêmes méthodes de test qu'on emploie habituellement sur l'IT. C'est l'objet de cet article.

En s'appuyant sur nos retours d'expérience issus d'une trentaine de tests d'intrusion de systèmes industriels réalisés ces six dernières années pour des clients de différents secteurs, nous vous proposons de découvrir les spécificités, le déroulement (avec ses enjeux et ses difficultés) et la portée de ce type de tests.

2 Vue d'ensemble d'un système d'information industriel

Lors d'un test d'intrusion en milieu industriel, la surface d'attaque principale est le système d'information industriel (OT). L'exemple le plus parlant pour expliquer de quoi il s'agit est celui d'une chaîne de production dans une usine, qui a pour fonction d'assembler, conditionner et emballer de manière automatisée des produits manufacturés à partir d'ordres de fabrication informatiques. Mais il serait réducteur de se limiter à ce type d'usage. En effet, une gestion centralisée de la climatisation d'un bâtiment, un dispositif de signalisation du trafic ferroviaire, un entrepôt logistique, un procédé d'assainissement de l'eau ou encore un tracteur connecté sont autant d'environnements que l'on peut inclure dans cette catégorie. Ils comprennent ainsi un ensemble de composants coordonnés en vue de la réalisation de leurs fonctions. Ces fonctions peuvent être très diverses

et spécifiques selon les environnements et au sein d'un même système. Tentons tout de même de décrire une organisation "type" de cet ensemble, simplifiée ici pour une meilleure compréhension, en gardant à l'esprit qu'à part ce qui concerne l'interaction avec le monde physique, aucun de ces composants n'est systématique. Dans la suite de cet article, je désignerais ces environnements comme "la production" pour simplifier le propos, même lorsque les procédés désignés ne sont pas destinés à produire des marchandises manufacturées.

Il y a d'abord la couche "terrain", composée de capteurs et d'actionneurs qui permettent d'agir dans l'environnement physique. Ces équipements sont souvent pilotés par des automates de complexité variable (ou des équipements équivalents) selon des programmes qui définissent l'ordonnancement, les conditions et le déclenchement des actions. Par exemple, sur une infrastructure de gestion technique de bâtiment (ou centralisée), notre capteur pourrait être une sonde de température et notre actionneur une climatisation. Le programme comporte alors probablement une action consistant à ajuster les réglages de la climatisation lorsque la sonde remonte une température trop élevée.

Les programmes des automates sont généralement réalisés et maintenus sur des ordinateurs nommés stations de programmation (ou d'ingénierie). Le pilotage et la surveillance des procédés de production s'effectuent souvent via des interfaces hommes-machines (IHM) industrielles et des postes opérateurs (habituellement des ordinateurs bureautiques). Ces procédés et les informations les concernant génèrent des données qui servent à superviser l'ensemble de la production grâce à ce qu'on appelle des systèmes SCADA (Supervision Control and Data Acquisition, terme qu'on utilise parfois à tort pour désigner l'ensemble du système d'information industriel). D'autres types de serveurs sont habituellement utilisés pour le stockage des données de fonctionnement, pour l'historisation des données de production (historian), et pour d'autres usages selon l'environnement métier (par exemple, des serveurs applicatifs pour faire fonctionner des machines).

On notera finalement que le système industriel reçoit généralement des données en entrée pour la réalisation de ses fonctions. Par exemple, dans les usines, les ordres de fabrication sont donnés par des solutions MES, Manufacturing Execution System. Ces solutions sont intégrées à l'OT mais sont généralement en lien avec l'ERP (Entreprise Resource Planning) côté IT. Des données sont également remontées par le système industriel pour donner des informations sur son exécution et son fonctionnement. Ainsi, les liaisons entre l'OT et l'IT sont la plupart du temps indispensables pour

le bon fonctionnement de l'ensemble et les deux sont parfois fortement liés. Au point que, désormais, certains systèmes industriels ne peuvent plus fonctionner s'ils perdent le contact avec l'IT.

D'un point de vue technique, on trouve dans un système d'information industriel des éléments que l'on retrouve dans l'IT, notamment des postes et serveurs, même s'ils conservent généralement une particularité industrielle. Par exemple, il peut s'agit de matériel durci physiquement pour les environnements très poussiéreux. Il peut même y avoir un annuaire Active Directory, souvent distinct de l'AD IT, mais pas toujours. Nous avons déjà croisé des environnements où le même AD était utilisé pour l'IT et l'OT, ce qui peut avoir ses avantages (notamment la mutualisation de la gestion) et ses inconvénients (par exemple, un problème sur l'AD peut se propager sur l'ensemble du système). Selon notre expérience, il reste fréquent que le système industriel ne comporte pas d'Active Directory du tout, ce qui est parfois très déstabilisant pour un auditeur qui vient de l'IT. Les logiciels utilisés peuvent également être spécifiques aux procédés industriels auxquels ils sont rattachés. On trouve aussi des équipements issus du monde industriel mais qui intègrent des standards utilisés dans l'IT et des équipements terrains parfois totalement déconnectés de la partie informatique.

Au niveau réseau, cela se matérialise en théorie par la présence d'un réseau industriel avec des liaisons filaires et parfois sans fil. Sur celui-ci, les postes, serveurs et équipements industriels connectés dialoguent sur le réseau IP en utilisant des protocoles IT (RDP, SMB, SSH, etc.) et des protocoles de communication industriels dédiés, très nombreux et parfois destinés à des cas d'usage extrêmement précis. Ces protocoles peuvent transiter directement sur le réseau IP ou sur d'autres types de liaisons que nous appellerons "terrain" (série, radio, etc.). Des équipements (passerelles) peuvent parfois assurer la liaison entre les deux, et donc rendre accessible cette couche terrain depuis le réseau informatique.

Toujours en théorie, ce réseau informatique industriel, même s'il communique avec le réseau bureautique, est distinct de ce dernier et normalement isolé autant que possible. L'état de l'art stipule que les échanges réseaux entre le système d'information industriel et l'extérieur devraient être fortement restreints et contrôlés (DMZ). De même, le réseau industriel devrait être lui-même segmenté en zones de confiance définies selon des critères techniques ou métiers. Le Purdue Model [28] représenté en figure 1 montre une architecture dont il est recommandé de s'inspirer. Nous verrons que, dans la pratique, certains systèmes en sont bien éloignés.

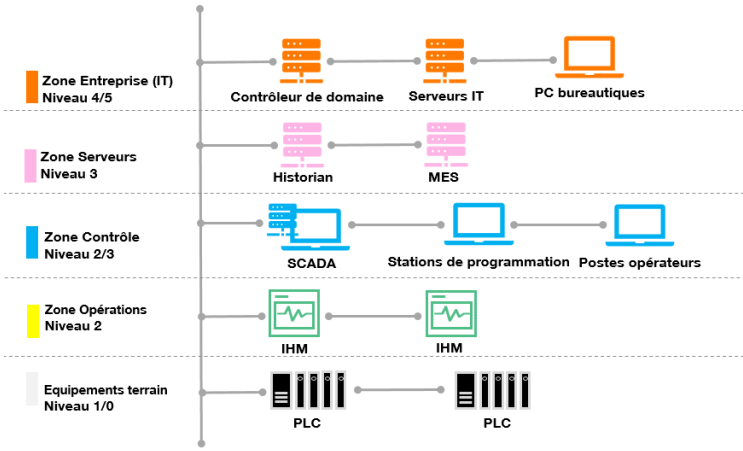

Fig. 1. Organisation d'un SI industriel selon la Purdue Enterprise Reference Architecture (PERA)

Nous pouvons finalement mentionner l'arrivée progressive, bien que timide, de ce que l'on appelle parfois l'industrie 4.0. Ce terme désigne une "révolution" technique dans l'industrie caractérisée par l'intégration du numérique jusque dans les éléments du monde physique. On pourrait rapprocher ce concept de l'Internet des objets (IoT) où ce sont effectivement des "objets", interagissant avec leur environnement physique, qui sont connectés aux systèmes informatiques, en utilisant des technologies IT, OT ou des standards qui leur sont propres (par exemple, les protocoles réseau sans fil dédiés IoT type ZigBee ou LoRaWAN). Cela implique alors que les équipements sur des couches de plus en plus proches du terrain, jusqu'aux capteurs et actionneurs, deviennent interconnectés au réseau IP, sur un réseau interne voire directement sur Internet.

Ce sont des composants que nous voyons peu pour l'instant, même si nous y avons déjà été confrontés à plusieurs reprises. On peut par exemple trouver des objets connectés dans des endroits difficiles d'accès physiquement pour faciliter la remontée d'informations (entre autres dans des systèmes de traitement de l'eau). Nous avons également audité une clé dynamométrique connectée qui, à chaque manipulation sur des boulons, envoyait les valeurs de serrage à un serveur de supervision "dans le cloud". Ces valeurs devaient être précises pour éviter des problèmes de fabrication causés par des serrages trop forts ou trop faibles. Lors de l'audit, nous pouvions modifier les données remontées au serveur, par exemple pour faire en sorte qu'elles soient systématiquement valides même lorsque le

serrage n'était pas bon, ce qui risquait de créer des défauts non détectés et potentiellement dangereux.

