République Algérienne Démocratiques Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université 20 Aout 1955-Skikda

Faculté des sciences

Département d'informatique

Mémoire de fin d'étude en vue de l'évaluation du diplôme

Master en informatique

Option : Génie Logiciel des Applications Avancées

THEME

ETUDE DU FONCTIONNEMENT D'UN HONEYPOT AU SEIN DES RESEAUX

- RÉALISÉ PAR :
  - BOUSSOUF AHMED TAKI EDDINE
  - MERAISSIA ABDESSAMI
- ENCADRÉ PAR:
  - MR. TOUIL GHASSEN

Année Universitaire 2021/2022

REMERCIEMENTS

Tout d'abord, nous remercions et louons infiniment
Dieu Tout-Puissant pour nous avoir permis
d'accomplir ce travail facilement et d'achever le
cheminement académique avec succès.
Nous adressons également nos sincères remerciements
à tous les enseignants du département, qui nous ont aidés à finaliser ce mémoire
leurs conseils nous ont aidés, que Dieu les récompense
pour tout ce qu'il nous ont offert.
N'oublions pas non plus de remercier le personnel administratif
qui ont toujours veillé à créer une atmosphère propice
aux études.

Dédicace

A mes chers parents, pour tous leur amour, leur soutien et leurs prières tout au long mes études.
A toute ma famille pour leur soutien tout a long de mon parcours universitaire
Que ce travail soit accomplissement de vos vœux tant allégués, et le fuit de votre soutien infaillible,
Merci à tous ceux qu'y ont consacré leurs vies et leurs carrières à la science.
Nous espérons pouvoir apporter le plus durant notre carrière professionnelle

Dédicace

Je suis honoré de dédier le fruit de mes efforts et de ma diligence à ceux qui ont travaillé dur et avec diligence pour répondre à mes besoins, mon père et ma mère, que Dieu les protège.

À toute ma famille pour leur soutien tout au long de ma carrière d'étudiants, j'espère que ce travail sera fait avec votre confiance, et grâce à votre soutien continu, merci à tous ceux qui ont consacré leur temps à nous soutenir dans le domaine de la science.

Nous espérons pouvoir tirer le meilleur parti de notre carrière.

Boussouf Ahmed Taki Eddine

Sommaire

TABLE DE FIGURE

LISTE DES TABLEAUX

Introduction générale

Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur internet.

Par ailleurs, avec le nomadisme, consistant à permettre aux personnels de se connecter au système d'information à partir de n'importe quel endroit, les personnels sont amenés à « transporter » une partie du système d'information hors de l'infrastructure sécurisé de l'entreprise.

La menace (en anglais « thread ») représente le type d'action susceptible de nuire dans l'absolu, tandis que la vulnérabilité (en anglais « vulnérabilité », appelée parfois faille ou brèche)représente le niveau d'exposition face à la menace dans un contexte particulier. Enfin la contre- mesure est l'ensemble des actions mises en œuvre en prévention de la menace. Les contre-mesures à mettre en œuvre ne sont pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un ensemble de règles clairement définies.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'ennemi. Le but de ce dossier est ainsi de donner un aperçu des motivations éventuelles des pirates, de catégoriser ces derniers, et enfin de donner une idée de leur façon de procéder afin de mieux comprendre comment il est possible de limiter les risques d'intrusions Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger.

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

CHAPITRE I

LA SECURITE DES SYSTEMES INFORMATIQUES

1. Introduction

Dans cette partie du mémorandum, nous aborderons quelques concepts de base liés à la cyber sécurité et à la sécurité des réseaux, et nous essaierons de présenter des idées sur les attaques piratées qui menacent la sécurité du réseau et peuvent endommager l'ensemble du matériel. L'ordre des concepts que nous avons adopté aidera le lecteur à comprendre ce qui est requis et ce qui est nécessaire pour travailler dans la sécurité informatique et réseau.

2. Historique de la sécurité informatique

À la fin des années 1960 et au début des années 1970, on assiste à l'émergence du stockage numérique. De grands ordinateurs centraux occupant la superficie d'une pièce entière stockaient ces informations. L'accès à ces répertoires de stockage se faisait en se connectant directement à ces ordinateurs ou en accédant aux données depuis l'un des nombreux terminaux présents dans le bâtiment. Les adeptes de la première heure du stockage numérique ne rencontraient aucune difficulté pour protéger les informations sensibles. En effet, ils devaient être présents dans le bâtiment pour obtenir l'information.

