RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

COLLECTION
GESTION DES RISQUES CYBER

GUIDE EBIOS RISK MANAGER

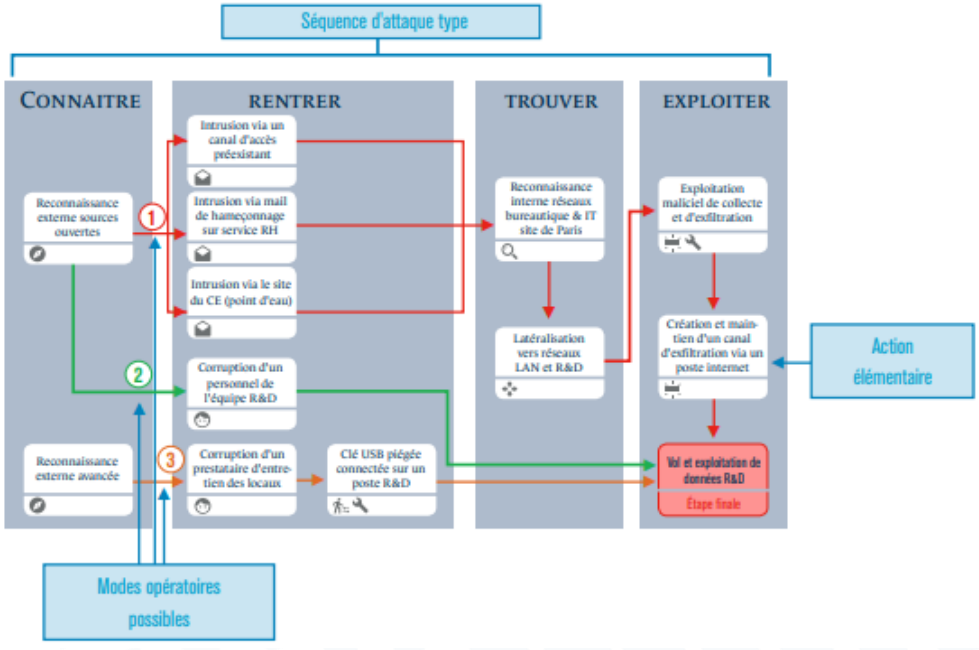
FICHE METHODE – Atelier 4

CONSTRUIRE LA CARTOGRAPHIE DE MENACE NUMERIQUE DE L'ECOSYSTEME

Les fiches méthodes permettent aux responsables de la démarche d'analyse de risque d'identifier les points essentiels d'attention en fonction de la typologie du système d'information ou des concepts utilisés.

Elles n'ont pas vocation à remplacer les guides techniques de l'ANSSI ou les politiques de sécurité et les réglementations en vigueur qui doivent être appliquées.

Un scénario opérationnel peut être représenté sous la forme d'un graphe d'attaque permettant de visualiser les modes opératoires planifiés par l'attaquant pour atteindre son objectif. Le graphe d'attaque se présente sous la forme d'un e**nchaînement d'actions élémentaires sur des biens supports.** Plusieurs modes opératoires peuvent être réalisés par la source de risque pour atteindre son objectif visé : ils sont représentés par des chaînes séquentielles différentes avant d'atteindre l'étape finale. Un exemple de scénario opérationnel est donné ci-après.



Pour chaque chemin d'attaque, le graphe d'attaque devrait satisfaire les règles suivantes :

- le point de départ est accessible par défaut par la source de risque ou la partie prenante par laquelle elle passe ;
- le point d'arrivée a un lien clair avec l'objectif visé ;
- toute action élémentaire du graphe doit remplir les conditions de réalisation de l'action suivante.

MODELE DE SEQUENCE D'ATTAQUE

Les scénarios opérationnels peuvent être structurés selon une séquence d'attaque type. Le modèle proposé s'articule autour de 4 phases :

CONNAITRE : ensemble des activités de ciblage, de reconnaissance et de découverte externes menées par l'attaquant pour préparer son attaque et accroître ses chances de succès (cartographie de l'écosystème, recherche d'information sur les personnes et les systèmes clés, recherche et évaluation de vulnérabilités, etc.). Ces informations sont collectées par tous les moyens possibles selon la détermination et les ressources de l'attaquant: renseignement, intelligence économique, exploitation des réseaux socioprofessionnels, approches directes, cybermercenaires pour obtenir de l'information inaccessible en source ouverte, etc.