Finalement, ces objets connectés sont introduits pour permettre un meilleur contrôle d'un procédé industriel, mais de notre point de vue, cela signifie surtout que les couches terrain, celles qui n'étaient accessibles que physiquement, sont désormais atteignables par le réseau informatique et doivent faire partie de la stratégie de cybersécurité. On pourrait aller plus loin en disant que les objets connectés offrent, dans certains cas, un chemin d'attaque parallèle qui ne dépend plus du réseau de l'entreprise et passe par d'autres canaux de communication, notamment sans fil, sur IP ou non. Dans d'autres cas, ils pourraient constituer un point d'entrée alternatif vers le système d'information industriel qui ne passerait pas par la bureautique (IT) mais directement par Internet.

3 Où en est la cybersécurité ?

La première conséquence d'une cyberattaque ciblant les systèmes industriels à laquelle on pense est liée à sa définition même : puisqu'un tel système implique une interaction avec son environnement, une attaque peut causer des dégâts physiques, et donc matériels voire humains. La bonne nouvelle est qu'il n'est pas si facile de faire exploser une centrale ou de déverser du métal en fusion dans une aciérie, dans la mesure où il existe des équipements (SIS, Safety Instrumented Systems [6] qui servent justement à assurer la sûreté physique des installations. Bien que nous ayons connaissance d'au moins un cas d'attaque ciblant ces systèmes, qui avait justement pour but de causer d'importants dégâts matériels (le malware Triton, en 2017 [15]), il s'agit d'une attaque très complexe qui n'a heureusement pas abouti. Pour autant, les risques physiques existent bel et bien. Par exemple, il nous a déjà été possible d'accéder à distance et sans authentification à une interface web permettant de contrôler une machine de thermoformage. Après l'avoir montrée au contact côté client, il a immédiatement pensé au fait que nous pouvions activer la machine sans savoir si un technicien était en train d'intervenir dessus. Si nous l'avions fait au mauvais moment, nous aurions pu lui broyer la main.

Cependant, il est évident que ce ne sont pas les seuls impacts envisageables. En sécurité informatique, les critères de confidentialité, intégrité, disponibilité et traçabilité sont largement admis pour caractériser et évaluer les menaces qui ciblent un système d'information. Pour la partie industrielle, on entend régulièrement que les critères sont les mêmes, mais dans un ordre de priorité différent. La disponibilité serait souvent priori-

taire pour éviter des pertes financières et autres dangers causés par une perte de service. Par exemple, immobiliser une ligne de production dans une usine entraîne, en plus des conséquences pécuniaires, des réactions en chaîne qui se résolvent souvent sur le long terme (congestion et dysfonctionnements sur les autres parties du procédé industriel, saturation des espaces de stockage, etc.). Ensuite viendrait l'intégrité, puisque modifier des données de fonctionnement ou des ordres de production peut causer des dégâts financiers mais également matériels et humains. On notera sur ce sujet le célèbre malware Stuxnet en 2010 [17]. Le critère suivant serait la traçabilité, dont la perte pourrait être significative, par exemple dans l'industrie agro-alimentaire où le fait de ne pas pouvoir retracer le parcours d'un lot le rendrait impossible à distribuer. Finalement, la confidentialité arriverait en dernier, et concernerait en majorité les données liées aux brevets ou au secret des procédés de fabrication. Il est important de nuancer cette vision, car cette hiérarchie varie selon les enjeux métiers et les spécificités techniques. Par exemple, la traçabilité peut être moins importante dans un système de climatisation, tandis que la disponibilité peut être secondaire dans l'industrie pharmaceutique face aux contraintes réglementaires de traçabilité qui pourraient empêcher des mises sur le marché. Les facteurs influençant l'exposition aux menaces sont nombreux, rendant difficile toute généralisation. Lors d'un test d'intrusion, cela fait partie du travail de l'auditeur ou de l'auditrice d'identifier autant que possible les menaces pertinentes et les cibles à privilégier pour l'environnement audité, notamment en discutant avec son client.

4 Initialisation des tests d'intrusion

Le scénario qui nous est le plus souvent demandé en tests d'intrusion industriel est le suivant : depuis un accès au réseau bureautique (IT), l'attaquant cherche à accéder au SI industriel (OT). S'il y arrive, qu'est-il en capacité de faire sur celui-ci ? Jusqu'où peut-il aller ? C'est ce scénario que nous allons parcourir dans la suite de l'article. Cependant, il existe d'autres manières de faire des tests d'intrusion sur ce type de systèmes : on peut tester l'OT sans passer par l'IT, on peut ne tester qu'une partie de l'OT, voire qu'un seul composant (serveur SCADA, poste opérateur, automate, équipement réseau industriel ou autre composant connecté).

Notons dès à présent qu'il est dangereux de réaliser des tests d'intrusion sur des systèmes d'information industriels. Nous avons déjà vu que les attaques peuvent avoir des conséquences désastreuses. La maturité sur les questions de cybersécurité est également très variable selon les contextes.

Nous auditons des systèmes avec des niveaux de cybersécurité très élevés, mais aussi d'autres qui sont moins protégés et parfois plus fragiles. Pour cette raison, il est fortement déconseillé de réaliser des tests d'intrusion sur des environnements qu'on appelle "en production", c'est-à-dire en fonctionnement et en conditions d'opération réelles. Dans un monde idéal, les tests d'intrusion devraient toujours être faits sur un environnement de test représentatif de celui de production. Les auditeurs et auditrices pourraient ainsi travailler sans craindre les conséquences bien réelles que leurs tests pourraient avoir. Il nous arrive parfois de pouvoir faire certains tests sur un équipement ou sur un banc de test avec quelques composants, sur une simulation partielle ou, plus fréquemment, sur un élément du système industriel qui n'est pas en fonctionnement au moment de l'audit, mais il reste globalement rare que nos clients disposent de tels environnements. Cela signifie que tous nos autres tests ont été réalisés sur des systèmes en fonctionnement ("en production"), et donc qu'il est systématiquement nécessaire de suivre une méthodologie spécifique et d'adapter nos techniques pour éviter tout effet de bord. Dans la suite de cet article, nous allons donc nous concentrer sur les tests d'intrusion en production avec toutes les précautions que cela implique. Sauf mention contraire, tous les exemples mentionnés ont été réalisés dans ces conditions.

5 Atteindre le système d'information industriel

Il est vrai que le point d'entrée le plus fréquent vers l'OT semble être l'IT, notamment car il est relié à Internet, mais aussi car il est généralement mieux connu des attaquants. Plusieurs malwares industriels ont été introduits via des emails de phishing et se sont répandus jusqu'à atteindre leurs cibles côté OT [14]. Ainsi, pour le scénario de tests d'intrusion dont nous avons parlé plus tôt, nous commençons l'audit depuis l'IT. Nous nous connectons au réseau bureautique de l'entreprise, dans un sous-réseau utilisateur standard. Depuis ce point d'entrée, nous reproduisons par exemple un acte de malveillance causé par un collaborateur, la compromission d'un poste par un attaquant (introduit par phishing ou autre) ou le cas d'une intrusion physique. Jusque-là, cela ressemble à la méthode d'un test d'intrusion sur SI bureautique "classique", mais avec un but précis : notre objectif est de trouver au moins un moyen d'atteindre (virtuellement) des composants industriels depuis une position standard sur le réseau bureautique.

La plupart du temps, il y a une distinction claire sur le réseau, au moins au niveau de l'organisation des sous-réseaux, entre les zones IT et OT. Nous

avons cependant eu des cas où certains composants OT se situaient dans des zones IT (exemple : un automate dans un VLAN utilisateurs), voire où les composants IT et OT étaient mélangés sur le réseau sans distinction. Dans ces situations, il est nécessaire d'appliquer à l'ensemble des sous-réseaux où l'on est susceptible de trouver des composants OT les mêmes précautions que si l'on était dans un environnement purement industriel. Dans le cas le plus fréquent, celui où l'IT et l'OT sont sur des sous-réseaux distincts, nous allons d'abord rechercher sur l'IT toute information qui pourrait nous donner des indications sur le chemin à prendre pour atteindre des composants OT (hostname ou constructeur explicite, port d'un protocole industriel ouvert, etc.). Nous pouvons également rechercher des informations dans les fichiers sur les partages réseaux. Il nous est arrivé à plusieurs reprises de trouver des matrices de flux réseaux qui indiquaient quels étaient les flux ouverts entre l'un et l'autre. Notre contact technique côté client durant l'audit peut également nous aiguiller, par exemple en nous fournissant les plages réseaux correspondant aux systèmes industriels.

Comme nous l'avons dit, l'état de l'art en matière d'architecture réseau mentionné précédemment n'est que rarement appliqué. Nous n'avons pas toujours de zones de confiance au sein d'un même réseau et nous avons rarement une vraie DMZ entre l'IT et l'OT. Parfois, les sous-réseaux IT et OT sont bien distincts mais ne sont pas isolés les uns des autres, on peut donc atteindre les équipements côté OT directement. Une configuration que nous rencontrons souvent est celle où les deux mondes sont bel et bien cloisonnés, et où il existe quelques points de passage direct entre les deux. Il s'agit souvent de postes et serveurs qui, généralement pour un besoin métier, ont des droits spécifiques dans les pares-feux (par exemple, pour l'administration des ressources côté OT) ou une carte réseau dans chaque sous-réseau, pour pouvoir dialoguer à la fois avec des composants IT et OT. Malgré son ancienneté, l'utilisation de SNMPv1 ou SNMPv2 avec le nom de communauté `public` fonctionne souvent encore pour obtenir sans authentification les configurations réseaux des postes et serveurs pour trouver des liens avec l'OT (avec les scripts nmap `snmp-interfaces`, `snmp-netstat` et `snmp-processes`). Ainsi, il nous est arrivé plusieurs fois de rencontrer des serveurs ayant jusqu'à cinq cartes réseaux, dans cinq sous-réseaux IT et OT différents (figure 2). En y accédant, nous avions donc accès à quatre zones de confiance du SI industriel depuis la zone bureautique.

