GS21

Analyse Forensique d'un Poste de Travail

1. Stockage des Traces de Compromission

La réalisation d'une analyse forensique sur un système informatique compromis nécessite une approche méthodique pour détecter, extraire, analyser les données et mettre en place des mesures correctives. Cette méthodologie complète aborde les principaux composants susceptibles de contenir des traces de compromission.

1.1 Fichiers Système

Logs du Système d'Exploitation : Les journaux d'événements, tels que les Windows Event Logs ou les syslog sur Linux, offrent une chronique détaillée des activités système, de sécurité et des applications, permettant de détecter des événements suspects.

Fichiers de configuration Système Compromis : Les fichiers système, tels que /etc/passwd sur Linux ou le Registre Windows, peuvent être altérés de manière malveillante. Un examen approfondi de ces fichiers est essentiel pour détecter des signes de compromission.

1.2 Registre Windows

Modifications malveillantes : Le Registre Windows, base de données centrale, peut contenir des modifications malveillantes impactant la configuration système, les autorisations ou créant des vulnérabilités. Une analyse détaillée est nécessaire.

1.3 Fichiers de Logs d'Applications

Logs Spécifiques aux Applications : Les logs d'applications renferment des informations cruciales sur les activités des programmes, permettant la détection d'une utilisation abusive, d'accès non autorisés ou de transactions suspectes.

1.4 Mémoire Système

Données en Mémoire Volatile : La mémoire système, étant volatile, peut contenir des traces temporaires d'activités malveillantes. Une analyse attentive peut révéler des éléments tels que des processus non autorisés ou des injections de code.

1.5 Systèmes de Fichiers Temporaires

Fichiers temporaires : Les systèmes de fichiers temporaires, souvent exploités pour des opérations temporaires, peuvent dissimuler des outils malveillants. L'examen de ces zones est crucial pour identifier des anomalies.

1.6 Comptes d'Utilisateurs Compromis

Traces dans les Comptes Compromis : Les comptes d'utilisateurs compromis sont des points de départ essentiels. Les journaux d'activité, les changements de privilèges ou les connexions inhabituelles peuvent révéler des signes d'accès non autorisés.

Cette approche méthodique offre une base complète pour mener une analyse forensique approfondie sur un poste de travail compromis, permettant ainsi d'identifier, d'extraire et d'analyser les traces de compromission avec précision.

2. Méthode d'Extraction des Données en Analyse Forensique

L'analyse forensique exige des méthodes d'extraction rigoureuses pour collecter des données cruciales permettant de reconstruire des événements et de détecter des signes de compromission. Trois approches principales sont couramment utilisées dans cette tâche complexe : l'utilisation d'outils de forensique numérique, l'exploitation des commandes natives du système d'exploitation, et l'utilisation d'outils en ligne de commande.

2.1 Outils de Forensique Numérique :

Les outils spécialisés en forensique numérique sont réputés pour leurs fonctionnalités avancées dans l'acquisition, l'analyse, et la présentation de données. Parmi eux, on retrouve des références notables :

EnCase : Renommé pour son exhaustivité, il simplifie l'acquisition de données, l'analyse des fichiers, et la récupération d'informations essentielles.
FTK (Forensic Toolkit) : Offre des fonctionnalités complètes pour l'indexation, la recherche, et l'analyse approfondie des données forensiques.
Autopsy : Interface graphique pour Sleuth Kit, une approche open source pour l'examen détaillé de disques et de fichiers.
Volatility : Spécialisé dans l'analyse de la mémoire volatile, il permet d'extraire des artefacts pour identifier des activités suspectes en cours.

2.2 Commandes Natives du Système d'Exploitation :

Les systèmes d'exploitation fournissent des commandes natives facilitant l'extraction d'informations spécifiques. Ces commandes varient selon la plateforme :

Event Viewer sur Windows : Permet l'exploration et l'extraction d'informations des journaux d'événements Windows, essentiels pour comprendre l'historique des activités du système.
dmesg sur Linux : Offre des détails sur les messages du noyau Linux, une source précieuse pour identifier des erreurs matérielles et des événements système.