RENTRER : ensemble des activités menées par l'attaquant pour s'introduire numériquement ou physiquement, soit directement et frontalement dans le système d'information de la cible, soit dans celui de son écosystème en vue d'une attaque par rebond. L'intrusion se fait généralement via des biens supports périmétriques qui servent de points d'entrée du fait de leur exposition. EXEMPLE : poste utilisateur connecté à Internet, tablette de maintenance d'un prestataire, imprimante télé-maintenue, etc.

TROUVER : ensemble des activités de reconnaissance interne des réseaux et systèmes, de latéralisation, d'élévation de privilèges et de persistance qui permettent à l'attaquant de localiser les données et biens supports recherchés. L'attaquant cherche généralement à rester discret et à ne pas laisser de traces.

EXPLOITER : ensemble des activités d'exploitation des données et biens supports trouvés dans l'étape précédente. Par exemple, dans le cas d'une opération de sabotage, cette phase inclut le déclenchement de la charge active, dans le cas d'une opération d'espionnage visant à exfiltrer des mails, il peut s'agir de mettre en place et maintenir la capacité discrète de recueil et d'exfiltration des données. EXEMPLE : rançongiciel.

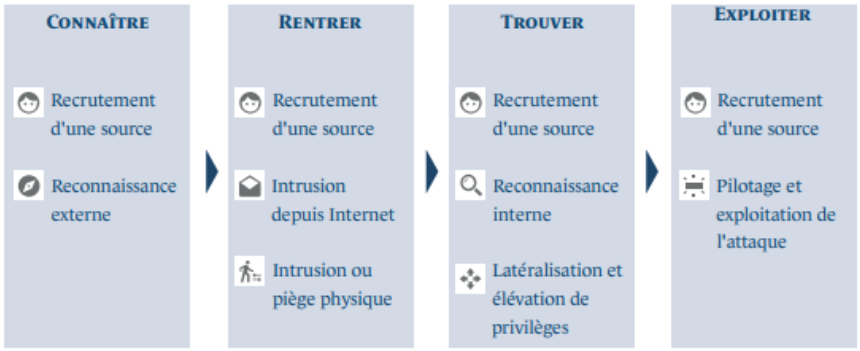
Vous pouvez adopter des modèles de séquences d'attaque plus sophistiqués et les décliner en variantes selon la technique d'attaque de la source de risque pour atteindre son objectif (exfiltration d'information, écoute passive, déni de service, rançongiciel, etc.).

NOTE : pour la phase « Rentrer », nous vous recommandons de distinguer dans le séquencement les actions élémentaires pour s'introduire dans les systèmes d'information de l'écosystème, et celles portant sur les biens supports de l'objet de l'étude. S'agissant de l'écosystème, vous ne pourrez pas toujours décrire avec précision quels seront les biens supports ciblés chez la partie prenante concernée. Dans ce cas, restez à un niveau de description macroscopique et fonctionnel (exemple : SI bureautique, chaîne de production).

Il est également possible de s'appuyer sur des référentiels d'attaques (MITRE ATT&CK®). Des exemples d'utilisation de MITRE peuvent être trouvés sur le site du Club EBIOS : https://club-ebios.org/site/selecteur-de-techniques-dattaque-outillage-pour-latelier-4/.

CATEGORIES D'ACTIONS ELEMENTAIRES ET MOYENS MIS EN ŒUVRE

L'illustration ci-après propose une catégorisation d'actions élémentaires en lien avec le modèle de séquence d'attaque proposé précédemment. Les moyens et techniques couramment observés sont précisés pour chaque catégorie d'actions élémentaires (puces). N'hésitez pas à adapter cette base à votre contexte et à l'enrichir de toute information issue de vos activités de veille. EX : exploitation des bulletins du CERT-FR et des bulletins de veille des cyberattaques.



NOTE : dans certains cas, lorsqu'un canal d'exfiltration est nécessaire et diffère du canal d'infiltration, une intrusion depuis Internet ou par piège physique peut être réalisée dans la phase « Exploiter ». L'intrusion initiale peut par exemple être réalisée via Internet, mais l'exfiltration via un canal physique ad hoc mis en place (cas des systèmes isolés).