Parfois, ces points de passage sont des serveurs de rebond, accessibles depuis l'IT, souvent via RDP. Cela permet de créer des points d'entrée dédiés vers l'OT et d'éviter les flux non maîtrisés entre les deux SI, ce qui

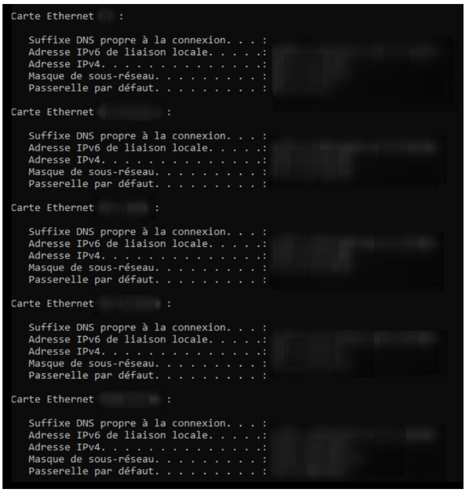

Fig. 2. Résultat de la commande "ipconfig" sur un serveur Windows avec cinq cartes réseaux

est une bonne pratique. Cependant, il arrive souvent que la configuration de ces serveurs et la façon dont ils sont utilisés les rendent particulièrement vulnérables. Par exemple, nous avons constaté plusieurs fois que leur système exploitation n'était pas à jour et concerné par des vulnérabilités permettant d'obtenir un accès puis de rebondir ensuite sur l'OT. Dans certains cas, les utilisateurs s'y connectaient avec un compte générique unique, connu d'un grand nombre de personnes, et pour lequel retrouver le mot de passe dans les partages réseaux, dans les locaux de l'entreprise, ou en discutant avec le personnel est souvent un jeu d'enfant. Finalement, ces serveurs censés améliorer la sécurité du passage de l'IT à l'OT deviennent des boulevards pour les attaquants.

Tous ces composants constituent donc un point d'entrée potentiel vers l'OT depuis l'IT, aussi nous allons essayer de nous en servir comme "pivot". Il est en revanche nécessaire d'avoir obtenu au préalable des privilèges suffisants sur ces postes ou serveurs, notamment en utilisant des techniques de tests d'intrusion IT ciblant l'Active Directory. Ensuite, nous pouvons créer un tunnel SSH ou utiliser des outils existants de tunneling type Chisel [21] ou Ligolo-ng [8] pour atteindre le réseau industriel.

6 Premiers pas dans l'environnement industriel

Lorsque nous sommes parvenus au réseau industriel, quel que soit le sous-réseau atteint, nous pouvons commencer à tester le système industriel

en lui-même. Notons qu'il arrive parfois que l'on audite uniquement cette partie et non les possibilités d'y accéder. Nous sommes alors dans la position d'un attaquant ou d'un malware introduit directement dans l'environnement, via une clé USB malveillante branchée sur un équipement, via un ordinateur compromis connecté au réseau industriel, ou dans le cas d'un utilisateur interne ou d'un prestataire malveillant qui a accès à l'environnement. C'est une préoccupation fréquente chez nos clients : des sous-traitants utilisent leurs propres ordinateurs portables pour la maintenance des machines chez tous leurs clients, et leur sécurité n'est pas toujours contrôlée.

Avant l'audit, nous demandons systématiquement un entretien avec un contact technique côté client pour obtenir les informations nécessaires sur l'architecture et le fonctionnement des procédés industriels. Lorsque nous sommes sur un environnement en production, cet entretien nous permet aussi d'anticiper un certain nombre de précautions, notamment en nous informant sur la localisation des zones et équipements considérés comme étant à risque. Ces discussions nous ont permis plusieurs fois d'identifier des automates très anciens ou des composants connus pour leur fragilité (par exemple, un serveur Linux sur une Raspberry Pi 1 connu pour redémarrer au moindre scan réseau) que le client préférait que nous évitions. Nous pouvons objecter à cette méthode qu'un attaquant réel n'aurait peut-être pas accès aux mêmes informations que nous, ce qui faciliterait nos tests. Certains clients choisissent de ne rien partager pour cette raison. Cependant, disposer de ces informations nous aide à isoler et à tester efficacement les composants en fonction de leurs caractéristiques, et nous évite de perdre du temps à rechercher des données que nous pourrions découvrir de toute façon. Mais nous évaluons toujours dans quelle mesure nous aurions pu obtenir ces informations par nous-mêmes afin d'apporter de la nuance aux résultats.

7 Phase de découverte

Dans un système industriel, nous allons voir des serveurs, des postes, des équipements réseaux, des équipements industriels divers et tout un tas d'autres composants qui ont généralement à la fois des caractéristiques IT et OT (logiciels, protocoles, ports physiques, etc.). Cela englobe donc les éléments nécessaires au fonctionnement physique de la production mais aussi tout ce qui permet son automatisation et l'interaction avec des utilisateurs humains. Pour être efficace, il est important de connaître les grandes catégories de composants qu'on peut trouver dans de tels systèmes.

Vu la diversité des types de systèmes qu'il est possible de rencontrer, nous ne sommes pas toujours compétents pour identifier exactement quel type de composant nous avons sous les yeux et il vaut mieux demander des précisions au client.

Puisque notre scénario initial implique que nous arrivons et testons depuis le réseau IP, nous n'interagissons qu'avec ce qui y est également connecté, ou ce qui est rendu visible par l'intermédiaire d'un composant qui sert de passerelle. Nous ne pouvons pas toujours faire confiance aux documents fournis (ils peuvent ne pas être à jour ou comporter des erreurs), aussi nous allons toujours faire une reconnaissance préalable, que nous appelons phase de découverte, qui va nous permettre de nous faire notre propre cartographie. Les types d'équipements que nous allons pouvoir contacter dépendent bien évidemment des sous-réseaux dans lesquels nous nous situons et de ceux que l'on peut atteindre. Pour simplifier ici, nous allons partir du principe que depuis là où nous sommes, nous pouvons "voir" sur le réseau IP tous types de composants : soit qu'ils sont tous mélangés sur un VLAN (cela arrive parfois), soit qu'il y a bien des VLAN dédiés pour chaque fonction, mais qu'ils ne sont pas isolés les uns des autres (cela arrive régulièrement). Lorsque les VLAN sont séparés et cloisonnés, nous devons, comme lors du passage de l'IT à l'OT, trouver des pivots pour passer d'une zone à l'autre.

7.1 Adapter les scans réseaux

Lors des tests d'intrusion IT, nous sommes généralement habitués à lancer des outils semi-automatisés (scanners) type nmap pour "découvrir" nos périmètres et nos cibles. Cette méthode s'applique également aux tests d'intrusion industriels mais nécessite de prendre quelques précautions supplémentaires dans les environnements en production. Aussi, nous respectons les principes suivants :

— Ne jamais y aller à l'aveugle
— Ne pas surcharger le réseau et les équipements
— Maîtriser ses outils

Ces trois règles excluent d'office certaines actions qu'on peut habituellement réaliser lors de tests d'intrusion IT. D'abord, nous ne pouvons pas faire de scan réseau "massif", pour obtenir un maximum d'informations sur le plus de composants possibles. Aussi, les scans réseaux et les scans de vulnérabilités doivent être ciblés et paramétrés spécifiquement pour éviter les effets de bord. Cela implique donc qu'il y a certaines spécificités à connaître concernant nos outils et leur réception par les équipements ciblés.

Mentionnons par exemple le fonctionnement de nmap : L'option `-sS` (SYN Scan) ne termine pas le handshake TCP et pourrait mettre un équipement ciblé dans un état instable, "bloqué" dans un état d'ouverture de connexion. Nous choisissons alors de privilégier l'option `-sT` (Connect Scan) que nous considérons plus sûre, mais il faut savoir que cela ne résorbe pas totalement les possibilités de mettre en défaut un équipement : en terminant le handshake TCP et donc en établissant réellement la connexion, il est possible que nous monopolisions sans le vouloir des emplacements de connexion pendant un temps indéfini sur certains équipements, qui sont alors inutilisables par d'autres procédés légitimes. Nous devons être conscients de ces problématiques lorsque nous paramétrons l'outil. De même, le fonctionnement des scans UDP (`-sU`), qui envoient par défaut des requêtes vides, peut aussi être problématique dans certains cas. Cependant on peut difficilement s'en passer car beaucoup de protocoles réseaux industriels avec une couche IP utilisent UDP. Aussi il est recommandé de ne les utiliser sur une cible que dans un second temps, lorsque l'on s'est assuré de sa robustesse. Pour aller plus loin sur ce sujet, il est possible de se référer à l'excellente présentation "Scanning highly sensitive networks" de Justin Searle [23].

