

Guide d'Analyse Forensique et de Sécurité des Réseaux

Ce texte constitue une introduction technique à l'**analyse forensique des réseaux**, mettant l'accent sur la surveillance des communications entre terminaux pour reconstituer le cycle de vie d'une cyberattaque. L'auteur détaille l'importance de maîtriser les **protocoles de transport** comme TCP et UDP, ainsi que la reconnaissance des **ports de service** essentiels pour identifier le trafic suspect. Il explore les diverses méthodes de déploiement des outils de sécurité, comparant les approches physiques, virtuelles et infonuagiques, tout en soulignant la visibilité cruciale du **trafic interne** (est-ouest). Les sources présentent également les capacités d'investigation offertes par les pare-feux, les systèmes de détection d'intrusion et les solutions de **contrôle d'accès au réseau** (NAC). Enfin, l'ouvrage distingue la **capture de paquets**, riche en détails mais coûteuse, de la technologie **NetFlow**, plus légère et efficace pour surveiller les comportements anormaux à l'échelle d'une infrastructure complète.

Comment l'analyse forensique des réseaux aide-t-elle à reconstituer une cyberattaque ?

L'analyse forensique des réseaux permet de reconstituer une cyberattaque en allant au-delà des simples alertes automatisées pour cartographier et expliquer le **cycle de vie complet d'un incident**. Elle s'appuie sur plusieurs technologies, types de données et méthodes d'analyse pour comprendre précisément comment l'attaque s'est déroulée :

1. La capture de paquets (PCAP) : la preuve la plus fiable

La capture de paquets réseau constitue la méthode la plus précise pour reconstituer le déroulement d'une attaque. Elle permet de :

- **Rejouer l'événement** en fonction de l'horodatage de l'alerte pour visualiser une simulation en temps réel de ce qui s'est passé.
- **Confirmer la réalité de l'attaque** et écarter les fausses alertes.

- **Analyser le détail des transactions** pour identifier précisément les types de données transférées, les commandes exécutées et même récupérer des identifiants de connexion (à condition que le trafic ne soit pas chiffré).

2. Les données de flux (NetFlow) : visibilité globale et comportementale
Contrairement à la capture complète de paquets, NetFlow enregistre uniquement les détails des connexions (comme les adresses IP impliquées, les protocoles, les ports et les horodatages) sans stocker le contenu des paquets. En matière de reconstitution, NetFlow permet de :

- **Suivre rapidement le trafic** sur l'ensemble des équipements du réseau (routeurs, commutateurs, serveurs virtuels, etc.).
- **Établir des bases de référence** du comportement normal afin de repérer les activités inhabituelles (comme des pics de bande passante ou des tunnels chiffrés inattendus).
- **Identifier la propagation interne** d'un logiciel malveillant en comparant les écarts de comportement des systèmes pour détecter d'autres machines compromises.

3. La centralisation des événements grâce au SIEM

Les cyberattaques modernes impliquent souvent de multiples outils de sécurité (pare-feu, IPS, filtres de contenu) qui ne perçoivent chacun qu'une partie de l'incident. Un gestionnaire d'informations et d'événements de sécurité (**SIEM**) facilite la reconstitution en :

- **Centralisant tous les journaux** dans un référentiel unique.
- **Corrélant des événements mineurs** provenant de différents systèmes pour révéler une attaque de plus grande ampleur.
- **Reconstituant le puzzle de l'attaque** à travers les différentes solutions afin d'aider l'enquêteur à cartographier le parcours complet de l'intrus.

4. Le traçage des étapes méthodologiques de l'attaquant

L'analyse forensique réseau permet de documenter précisément chaque phase de l'attaque :

- **Reconnaissance** : Repérer les balayages et scans de ports (scans SYN, XMAS, etc.) grâce à des filtres de capture (Wireshark) ou des règles de détection d'intrusion (Snort).
- **Exploitation** : Analyser les journaux de sécurité (comme ceux de l'IPS) et les associer aux valeurs de vulnérabilité publique (**CVE**)

pour identifier la faille de sécurité ciblée, évaluer sa pertinence technologique et déterminer si l'exploitation a réussi ou s'il s'agissait d'une tentative infructueuse.

- **Émission de signaux (Beaconing)** : Déceler les communications discrètes et périodiques qu'un logiciel malveillant utilise pour appeler un serveur de commande et de contrôle (C2) externe, même lorsque ces signaux sont lents pour se dissimuler dans le trafic standard sur le port 443.
- **Exfiltration** : Identifier la fuite de données sensibles en surveillant les communications vers des destinations suspectes (comme le réseau Tor), l'utilisation de la géolocalisation pour des pays inhabituels, ou en détectant des volumes de transfert de données qui dépassent les seuils de référence établis.

5. L'usage d'environnements de test contrôlés

Pour reconstituer l'activité de programmes suspects identifiés sur le réseau :

- Un **bac à sable (sandbox)** permet d'exécuter un logiciel suspect de manière isolée pour analyser son comportement (processus lancés, clés de registre modifiées, destinations réseau contactées), aidant ainsi l'enquêteur à le traquer sur d'autres segments du réseau.
- Un **pot de miel (honeypot)** sert de leurre vulnérable pour attirer l'attaquant, permettant d'étudier en direct ses techniques d'exploitation et de comprendre comment il interagit avec les systèmes compromis.

 Je pourrais concevoir un tableau comparatif détaillé mettant en contraste les avantages, les limites et l'impact sur le stockage de la capture de paquets (PCAP) par rapport aux données de flux (NetFlow) pour guider vos stratégies d'enquête.

C'est quoi la différence entre un SPAN et un TAP ?

Vos sources indiquent que le **SPAN** et le **TAP** réseau sont deux méthodes utilisées lors de déploiements passifs de solutions de sécurité. Elles permettent d'observer le trafic réseau et d'en capturer des

copies pour les envoyer à un dispositif de sécurité (comme un IDS ou une solution de capture de paquets) sans interrompre les communications en cours.

Cependant, les documents fournis ne détaillent pas les différences de fonctionnement ou les caractéristiques techniques qui distinguent un port SPAN d'un équipement TAP.

Souhaitez-vous que j'effectue une recherche sur le Web pour vous expliquer en détail ce qui les différencie ?

Comment fonctionne NetFlow ?

1. Une collecte de métadonnées (et non du trafic brut) Contrairement à la capture complète de paquets (PCAP) qui enregistre l'intégralité du contenu des communications, NetFlow est une technologie de **surveillance basée sur les flux**. Elle n'enregistre pas le contenu même des paquets, mais capture des **détails sur les connexions réseau** (les métadonnées).

2. Une génération directe par les équipements réseau NetFlow utilise des **entrées de flux mises en cache directement par le matériel** qui produit ou achemine le trafic. Les équipements déjà présents dans l'infrastructure — tels que les routeurs, commutateurs, points d'accès sans fil ou serveurs virtuels — agissent ainsi comme de véritables **points de contrôle de sécurité** passifs.