RECRUTEMENT D'UNE SOURCE, CORRUPTION DE PERSONNEL

Une opération de « recrutement » d'une source à l'intérieur de l'organisation ou y ayant accès peut être longue et complexe, mais très utile pour mettre en place un piège matériel ou obtenir des informations sur le système ciblé. Les raisons poussant une cible à trahir son entité d'origine – potentiellement à son insu – sont couvertes par quatre grandes catégories, dites « MICE » (*Money, Ideology, Compromission, Ego*). Des officines spécialisées en matière de recrutement de sources existent.

RECONNAISSANCE EXTERNE DE LA CIBLE

Lors de la phase de reconnaissance, la source de risque va rechercher dans l'ensemble de ses bases disponibles les informations nécessaires à la planification de son attaque. Les données collectées peuvent être de nature technique ou concerner l'organisation de la cible et de son écosystème. Les moyens employés peuvent être très variés :

- réseaux sociaux (*social engineering*) ;
- Internet (poubelles numériques, sites) ;
- forums de discussion sur Internet ;
- forums et salons professionnels ;
- faux client, faux journaliste, etc. ;
- prise de contact directe (anciens salariés, etc.) ;
- officines ou agences spécialisées (sources non ouvertes) ;
- renseignement d'origine électromagnétique (interceptions).

INTRUSION DEPUIS INTERNET OU DES RÉSEAUX INFORMATIQUES TIERS

L'intrusion initiale a pour objectif d'introduire un outil malveillant dans le système d'information ciblé ou dans un autre appartenant à l'écosystème (par exemple la chaîne d'approvisionnement – *supply chain*), en général au niveau d'un bien support plus particulièrement exposé. Idéalement pour l'attaquant, l'intrusion initiale de l'outil malveillant est réalisée depuis Internet. Les techniques et vecteurs d'intrusion les plus couramment utilisés sont :

- les attaques directes à l'encontre des services exposés sur Internet ;
- les mails d'hameçonnage (*phishing*) ou de harponnage (*spearfishing*) ;
- les attaques via des serveurs spécifiquement administrés à cet effet ou compromis (attaques dites par point d'eau ou *waterhole*) ;
- le piège d'une mise à jour a priori légitime.

INTRUSION OU PIÈGE PHYSIQUE

Cette méthode d'intrusion est utilisée pour accéder physiquement à des ressources du système d'information afin de le compromettre.

Elle peut être réalisée par une personne externe ou simplifiée par le recrutement d'une source interne à l'organisation ciblée. L'intrusion physique est notamment utile à l'attaquant qui souhaite accéder à un système isolé d'Internet, ce qui nécessite de franchir un ou plusieurs *air gaps*. Des techniques d'intrusion physique couramment utilisées sont données ci-après :

- connaissance des identifiants de connexion ;
- compromission de la machine (exemple : clé USB piégée) ;
- connexion au réseau d'un matériel externe au système d'information ;
- intrusion via un réseau sans fil mal sécurisé ;
- piège d'un matériel en amont *via* la chaîne d'approvisionnement (attaque dite de la *supply chain*) ;
- utilisation abusive de moyens d'accès légitimes au système d'information.

EXEMPLE : vol et utilisation du téléphone portable professionnel d'un personnel.

RECONNAISSANCE INTERNE

En général, à l'issue de l'intrusion initiale, l'attaquant se retrouve dans un environnement de type réseaux locaux dont les accès

peuvent être contrôlés par des mécanismes d'annuaires (*Active Directory, OpenLDAP, etc.*). De fait, il doit mener des activités de reconnaissance interne lui permettant de cartographier l'architecture réseau, identifier les mécanismes de protection et de défense mis en place, recenser les vulnérabilités exploitables, etc. Lors de cette étape, l'attaquant cherche à localiser les services, informations et biens supports, objets de l'attaque. Les techniques de reconnaissance interne ci-après sont largement utilisées :

- cartographie des réseaux et systèmes pour mener la propagation (scan réseau) ;
- cartographie avancée (exemple : dump mémoire) ;
- recherche de vulnérabilités (par exemple pour faciliter la propagation) ;
- accès à des données système critiques (plan d'adressage, coffres forts, mots de passe, etc.) ;
- cartographie des services, bases de données et biens supports d'intérêt pour l'attaque ;
- dissimulation des traces ;
- utilisation de maliciel générique ou à façon permettant d'automatiser la reconnaissance interne.