Mais pourquoi prendre de telles précautions ? La manière de concevoir le cycle de vie du matériel informatique dans les environnements industriels est la plupart du temps très différente de ce à quoi l'on peut être habitué sur l'IT. Les équipements industriels coûtent souvent très chers, remplissent une fonction qui ne change pas ou peu et sont conçus pour durer. Ils peuvent également être difficiles à installer (physiquement et logiquement), à configurer et à intégrer dans l'environnement de production afin qu'ils fonctionnent sans danger. Également, certains environnements industriels fonctionnent en permanence, et ne peuvent pas être interrompus pour modifier des éléments. Cela signifie que, tant qu'il n'y a pas de problème avec un équipement, les équipes techniques préfèrent souvent ne pas y toucher pour éviter les dysfonctionnements. Dans certains cas, un changement peut aussi déclencher un nouveau processus de test, voire une nouvelle phase d'homologation complète du système. Ainsi, il est fréquent de trouver des équipements très anciens, qui ne disposent d'aucune fonctionnalité de sécurité. On trouve parfois des équipements conçus à une époque où l'OT fonctionnait en vase clos, et où ils n'étaient censés recevoir que des requêtes valides qui leur étaient destinées sur le réseau. Ces équipements pourraient ne pas supporter un trafic réseau important, voire planter s'ils reçoivent une requête qu'ils ne peuvent pas

interpréter. Ainsi, vous comprendrez qu'il devient très difficile de scanner un environnement dans lequel on pourrait trouver de tels équipements.

Au-delà du paramétrage d'outils que nous avons mentionné précédemment, il est préférable de restreindre les scans à un petit ensemble de composants à chaque fois, pour intervenir au plus vite en cas de perturbation (il est plus facile de surveiller 10 adresses IP que 254). De même, il est recommandé de d'abord scanner quelques ports pertinents, puis d'élargir les scans ensuite. Ce fonctionnement par étape est celui que nous appliquons habituellement. Nous commençons par un (ou plusieurs) premiers scans réduits pour identifier les cibles, suivis de scans adaptés à chaque type de cible. Lors du premier scan de découverte, nous ciblons habituellement les ports suivants : FTP, SSH, Telnet, HTTP, HTTPS, SMB, RDP et VNC. Il peut nous arriver de restreindre encore cette liste ou de faire une découverte port par port lorsque l'environnement nous semble trop peu robuste. Le fait qu'un port spécifique soit ouvert puis l'accès aux services avec des clients dédiés nous permet souvent d'identifier le type d'équipement, par exemple via les headers ou autres informations affichées. Notons que notre première liste ne comprend que des services IT, car nous considérons qu'il est préférable de commencer la phase de découverte par les standards IT, et de ne regarder les services purement OT que dans second temps. Cela nous semble d'une part plus efficace, car on retrouve toujours à peu près les mêmes services IT, et d'autre part plus sûr, car ces services sont bien mieux connus et nous disposons donc déjà des bons outils pour communiquer avec eux sans risque.

7.2 Autres méthodes de découverte

Une méthode qui donne de précieuses informations sur les composants du réseau est la découverte passive avec un outil de capture réseau type Wireshark. Ce dernier intègre déjà énormément de dissecteurs pour des protocoles industriels [10], ce qui facilite beaucoup la découverte et la compréhension de leur fonctionnement. On peut par exemple trouver des dissecteurs pour des protocoles issus du secteur automobile tels que CAN, DeviceNet ou SOME/IP. Puisque nous ne faisons aucune requête nous-même et nous contentons d'écouter le trafic réseau, il n'y a pas d'impact sur le fonctionnement du système. Cette technique peut également être utile dans le cadre d'audits nécessitant une approche plus discrète de type Red Team.

Sur les systèmes industriels, il n'est pas rare que des équipements communiquent uniquement par broadcast. Ce fonctionnement, où chaque équipement reçoit tout mais ne traite que ce qui lui est destiné, est parfois

hérité des modèles antérieurs à l'interconnexion des systèmes industriels au réseau informatique. Mais il permet surtout de pallier à l'absence, dans certaines architectures, d'équipements réseaux tiers pour l'attribution des adresses et des messages. Nous l'avons par exemple déjà rencontré dans des réseaux d'équipements de signalisation de transports en commun, où chaque automate recevait des informations de tous les autres via un protocole réseau industriel propriétaire dédié à ce système.

De même, l'utilisation du multicast est courante sur ce type de réseau. En connaissant la bonne adresse, il est possible d'y envoyer une requête qui ne sera distribuée qu'à ceux qui la supportent, et éventuellement d'y souscrire. Par exemple, le protocole industriel KNXnet/IP utilise l'adresse multicast `224.0.23.12`. En envoyant une `Description Request` sur cette adresse, tous les équipements qui y ont souscrit renverront individuellement une `Description Response`, nous permettant ainsi d'établir une liste (avec informations détaillées) de ce type d'équipements (figure 3).

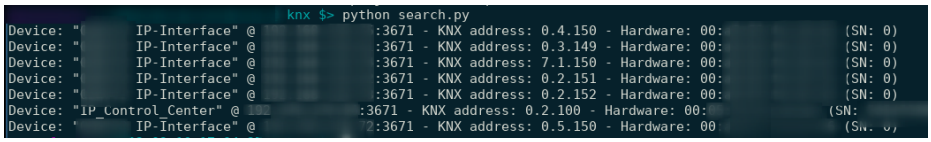

Fig. 3. Exemple de réponse à une `Description Request` envoyée sur l'adresse multicast de KNXnet/IP

A l'issue de cette première étape de découverte, nous sommes habituellement capables de catégoriser nos cibles (les postes, les serveurs, les équipements réseaux et autres équipements industriels). Sur certains, nous avons déjà suffisamment d'informations pour les identifier grâce aux services consultés précédemment. Sur d'autres il va falloir aller plus loin et faire une découverte ciblée.

Un certain nombre d'éléments identifiés se retrouvent aussi dans l'IT : systèmes d'exploitation Windows ou Linux, protocoles réseaux type FTP, SSH ou RDP, annuaires Active Directory, etc. Nous allons laisser ces éléments de côté et nous concentrer sur les composants purement OT. Notons simplement sur ce sujet que les précautions dont nous avons discuté plus haut peuvent s'appliquer, notamment parce que, pour les raisons que nous avons évoquées, il peut y avoir des composants anciens. Par exemple, nous voyons encore très régulièrement des postes sous Windows XP, voire Windows 98 ou 95, qui continuent à être maintenus pour des logiciels spécifiques utilisés par des machines industrielles. Restent les composants

OT qui, à notre niveau vont plutôt prendre la forme de logiciels dédiés à des procédés industriels (utilisables sur les postes et serveurs après avoir obtenu un accès, légitime ou non) et les protocoles réseaux industriels. Ces derniers sont ce que l'on voit et auxquels on accède le plus facilement depuis notre position sur le réseau. C'est en les interrogeant que nous obtiendrons le plus d'informations pour identifier l'équipement et pour préparer la suite des tests d'intrusion.

8 Les protocoles réseaux industriels

Il existe une multitude de protocoles réseaux industriels sur des liaisons filaires et sans fil très variées. Ces derniers peuvent être spécifiques à un constructeur (exemples : S7comm pour Siemens, FINS pour Omron) ou à un secteur (exemples : DICOM pour la gestion d'images médicales, les protocoles de la norme IEC-61850 pour les réseaux électriques). Ils peuvent aussi être issus de consortium ou d'organismes pour devenir des standards, tels que CIP et Ethernet/IP (ODVA) ou OPC-UA (OPC Foundation). Au moment où cet article est rédigé, nous en avons recensé 66 [10] tout en sachant que nous sommes très loin de la réalité : avec un peu de motivation on pourrait en découvrir tous les jours. Nous rencontrons également de temps en temps des protocoles propriétaires développés directement par nos clients.

Historiquement, beaucoup d'entre eux servaient à l'échange d'informations entre des équipements purement "terrains" via un lien série (ex : RS-232 ou RS-485). Puis, certains ont été adaptés, ou de nouveaux protocoles ont été créés pour répondre aux problématiques d'interconnexion. Cela concerne en premier lieu le réseau IP (par exemple, le protocole HART dispose d'une version HART-IP) mais également d'autres standards de communication plus récents (notamment le standard sans fil ISA100.11a dédié aux systèmes industriels et objets connectés [20]). Mais cela ne signifie pas pour autant que les anciens protocoles ont disparu. Aussi, dans un système industriel, il est fréquent de rencontrer, en filaire et sans fil, à la fois des protocoles sur IP et d'autres protocoles sur différents canaux.

Lors d'un test d'intrusion, nous pouvons interagir directement avec ceux sur le réseau IP, mais nous ne pouvons atteindre les autres que si nous disposons d'outils spécifiques ou si nous découvrons une passerelle qui fait de la traduction vers d'autres canaux. Puisque qu'il faudrait un article à part entière pour aborder de manière exhaustive les tests de protocoles industriels, et que dans l'environnement qui nous intéresse ici

(la production) nous devons de toute façon limiter nos tests ciblant les composants OT, nous allons nous focaliser dans la suite sur la couche IP.

Les protocoles que l'on est susceptible d'y trouver sont donc très variés. Nous en voyons certains fréquemment, et d'autres de manière plus anecdotique. Cela dépend des contraintes et préférences de nos clients, de leur activité et secteur industriel, mais également de leur localisation géographique. Par exemple, nous voyons souvent les protocoles S7comm et Modbus en France car il y a beaucoup d'automates programmables (PLC) de marque Siemens ou Schneider Electric, ce qui n'est pas forcément le cas dans d'autres pays.

Comment les identifier lors de la phase de la découverte ? Nous avons déjà mentionné la découverte par broadcast et multicast qui peut être très utile. Pour le reste, nous pouvons rechercher les ports industriels ouverts sur les équipements. Avec l'expérience viennent certains réflexes : face à un automate Rockwell, il est souvent intéressant de scanner le port Ethernet/IP par défaut (44818/tcp). Sur un système de gestion technique de bâtiment (GTB), nous sommes notamment susceptibles de croiser KNXnet/IP (3671/udp) ou BACnet/IP (47808/udp). Les ports utilisés par les protocoles industriels sont rarement dans le top 1000 nmap (les ports scannés par défaut). Aussi, pour éviter de scanner 65535 ports, il est nécessaire de savoir reconnaître les protocoles les plus utilisés et de savoir comment dialoguer avec.

8.1 La question de l'outillage

Qu'avons-nous à notre disposition pour communiquer avec les équipements en utilisant ces protocoles industriels ? Soyons francs : le sujet est un peu compliqué. Un moyen sûr de dialoguer via un protocole industriel serait d'utiliser un outil officiel (par exemple, un logiciel de programmation fourni par l'éditeur d'une solution industrielle). Cela arrive parfois, mais le monde des standards et des constructeurs industriels est globalement très fermé et fait de logiciels onéreux et de protocoles propriétaires. Cela implique que les outils légitimes que nous pourrions utiliser sont souvent difficiles à trouver et très chers. Il est aussi compliqué d'obtenir des spécifications ou autres informations techniques, et encore plus de trouver des alternatives comme des implémentations open source (même si cela existe quand même, par exemple avec FreeOpcUa [2]). Finalement, même lorsque nous avons des spécifications à disposition ou que nous avons la possibilité de faire de la rétro-ingénierie sur ces protocoles, beaucoup restent très difficiles à utiliser à cause de leur fonctionnement très spécifique ou à cause de leur complexité.

Ensuite, comme il y a beaucoup de secteurs industriels différents, de constructeurs, de technologies, d'équipements, de standards et finalement de protocoles, il faudrait se constituer un arsenal impressionnant pour pouvoir s'adapter à toutes les situations et tous les protocoles que nous rencontrons. On trouve évidemment quelques outils qui permettent d'interagir avec des composants en utilisant certains protocoles (ex : ctmodbus [9] ou ModbusDoctor [16] pour Modbus, Snap7 [18] pour S7comm, etc.), mais il devient vite difficile de se reposer sur des solutions existantes lorsqu'on s'écarte des protocoles les plus connus. Il faut donc souvent développer nos propres scripts en fonction des situations que nous rencontrons. On pourrait d'ailleurs étendre ce constat plus globalement aux outils de test offensifs : Malgré quelques essais épars (tels que ISF [12]) et la présence de quelques modules OT dans des outils généralistes (par exemple, les scanners "Scada" de Metasploit [22]), nous n'avons pas d'outillage offensif OT aussi complet que ce qui existe pour l'IT, et il faut souvent mettre la main à la pâte.

Se pose finalement la question du test de ces outils existants ou développés par nos soins. Interagir avec les protocoles industriels durant un test d'intrusion sur un environnement en production n'est pas anodin : une requête invalide ou malveillante peut avoir un effet bien réel sur le comportement d'un équipement (comme nous le verrons bientôt). Aussi, il est nécessaire de le faire selon une méthode ou avec un outil que l'on a déjà testé au préalable afin de réaliser ce type de requête en sécurité. Puisque nous ne pouvons évidemment pas tester en production, cela nécessite l'accès à des environnements de test chez nos clients, ou de créer nos propres infrastructures de test. Cela peut également être difficile, encore une fois pour des raisons d'accessibilité des outils et des standards, mais aussi de complexité de mise en place de tels environnements.

8.2 Utiliser les protocoles industriels

Résumons : lorsque nous voulons interagir avec des protocoles industriels lors d'un test d'intrusion, nous avons pour l'instant accès à un nombre limité d'outils existants, et il faut avoir la capacité de les tester en amont. Malgré ces lacunes, il serait dommage de laisser de côté les protocoles industriels. Bien utilisés, il est possible d'en tirer partie pour obtenir des informations essentielles durant nos tests d'intrusion et pour démontrer la faisabilité de certaines attaques spécifiques au monde industriel.

Pour illustrer cela, nous pouvons tout d'abord regarder comment utiliser ces protocoles lors de notre phase de découverte pour obtenir des informations supplémentaires sur les équipements ciblés (par exemple,

la version du firmware, à quoi il sert, avec quels autres équipements il dialogue, etc.). Pour tous ceux que nous avons déjà rencontrés, il existait au moins un type de requête à envoyer pour demander à l'équipement de se décrire, comme les `Description Request` KNXnet/IP que nous avons vu précédemment.

Pour les protocoles les plus connus, il existe des scripts directement intégrés dans nmap, comme `modbus-discover`, `enip-info`, `bacnet-info`, etc. Il existe également des scripts nmap externes que nous pouvons utiliser (tant que nous sommes sûrs de la confiance que nous pouvons leur accorder), comme ceux proposés dans le dépôt Redpoint [7].

Nous pouvons également créer un script qui envoie une requête de découverte pour un protocole particulier et interprète la réponse reçue par l'équipement. Pour cela, nous nous reposons beaucoup sur Scapy [24], qui est extrêmement efficace non seulement pour créer des requêtes à partir d'implémentations de protocoles existantes, mais également pour créer de nouvelles implémentations rapidement. Notons d'ailleurs que plusieurs protocoles industriels sont déjà intégrés à Scapy. Voici un exemple de script utilisant Scapy pour la découverte Ethernet/IP (bien qu'on puisse aussi le faire avec nmap pour ce protocole) :

Listing 1: Découverte Ethernet/IP avec Scapy

```
from sys import argv
from socket import socket
from scapy.all import StreamSocket, raw, Raw
from scapy.contrib.enipTCP import ENIPTCP

s = socket()
s.connect((argv[1], 44818))
ss = StreamSocket(s, Raw)
# Creation de la requete
pkt = ENIPTCP()
pkt.commandId = 0x63
# Envoi de la requete, reception de la reponse
resp = ss.sr1(pkt)
resp = ENIPTCP(raw(resp))
resp.show2()
```

En l'exécutant, nous obtenons une réponse telle que présentée en figure 4. Nous savons ainsi qu'ici nous avons bien affaire à un équipement qui utilise le protocole Ethernet/IP, sans authentification, nommé `Anybus Communicator`. Nous connaissons son fabricant, son numéro de série, la version de son firmware, ce qui est une bonne base quand l'objectif est de rechercher des vulnérabilités.

```
SSTIC DEMO python enip_discovery.py 192.168.1.241
Begin emission:
Finished sending 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
###[ ENIPTCP ]###
  commandId = ListIdentity
  length    = 59
  session   = 0x0
  status    = success
  senderContext= 0
  options   = 0
###[ ENIPListIdentity ]###
     itemCount = 256
     \items     \
      |###[ ENIPListIdentityReplyItem ]###
      |  itemTypeCode= CIP Identity
      |  itemLength= 53
      |  protocolVersion= 1
      |  sinFamily = 2
      |  sinPort   = 44818
      |  sinAddress= 192.168.1.241
      |  sinZero   = 0
      |  vendorId  = 90
      |  deviceType= Communications Adapter
      |  productCode= 93
      |  revisionMajor= 1
      |  revisionMinor= 8
      |  status    = 48
      |  serialNumber= 0xa06f262f
      |  productNameLength= 19
      |  productName= 'Anybus Communicator'
      |  state     = 255
```

Fig. 4. Réponse à une requête Ethernet/IP `ListIdentity`

9 Recherche de vulnérabilités

Passé la découverte, nous avons logiquement une meilleure appréciation de notre environnement. Cependant, nous ne sommes pas là pour faire de la cartographie mais bien pour trouver des vulnérabilités. Soulignons d'abord que le fait que nous soyons le plus souvent sur des environnements en production nous empêche d'aller plus loin dans certains cas. En particulier, nous ne pouvons pas déclencher des actions qui pourraient altérer le comportement, le paramétrage ou les données des composants. Il n'est pas non plus possible de nous servir de vulnérabilités (type CVE [1]) qui nécessitent d'exploiter des bugs logiciels pour amener un composant à effectuer des actions non prévues, puisque cela le met souvent dans un état instable. Nous sommes cependant généralement capables de déduire ce que nous sommes en mesure de faire, en fonction des versions des composants, du comportement, ou en réalisant des tests non destructifs qui montrent que l'on pourrait utiliser le même procédé de manière malveillante. Nous pouvons également parfois valider nos hypothèses si le client peut nous fournir des équipements hors production qu'on peut tester de manière plus approfondie. Malgré ces contraintes, nous découvrons

presque systématiquement des problèmes de sécurité. Ils peuvent alors être utilisés pour interrompre ou modifier le procédé industriel ou au moins certains composants sensibles (nous ne le faisons pas durant l'audit, sauf sur demande du client), altérer des données de fonctionnement, obtenir des données sensibles, etc. En réalité, une bonne partie de ces défauts vont se déclarer d'eux-mêmes pendant la phase de découverte, et nous allons voir ci-dessous ceux que nous retrouvons le plus souvent et qui peuvent conduire à ce type de résultats.

9.1 Ancienneté des composants

Nous avons insisté précédemment sur les différences de cycle de vie des composants, sur le fait qu'il n'est pas toujours possible de les remplacer, de les mettre à jour, voire d'appliquer les correctifs lorsque c'est nécessaire. Cela implique donc que, la plupart du temps, nous découvrons des composants qui ne sont pas dans une version récente, voire qui ne sont plus maintenus. Nous avons déjà vu les problèmes relatifs à Windows et aux logiciels industriels. Certains composants, y compris des équipements industriels, sont susceptibles d'être concernés par des vulnérabilités mais ne peuvent pas être mis à jour. L'une des CVE que nous avons publiée en 2024 sur une passerelle réseau industrielle révèle un déni de service après l'envoi d'un petit nombre de requêtes réseaux sur l'un de ses ports, qui peut aussi être déclenché involontairement [26]. La solution proposée par le fabricant pour s'en prémunir est de remplacer l'équipement, ce qui n'est pas si facile à mettre en œuvre et coûte cher.

De même, les protocoles, services, logiciels, etc. peuvent ne pas disposer des fonctions de sécurité que l'on préconise de nos jours. Sur ce sujet, on peut citer les mécanismes d'authentification qui, quand il y en a, ne respectent pas les standards actuels : communication non chiffrée, mode d'authentification peu sécurisé, mot de passe administrateur non modifiable, etc. Dans ce cas, contourner l'authentification ou obtenir des identifiants devient donc une simple formalité, et permet ensuite d'accéder aux fonctionnalités sensibles qu'elle est supposée protéger.

Grâce à cela, nous avons par exemple pu accéder à des logiciels d'entrepôts logistiques (WMS, pour Warehouse Management Systems), depuis lesquels il était notamment possible de modifier les données relatives aux marchandises stockées. Cela n'a normalement pas un impact fort, car selon les cas cela pourra être détecté et rétabli rapidement, par exemple en restaurant une sauvegarde. On pourrait cependant imaginer un scénario d'attaque où les données sont falsifiées progressivement sur un temps suffisamment long pour que toutes les sauvegardes soient également

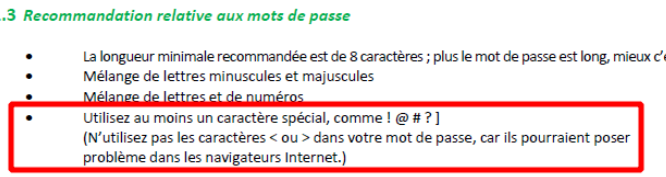

Fig. 5. Extrait du manuel utilisateur d'une passerelle de gestion technique de bâtiment suggérant que l'application associée pourrait être vulnérable aux injections

corrompues. Dans ce cas-là, cela rendrait le traitement des commandes difficile voire impossible le temps de rétablir la situation, ce qui pourrait représenter un coût financier significatif.

9.2 Sécurité des protocoles réseaux

Nous avons aussi vu que certains anciens protocoles d'administration IT sont toujours utilisés dans une partie des environnements industriels sur lesquels nous intervenons. C'est également le cas de beaucoup de protocoles réseaux industriels. Les protocoles que nous avons cités pour notre phase de découverte ne nécessitent pas d'authentification pour obtenir des informations détaillées sur les équipements. Un bon exemple pour montrer ce cheminement est, encore une fois, le protocole KNXnet/IP, qui est un portage du protocole KNX, qui communique via une liaison "terrain" (le bus KNX). Par défaut, il ne comporte aucune sécurité, pas de chiffrement, pas d'authentification, pas de signature, etc. Une requête valide reçue par un équipement sur le port 3671/udp sera réceptionnée et exécutée. Ainsi, en suivant le même procédé que pour l'envoi d'une `Description Request` un peu plus haut pour obtenir des informations, nous pourrions envoyer une `Configuration Request` ou un autre paquet qui pourrait altérer le fonctionnement d'un équipement. Ces observations sont également valables pour de nombreux autres protocoles. Nous pouvons par exemple mentionner le cas de protocoles utilisés dans le milieu médical, comme DICOM ou HL7, dont les problèmes de sécurité ont été exposés à plusieurs reprises dans des conférences de sécurité offensive [11].

Hors production, nous pouvons être amenés à démontrer que nous avons la capacité d'extraire le programme d'un automate, de le modifier et de le réinjecter sur l'automate afin de modifier son comportement. Une façon de réaliser une telle attaque, qui a souvent marché pour nous, est d'envoyer directement à l'automate des commandes via ces protocoles industriels. Cela nécessite par contre d'avoir des notions de programmation automate (logique, langages types Ladder ou Graphcet, etc.). L'attaque

devient particulièrement aisée si le protocole n'est ni chiffré, ni authentifié, et si l'automate ne vérifie pas l'authenticité du programme. Notons qu'il pourrait être possible d'arriver au même résultat en compromettant une station de programmation (souvent un poste sous Windows), et donc en poussant des programmes corrompus depuis une source légitime.

9.3 Configuration

Au-delà des mécanismes vulnérables ou de l'absence de fonctions de sécurité, on pourrait mentionner que, même lorsqu'il y en a et qu'elles peuvent être modifiées, elles ne sont pas systématiquement configurées de manière sécurisée. Par exemple, il reste très fréquent de voir des équipements qui ont été laissés dans leur configuration initiale. En général, les intégrateurs ne sont pas des informaticiens, ils ne sont peut-être même pas en contact avec la partie informatique, et encore moins avec la cybersécurité. C'est donc par manque de sensibilisation à ce sujet [4], parfois également par habitude, que ces configurations ne sont pas changées. Cela se traduit souvent par la présence d'identifiants par défaut pour se connecter aux services de l'équipement et pour l'administrer. Cela signifie que nous pouvons les retrouver, car ils sont donnés dans le manuel utilisateur du composant, généralement publié sur Internet. Il existe aussi des bases telles que SCADAPASS [25] qui recensent les identifiants par défaut d'un nombre important d'équipements industriels. Souvent, les services par défaut sont aussi laissés actifs, dans leur paramétrage d'origine, même lorsqu'ils ne sont pas utilisés. Ils constituent autant de portes d'entrée potentielles pour un attaquant.

9.4 Pratiques

Même lorsqu'il y a une volonté de renforcer la sécurité d'un système, les moyens mis en oeuvre se heurtent aux pratiques opérationnelles : le système doit rester utilisable par ses utilisateurs avec le moins de contraintes possibles pour ces derniers, tout en répondant aux contraintes de fonctionnement des procédés industriels. Durant un test d'intrusion, c'est plutôt sur les problématiques d'authentification que nous sommes confrontés au poids des pratiques opérationnelles. Un cas récurrent est celui des postes opérateurs. Ils sont souvent accessibles sans authentification ou avec un mot de passe écrit - voire gravé - sur l'écran ou le clavier, avec un compte unique utilisé par tous. Les bonnes pratiques préconisent que chacun établisse une session authentifiée à son nom sur le poste qu'il ou elle utilise. Cependant, il y a de nombreuses raisons qui font que ce

n'est pas toujours possible : plusieurs personnes qui utilisent le poste en même temps, nécessité d'intervenir en urgence qui rend impossible la saisie systématique d'un mot de passe, etc. Rappelons également que, dans beaucoup d'environnements industriels, les utilisateurs ont des priorités bien éloignées du monde de la cybersécurité et qu'il est bien évident qu'ils préfèrent assurer la sécurité de leurs collègues plutôt que celle des systèmes informatiques. Finalement, comme sur l'IT, les personnes qui administrent le SI industriel manipulent une multitude de mots de passe. Même si la tendance est plutôt à l'adoption de gestionnaires de mots de passe (ce qui n'est d'ailleurs pas toujours pratique pour elles), il n'est pas rare de trouver des environnements où le même mot de passe est utilisé partout. Ainsi, en le retrouvant, nous avons accès à tous les composants du système industriel.

9.5 Robustesse des équipements

Puisque nous prenons les précautions nécessaires pour ne pas rendre indisponibles les environnements en production, ce point n'est pas systématiquement remonté. Il nous arrive toutefois de signaler des équipements particulièrement fragiles qui dysfonctionnent même après une action non intrusive, car cela implique qu'une action légitime hors test d'intrusion pourrait aussi les rendre indisponibles. Il peut aussi arriver que nous réalisions des audits qui ciblent uniquement un composant industriel (par exemple, une passerelle GTB ou un PLC). Dans ces cas-là, nous pouvons tester de manière approfondie toutes les couches du système : le matériel, les ports physiques, le firmware, le système de fichiers, les services, les applications, le réseau filaire et sans fil, l'interface ou tout autre élément qui constitue cet équipement. La robustesse des éléments logiciels fait généralement partie des aspects vérifiés.