3. Les informations contenues dans un enregistrement La version 9 de NetFlow est la plus récente et la plus riche en détails. Un enregistrement type contient une multitude de champs clés :

- Les **systèmes impliqués** (les adresses IP de l'expéditeur et du destinataire).
- Les **protocoles** et ports de transport utilisés.
- L'**heure** et la chronologie de la transaction.

4. La consolidation des données (Fusion et Déduplication) Dans un réseau actif, une simple action utilisateur (comme charger une page web) génère une multitude de flux individuels aller-retour. Pour faciliter l'analyse, de nombreuses solutions de collecte intègrent des fonctionnalités de :

- **Déduplication** : élimination des données redondantes.

- **Fusion ou concaténation** : assemblage automatique des enregistrements de flux individuels d'un chemin réseau en un seul enregistrement consolidé représentant la session globale.
- *Note de l'enquêteur* : Bien que la fusion facilite grandement la visualisation, elle présente un **risque de corruption ou de perte de granularité** dans les enregistrements. Pour les enquêtes de haute précision, il est recommandé de disposer d'une option permettant de désactiver ces fusions afin d'analyser les flux bruts.

5. L'exploitation analytique pour la sécurité Une fois ces données de flux collectées par des solutions spécialisées (comme Cisco Stealthwatch), elles permettent de :

- Établir des **bases de référence du comportement normal** du réseau (baselines).
- Détecter les anomalies et comportements suspects (pics anormaux de bande passante, tunnels chiffrés inattendus, communications d'exfiltration ou signaux périodiques de logiciels malveillants).
- Analyser rapidement de très grands volumes de données à l'échelle de l'entreprise avec des **coûts de stockage bien inférieurs** à ceux d'une conservation de paquets PCAP.

 Si vous le souhaitez, je peux rédiger un rapport comparatif détaillé mettant en contraste NetFlow et la capture complète de paquets (PCAP), afin d'évaluer précisément leurs compromis respectifs en matière de stockage et de finesse d'analyse lors d'une enquête.

Comment fonctionne l'intégration de Cisco Stealthwatch et ISE ?

L'intégration de **Cisco Stealthwatch** (un outil basé sur NetFlow) et de **Cisco ISE** (une solution de contrôle d'accès réseau ou NAC) repose sur deux piliers majeurs : **l'apport de contexte** pour faciliter les enquêtes et **la mise en quarantaine automatique** pour stopper la propagation des menaces.

1. L'enrichissement contextuel des données réseau

En temps normal, les outils de surveillance réseau comme Stealthwatch identifient et affichent les menaces uniquement sous forme d'adresses

IP. L'intégration avec Cisco ISE résout cette limite grâce au partage d'informations :

- **Identification immédiate** : Stealthwatch récupère directement le contexte utilisateur et matériel auprès de Cisco ISE. Une simple adresse IP suspecte est ainsi automatiquement associée à un utilisateur réel (par exemple, *Vicki*) et à un type de terminal précis (par exemple, *un poste de travail Windows 7*).
- **Intégration de l'annuaire (Active Directory)** : Si l'organisation utilise un annuaire, l'enquêteur peut visualiser instantanément des détails professionnels liés au compte de l'utilisateur, comme son adresse e-mail ou son numéro de téléphone.
- **Bénéfice pour l'enquête** : Ce partage de données évite à l'enquêteur de devoir faire des recoupements manuels laborieux, lui permettant de collecter très rapidement une mine d'informations sur n'importe quel équipement suspect détecté sur le réseau.

2. La mise en quarantaine et la réponse active aux menaces

Au-delà de la visibilité, l'intégration permet d'utiliser le contrôle d'accès réseau (ISE) comme un dispositif de sécurité actif et réactif :

- **Retrait automatique du réseau** : Lorsqu'un comportement malveillant ou une menace est détecté par Stealthwatch, le système peut être configuré pour ordonner automatiquement à Cisco ISE de déconnecter ou d'isoler l'équipement compromis.
- **Contention des épidémies** : En plaçant immédiatement les terminaux suspects en quarantaine, l'organisation réduit drastiquement le risque d'infection généralisée ou de mouvement latéral au sein du réseau.
- **Facilitation du travail de réponse** : L'enquêteur peut alors mener ses investigations en toute sécurité, directement sur le système identifié et isolé du reste de l'infrastructure.

✚ Si vous le souhaitez, nous pourrions explorer d'autres méthodes d'investigation post-compromission abordées dans vos sources, comme l'analyse du comportement de communication périodique (le balisage ou *beaconing*) utilisé par les logiciels malveillants pour appeler leurs serveurs de contrôle.

Comment analyser le beaconing ?

L'**analyse du beaconing** (ou émission de signaux/balisage) est l'un des aspects les plus critiques de l'analyse forensique post-compromission, car environ **90 % des logiciels malveillants** qui s'introduisent sur un réseau utilisent ce comportement pour communiquer avec l'extérieur. Le principe de base est qu'un système infecté tente d'établir une communication avec une ressource externe (un serveur de commande et de contrôle, ou C2) afin de télécharger du code d'exploitation supplémentaire, d'offrir un accès interactif à un attaquant, ou d'indiquer qu'il est prêt à être contrôlé.

Pour analyser et détecter efficacement ce comportement souvent très discret, les enquêteurs s'appuient sur plusieurs méthodes méthodologiques et techniques :

1. Comprendre la furtivité du signal (Le « battement de cœur »)

Le beaconing peut être asynchrone et extrêmement lent. Le logiciel malveillant se connecte brièvement, télécharge ses instructions, puis se met en veille pour éviter une connexion continue qui éveillerait les soupçons.

- Un signal furtif typique peut se manifester sous la forme d'un « **battement de cœur** » (**heartbeat**) régulier, par exemple un minuscule paquet envoyé toutes les 30 minutes vers la même destination sur le port 443 (HTTPS) pour se dissimuler au milieu du trafic web légitime.

2. L'analyse statistique par filtres de temps et de variance

Sur un grand réseau, repérer manuellement ces signaux est complexe en raison du volume de bruit. L'analyse repose donc sur des filtres mathématiques appliqués aux données de capture de paquets (PCAP) ou aux enregistrements NetFlow :

- **La période d'observation** : Il est recommandé de travailler sur une capture de trafic s'étendant sur **trois à cinq jours**.
- **Le filtrage temporel** : Définissez des filtres basés sur le temps et la variance des intervalles (en autorisant une marge de tolérance raisonnable).
- **Exemple de filtre pratique** : Vous pouvez limiter votre échantillon initial (par exemple, aux 100 000 premières connexions TCP SYN) et cibler spécifiquement les connexions présentant un intervalle de

signal constant supérieur à 60 secondes. En ajustant progressivement ce filtre, vous parviendrez à isoler les anomalies.

- **L'analyse de variance** : Elle permet de mesurer l'écart entre les pulsations afin de repérer les logiciels malveillants en veille qui programment leurs appels de manière hautement périodique.

3. Le filtre de rareté des destinations (Unicité)

Plutôt que de chercher des destinations populaires, l'enquêteur doit chercher l'inverse :

- **Recherche de sites uniques** : Configurez des filtres pour identifier un très petit nombre d'utilisateurs ou d'équipements internes se connectant à un hôte externe unique (contrairement à des sites massivement visités comme Facebook).
- **Exclusion du trafic normal** : Pour affiner la recherche, excluez les protocoles et les ports connus qui génèrent structurellement du trafic périodique légitime, comme le port 25 utilisé pour la messagerie électronique.

4. La corrélation multi-systèmes

Si un outil d'analyse révèle un motif de beaconing spécifique (avec un intervalle et une variance identiques) affectant plusieurs machines distinctes sur le réseau, cela confirme généralement que **ces hôtes sont infectés par la même variante de logiciel malveillant**.

Cartographier ces similitudes permet de mesurer l'étendue réelle de la compromission.

5. L'exploitation des outils et du contexte de sécurité

L'analyse forensique du beaconing s'appuie également sur des solutions automatisées pour corroborer les découvertes :

- **Renseignement sur les menaces (Threat Intelligence)** : Les solutions de sécurité (comme Cisco Stealthwatch) comparent le trafic sortant avec des listes de réputation pour identifier immédiatement les connexions établies vers des serveurs C2 ou des botnets connus.
- **Bacs à sable (Sandboxes)** : Si vous découvrez un fichier suspect sur un hôte identifié, son exécution dans un environnement contrôlé (sandbox) permettra d'observer directement son comportement de beaconing, les ports utilisés, ainsi que les adresses IP exactes qu'il tente de contacter.

🔍 Souhaitez-vous que nous étudions d'autres comportements d'attaque post-compromission décrits dans vos sources, comme les techniques d'exfiltration de données vers le Darknet (Tor) ou l'analyse des requêtes DNS (avec la commande dig) ?

Comment exfiltrer des données vers le réseau Tor ?

Selon les principes de l'analyse forensique décrits dans vos documents, les attaquants s'appuient sur des techniques spécifiques pour exfiltrer discrètement des données vers des réseaux clandestins comme Tor :

1. La préparation et la dissimulation des données

Pour éviter que le transfert de données ne soit détecté par les systèmes de surveillance réseau, les attaquants préparent minutieusement les fichiers :

- Ils utilisent généralement des **canaux de communication courants** et légitimes, tels que les protocoles HTTP et HTTPS, pour que le trafic d'exfiltration se confonde avec l'activité web normale des utilisateurs.
- Ils prennent le soin de **compresser, chiffrer et protéger par mot de passe** les données dérobées avant l'envoi, ce qui leur permet de dissimuler le contenu sensible dans le bruit de fond du réseau.

2. L'aiguillage vers le réseau Tor

Une fois les données préparées, l'attaquant initie des communications sortantes destinées à traverser la périphérie du réseau interne vers des infrastructures du Darknet, incluant spécifiquement le réseau Tor.

Comment l'analyse forensique permet-elle de détecter ce comportement ?

Le rôle de l'enquêteur consiste à identifier ces tentatives d'exfiltration à travers plusieurs indicateurs clés :

- **La surveillance des connexions vers le Darknet** : Les outils de sécurité recherchent activement les flux de trafic sortants s'établissant vers des nœuds ou des sources non autorisées appartenant au réseau Tor.
- **L'utilisation du renseignement sur les menaces (Threat Intelligence)** : L'intégration de flux de réputation permet d'associer

automatiquement les adresses IP externes contactées à des listes connues de serveurs malveillants ou de relais Tor.

- **La géolocalisation du trafic** : Les enquêteurs analysent si des flux de données sont dirigés vers des zones géographiques ou des pays inhabituels avec lesquels l'organisation n'a pas de relations d'affaires légitimes.
- **L'analyse des écarts de référence (Baselines)** : En comparant le trafic actuel à un comportement réseau préalablement modélisé comme "normal", l'analyste peut repérer des anomalies telles qu'un volume de données anormalement élevé ou sporadique quittant le réseau.
- **Le déclenchement de seuils comportementaux** : Des alertes peuvent être configurées pour signaler des transferts massifs en dehors des heures de bureau ou des flux traversant de manière illégitime la segmentation du réseau (par exemple, un transfert de données depuis un centre de données sécurisé).

 Nous pourrions explorer comment l'utilisation d'outils de réputation de domaine (comme Cisco Umbrella Investigate) ou l'analyse forensique des requêtes DNS (avec la commande **dig**) aide à obtenir des détails précis sur la dangerosité de ces adresses de destination externes.

Analyser le DNS avec dig

Dans le prolongement de notre discussion sur la détection de l'exfiltration de données, l'analyse du DNS est une étape d'investigation essentielle lorsqu'un hôte interne contacte une destination externe inhabituelle. C'est à ce moment que la commande **dig** intervient comme un outil de regroupement d'informations de domaine.

Rôle et fonctionnement de la commande dig

La commande dig permet à l'enquêteur d'interroger directement les serveurs de noms afin de collecter des détails sur l'infrastructure de la menace :

- **Identifier les serveurs DNS faisant autorité** pour le domaine externe recherché.
- **Consulter les hôtes** qui disposent d'entrées DNS sous ce même domaine.
- **Comprendre l'infrastructure de l'attaquant** : par exemple, si un système contacte le domaine suspect maliciouswebsite.com, l'utilisation de dig peut révéler d'autres hôtes liés comme sharepoint.maliciouswebsite.com ou maliciouswebsite.mail. Cette cartographie aide l'analyste à mieux cerner l'écosystème de la source et la nature des données qui transitent par le système.

Autres outils d'investigation DNS complémentaires

Pour approfondir la recherche au-delà des requêtes DNS de base proposées par dig, les sources présentent d'autres solutions :

- **Fierce** : Cet outil, disponible sous Kali Linux, permet d'extraire l'intégralité des entrées DNS d'un domaine cible (en saisissant la commande `fierce.pl -dns <cible>`), à condition que les transferts de zone (zone transfers) soient autorisés sur le serveur cible.
- **Cisco Umbrella Investigate** : Une technologie de niveau entreprise qui permet de recueillir des informations DNS extrêmement détaillées et des indicateurs de réputation sur une source suspecte.

 Je pourrais vous concevoir un aide-mémoire (cheat sheet) au format PDF regroupant les syntaxes et les cas d'usage de ces commandes réseau (comme dig, traceroute) ainsi que les commandes Linux d'analyse de journaux (grep, cut, awk) présentées dans votre guide.

Quels autres indicateurs d'exfiltration vers Tor faut-il surveiller ?

Pour surveiller et détecter efficacement l'exfiltration de données, notamment vers des réseaux clandestins comme **Tor**, les enquêteurs doivent s'appuyer sur plusieurs indicateurs et méthodes d'analyse complémentaires :

1. La surveillance des communications vers le Darknet et les sources suspectes

- **La communication avec des réseaux clandestins (dark networks)** : Il s'agit de surveiller activement toute tentative de connexion sortante dirigée vers des nœuds ou relais Tor connus. Les outils s'appuient sur des flux de réputation ou de renseignements sur les menaces (Threat Intelligence) pour identifier ces adresses IP malveillantes.
- **La géolocalisation du trafic** : Signaler toute communication s'établissant vers des pays ou des zones géographiques avec lesquels l'organisation n'a pas d'activité habituelle.

2. L'analyse des écarts par rapport aux références (Baselines)

- **Les comportements et pics de trafic inhabituels** : L'établissement d'une base de référence du trafic normal permet de repérer des anomalies telles que des pics de transfert volumineux et sporadiques, en particulier s'ils proviennent d'utilisateurs qui n'ont jamais partagé de données de cette manière auparavant.
- **Le profilage des utilisateurs** : Les écarts de comportement doivent être analysés selon la catégorie d'utilisateur. Par exemple, l'utilisation de protocoles comme SSH ou le transfert de fichiers est attendue de la part d'un administrateur système, mais elle représente un fort indicateur de risque ou de compromission si elle provient d'un profil non technique (comme les ressources humaines ou la finance).

3. Le franchissement de seuils comportementaux spécifiques

La mise en place d'alertes basées sur des seuils stricts permet de détecter l'exfiltration même si l'attaque semble légitime :

- **Le volume de données** : Déclencher une alarme dès qu'une quantité de données supérieure à un seuil défini (par exemple, plus d'un gigaoctet exporté pour la première fois par un utilisateur) quitte le réseau.
- **Les anomalies temporelles** : Surveiller tout transfert massif ou inhabituel de données s'effectuant en dehors des heures de bureau.
- **Les violations de segmentation réseau** : Identifier des flux de données traversant de manière illégitime des segments réseau spécifiques, par exemple un équipement qui transfère des fichiers

depuis une zone sécurisée (comme un centre de données) vers une zone non critique (comme le réseau des imprimantes).

4. L'utilisation de chiffrements ou protocoles anormaux

- **Le chiffrement non autorisé ou inhabituel** : Étant donné que les attaquants cherchent souvent à dissimuler l'exfiltration en compressant, chiffrant et protégeant par mot de passe les données volées, l'apparition d'un chiffrement non standard ou non autorisé (au sein du réseau ou en provenance de celui-ci) constitue un indicateur suspect majeur.
- **La surveillance des ports et protocoles inhabituels** : Traquer l'utilisation de canaux ou de ports qui ne sont pas censés communiquer directement vers Internet.

5. L'exploitation des outils de prévention des pertes de données (DLP)

- **Le suivi des fichiers sensibles** : Les technologies DLP permettent d'attribuer des niveaux de confiance spécifiques aux fichiers de l'organisation et de surveiller l'ensemble de leurs déplacements, générant des alertes immédiates en cas de tentative de suppression ou d'exfiltration non autorisée de ces données sensibles.

✖ Si vous le souhaitez, je pourrais vous aider à concevoir une fiche de procédure ou une check-list d'investigation pour vos analystes SOC, structurant étape par étape la recherche de ces indicateurs d'exfiltration.

Comment le SIEM aide-t-il à reconstituer le puzzle d'une attaque ?

Le gestionnaire d'informations et d'événements de sécurité (**SIEM**) joue un rôle fondamental dans la reconstitution d'une cyberattaque en agissant comme le point central de l'investigation. Voici comment il permet d'assembler les pièces du puzzle :

1. Centralisation de la visibilité réseau

Dans les infrastructures modernes, la multiplicité des outils de sécurité engendre une dispersion des informations à travers plusieurs interfaces de gestion distinctes. De plus, la plupart de ces outils ne perçoivent qu'une partie isolée d'une attaque, ce qui limite considérablement la compréhension de son impact sur l'ensemble de l'organisation. Le SIEM résout ce problème en servant de **référentiel centralisé** pour tous les

événements de sécurité, offrant ainsi une vue unique et globale à l'administrateur.

2. Corrélation des événements mineurs

Une attaque complexe peut être composée de plusieurs actions discrètes sur différents systèmes. Le SIEM analyse et **corrèle les événements envoyés** par l'ensemble des équipements. Cela lui permet de lier entre eux de nombreux événements mineurs provenant de systèmes différents qui, pris isolément, pourraient sembler anodins, afin de révéler une attaque de plus grande ampleur. Cette corrélation globale aide à optimiser les stratégies de réponse aux incidents.

3. Assemblage des fragments d'informations

Lors d'une infection d'envergure, chaque outil de sécurité du réseau n'enregistre généralement qu'un fragment du trafic global associé à l'événement. Le SIEM est le seul outil capable de **rassembler et d'identifier ces fragments épars** pour reconstituer l'événement dans son intégralité. Sans cette centralisation, ces fragments d'informations risqueraient de passer totalement inaperçus si les outils de sécurité individuels ne sont pas parfaitement configurés.

4. Cartographie et point de départ de l'enquête

En raison de cette centralisation, la grande majorité des enquêtes forensiques sur des incidents réseau commencent par l'analyse du SIEM. Il permet à l'enquêteur de **cartographier précisément le parcours de l'attaque** à travers les différentes solutions de sécurité de l'entreprise. Une fois cette vue d'ensemble obtenue, l'analyste peut orienter ses recherches pour approfondir l'analyse de chaque système spécifique ayant envoyé des alertes.



Ce sujet sur le rôle du SIEM et la corrélation d'événements ferait une excellente discussion audio si vous souhaitez générer un aperçu rapide et dynamique à écouter lors de vos déplacements.

Comment utiliser Fierce pour l'extraction DNS ?

Fierce est un outil de reconnaissance DNS disponible sous la distribution **Kali Linux**. Son rôle principal dans une enquête forensique est de vous aider à cartographier l'infrastructure d'un domaine externe

suspect en tentant d'en obtenir tous les hôtes et sous-domaines associés.

Voici comment l'utiliser et comment il fonctionne selon vos sources :

1. La condition préalable : Le transfert de zone

Pour que Fierce puisse extraire automatiquement et instantanément l'intégralité des enregistrements DNS d'un domaine, **les transferts de zone (zone transfers) doivent être autorisés** sur le serveur DNS ciblé. Si les transferts de zone ne sont pas autorisés (ce qui est le cas le plus fréquent pour des raisons de sécurité), l'outil indique que la tentative a échoué et bascule généralement sur une recherche classique par force brute à l'aide d'un dictionnaire de mots pour deviner les sous-domaines existants.

2. Syntaxe et commande d'exécution

Pour lancer l'outil, vous devez ouvrir un terminal sous Kali Linux et utiliser la syntaxe suivante :

```
fierce.pl -dns <cible>
```

3. Exemple pratique

Si vous souhaitez analyser un domaine comme thesecurityblogger.com, vous devez exécuter la commande suivante :

```
fierce.pl -dns thesecurityblogger.com
```

(Note : Bien que le texte de votre guide contienne une légère coquille matérielle en écrivant "ferious.pl", la capture d'écran du terminal Kali Linux confirme que la commande exacte à saisir est bien fierce.pl).

4. Interprétation des résultats

Lors de l'exécution, Fierce effectue les actions suivantes dans l'ordre :

1. Il identifie et liste les serveurs DNS qui font autorité pour le domaine cible (par exemple, ns1.dreamhost.com, ns2.dreamhost.com).
2. Il teste un par un le transfert de zone sur ces serveurs.
3. Si un serveur l'autorise, Fierce affiche l'ensemble des entrées de la zone DNS (permettant de découvrir d'autres serveurs, des portails d'administration, des sous-domaines de messagerie ou des zones de partage de fichiers temporaires liés à l'attaquant).

✖ Nous pourrions concevoir un aide-mémoire (cheat sheet) au format PDF regroupant toutes les commandes de reconnaissance et d'analyse de journaux réseau présentées dans votre guide (comme dig, fierce, grep, cut et awk).

Quels sont les ports TCP les plus critiques à surveiller ?

Selon votre guide d'analyse forensique, il existe 65 535 ports TCP. Bien qu'il ne soit pas nécessaire de tous les mémoriser, un enquêteur doit impérativement maîtriser les **ports les plus couramment utilisés** (parmi les 1 024 ports bien connus et réservés aux applications courantes) afin d'identifier rapidement la nature du trafic observé.

Voici la liste de référence des **ports TCP les plus critiques à surveiller** et à savoir identifier lors d'une investigation :

- **Port 21 : FTP (File Transfer Protocol)** – Utilisé pour le transfert de fichiers. C'est un port clé à surveiller pour détecter d'éventuels transferts non autorisés ou des attaques par force brute (générant des erreurs de connexion 530).
- **Port 22 : SSH (Secure Shell)** – Utilisé pour les connexions sécurisées à distance. Un trafic SSH provenant d'un utilisateur non technique (comme les ressources humaines) peut être le signe d'une compromission ou d'une exfiltration.
- **Port 23 : Telnet** – Service de connexion à distance non sécurisé (en clair).
- **Port 25 : SMTP (Simple Mail Transfer Protocol)** – Protocole de transfert de courrier électronique. C'est un port couramment exclu lors de la recherche de signaux de balisage (*beaconing*) car il génère naturellement un trafic périodique légitime.
- **Port 53 : DNS (Domain Name System)** – Bien qu'également très associé à UDP, il est utilisé pour la résolution de noms de domaine. C'est un protocole critique à surveiller car les attaquants l'utilisent parfois comme canal pour émettre des signaux (*beacons*) ou tenter des dépassements de tampon dans la charge utile des requêtes.
- **Port 80 : HTTP** – Protocole de transfert hypertexte non sécurisé utilisé sur le Web. C'est l'un des principaux canaux utilisés par les

attaquants pour rediriger les victimes vers des kits d'exploitation ou exfiltrer des données en se dissimulant dans le trafic standard.

- **Port 110 : POP3** – Protocole de réception de courrier électronique, sujet à des attaques par déni de service (DoS) à surveiller en cas de commandes répétitives.
- **Port 119 : NNTP** – Protocole de transfert de nouvelles réseau.
- **Port 123 : NTP** – Protocole de temps réseau, essentiel pour la synchronisation temporelle.
- **Port 143 : IMAP** – Protocole d'accès aux messages Internet pour la messagerie.
- **Port 161 : SNMP** – Protocole simple de gestion de réseau.
- **Port 194 : IRC (Internet Relay Chat)** – Protocole de messagerie instantanée.
- **Port 443 : HTTPS** – Protocole HTTP sécurisé (chiffré). Il s'agit d'un port hautement critique car les logiciels malveillants y cachent fréquemment leurs signaux de communication périodiques (*beacons*) ou leurs exfiltrations afin de contourner la détection en se mêlant au trafic web chiffré légitime.

Autres protocoles importants mentionnés

Bien qu'ils ne figurent pas dans la liste principale des ports TCP du guide, l'enquêteur doit également surveiller :

- **Le protocole SMB (Server Message Block)** : Ce protocole est indispensable à la réussite d'attaques majeures comme le rançongiciel WannaCry (qui exploite la faille *ExternalBlue*).

 Je peux vous créer une fiche mémo téléchargeable au format PDF regroupant ces ports clés, leurs protocoles et les commandes Linux essentielles d'analyse de logs (grep, cut, awk) pour vos enquêtes. Cela vous intéresse ?

Comment Cisco ISE facilite-t-il la mise en quarantaine ?

Cisco ISE, en tant que solution de contrôle d'accès au réseau (NAC), facilite la mise en quarantaine des équipements compromis grâce à un mécanisme de réponse automatisé et structuré :

- **Le retrait automatique du réseau** : Lorsqu'un autre outil de sécurité détecte une menace, il peut être configuré pour demander automatiquement à Cisco ISE de retirer immédiatement le périphérique concerné du réseau. L'appareil reste ainsi isolé jusqu'à ce que les administrateurs évaluent la situation.
- **La limitation de la propagation (confinement)** : En plaçant instantanément les systèmes suspects en quarantaine, Cisco ISE réduit de manière significative le risque d'épidémie ou de mouvements latéraux de logiciels malveillants au sein de l'infrastructure.
- **La facilitation de l'investigation** : Cette isolation permet à l'enquêteur de mener ses analyses de manière ciblée et sécurisée, en se concentrant uniquement sur les terminaux d'intérêt qui ont été isolés du reste du réseau de production.
- **L'intégration multi-éditeur via le SIEM** : Cette capacité de mise en quarantaine s'intègre très fréquemment avec une solution SIEM. De ce fait, tout élément identifié comme risqué par un outil tiers, quel que soit son fabricant, peut déclencher une correction et un isolement automatiques gérés par Cisco ISE.

 Nous pourrions étudier le concept de « **verrouillage d'hôte** » (**host lock**) dans Cisco Stealthwatch, qui applique un principe de restriction similaire en s'appuyant sur les données NetFlow.

Comment fonctionne Stealthwatch ?

Cisco Stealthwatch est un outil de sécurité réseau conçu pour surveiller le trafic interne et identifier les menaces en s'appuyant sur les technologies de flux. Voici ses principaux mécanismes de fonctionnement détaillés dans vos sources :

1. L'exploitation des données NetFlow

Stealthwatch n'analyse pas le trafic brut (comme le ferait une capture de paquets), mais utilise **NetFlow**. Il récupère les enregistrements de flux générés par les équipements réseau existants (routeurs, commutateurs, serveurs virtuels) pour obtenir une visibilité complète à l'échelle de l'infrastructure.

2. L'établissement de bases de référence (Baselines)

L'outil utilise des analyses de sécurité pour modéliser le comportement normal du réseau. En mesurant continuellement les performances et les flux de trafic habituels, il est capable de détecter immédiatement des écarts ou des anomalies comportementales, telles que l'établissement de tunnels chiffrés inhabituels.

3. L'enrichissement contextuel via Cisco ISE (NAC)

L'une des grandes forces de Stealthwatch est sa capacité à collaborer avec **Cisco ISE**. Au lieu d'afficher une simple adresse IP suspecte, Stealthwatch interroge ISE pour obtenir le contexte de connexion.

L'enquêteur peut ainsi voir instantanément quel utilisateur réel (par exemple, *Vicki*) et quel type d'appareil (par exemple, *un poste de travail Windows 7*) sont associés à l'adresse IP détectée.

4. Le déclenchement d'alertes comportementales spécifiques

- **Détection d'exfiltration de données** : Stealthwatch surveille les volumes de trafic sortant. Il déclenche une alarme si des seuils anormaux sont franchis, par exemple si un employé du service financier exporte pour la première fois plus d'un gigaoctet de données.
- **Identification des communications Command & Control (C2)** : En croisant le trafic réseau avec des flux de renseignement sur les menaces (Threat Intelligence), il met en évidence les machines internes qui tentent d'appeler ou de communiquer avec des serveurs de contrôle ou des botnets connus.
- **Le verrouillage d'hôte (Host Lock)** : Stealthwatch intègre une fonction appelée « verrouillage d'hôte ». Cette fonctionnalité permet d'appliquer automatiquement ou manuellement des règles restrictives ou de déclencher des alertes de violation de politique de sécurité dès qu'un hôte adopte un comportement indésirable ou non autorisé sur le réseau.

✚ Souhaitez-vous que nous examinions comment d'autres solutions d'entreprise mentionnées dans vos sources, comme **Cisco Umbrella Investigate**, complètent cette visibilité en analysant la réputation des domaines externes ?

NetFlow vs PCAP : les compromis ?

Le choix entre la capture complète de paquets (PCAP) et l'analyse de flux (NetFlow) repose sur un arbitrage fondamental entre la **profondeur des détails** et le **coût de stockage**.

1. La capture de paquets (PCAP) : La vérité brute du réseau

Le PCAP consiste à enregistrer l'intégralité du trafic réseau traversant un point d'accès.

- **Les avantages :**

- **Fidélité absolue** : C'est la méthode la plus fiable pour reconstituer le déroulement exact d'un incident.
- **Profondeur d'analyse** : Elle permet à l'enquêteur d'analyser précisément chaque étape d'une attaque, d'identifier la nature exacte des fichiers transférés et de récupérer des identifiants de connexion en clair.
- **Conformité et réglementation** : Pour répondre à des exigences réglementaires strictes, certaines organisations ont l'obligation légale de conserver ces enregistrements détaillés pendant une durée minimale.

- **Les limites :**

- **Coût de stockage massif** : Enregistrer chaque octet du trafic est extrêmement coûteux en infrastructures de stockage, ce qui limite souvent la durée de rétention de ces données.
- **La barrière du chiffrement** : Si le trafic est chiffré (HTTPS par exemple), le contenu reste illisible pour l'enquêteur à moins de disposer des clés de déchiffrement.

2. NetFlow : La cartographie comportementale et scalable

NetFlow n'enregistre pas le contenu des paquets, mais uniquement des métadonnées de connexion (les adresses IP, les protocoles, les ports et les horodatages des flux).

- **Les avantages :**

- **Couverture globale et économique** : Le stockage des flux est infiniment moins lourd que celui des paquets complets. Cela permet d'activer la surveillance sur l'ensemble des équipements réseau existants (routeurs, commutateurs,

pare-feux, serveurs virtuels) pour transformer chaque équipement en point de contrôle.

- **Parfait pour l'analyse de comportement** : Il est idéal pour repérer rapidement des anomalies globales (pics de bande passante, tunnels chiffrés inhabituels, balisage périodique ou exfiltration de données).
- **Les limites** :
 - **Absence de contenu** : NetFlow ne montre pas *ce qui* a été dit, mais seulement *qui* a parlé à *qui*. Si l'enquête exige d'analyser le code malveillant précis injecté ou les données exactes volées, NetFlow s'avère insuffisant et doit être complété par une capture PCAP.
 - **Risque de perte de granularité (Fusion/Déduplication)** : Pour faciliter la lecture humaine, les collecteurs fusionnent et concatènent souvent les flux individuels. Cette modification présente un risque de altération ou de perte de détails techniques. C'est pourquoi il est recommandé d'utiliser des enregistrements bruts non fusionnés pour les investigations de haute précision.

 Si vous le souhaitez, je peux vous créer un rapport détaillé au format PDF contenant un tableau comparatif prêt à être partagé avec vos équipes pour les aider à calibrer leurs politiques de rétention de journaux d'enquête.

Le rôle du SIEM dans l'enquête

Dans une enquête forensique, le gestionnaire d'informations et d'événements de sécurité (**SIEM**) sert de point d'ancrage centralisé pour reconstituer le déroulement complet d'un incident. Son rôle se manifeste à travers plusieurs aspects essentiels de l'investigation :

1. Un point de départ unique pour l'investigation

Dans la majorité des cas, les enquêtes numériques sur les incidents réseau commencent par l'analyse du SIEM. Les infrastructures modernes possèdent généralement une multitude d'outils de sécurité (pare-feu, filtres de contenu, IPS/IDS) qui génèrent chacun leurs propres

journaux dans des interfaces de gestion distinctes. Le SIEM élimine cette dispersion en regroupant toutes les alertes dans un **référentiel centralisé**. Cela permet à l'analyste d'obtenir une vue unifiée pour **cartographier le cheminement global de l'attaque** à travers les différents équipements avant d'aller inspecter en détail chaque système d'intérêt.

2. La corrélation et la reconstitution du "puzzle" réseau

La plupart des solutions de sécurité individuelles ne perçoivent qu'une partie d'une compromission, ce qui limite considérablement la compréhension de l'impact global de l'attaque. Lors d'une infection d'envergure, chaque équipement n'enregistre généralement qu'un fragment du trafic associé à l'incident.

Le SIEM est la seule technologie capable de **rassembler et d'identifier ces fragments d'informations épars** pour reconstituer l'événement dans sa globalité. De plus, son moteur de corrélation permet de lier entre eux de nombreux événements mineurs provenant de systèmes différents qui, pris isolément, passeraient inaperçus ou sembleraient anodins, révélant ainsi une attaque de plus grande envergure.

3. Les deux facettes spécialisées du SIEM (SIM vs SEM)

Les solutions SIEM se divisent généralement en deux orientations fonctionnelles complémentaires :

- Les outils **SIM (Security Information Management)** : ils permettent aux enquêteurs d'exploiter et de faire des recherches rapides au sein de très grands volumes de données afin d'extraire précisément les informations spécifiques sur les événements recherchés.
- Les outils **SEM (Security Event Management)** : ils se concentrent sur le traitement de flux massifs de journaux de sécurité pour aider les analystes à prioriser les événements et alertes les plus critiques.

4. La gestion de la rétention et l'accès aux archives

Pour mener à bien une enquête sur un incident survenu il y a plusieurs semaines, l'enquêteur doit prendre en compte les contraintes de stockage de l'infrastructure :

- En règle générale, un outil de sécurité conserve ses journaux locaux pendant une période de **30 à 90 jours** afin de garantir une consultation rapide.

- Si la chronologie de l'attaque dépasse cette durée de stockage local, l'analyste doit suivre une procédure spécifique pour récupérer, décompresser et réimporter les journaux correspondants qui ont été archivés sur des supports de stockage externes.

Les limites et pièges à anticiper lors de l'analyse

Bien que le SIEM facilite grandement la centralisation, l'enquêteur ne doit pas s'y fier aveuglément pour plusieurs raisons :

- **Faux sentiment de sécurité** : des attaques peuvent très bien passer inaperçues des systèmes de journalisation de sécurité configurés sur le réseau.
- **Surcharge d'alertes** : un flot excessif de faux positifs ou de faux négatifs peut noyer les indices réels.
- **Mauvaise orientation** : un moteur de corrélation mal paramétré peut ne pas hiérarchiser correctement les alertes critiques, égarant l'analyste sur une mauvaise piste.

Les journaux collectés par le SIEM ne représentent que l'espace effectivement surveillé et constituent des estimations dépendant de l'efficacité de l'outil d'origine. Il est donc fortement recommandé de **compléter toute observation issue du SIEM par une analyse forensique réseau plus approfondie** afin de confirmer formellement la réalité des faits.

✖ Si vous le souhaitez, je pourrais vous aider à concevoir un guide d'analyse manuelle des journaux réseau (avec les syntaxes de commandes d'extraction grep, cut et awk) pour vous aider à investiguer des logs archivés hors du SIEM.

Peut-on déjouer le chiffrement dans une capture PCAP ?

La capture de paquets (PCAP) est l'outil le plus complet pour reconstituer un incident, mais elle se heurte à la barrière du chiffrement.

Non, on ne peut pas lire directement le trafic chiffré dans une capture PCAP sans action supplémentaire. Bien qu'une capture réseau permette de visualiser presque tous les détails d'un événement, les données chiffrées y font exception : **le trafic chiffré doit**

obligatoirement être déchiffré, sans quoi il reste totalement illisible pour l'enquêteur.

Vos sources mettent en évidence plusieurs éléments clés à ce sujet :

- **La dissimulation des attaquants** : Les acteurs malveillants exploitent délibérément cette limite en utilisant des canaux chiffrés (comme le protocole **HTTPS sur le port 443**) ou des tunnels chiffrés pour compresser, chiffrer et masquer les données exfiltrées ou pour dissimuler leurs signaux de communication périodiques (*beacons*) au milieu du trafic légitime.
- **Absence de méthode de déchiffrement dans le guide** : Les documents fournis mentionnent qu'il est nécessaire de déchiffrer le trafic pour le rendre exploitable, mais **ils ne détaillent pas les procédures techniques** ou les mécanismes (tels que l'importation de clés privées, l'utilisation de fichiers de secrets de session *SSLKEYLOGFILE*, ou l'usage de proxys de déchiffrement) permettant d'y parvenir lors de l'analyse forensique.

Sans ces clés ou ces mécanismes de déchiffrement, l'enquêteur doit alors se rabattre sur des analyses comportementales ou des métadonnées (comme NetFlow) pour détecter des anomalies de trafic, même si le contenu précis des paquets lui échappe.

 Le guide restant très succinct sur ce point, je peux effectuer des recherches sur le Web pour vous expliquer les méthodes concrètes de déchiffrement du trafic TLS/SSL dans un outil comme Wireshark. Souhaitez-vous que nous explorions cela ?

Comment démarrer avec Kali Linux ?

Le guide fourni ne contient pas de procédure d'installation ou de guide de configuration initial pour démarrer de zéro avec Kali Linux. En revanche, il présente **Kali Linux comme la plateforme de travail idéale pour réaliser des exercices pratiques d'analyse offensive et défensive**.

Voici les cas d'usage et les outils spécifiques suggérés par vos sources pour commencer à manipuler cette distribution dans le cadre de votre apprentissage de la sécurité réseau :

1. Analyser et comprendre les balayages de ports (Reconnaissance)

Pour apprendre à identifier l'empreinte réseau d'un attaquant lors de sa phase de reconnaissance :

- Vous pouvez lancer l'analyseur de paquets **Wireshark** directement depuis votre système Kali Linux.
- En parallèle, utilisez l'outil de scan **Nmap** (présent sous Kali) pour effectuer différentes analyses (comme des scans de ports SYN, XMAS ou FIN) sur un système cible.
- Observez le résultat des captures dans Wireshark pour apprendre à créer des filtres de détection spécifiques (par exemple `tcp.flags.syn && tcp.flags.ack==0` pour isoler les paquets SYN sans accusé de réception) et ainsi distinguer le trafic d'analyse du reste du trafic réseau.

2. S'initier à l'exploitation de vulnérabilités

Le guide propose d'étudier le comportement d'un intrus lorsqu'il s'attaque à une faiblesse du système :

- Vous pouvez utiliser l'outil d'exploitation graphique **Armitage** sous Kali Linux pour cibler une vulnérabilité (comme l'exploitation d'une faille Struts sur un serveur Apache).
- Cette manipulation vous permet de comprendre comment l'attaquant parvient à exécuter des commandes à distance avec des privilèges élevés (root) en validant son accès via la commande `whoami`.
- L'objectif est d'étudier ensuite les alertes générées par les outils de défense (comme Snort ou Cisco Firepower) pour comprendre comment documenter l'incident et évaluer si l'exploitation a réussi.

3. Extraire des informations DNS avec Fierce

Kali Linux intègre des utilitaires légers pour cartographier l'infrastructure d'un domaine externe :

- Utilisez l'outil de reconnaissance DNS **Fierce** préinstallé sur la distribution.
- Saisissez la commande `fierce.pl -dns <cible>` (par exemple `fierce.pl -dns thesecurityblogger.com`) dans votre terminal Kali.
- Si le serveur DNS de la cible autorise les transferts de zone (zone transfers), Fierce extraira instantanément l'intégralité des sous-

domaines et hôtes liés, vous aidant à visualiser l'écosystème externe de la cible.

4. S'entraîner de manière concrète sur des plateformes de défis

Les sources insistent sur le fait que la meilleure façon d'acquérir de l'expérience est de participer à des exercices de type « **capture du drapeau** » (**CTF**). Vous pouvez utiliser votre machine Kali Linux pour vous mesurer à des scénarios réels sur les plateformes recommandées suivantes :

- **VulnHub** : Idéal pour télécharger des machines virtuelles volontairement vulnérables à exécuter localement et à attaquer avec vos outils Kali.
- **OverTheWire** et **Hack This Site** : Parfaits pour apprendre les bases de l'exploitation et du piratage pas à pas.
- **CTFLearn** ou **Microcorruption** : Pour travailler sur des problématiques spécifiques de sécurité et de reverse engineering.

🎮 Si vous le souhaitez, je peux vous lister de manière exhaustive l'ensemble des plateformes d'entraînement (CTF) recommandées dans vos sources ainsi que les adresses web associées pour que vous puissiez créer vos comptes et débiter vos premiers défis de sécurité.

Comment installer Kali Linux ?

Le guide fourni ne contient pas d'instructions ou de procédure pour installer Kali Linux.

Vos sources mentionnent uniquement son utilisation comme une plateforme de travail préexistante permettant d'exécuter des outils d'analyse de sécurité (tels que **Wireshark**, **Nmap**, **Armitage** et **Fierce**) et pour réaliser des exercices pratiques ou des défis de type Capture The Flag (CTF).

Souhaitez-vous que j'effectue une recherche sur le Web afin de vous fournir un guide étape par étape pour télécharger et installer Kali Linux (par exemple au sein d'une machine virtuelle) ?

Quelles plateformes CTF recommandez-vous?

Pour acquérir de l'expérience pratique et simuler des incidents de sécurité réels, le guide recommande de participer à des exercices de type « **capture du drapeau** » (**CTF**). Que vous choisissiez d'adopter la perspective de l'attaquant pour comprendre ses méthodes ou celle du défenseur pour perfectionner vos compétences en détection, voici les plateformes d'entraînement référencées :

- **CTFLearn** : <https://ctflearn.com/>
- **OverTheWire (Wargames)** : <http://overthewire.org/wargames/>
- **Hack This Site** : <https://www.hackthissite.org/>
- **VulnHub** : <https://www.vulnhub.com/>
- **Microcorruption** : <https://microcorruption.com/login>
- **Pwnable.kr** : <http://pwnable.kr/>
- **Reversing.kr** : <http://reversing.kr/>
- **W3Challs** : <https://w3challs.com/>
- **Ringzer0 Team** : <https://ringzer0team.com/>
- **Hax.tor.hu** : <http://hax.tor.hu/welcome/>
- **Hellbound Hackers** : <https://www.hellboundhackers.org/>
- **KomodoSec CTF** : <http://ctf.komodosec.com>

Ces environnements vous permettront de vous exercer à utiliser des outils de sécurité, à analyser des captures de paquets et à comprendre concrètement le cycle de vie des attaques.

 Si vous le souhaitez, nous pouvons étudier plus en détail les filtres Wireshark essentiels à connaître pour repérer un scan de ports (comme les scans SYN ou XMAS) lors de vos premières simulations.

Détection d'un scan de ports SYN

Le balayage (ou scan) de ports SYN est l'une des formes de reconnaissance les plus courantes utilisées par un attaquant pour évaluer les systèmes d'un réseau à la recherche de ports ouverts. Pour détecter ce comportement, l'analyse forensique s'appuie sur des approches manuelles d'analyse de paquets et des solutions de détection automatisées.

1. L'analyse manuelle et le filtrage avec Wireshark

Dans le cadre de l'analyse d'une capture de paquets (PCAP), un scan de ports se manifeste par des requêtes de ressources répétitives et inhabituelles. Pour isoler ce comportement spécifique au milieu d'un trafic réseau important, l'enquêteur peut utiliser des filtres Wireshark ciblés :

- **Pour identifier les paquets SYN sans accusé de réception** (qui caractérisent les tentatives d'ouverture de connexion du scan SYN sans finalisation de la liaison à trois voies) :

`tcp.flags.syn && tcp.flags.ack==0`

- **Pour repérer les tentatives de connexion vers des ports fermés** (en recherchant les paquets de réinitialisation/Reset renvoyés par la cible à l'adresse de l'attaquant) :

`ip.src==192.168.1.20 && tcp.flags.reset && tcp.flags.ack`

(Note : Remplacez l'adresse IP source par celle du système suspect à analyser).

L'objectif de ces filtres est de mettre en évidence un terminal qui cherche activement de nouvelles cibles ou des méthodes de communication sur le réseau.

2. La détection automatisée par IDS (ex: Snort)

La plupart des administrateurs réseau ne pouvant pas analyser manuellement le trafic brut au quotidien, ils déploient des systèmes de détection d'intrusion (IDS) pour surveiller les communications internes. Le logiciel open source **Snort** intègre une règle de pré-analyse spécifique permettant de détecter la majorité des analyses de ports (comme celles générées par Nmap). Pour l'exploiter, il est nécessaire de l'activer dans le fichier de configuration (Snort.config) car elle est inactive par défaut, en saisissant la directive suivante :

```
Preprocessor sfportscan: proto {all} sense_level {high} logfile {LOCATION}
```

(Les champs entre crochets doivent être adaptés selon les spécificités de votre infrastructure Snort).

3. La détection de niveau entreprise et la corrélation SIEM

Les solutions d'entreprise, telles que **Cisco Firepower**, détectent automatiquement ces balayages de ports grâce à leurs fonctionnalités

IPS intégrées. Elles offrent une console d'analyse où l'enquêteur peut directement cliquer sur l'événement pour obtenir des détails cruciaux : l'adresse IP source suspecte, la cible visée, les ports scannés et la géolocalisation du trafic.

Ces alertes sont ensuite exportées vers un **SIEM** (gestionnaire d'événements de sécurité). Le SIEM permet de corréler ces scans mineurs avec d'autres anomalies survenues sur différents équipements réseau afin de reconstituer le puzzle global de l'attaque et de comprendre l'étendue exacte de la compromission.