LATÉRALISATION ET ÉLÉVATION DE PRIVILÈGES

À partir de son point d'accès initial, l'attaquant va mettre en œuvre des techniques de latéralisation et d'élévation de privilèges

afin de progresser et de se maintenir dans le système d'information. Il s'agit généralement pour lui d'exploiter les vulnérabilités structurelles internes du système (manque de cloisonnement des réseaux, contrôle d'accès insuffisant, politique d'authentification peu robuste, négligences relatives à l'administration et à la maintenance du système d'information, absence de supervision, etc.). Les techniques ci-après sont largement utilisées :

- exploitation de vulnérabilités logicielles ou protocolaires (notamment identifiées lors de la reconnaissance) ;
- modification ou abus de droits sur des comptes clés utilisateurs, administrateurs, machines ;
- autres techniques spécifiques: attaque par force brute, dump mémoire, attaque « *pass-the-hash* ».

NOTE: les phases de reconnaissance interne et de latéralisation / élévation de privilèges sont en pratique itératives et interviennent au fur et à mesure que l'attaquant progresse dans le système d'information.

PILOTAGE ET EXPLOITATION DE L'ATTAQUE

Cette ultime étape correspond à la réalisation de l'objectif visé par la source de risque. Selon cet objectif, il peut par exemple s'agir de déclencher la charge malveillante destructrice, d'exfiltrer ou de modifier de l'information. L'attaque peut être ponctuelle (par exemple dans le cas d'une opération de sabotage) ou durable et se réaliser en toute discrétion (par exemple dans le cas d'une opération d'espionnage visant à régulièrement exfiltrer des informations). Les moyens et techniques d'exploitation d'une attaque vont dépendre de l'objectif visé. Dans le cas où celui-ci perdure dans le temps et nécessite d'être orienté, l'attaquant devra mettre en place un canal de pilotage, qu'il soit synchrone ou asynchrone, voire même physique dans le cas d'un *air gap*.

Ci-après quelques exemples de techniques d'exploitation utilisées selon l'objectif visé :

ESPIONNAGE

- Exfiltration de données ;
- Observation ou écoute passive à distance (drone, matériel d'écoute, etc.) ;
- Interception et exploitation de signaux parasites compromettants (menace TEMPEST[1]).

ENTRAVE AU FONCTIONNEMENT (SABOTAGE, NEUTRALISATION)

- Attaque par déni de service distribué (DDoS) ;
- Atteinte à l'intégrité d'un bien support ou d'une donnée (effacement, chiffrement, altération) ;
- Brouillage d'un bien support (pour rendre aveugle ou neutraliser) ;
- Leurre[2] d'un bien support (pour tromper ou falsifier) ;
- Systèmes industriels : envoi de commandes à risque pour la sûreté de fonctionnement[3]6 ;
- Agression électromagnétique intentionnelle (AGREMI).

LUCRATIF (FRAUDE, DÉTOURNEMENT D'USAGE, FALSIFICATION)

- Modification d'une base de données (par exemple pour dissimuler une activité frauduleuse) ;
- Altération ou détournement d'usage d'une application métier ou support[4];
- Usurpation d'identité (dans une logique d'abus de droits) ;
- Détournement ou extorsion d'argent.

EXEMPLE : rançongiciel, mineur de crypto monnaie.

INFLUENCE (AGITATION, PROPAGANDE, DÉSTABILISATION)

- Défiguration de sites Internet ;
- Diffusion de messages idéologiques via la prise de contrôle d'un canal d'information ;
- Usurpation d'identité (dans une logique d'atteinte à la réputation).

1 La menace TEMPEST peut également être exploitée de façon active en piégeant préalablement, par exemple via la supply chain, un périphérique (câble, clavier, souris, vidéoprojecteur). Il devient alors une source de signaux parasites compromettants activable et désactivable à distance à condition de disposer d'émetteurs suffisamment puissants pour créer un canal de fuite

2 Les techniques de leurre cognitif en vue d'induire en erreur ou dissimuler une activité aux yeux d'un utilisateur (exemple : demande d'authentification illégitime, message d'alerte masqué)

3 Par exemple pour entraîner une usure prématurée d'un équipement ou modifier des seuils d'alerte sur des paramètres de fonctionnement clés. L'évaluation fine des modes d'exploitation d'une attaque sur un système industriel est indissociable des analyses de sûreté de fonctionnement: