



Scénario 1 : Phishing et déploiement d'un ransomware

L'unité d'une entreprise qui a détecté une intrusion naît après qu'un employé ait cliqué sur un lien de phishing. Le ransomware a commencé à chiffrer

- Quelles actions immédiates allez-vous prendre pour limiter l'impact de l'attaque ?
- Quelles preuves numériques devez-vous collecter pour l'investigation ?

En menant une analyse forensique, vous découvrez des fichiers malveillants sur plusieurs postes de travail.

- Quels outils et techniques allez-vous utiliser pour analyser ces fichiers afin d'identifier leur mode d'action ?
- Comment allez-vous tracer l'origine de l'attaque et évaluer son impact ?

Un employé rapporte un comportement étrange sur son poste de travail, mais aucune alerte automatique n'a été déclenchée par les solutions de sécurité.

- Quels indices recherchez-vous pour confirmer ou infirmer une infection par un malware ?

Scénario 2 : Compromission d'un serveur via des vulnérabilités logicielles

Après une investigation initiale, vous constatez que des logs sur un serveur montrent une activité inhabituelle provenant d'une adresse IP externe.

- Quels logs ou données devez-vous examiner pour confirmer une compromission ?
- Quelle méthodologie allez-vous adopter pour analyser la vulnérabilité exploitée ?

Les fichiers système critiques du serveur semblent avoir été modifiés.

- Quels outils utilisez-vous pour détecter et comparer les empreintes (hashes) avec les originaux ?
- Quels mécanismes de protection proposez-vous pour éviter une telle attaque à l'avenir ?

Scénario 3 : Analyse de malware et environnements de test

Un fichier suspect vous est transmis pour analyse, et il pourrait contenir un cheval de Troie.

- Quels sont les avantages et les risques d'utiliser une machine virtuelle pour l'analyse dynamique ?
- Quelles précautions allez-vous prendre pour isoler l'environnement d'analyse de votre réseau de production ?

Après l'analyse d'un malware, vous découvrez qu'il se connecte à un serveur C2 (C2).

- Comment allez-vous analyser le trafic réseau généré par ce malware ?
- Quelles informations essentielles pouvez-vous obtenir en surveillant les communications entre le malware et son serveur C2 ?

Scénario 4 : Exfiltration de données et détection

Un audit réseau révèle qu'une exfiltration de données sensibles s'est produite via des requêtes DNS inhabituelles.

- Quels outils et méthodes allez-vous utiliser pour identifier les domaines utilisés par les attaquants ?
- Comment allez-vous bloquer ce type d'attaque à l'avenir tout en garantissant la continuité du service DNS ?

Un employé soupçonné de comportement malveillant a été identifié.

- Quels dispositifs allez-vous mettre en place pour collecter des preuves sans interrompre son activité ou éveiller ses soupçons ?
- Comment garanzissez-vous l'intégrité des preuves numériques pour leur utilisation en justice ?

Scénario 5 : Investigations sur un fichier PE malveillant

Vous analysez un fichier Portable Executable (PE) trouvé sur un poste de travail compromis.

- Quels outils spécifiques utilisez-vous pour inspecter la structure du fichier PE ?
- Quelles informations (e.g., imports, exports, sections) sont critiques pour comprendre le comportement du programme ?

Vous détectez que ce fichier PE contient un code obfusqué.

- Quelles techniques allez-vous utiliser pour contourner cette obfuscation et analyser le code ?
- Comment identifiez-vous si ce fichier contient des mécanismes anti-analyse (anti-debugging ou anti-virtualisation) ?

Scénario 6 : Gestion d'un incident de vol de données

Une entreprise découvre que des données sensibles ont été volées et publiées sur le dark web.

- Quelle méthodologie adoptez-vous pour retracer les étapes de l'attaquant et identifier les failles exploitées ?
- Comment analysez-vous les traces laissées sur les systèmes pour déterminer l'étendue des données compromises ?

Après investigation, vous identifiez que l'attaquant a laissé un backdoor actif sur le réseau.

Comment neutralisez-vous cette backdoor ?
Comment pouvez-vous empêcher des réinfections similaires ?

Scénarios

Quels choisiriez-vous pour analyser une attaque et pourquoi ?

- Autopsy
- FTK Imager
- En quoi l'analyse de la mémoire vive (RAM) peut-elle être déterminante dans une investigation, et comment utiliser des outils comme Volatility pour extraire des informations cruciales ?

► Réponses :

Scénario 1 : Intrusion par phishing et déploiement d'un ransomware

Actions immédiates à prendre :

- Isoler immédiatement les postes infectés du réseau pour éviter la propagation.
- Désactiver les comptes utilisateurs compromis.
- Informer les employés de ne pas interagir avec les fichiers ou messages suspects.
- Préserver les preuves en effectuant des copies des disques durs et des journaux système.

Preuves numériques à collecter :

- Logs réseau (firewall, proxy, etc.) pour analyser le trafic sortant.
- Journaux système des machines infectées pour identifier le vecteur initial.
- Hash des fichiers chiffrés pour comparer avec des bases de données de ransomwares connus.

Indices pour confirmer une infection :

- Présence de processus suspects ou utilisation anormale des ressources système.
- Modifications inattendues des fichiers ou des clés de registre.
- Communication réseau inhabituelle vers des adresses IP ou des domaines externes.

Scénario 2 : Compromission d'un serveur via des vulnérabilités logicielles

Logs ou données à examiner :

- Journaux d'accès HTTP/HTTPS pour détecter des requêtes anormales.
- Logs SSH pour identifier des connexions non autorisées.
- Journaux des modifications de fichiers ou des permissions.

Méthodologie pour analyser la vulnérabilité :

- Identifier la version du logiciel et la comparer avec les vulnérabilités connues (bases CVE).
- Reproduire l'attaque dans un environnement isolé pour comprendre le vecteur exact.
- Examiner les patches ou mises à jour disponibles pour combler la faille.

Outils pour détecter les fichiers compromis :

- Tripwire ou AIDE pour vérifier l'intégrité des fichiers.
- sha256sum ou md5sum pour comparer les empreintes des fichiers suspects avec les versions originales.
- Scénario 3 : Analyse de malware et environnement sécurisé

Avantages et risques d'une VM pour l'analyse dynamique :

- Avantages : Isolation, possibilité de restaurer des snapshots, contrôle total de l'environnement.
- Risques : Certains malwares détectent les environnements virtuels et changent leur comportement.

Précautions pour isoler l'environnement :

- Déconnecter la VM d'Internet ou utiliser un réseau isolé.
- Limiter l'accès aux périphériques physiques.
- Configurer des règles strictes sur l'hôte pour empêcher toute fuite de données.

Analyse du trafic réseau généré par le malware :

- Utiliser Wireshark pour capturer les paquets réseau et examiner les requêtes DNS, HTTP ou autres protocoles utilisés.
- Identifier les domaines et IP utilisés pour la communication C2.
- Examiner le contenu des paquets pour détecter des commandes ou des données exfiltrées.

nnées et détection lines malveillants :

pour capturer le trafic DNS.
ur analyser les requêtes DNS en temps réel.
le serveur pour repérer des noms de domaine suspects.

Bloquer ce type d'attaque à l'avenir :

- Implémenter des listes noires de domaines ou adresses IP connus pour le tunneling DNS.
- Activer des filtres DNS pour détecter des requêtes anormales.
- Configurer un IDS/IPS pour surveiller les communications réseau.

Scénario 5 : Investigations sur un fichier PE malveillant

Outils pour analyser un fichier PE :

- PES studio pour analyser les sections du fichier et les imports/exports.
- LordPE ou PEView Explorer pour inspecter les structures PE.
- IDA Pro ou Ghidra pour effectuer une analyse statique avancée.

Informations critiques à déduire :

- Imports utilisés par le fichier (API appelées).
- Sections anormales ou obfusquées (par exemple, .text ou .data inhabituelles).
- Signature du fichier pour voir s'il est connu dans les bases de données de malwares.

Techniques pour contourner l'obfuscation :

- Déobfuscation manuelle en décompilant le code.
- Utilisation d'un débogueur (par ex. x64dbg) pour suivre l'exécution du fichier.
- Charger le fichier dans un environnement dynamique pour capturer son comportement réel.

Scénario 6 : Gestion d'un incident de vol de données

Méthodologie pour retracer l'attaquant :

- Analyser les logs réseau pour repérer l'origine des connexions suspectes.
- Examiner les fichiers modifiés ou exfiltrés.
- Rechercher des backdoors ou des logiciels malveillants installés sur les machines compromises.

Protéger les preuves numériques :

- Effectuer des copies forensiques des disques durs avec des outils comme FTK Imager ou dd.
- Capturer les logs système et les journaux réseau.
- Utiliser des outils comme Autopsy pour analyser les artefacts numériques.

Scénario 7 : Outils incontournable

Outils :

- Volatility : Analyse de la mémoire vive pour récupérer des processus, connexions réseau, etc.
- Wireshark : Analyse du trafic réseau pour détecter des anomalies.
- IDA Pro : Désassemblage pour analyser le code malveillant.
- Autopsy : Analyse des artefacts sur disque dur (fichiers supprimés, journaux, etc.).
- FTK Imager : Acquisition forensique des disques et des partitions.

Analyse de la RAM avec Volatility :

- Récupérer les processus en cours pour repérer des logiciels malveillants.
- Identifier les connexions réseau actives.
- Détecter des traces de logiciels ou de commandes exécutés récemment.