L'un de nos audits comportait des tests visant à évaluer la résistance d'équipements en réseau dans un environnement simulé en les soumettant à une charge réseau élevée et à des requêtes invalides envoyées sur le port de leur protocole propriétaire. L'outil idéal pour ce genre de test est un fuzzer réseau. Nous en avons conçu un simplifié qui sert habituellement pour nos recherches [27], pour envoyer un grand nombre de requêtes, avec un contenu totalement aléatoire, dans un premier temps, puis avec un header valide suivi d'un contenu aléatoire pour qu'il passe les premières vérifications du service. Le résultat ne s'est pas fait attendre, un CPU à 100%, des messages d'erreur dans l'IHM comme s'il en pleuvait, un client dépité mais satisfait, et un bon souvenir d'audit pour nous.

10 Protéger les systèmes industriels

Vous l'aurez compris, l'obsolescence est un problème mais les responsables de ces systèmes ne peuvent pas toujours y faire grand-chose. Les configurations ne sont pas toujours modifiables, et quand elles le sont, elles dépendent des connaissances en la matière de ceux qui les définissent. Elles sont aussi conditionnées par les pratiques opérationnelles qui dépendent des fortes contraintes qui s'appliquent à ces systèmes.

Sachant tout cela, comment corriger les vulnérabilités que nous découvrons durant ces audits ? Premièrement, en mettant à jour et en durcissant ce qui peut l'être, en sensibilisant les utilisateurs. Parfois il y a quand même des possibilités pour améliorer la situation sans que cela ne devienne une contrainte insurmontable. Il est également recommandé d'appliquer des mesures de sécurisation du côté de la gestion d'identité, du durcissement des composants (par exemple, avec des solutions de scellement de poste), de la résilience ou encore de la surveillance de ces systèmes. Pour cela, il est possible de se référer aux guides de l'ANSSI dédiés à la sécurité des systèmes industriels [3] et à l'administration sécurisée des SI [5], ou à d'autres référentiels tels que ceux du NIST [19].

Le cloisonnement réseau, c'est-à-dire la mise en place de mesures de contrôle et de restriction des flux réseaux entre les zones sur le réseau informatique, est probablement la mesure la plus importante à l'heure actuelle pour la sécurisation des systèmes d'information industriels. Si on ne peut pas joindre l'équipement sur le réseau, on ne peut pas s'authentifier dessus. Si on ne peut pas atteindre le service qui nous le permet, on ne peut pas envoyer des requêtes pour changer le comportement du composant. Cela ne dispense pas pour autant d'appliquer des mesures de sécurité à l'intérieur du système autant que possible. En se basant sur les référentiels cités précédemment, il est recommandé de faire en sorte que le SI industriel n'ait qu'un seul point de contact avec l'extérieur : une DMZ étroitement surveillée par laquelle passent tous les flux nécessaires. Cela implique de supprimer toute connexion internet directe depuis l'OT, y compris les accès distants via VPN, très fréquents pour la maintenance à distance des machines, qui doivent donc passer par l'IT puis par la DMZ. Entre cette DMZ et l'OT, et à l'intérieur même de l'OT, nous préconisons de n'autoriser que les échanges réseaux nécessaires au bon fonctionnement de l'ensemble. Il est recommandé pour cela de définir des "zones de confiance" (trust zones) pour séparer les composants selon leur criticité et/ou selon le type d'autorisation nécessaires pour y accéder. La version orientée cybersécurité du Purdue Model schématisée en figure 6 montre un modèle

standard d'architecture réseau qui intègre ces mesures de cloisonnement. Tout ceci mis bout à bout permet de réduire la surface d'attaque et de rendre l'accès aux composants sensibles le plus difficile possible. Cependant, ces recommandations nécessitent un fort investissement pour définir et maintenir ces règles sur le long terme, il vaut donc mieux y aller par étapes. Mais nous constatons que, chez nos clients qui ont réussi à aller jusqu'au bout de la démarche, ces mesures sont efficaces et nous sommes vite bloqués dans nos tests.

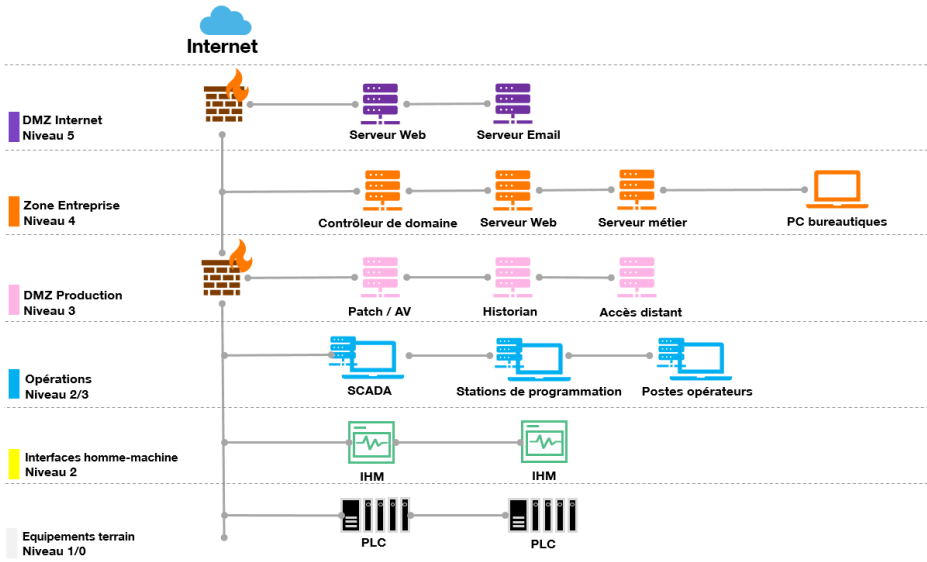

Fig. 6. Purdue Model orienté cybersécurité

11 Construction des scénarios

La dernière étape de l'audit consiste à combiner les vulnérabilités que nous avons trouvé pour concevoir des scénarios d'exploitation applicables techniquement, et surtout dont les impacts potentiels sont pertinents dans le contexte de notre client. Pour cela, il est encore une fois préférable de discuter avec nos contacts pour appréhender les aspects métiers que nous ne faisons qu'effleurer durant le temps imparti à l'audit.

Bien que chaque situation soit spécifique à l'environnement et aux enjeux métiers sous-jacents, un scénario type que nous retrouvons fréquemment est le suivant : L'attaquant obtient un accès au système d'information

industriel par l'intermédiaire d'un serveur qui dispose d'un accès à la fois à l'IT et à l'OT. Il peut ensuite atteindre les composants sensibles du SI industriel (par exemple, des automates programmables (PLC), des logiciels industriel, etc.) sur le réseau, dont il peut utiliser les fonctions sans privilège ou en ayant obtenu les privilèges suffisants pour le faire. Ce faisant, il pourrait être en mesure d'arrêter totalement le fonctionnement du procédé industriel, de contrôler tel ou tel élément impliqué dans ce procédé ou de modifier son paramétrage (par exemple, la teneur en produits chimiques d'une solution). Il pourrait aussi falsifier les informations remontées à la supervision et les journaux d'événements (par exemple, pour que tout ait l'air normal), obtenir des informations techniques ou métiers sensibles, ou tout autre événement redouté par notre client, selon son activité et la nature de son système.

Pour changer de l'exemple d'une usine avec des chaînes de production, illustrons avec un environnement GTB (Gestion Technique de Bâtiment) contenant des éléments relativement similaires selon les typologies de clients (sauf s'ils disposent de composants ou salles spécifiques, comme des entrepôts frigorifiques). Cet environnement type comporte les éléments nécessaires pour la gestion de la température, des lumières, des volets et de la vidéosurveillance d'un bâtiment. Un scénario possible, résumé en figure 7, consiste à d'abord obtenir des droits et accès sur le système d'information bureautique en compromettant l'Active Directory. L'obtention de droits supplémentaires nous permet de nous connecter au serveur permettant de contrôler la GTB qui se situe lui aussi sur l'IT, car il est utilisé par le personnel du PC sécurité dont les ordinateurs sont reliés à l'AD. En passant par ce serveur (par exemple, via RDP ou en établissant un tunnel sur le réseau), nous avons accès aux composants GTB, situés sur un réseau dédié, que le serveur GTB permet de contrôler. Puisqu'il n'y a pas de cloisonnement, ou pas de filtrage, au sein même de ce réseau dédié, une fois un premier accès obtenu nous voyons tout ce qui s'y trouve. Cela inclut notamment d'autres serveurs (des serveurs applicatifs, des serveurs d'enregistrement pour la vidéo (NVR), etc.) et des ordinateurs dédiés au contrôle d'un aspect de la GTB (comme des postes sous Windows permettant la gestion globale de la température et permettant d'ajuster indivuellement la température des salles). On y trouve également des IHM et autres "contrôleurs" pour interagir directement avec le paramétrage des équipements, ou encore des passerelles permettant l'interfaçage entre le réseau IP d'où proviennent les instructions et le réseau terrain où sont situés les capteurs et actionneurs finaux (sondes, interrupteurs et autres

panneaux de commande, lumières, volets, caméras, chauffage/climatisation, etc.).

En tirant partie des défauts de configuration, nous pouvons nous connecter à un certain nombre de services exposés par les différents composants. Dans cet exemple, si nous ciblons les fonctionnalités liées à la température du bâtiment, nous pouvons par exemple accéder en RDP à un ordinateur utilisé pour la gestion de la température et la synchronisation avec la supervision en utilisant des identifiants locaux Windows découverts dans un partage réseau côté IT. Via ce poste, nous sommes capables de modifier les données de fonctionnement et la remontée d'informations. Nous pouvons également nous connecter à l'interface web d'un contrôleur de température, qui ne nécessite pas d'authentification, et changer directement ses configurations techniques (par exemple, son adresse IP, le rendant injoignable sur le réseau par les équipements auxquels il est relié) ou ses valeurs de fonctionnement (la valeur définie, les seuils de température tolérés, etc.). Nous pouvons finalement passer directement par les protocoles réseaux industriels. Sur ce type de système, nous sommes par exemple susceptibles de trouver le protocole BACnet/IP, et avons alors la possibilité d'envoyer des trames (non authentifiées) à une passerelle BACnet qui seront transmises au matériel final ciblé (par exemple, une climatisation) pour changer son comportement. Evidemment, nous ne le faisons pas sur un environnement en fonctionnement car cela pourrait causer des dégâts : arrêter ou dérégler la climatisation pourrait par exemple endommager le matériel d'une salle serveur, ou la santé des employés dans une tour en verre à La Défense en plein mois d'août.

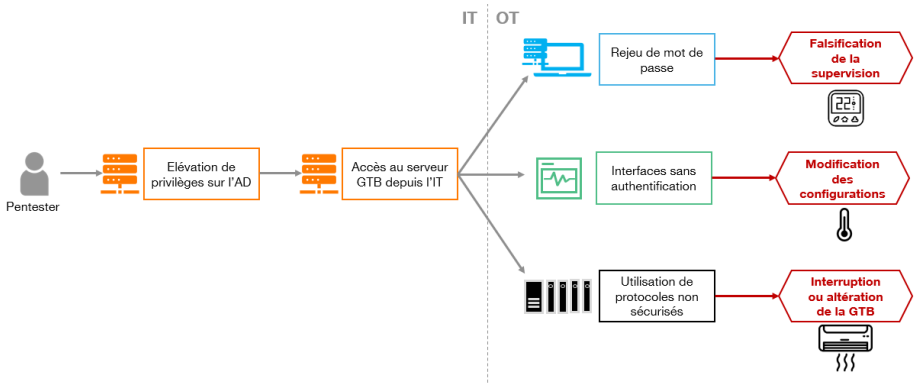

Fig. 7. Schéma d'intrusion simplifié sur un système de gestion de la climatisation d'un bâtiment

12 Conclusion

Ainsi s'achève un test d'intrusion interne en milieu industriel. En lisant cet article, vous avez peut-être eu la sensation que le niveau de cybersécurité sur les systèmes industriels était très bas. Rassurez-vous, ce n'est pas le cas. Certes, on constate un retard global par rapport à l'IT mais, si l'on compare à la situation d'il y a cinq ou dix ans, nous rencontrons de plus en plus de clients très matures sur ces questions qui, en plus d'être soumis aux réglementations gouvernementales, sont conscients de l'impact des cyberattaques et agissent en conséquence. Et comme le monde n'est pas binaire, la plupart des environnements que nous rencontrons ont des points forts et des points faibles. Aussi, il peut rester au moins un équipement très fragile même dans un environnement qui respecte l'état de l'art en matière de sécurité qui justifie que l'on continue à prendre nos précautions.

Nous avons essentiellement parlé tests d'intrusion sur des systèmes industriels complets en fonctionnement - même si nous avons fait quelques écarts - car c'est la configuration que nous rencontrons le plus souvent. Mais on pourrait faire un article tout aussi long sur ce qu'il est possible de faire lorsque nous travaillons en environnement de test, physique ou simulé, lorsque nous réalisons des tests approfondis d'un équipement industriel, ou encore lorsque notre audit a des objectifs différents, comme tester le bon fonctionnement des systèmes de détection d'intrusion mis en place dans les environnements industriels (Purple Team). Nous pourrions finalement nous intéresser en détail à la logique des procédés industriels ciblés, notamment via les programmes automates, et à la meilleure façon de les détourner.

Concluons avec un petit appel à la prudence : vous aurez remarqué au fil de l'article à quel point il est important de tester ces systèmes souvent critiques. Mais vous aurez aussi compris qu'on ne peut pas les tester comme n'importe quel autre système. Nous pensons qu'il est nécessaire que ce type d'audit soit mieux connu par les commanditaires d'audits et par les exécutants. J'entends trop souvent des histoires d'auditeurs, toutes entreprises confondues, qui se sont retrouvés malgré eux face à des environnements industriels car leur client ne connaissait ni les méthodologies d'audits, ni les impacts possibles. Ces auditeurs les ont testés comme n'importe quel autre système, sans prendre de précautions, causant parfois des dégâts, et sans inclure dans les tests les éléments techniques qui sont spécifiques au monde industriel. Aussi, puisque ce type de tests tend à se répandre, il devient urgent que tous les acteurs comprennent bien ce

qu'un test d'intrusion sur un système industriel implique et testent de manière appropriée pour éviter les catastrophes.

Références

1. CVE (Common Vulnerabilities and Exposures. https://cve.mitre.org/.
2. Free OPC-UA Library. https://freeopcua.github.io/.
3. ANSSI. La cybersécurité des systèmes industriels. https://cyber.gouv.fr/publications/la-cybersecurite-des-systemes-industriels, 2014.
4. ANSSI. Guide pour une formation sur la cybersécurité des systèmes industriels. https://cyber.gouv.fr/publications/guide-pour-une-formation-sur-la-cybersecurite-des-systemes-industriels, 2015.
5. ANSSI. Recommandations relatives à l'administration sécurisée des SI. https://cyber.gouv.fr/publications/recommandations-relatives-ladministration-securisee-des-si, 2021.
6. Kenny Chua (Schneider Electric Blog). What is a safety instrumented system ? https://blog.se.com/sustainability/2024/04/29/what-is-a-safety-instrumented-system/, 2024.
7. Digital Bond. Redpoint. https://github.com/digitalbond/Redpoint.
8. Nicolas Chatelain. Ligolo-ng. https://github.com/nicocha30/ligolo-ng.
9. ControlThings.io. ctmodbus. https://github.com/ControlThings-io/ctmodbus.
10. Claire Vacherot (Orange Cyberdefense). Awesome Industrial Protocols. https://github.com/Orange-Cyberdefense/awesome-industrial-protocols.
11. Christian Dameff, Jeffrey Tully, and Maxwell Bland (Black Hat USA). Pestilential Protocol : How Unsecure HL7 Messages Threaten Patient Lives. https://www.youtube.com/watch?v=66x3vfac8rA, 2018.
12. dark lbp. ISF (Industrial Control System Exploitation Framework. https://github.com/dark-lbp/isf.
13. Mark Graham, Carolyn Ahlers, and Kyle O'meara (Dragos inc.). Impact of FrostyGoop ICS Malware on Connected OT Systems. https://hub.dragos.com/hubfs/Reports/Dragos-FrostyGoop-ICS-Malware-Intel-Brief-0724_.pdf, 2024.
14. Dragos inc. CRASHOVERRIDE. Analysis of the Threat to Electric Grid Operations. https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf, 2017.
15. Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, and Nathan Brubakerand Christopher Glyer (Mandiant). Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. https://cloud.google.com/blog/topics/threat-intelligence/attackers-deploy-new-ics-attack-framework-triton/?hl=en, 2024.
16. KScada. Modbus Doctor. https://www.kscada.com/modbusdoctor.html.
17. Ralph Langner. To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve. *The Langner Group*, 2013.
18. Davide Nardella. Snap7. https://snap7.sourceforge.net/.
19. NIST. NIST SP 800-82 Rev. 3 : Guide to Operational Technology (OT) Security. https://csrc.nist.gov/pubs/sp/800/82/r3/final, 2023.

20. Internal Society of Automation (ISA). ISA100, Wireless Systems for Automation. https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa100.
21. Jaime Pillora. Chisel. https://github.com/jpillora/chisel.
22. Rapid7. Metasploit framework, SCADA modules. https://github.com/rapid7/metasploit-framework/tree/master/modules/auxiliary/scanner/scada.
23. Justin Searle. Scanning Highly Sensitive Networks v3. https://drive.google.com/file/d/1_22MtEjveuv-Apl2ghQrfR5TaSnSPJAG/view, 2022.
24. SecDev. Scapy. https://github.com/secdev/scapy.
25. SCADA StrangeLove. SCADAPASS. https://github.com/scadastrangelove/SCADAPASS.
26. Claire Vacherot. CVE-2024-23765. https://nvd.nist.gov/vuln/detail/CVE-2024-23765.
27. Claire Vacherot. Le Fuzzer Con. https://github.com/claire-lex/le-fuzzer-con.
28. T.J. Williams. The purdue enterprise reference architecture. *Computers in industry*, 24(2-3) :141–158, 1994.