2.3 Lignes de Commande :

L'utilisation d'outils en ligne de commande constitue une approche flexible et puissante pour extraire des données spécifiques. Des commandes telles que grep, awk, et sed sont couramment employées pour filtrer et manipuler des informations textuelles, en particulier issues de fichiers de logs ou de résultats de commandes système.

2.4 Outils Spécifiques à la Plateforme :

Chaque système d'exploitation dispose d'outils dédiés pour extraire des logs et des données système. L'intégration de ces outils dans le processus d'analyse permet une extraction spécifique et précise en fonction de la plateforme utilisée.

L'utilisation conjointe de ces méthodes assure une collecte exhaustive des données nécessaires à une analyse forensique approfondie. Cette approche multidimensionnelle offre aux experts en sécurité la possibilité de naviguer à travers les couches complexes des systèmes informatiques, facilitant la découverte des éléments clés liés à une éventuelle compromission.

3. Méthode d'Analyse des Données Extraites en Analyse Forensique

L'analyse des données extraites constitue l'épine dorsale de l'enquête forensique, cherchant à dévoiler les éléments cachés et à reconstruire les séquences d'événements critiques. Cette approche méthodique s'organise autour de phases distinctes, chacune se consacrant à un aspect spécifique des données extraites.

3.1 Analyse des Logs :

Identification des Anomalies : Scruter les logs système pour repérer des événements inattendus ou des schémas incohérents, révélant ainsi des activités potentiellement malveillantes.

Détection de Connexions Suspectes : Examiner les logs pour identifier des connexions réseau inhabituelles, des accès non autorisés, ou des tentatives d'intrusion.

Surveillance des modifications dans les Fichiers Système : Analyser les logs pour repérer des altérations dans les fichiers système, offrant des indices sur des modifications non autorisées.

3.2 Corrélation des Événements Temporels :

Chronologie des Activités : Relier les événements dans le temps pour établir une chronologie des activités, facilitant la compréhension des attaques dans leur contexte temporel.

Étude des Interventions : Identifier les moments clés où des modifications majeures ont eu lieu, contribuant à la compréhension des tactiques de l'attaquant.

3.3 Analyse de la Mémoire :

Recherche de Processus Malveillants : Identifier des processus en mémoire indiquant la présence d'un logiciel malveillant actif.

Identification des Connexions Réseau Suspectes : Examiner les connexions réseau actives en mémoire pour détecter d'éventuelles communications malveillantes.

3.4 Analyse des Fichiers Temporaires :

Recherche d'Outils malveillants : Scruter les fichiers temporaires à la recherche d'outils, de scripts ou de programmes malveillants.

Analyse des Scripts : Étudier les scripts dans les fichiers temporaires pour détecter des actions malveillantes potentielles.

3.5 Analyse des Comptes Utilisateurs :

Vérification des Activités liées aux Comptes Compromis : Examiner les logs pour détecter des connexions inattendues, des changements de privilèges, ou d'autres activités anormales liées aux comptes compromis.

L'intégration de ces méthodes dans le processus d'analyse forensique offre une vision holistique, permettant aux enquêteurs de démêler les tenants et aboutissants des incidents de sécurité. Cette approche systématique, allant des logs à la mémoire en passant par les fichiers temporaires et les comptes utilisateurs, facilite la découverte des éléments critiques et guide les actions de réponse en cas d'incident.

4. Méthode de Remédiation en Cas de Compromission

Face à une compromission détectée, la mise en œuvre d'une méthode de remédiation rapide et efficace est essentielle pour minimiser les risques, restaurer l'intégrité du système, et prévenir toute propagation ultérieure. La démarche de remédiation comprend plusieurs étapes clés, visant à isoler, éliminer, renforcer la sécurité, et sensibiliser les acteurs impliqués.

4.1 Isolation du Système :

La première étape cruciale consiste à isoler le poste de travail compromis pour empêcher la propagation éventuelle de l'infection. Mettre le système en quarantaine permet de limiter l'impact sur d'autres composants du réseau et d'empêcher la compromission de se propager à d'autres systèmes.

4.2 Suppression des Malwares :

Utiliser des outils spécialisés de suppression de malwares pour éliminer toute trace de logiciels malveillants présents sur le système compromis. Ces outils sont conçus pour détecter, isoler et supprimer les fichiers et processus malveillants, contribuant ainsi à la restauration de l'intégrité du système.

4.3 Mise à Jour de la Sécurité :

Appliquer rapidement les correctifs de sécurité disponibles pour remédier aux vulnérabilités exploitées lors de l'attaque. Mettre à jour les logiciels antivirus et les signatures permet d'assurer une meilleure protection contre les menaces connues.

4.4 Réinitialisation des Mots de Passe :

En réponse à une compromission, il est impératif de réinitialiser tous les mots de passe compromis. Cette mesure vise à bloquer l'accès non autorisé à des comptes et à renforcer la sécurité des identifiants.

4.5 Analyse Post-Incident :

Procéder à une analyse post-incident en examinant d'autres systèmes pour détecter des traces similaires. Cette étape permet de déterminer l'étendue de l'attaque, d'identifier d'autres points de compromission potentiels, et de prendre des mesures préventives additionnelles.

4.6 Formation et Sensibilisation :

Sensibiliser les utilisateurs aux pratiques de sécurité et aux signes d'intrusion est une initiative préventive. La formation renforce la résilience de l'ensemble de l'organisation en encourageant une culture de sécurité proactive, où les utilisateurs sont conscients des risques potentiels et adoptent des comportements sécurisés.

La mise en œuvre méticuleuse de ces étapes de remédiation contribue à restaurer l'intégrité du système compromis, à réduire les risques de récidive, et à renforcer la posture globale de sécurité de l'infrastructure informatique. Une réponse rapide et coordonnée est cruciale pour minimiser les impacts d'une compromission et prévenir de futures attaques.

L'analyse forensique doit être effectuée avec soin pour préserver l'intégrité des preuves. En cas de doute, il est recommandé de faire appel à des experts en forensique numérique.

Analyse Forensique des Traces Réseaux

Lors d'une analyse forensique des traces réseau après une attaque, il est crucial de cibler les composants pertinents, extraire les données de manière efficace, et analyser les indices de compromission. Voici une méthodologie complète pour cette tâche :

1. Stockage des Traces de Compromission :

Lorsqu'il s'agit d'analyser des incidents de sécurité et de déterminer les causes d'une compromission, les traces laissées dans les logs des différents composants réseau sont d'une importance cruciale. Chacun de ces composants joue un rôle spécifique dans la détection, la prévention et la réponse aux incidents, fournissant des informations vitales pour l'analyse forensique.

1.1. Logs du Pare-feu :

Les logs du pare-feu sont une mine d'informations sur les activités réseau. Ils enregistrent :

Connexions entrantes et sortantes : Répertoriant les flux de données entrants et sortants, ils permettent d'identifier des connexions non autorisées ou suspectes.
Règles Modifiées : Tout changement dans les règles de pare-feu est enregistré, fournissant un indicateur potentiel de manipulation par un attaquant.
Tentatives d'intrusion : Les logs du pare-feu signalent les tentatives d'intrusion, aidant à détecter les attaques en cours.

1.2. Logs du Routeur :

Les logs du routeur offrent un aperçu détaillé des activités réseau, y compris :

Flux de Données : Enregistrant les flux de données, ils permettent de suivre la circulation des informations à travers le réseau.
Connexions Réseau : Identifiant les connexions établies, ils aident à détecter des connexions anormales ou des activités suspectes.
Attaques de Type DDoS : Les logs du routeur peuvent signaler des patterns caractéristiques des attaques par déni de service distribué (DDoS).

1.3. Logs des Serveurs Proxy :

Les serveurs proxy conservent des logs spécifiques aux activités web, dont :

Requêtes HTTP : Enregistrant les requêtes web, ils permettent de suivre l'activité en ligne des utilisateurs.
Sites Visités : Les logs des serveurs proxy fournissent une trace des sites web visités, essentielle pour l'analyse des comportements utilisateur.
Connexions Bloquées : Ils signalent les tentatives d'accès à des sites bloqués, indiquant potentiellement une activité malveillante.

1.4. Logs du Système de Détection d'Intrusion (IDS) :

Les IDS enregistrent des événements liés à des activités suspectes, dont :

Détection d'Activités Malveillantes : Les logs de l'IDS fournissent des alertes sur des comportements ou des patterns d'activité pouvant indiquer une compromission.

Informations sur les Intrusions : Ils capturent des données spécifiques sur les méthodes et vecteurs d'attaque.

1.5. Logs du Système de Prévention d'Intrusion (IPS) :

Les IPS enregistrent les réponses aux tentatives d'intrusion, incluant :

Actions Prises en Réponse : Les logs de l'IPS indiquent les mesures prises pour contrer les attaques, aidant à évaluer l'efficacité des contre-mesures.

1.6. Logs du Serveur DNS :

Les logs du serveur DNS peuvent révéler des activités potentiellement malveillantes, notamment :

Requêtes DNS Suspectes : En identifiant des requêtes DNS inhabituelles, ces logs peuvent signaler des tentatives d'utilisation malveillante de noms de domaine.
L'agrégation et l'analyse systématique de ces logs permettent aux experts en sécurité d'identifier les indicateurs de compromission, de reconstruire la séquence des événements et de mettre en œuvre des mesures de remédiation ciblées. En intégrant ces sources d'information, l'analyse forensique réseau devient une composante essentielle de la réponse aux incidents de sécurité.

2. Méthode d'Extraction des Données :

L'extraction méticuleuse des données en analyse forensique réseau est une étape cruciale pour identifier les anomalies, comprendre les attaques, et prendre des mesures correctives. Cette tâche complexe nécessite l'utilisation d'outils spécialisés et de lignes de commande précises pour collecter des informations pertinentes à partir des différents composants du réseau.

2.1. Outils de Capture et d'Analyse de Paquets :

Wireshark : Wireshark est un outil de capture et d'analyse de paquets réseau, offrant une interface conviviale pour examiner le trafic en temps réel. Il permet d'identifier les protocoles utilisés, de filtrer des paquets spécifiques, et d'analyser le contenu des échanges.

tcpdump : Une solution en ligne de commande pour capturer et analyser des paquets réseau. Avec ses nombreuses options de filtrage, tcpdump est puissant pour extraire des informations spécifiques du trafic réseau.

Snort : En tant que système de détection d'intrusion (IDS), Snort analyse le trafic réseau en temps réel, générant des alertes en cas d'activité suspecte. Il peut également être utilisé pour capturer des paquets pour une analyse ultérieure.

2.2. Utilisation d'Outils Spécifiques aux Composants Réseau :

Outils des Pare-feu, Routeurs, IDS/IPS : Chaque composant du réseau (pare-feu, routeur, IDS/IPS) a ses propres outils pour extraire des informations spécifiques. Par exemple, les interfaces d'administration des pare-feu et des routeurs permettent d'accéder aux logs, tandis que les IDS/IPS ont des consoles dédiées pour extraire des données liées aux événements de sécurité.

2.3. Lignes de Commande pour la Capture de Paquets :

Commandes comme tcpdump : L'utilisation de tcpdump en ligne de commande permet de capturer des paquets spécifiques en fonction de critères définis (protocole, adresse source/destination, port, etc.). Cela offre une flexibilité précieuse pour focaliser l'analyse sur des aspects particuliers du trafic.

2.4. Utilisation des Commandes Natives des Pare-feu et Routeurs :

Commandes Natives : Les pare-feu et routeurs disposent de commandes natives pour extraire des logs spécifiques. Par exemple, l'utilisation de commandes sur un pare-feu peut révéler des informations sur les connexions établies, les règles modifiées, ou les tentatives d'intrusion.
Cette méthode d'extraction diversifiée garantit la collecte complète de données provenant de sources variées au sein du réseau. Les outils spécialisés offrent une visualisation détaillée, tandis que les lignes de commande permettent une personnalisation approfondie. La combinaison de ces approches assure une analyse forensique réseau exhaustive, facilitant l'identification des comportements malveillants, la reconstruction des séquences d'attaques, et la prise de mesures correctives appropriées.

3. Méthode d'Analyse des Données Extraites :

L'analyse des données extraites en forensique réseau constitue une étape cruciale pour dévoiler les détails des incidents de sécurité, comprendre les méthodes des attaquants, et orienter la réponse aux incidents. Cette méthode se déploie à travers plusieurs facettes, chacune centrée sur l'exploration approfondie des données collectées.

3.1. Analyse des Flux de Données :

Connexions Réseau Suspectes : Examiner les connexions réseau inhabituelles permet de repérer des comportements anormaux. Les tentatives de connexion à des adresses inattendues ou l'établissement de flux de données non autorisés peuvent indiquer une activité malveillante.

Identification des adresses IP, Ports et Protocoles : Identifier les adresses IP, ports et protocoles impliqués offre une visibilité sur les vecteurs d'attaque et les méthodes utilisées par les intrus.

3.2. Analyse des Logs :

Recherche d'Anomalies dans les Logs : Scruter les logs à la recherche d'anomalies, comme des tentatives répétées de connexion ou des erreurs d'authentification, permet de détecter des comportements suspects.

Corrélation Temporelle : La corrélation temporelle aide à comprendre la séquence des événements, facilitant la reconstitution des attaques dans leur chronologie.

3.3. Analyse des Signatures IDS/IPS :

Identification des Signatures d'Attaques Connues : Les systèmes IDS/IPS génèrent des signatures pour des attaques connues. Identifier ces signatures dans les logs aide à reconnaître les méthodes d'attaques préalablement identifiées.

Examen des Événements IDS/IPS : Les événements générés par les systèmes IDS/IPS fournissent des indications sur les activités suspectes et les tentatives d'intrusion.

3.4. Analyse de la Charge Utile (Payload) :

Examen du Contenu des Paquets : L'analyse de la charge utile permet d'identifier des motifs malveillants dans le contenu des paquets. Cela inclut la recherche de commandes malicieuses, de tentatives d'injection SQL, ou d'autres formes d'exploitation de vulnérabilités.

3.5. Analyse du Trafic DNS :

Identification de Domaines Suspects : L'examen du trafic DNS permet de repérer des domaines suspects. Des requêtes DNS non autorisées ou des tentatives d'utilisation malveillante de noms de domaine peuvent être des signaux d'une activité malveillante.
Cette méthodologie d'analyse multidimensionnelle offre une vision complète des événements réseau, permettant aux analystes de déceler des modèles, d'identifier des comportements anormaux, et de reconstruire les séquences des attaques. En combinant ces différentes approches, les équipes de sécurité sont mieux équipées pour comprendre l'impact des incidents, prendre des mesures correctives appropriées, et renforcer la résilience du réseau face aux menaces futures.

4. Méthode de Remédiation :

Face à une compromission détectée au sein du réseau, la mise en œuvre d'une méthodologie de remédiation efficace est impérative pour contenir les dégâts, éradiquer les menaces, et renforcer la posture de sécurité. Cette démarche proactive englobe plusieurs étapes essentielles visant à isoler, protéger, et prévenir de futures intrusions.

4.1. Blocage des Adresses IP Malveillantes :

Règles de Pare-feu : Mettre en place des règles de pare-feu pour bloquer les adresses IP responsables de l'attaque est une mesure immédiate pour isoler l'intrus et éviter toute communication malveillante. Cette action contribue à contenir la menace et à protéger les ressources critiques.

4.2. Mise à Jour des Signatures :

IDS/IPS à Jour : Assurer que les signatures de l'IDS/IPS sont constamment mises à jour est essentiel pour détecter et bloquer les nouvelles menaces. Cette mise à jour régulière garantit une meilleure capacité à identifier les schémas d'attaques émergents.

4.3. Analyse des Politiques de Sécurité :

Examen et Ajustement des Règles : L'analyse des politiques de sécurité, notamment des règles du pare-feu et du routeur, permet d'identifier des lacunes potentielles et de les corriger. Il peut s'agir de renforcer les règles existantes, d'ajouter des restrictions spécifiques, ou de réviser les autorisations.

4.4. Surveillance Continue :

Mise en place d'une surveillance Continue : Établir une surveillance continue du trafic réseau est essentiel pour détecter rapidement les activités suspectes. L'utilisation d'outils de surveillance en temps réel permet d'identifier toute tentative d'intrusion ou d'activité malveillante émergente.

4.5. Formation du Personnel :

Sensibilisation et Formation : Sensibiliser le personnel à reconnaître et signaler les activités anormales renforce la première ligne de défense. La formation du personnel sur les meilleures pratiques en matière de sécurité et sur les signes d'intrusion contribue à prévenir de futurs incidents.
La combinaison de ces mesures de remédiation offre une réponse complète à une compromission réseau. En bloquant immédiatement les adresses IP malveillantes, en maintenant les systèmes de détection à jour, en ajustant les politiques de sécurité, en surveillant en continu, et en sensibilisant le personnel, les organisations renforcent leur capacité à réagir rapidement face aux incidents, à minimiser les risques, et à prévenir de futures attaques. Cette approche proactive est essentielle pour assurer la sécurité et l'intégrité des infrastructures réseau.

Il est crucial de documenter toutes les actions entreprises pendant l'analyse forensique et la remédiation, et de prendre des mesures préventives pour renforcer la sécurité du réseau. En cas de besoin, consulter des experts en sécurité réseau peut être recommandé.

Audits

1. Configuration d'Audit pour Serveurs Windows :

Pour renforcer la sécurité des serveurs Windows, il est essentiel de mettre en place des configurations d'audit via la stratégie de sécurité locale ou les Objets de Stratégie de Groupe (GPO). Voici comment procéder :

1.1. Stratégie de sécurité locale :

Accédez à l'éditeur de la stratégie de sécurité locale en exécutant secpol.msc.
Sous "Stratégies locales", choisissez "Audit de la stratégie de sécurité".
Configurez l'audit des événements de connexion, d'authentification, de modification de fichiers et des stratégies de groupe.

1.2. GPO (Objets de Stratégie de Groupe) :

Ouvrez l'éditeur de gestion des objets de stratégie de groupe (gpedit.msc) sur le contrôleur de domaine.
Allez dans "Configuration de l'ordinateur" > "Paramètres de sécurité" > "Stratégies locales" > "Audit de la stratégie de sécurité".
Configurez les paramètres d'audit nécessaires.

1.3. Audit des événements :

Activez l'audit des événements de connexion, d'authentification, de modification de fichiers et des stratégies de groupe via les paramètres de sécurité.

1.4. Transfert sécurisé des journaux avec WEF :

Configurez le service Windows Event Forwarding (WEF) pour transférer les journaux de manière sécurisée vers un serveur centralisé.
Créez des abonnements WEF pour spécifier les événements à transférer.
En suivant ces étapes, vous assurez une surveillance efficace des événements critiques, renforçant ainsi la résilience et la sécurité de vos serveurs Windows. La configuration du transfert sécurisé des journaux avec WEF offre une gestion centralisée des journaux, facilitant la détection précoce des menaces et la réponse aux incidents.

2. Configuration d'Audit pour Serveurs Linux :

La mise en place d'une configuration d'audit efficace avec Auditd sur les serveurs Linux est essentielle pour garantir la sécurité. Voici les étapes à suivre :

2.1. Installation d'Auditd :

Installez le paquet Auditd sur le serveur Linux en utilisant la commande appropriée pour votre distribution (apt, yum, etc.).

2.2. Configuration des règles d'audit :

Éditez le fichier de configuration auditd.conf (généralement situé dans /etc/audit/) pour définir les règles d'audit.
Utilisez la commande auditctl pour ajouter des règles spécifiques, par exemple, pour auditer les connexions SSH ou les changements de permissions.

2.3. Audit des connexions SSH et des changements de permissions :

Utilisez des règles telles que "auditctl -w /etc/ssh/sshd_config -p wa -k sshd_config" pour auditer les changements dans le fichier de configuration SSH.
Ajoutez des règles pour surveiller les connexions SSH, les modifications de fichiers sensibles, etc.

2.4. Utilisation de rsyslog pour la transmission sécurisée des journaux :

Configurez rsyslog pour transmettre les journaux auditd de manière sécurisée vers un serveur centralisé.
Modifiez la configuration de rsyslog (/etc/rsyslog.conf) pour spécifier le serveur distant et le protocole de transmission sécurisé.

En suivant ces étapes, vous établirez une surveillance robuste des événements sur vos serveurs Linux, renforçant ainsi la sécurité et facilitant la détection précoce des incidents.

3. Méthode d'Audit d'Active Directory :

3.1. Activation de l'Audit des Modifications :

Accédez à l'interface d'administration d'Active Directory sur le contrôleur de domaine.
Activez l'audit des modifications en accédant aux propriétés de l'objet à auditer, tel qu'un utilisateur ou un groupe.
Dans l'onglet "Sécurité", activez les options d'audit pertinentes, telles que "Audit des modifications".

3.2. Utilisation de la Journalisation Avancée :

Exploitez la fonctionnalité de journalisation avancée pour obtenir des détails approfondis sur les modifications.
Configurez les paramètres de journalisation avancée pour enregistrer des informations telles que l'ancienne et la nouvelle valeur des attributs modifiés.

3.3. Analyse des Journaux d'Audit :

Accédez aux journaux d'audit d'Active Directory pour examiner les événements de modification.
Recherchez des informations cruciales telles que l'identifiant de l'objet modifié, l'heure de la modification et le type de modification effectuée.

3.4. Utilisation d'Outils d'Audit Externes :

Considérez l'utilisation d'outils d'audit externes offrant des fonctionnalités avancées, notamment la corrélation des événements et des alertes en temps réel.
En suivant méticuleusement cette méthodologie, les administrateurs d'Active Directory renforcent la surveillance des changements, améliorant ainsi la sécurité du système et facilitant la détection précoce d'éventuelles activités malveillantes.

4. Scénarios de Corrélation :

4.1. Linux :

Scénario d'attaque : Tentative d'intrusion par SSH.
Éléments de journalisation : Logs d'auditd enregistrant les tentatives de connexion SSH.
Corrélation : Corréler les logs d'auditd avec les logs de rsyslog pour identifier les adresses IP source suspectes.

4.2. Windows :

Scénario d'attaque : Attaque brute force sur un compte utilisateur.
Éléments de journalisation : Événements de sécurité de Windows enregistrant les tentatives de connexion infructueuses.
Corrélation : Corréler les événements de sécurité pour identifier des schémas de tentatives répétitives.

5. Actions Complémentaires d'Investigation :

5.1. Surveillance des journaux système :

Examiner régulièrement les journaux système pour détecter des erreurs, des avertissements ou des activités suspectes.

5.2. Analyse du trafic réseau :

Utiliser des outils de surveillance du trafic réseau pour détecter des anomalies ou des schémas de trafic inhabituels.

5.3. Analyse des logs d'application :

Examiner les logs des applications critiques pour détecter des activités inattendues ou des erreurs.

5.4. Surveillance des comptes privilégiés :

Mettre en place une surveillance spécifique des activités des comptes ayant des privilèges élevés.

5.5. Mise en place d'alertes :

Configurer des alertes pour être averti en temps réel en cas d'activité suspecte ou de violations de sécurité.

Cette configuration d'audit et les mesures complémentaires contribueront à renforcer la sécurité du système et à détecter rapidement les activités malveillantes.

6. Actions Complémentaires d'Investigation sur le Reste du SI :

6.1. Détections d'anomalies réseau avec IDS/IPS :

Mettez en œuvre des systèmes de détection d'intrusion (IDS) et de prévention d'intrusion (IPS) pour surveiller le trafic réseau.
Configurez des règles pour détecter des anomalies telles que des tentatives d'intrusion, des comportements inhabituels, ou des attaques par déni de service (DDoS).

6.2. Analyse des journaux des applications métier :

Examinez régulièrement les journaux des applications métier pour détecter des activités anormales ou des accès non autorisés.
Identifiez les modèles de comportement inattendus qui pourraient indiquer une violation de sécurité.

6.3. Surveillance des logs des serveurs de bases de données :

Surveillez les logs des serveurs de bases de données pour repérer des requêtes suspectes, des tentatives d'accès non autorisées, ou des modifications de données inattendues.
Configurez des alertes pour les activités potentiellement malveillantes.

6.4. Alertes sur les événements de sécurité au niveau des passerelles Internet :

Mettez en place des alertes pour les événements de sécurité au niveau des passerelles Internet, tels que les tentatives d'accès non autorisées, les attaques par force brute, ou les comportements de phishing.
Intégrez des outils de gestion des événements de sécurité (SIEM) pour centraliser et corréler les données.

Cette approche proactive renforce la surveillance du système d'information, améliore la détection des activités malveillantes, et contribue à la protection globale du SI.

Conclusion

Le projet GS21 a représenté une exploration approfondie des domaines cruciaux de l'analyse forensique et des audits de sécurité informatique, visant à renforcer la robustesse du système d'information. Les conclusions majeures des différentes tâches peuvent être résumées comme suit :

Tâche 1 : Analyse Forensique d'un Poste de Travail

Stockage des Traces de Compromission : Les traces de compromission résident dans divers composants, tels que le registre système, les fichiers journaux, les artefacts du navigateur, et la mémoire vive.

Extraction des Données : L'utilisation d'outils tels qu'EnCase, Forensic Toolkit (FTK), et des commandes telles que "grep" (Linux) ou "Get-EventLog" (Windows) garantit une collecte exhaustive des données.

Analyse des Données Extraites : L'analyse doit se concentrer sur la recherche d'indices de compromission, tels que des modifications non autorisées et des connexions suspectes.

Remédiation : Des mesures proactives, telles que la mise à jour régulière des logiciels, la sensibilisation des utilisateurs, et une configuration adéquate des politiques de sécurité, sont essentielles pour prévenir la récurrence du problème.

Tâche 2 : Analyse Forensique des Traces Réseaux

Stockage des Traces de Compromission : Les traces de compromission réseau résident dans les logs des pare-feu, les enregistrements DNS, et les fichiers journaux des routeurs.

Extraction des Données : Des outils tels que Wireshark et Tcpdump, ainsi que des commandes comme "netsh" (Windows) ou "tcpdump" (Linux), sont utilisés pour extraire les données.

Analyse des Données Extraites : L'analyse vise à détecter des schémas de trafic suspects, des activités non autorisées, et des anomalies de connexion.

Tâche 3 : Audits

Configuration d'Audit : La configuration des audits sur les serveurs Windows et Linux s'effectue à travers les stratégies de sécurité locales, les objets de stratégie de groupe (GPO), et l'utilisation d'outils tels que Windows Event Forwarding (WEF) pour le transfert sécurisé des journaux.

Audit d'Active Directory : L'activation de l'audit d'Active Directory via l'interface d'administration, en utilisant la journalisation avancée, permet d'enregistrer des détails approfondis sur les modifications.

Scénarios de Corrélation : Des scénarios spécifiques ont été fournis pour chaque catégorie de système, illustrant des exemples d'attaques, les éléments de journalisation pertinents, et les méthodes de corrélation.

Actions Complémentaires d'Investigation : Des recommandations ont été formulées pour renforcer la surveillance du système d'information, incluant la détection d'anomalies réseau, l'analyse des journaux d'applications métier, la surveillance des logs des serveurs de bases de données, et l'alerte sur les événements de sécurité au niveau des passerelles Internet.

En intégrant ces stratégies, le projet GS21 vise à augmenter la résilience du système d'information, à assurer une détection rapide des incidents, et à prévenir les attaques futures. Les recommandations sont adaptables en fonction des besoins spécifiques de l'organisation, offrant une défense proactive contre les menaces émergentes.