Moins d'une décennie plus tard, alors que la quantité de données stockées augmentait, on s'est rendu compte que les données étaient précieuses et comprenaient de grandes quantités d'informations personnellement identifiables : données de carte de crédit, numéros d'informations sur les comptes bancaires, déclarations de revenus, détails personnels et informations démographiques sur populations importantes. Ce changement de perception a conduit à la marchandisation de l'information.
La diffusion rapide des données numériques a entraîné un risque sans précédent que les informations les plus sensibles tombent entre de mauvaises mains.
Alors que les données devenaient une marchandise très appréciée, la genèse de la cybercriminalité et l'approche moderne de la cyber sécurité ont émergé. Tout ce qui a de la valeur peut être acheté, vendu et, surtout, volé. **[01]**

3. Définition de la sécurité informatique

Sécurité informatique, est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher

l'utilisation non autorisée, le mauvais usage, la modification ou le détournement du système d'information. **[02]**

4. Objectif de la sécurité informatique

La sécurité des systèmes d'information vise les objectifs suivants (C.A.I.D.) :

4.1. Confidentialité des données

Seules les personnes autorisées à accéder aux informations qui leur sont affectées sont autorisées. **[03]**

4.2. Authenticité des identifiants

Les utilisateurs doivent les identifier à l'aide du mot de passe. La mention de confidentialité du nom d'identité publique indique que l'identifiant correct est enregistré. Cela permet de gérer les droits d'accès aux ressources concernées et de maintenir la confiance dans les relations d'échange. **[03]**

4.3. Intégrité des données

Les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. On distingue généralement deux types d'intégrité, dont les processus et méthodes peuvent varier :

4.3.1. L'intégrité physique

Elles reposent sur une protection de données unique et précise lors du stockage et de la récupération de données.

4.3.2. L'intégrité logique

L'intégrité logique est l'enregistrement des données en cours d'utilisation sur la base des données en haut. **[03]**

4.4. Disponibilité des données

Les services et ressources sont accessibles rapidement et régulièrement.

4.5. La traçabilité (ou « preuve »)

Garantir l'accès, la conservation et l'utilisation des éléments et des tentatives validées. **[03]**

4.6. La non-répudiation et l'imputation

Aucun utilisateur ne doit pouvoir contester les actions qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir revendiquer les actions d'un autre utilisateur. **[03]**

5. Relation entre attaque réseaux et sécurité informatique

La sécurité des ordinateurs a considérablement changé au cours de la dernière décennie. Autrefois limitée à l'application étendue du chiffrement sous forme d'algorithmes de chiffrement de disque et de protocoles d'authentification réseau, elle a été étendue à des périphériques plus sophistiqués et s'est répandue au grand public par le biais de cartes à puce. La sécurité est devenue une activité multidisciplinaire : le codage classique de la physique mathématique, les filigranes électroniques et métriques, l'ingénierie de réseau, différents systèmes de sécurité (cartes à puce, pare-feu, systèmes de détection d'intrusion, ateliers d'apiculture, biométrie) et infrastructures de sécurité. **[4]**

6. Types des attaques

6.1. Les attaques réseaux

L'objectif principal des attaques de réseau est de limiter la capacité du NIDS à détecter les attaques.

6.1.1. Technique de scan

Par les méthodes classiques de scan :

Exemple de scan furtif SYN implémenté par NMAP permettant de ne pas être détecté par les NIDS. A la réception d'un SYN/ACK qui signifie que le port est ouvert, il envoie un RST pour interrompre la connexion. Le but du scan SYN est de ne pas ouvrir une connexion complètement. **[5]**

6.1.2. IP Spoofing

Spoofing se divise en 3 catégories :

a) **L'e-mail spoofing**

Les e-mails contenant les virus de l'ordinateur sont envoyés depuis différentes adresses de messagerie. Le virus se propagera par mégarde à l'ouverture du courrier électronique.

b) **L'usurpation d'adresse IP**, **ou IP spoofing**

Cela signifie envoyer des paquets IP à partir de l'adresse IP source qui n'est pas attribuée à l'ordinateur qui envoie les paquets.

c) **Le smart-spoofing**

Il permet d'utiliser une application cliente quelconque grâce à l'usurpation d'une adresse IP. **[6]**

6.1.3. ARP Spoofing

Dans ce type d'attaque, les infiltrés envoient de faux paquets ARP pour le passage indécouvert entre deux systèmes de communication, pour intercepter ou traiter leur trafic. **[7]**

6.1.4. DNS Spoofing

Le DNS, acronyme de « Domain Name System », est un système mondial permettant de convertir les domaines en adresses IP. Le DNS fournit une adresse IP pour chaque nom de domaine. Ce processus est appelé « résolution de nom ». Pour que la résolution de nom puisse fonctionner, l'adresse IP d'un serveur DNS doit être enregistrée sur chaque terminal. Le terminal adresse ses requêtes DNS à ce serveur qui procède à la résolution de nom et renvoie une réponse. Si aucun serveur DNS n'est paramétré sur un terminal, le serveur du routeur local est automatiquement utilisé. **[7]**

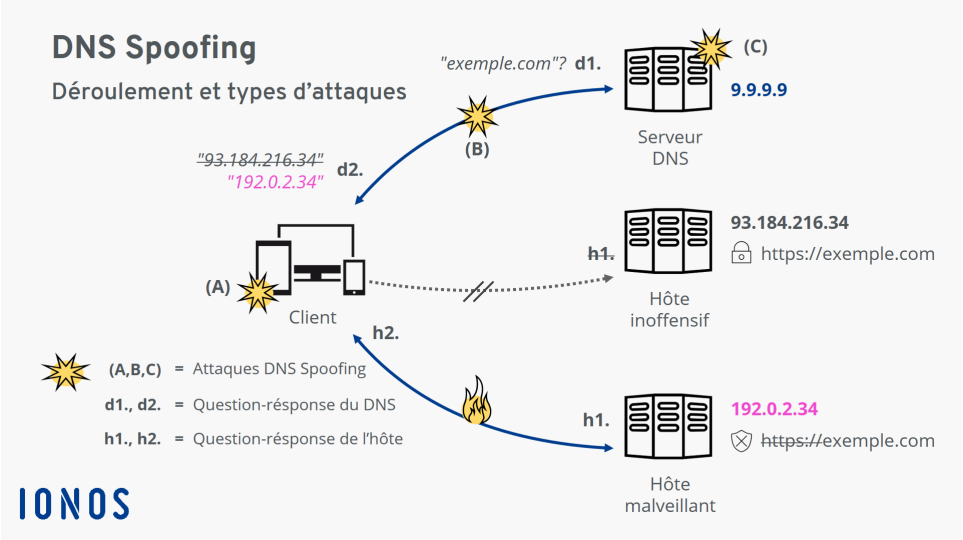

Figure 1.01 : Comment se déroule une attaque de DNS Spoofing.

6.1.5. Attaques de fragments

Le principe est de segmenter les paquets IP afin d'empêcher les réseaux NIDS de détecter les attaques lors desquelles les paquets seront regroupés à l'avenir. Il peut également envoyer des paquets IP illimités qui profiteraient de la faiblesse d'un

groupe IP spécifique (peut-être le son d'un IDS qui ferme tout trafic) pour désactiver le système. **[7]**

6.1.6. Détournement de session TCP (TCP session Hijacking)

Le but : rediriger un flux TCP afin de pouvoir outrepasser une protection par mot de passe. On connaît aujourd'hui quatre méthodes de conversion de session. C'est plus courant pour l'envoi d'un lien par e-mail, de sorte que la victime puisse cliquer dessus et que l'infiltré ait accès à l'ordinateur. Une autre technique appelée « Homo sapiens » (Homo sapiens in situ), dans laquelle l'attaquant intercepte le trafic pour soustraire les fichiers d'ouverture de session

Cela signifie que lorsque le contenu n'est pas chiffré, dès que la victime a saisi son mot de passe, l'agresseur peut naviguer avec l'utilisateur pour obtenir un nouveau mot de passe. La troisième méthode est le script ou le script. Les prédateurs utilisent cette méthode pour exécuter le code informatique sur l'ordinateur d'une victime. **[8]**

6.2. Les attaques applicatives

6.2.1. Problèmes des configurations

Il est rare que les administrateurs réseau configurent correctement le logiciel. Si elle n'est pas configurée, l'accès libre à certaines bases de données sensibles (fichiers de mots de passe ou utilisateurs) ou l'exécution de commandes malveillantes peut être autorisé. **[9]**

6.2.2. Les bogues

En raison d'un problème de code source, cela peut conduire à des déformations. Il n'est pas rare que le fonctionnement d'une machine soit interrompu par une erreur de programmation, mais nous ne devons rien y faire à moins que le développeur ne prenne des mesures correctives. **[15]**

6.2.3. Les buffer overflows

Les buffer overflows, ou plusieurs packagent sont une classe des bogues particulière. Une erreur de script rend ‘ Shelcode ‘ disponible à distance. Cette icône permettrait à quiconque involontairement pouvait exécuter les ordres à distance jusqu'à leur destruction. **[15]**

6.2.4. Les scripts

L'insuffisance de la programmation textuelle ou de l'utilisation des postes autorisés

peut conduire à une sécurité insuffisante. Chaque fois qu'un utilisateur entre dans la sortie générée sans vérifier l'ouverture de session de l'utilisateur ou le codage de l'application, il permet à l'administrateur d'envoyer un code incorrect à un autre utilisateur final. **[10]**

6.2.5. XSS (Cross-Site Scripting)

Les attaques Cross-Site Scripting (XSS) utilisent ces occasions pour transmettre des scripts malveillants vers des sites Web sécurisés qui finissent par être envoyés aux autres utilisateurs d'applications et deviennent ainsi victimes d'attaques. Les attaques XSS peuvent être classées en deux catégories : Stocker et réfléchies. **[10]**

6.2.6. Les injection SQL

L'injection SQL est une forme d'attaque électronique par laquelle un pirate utilise une pièce du SQL (le langage de chiffrement structurel) pour gérer une base de données et accéder des informations importantes. **[11]**

6.3. Le déni de service

Ce type de défaillance empêche l'exécution du logiciel et la réponse aux demandées. Cette technique est simple et suffisante pour utiliser un bogue connu pour lancer le programme de services. **[9]**

6.4. Les attaques des données

6.4.1. Virus

Un virus informatique est un logiciel auto-géré. Certains de ces symboles sont inoffensifs et d'autres contiennent des symboles malveillants. Après tout, les virus informatiques sont conçus pour s'étendre à d'autres ordinateurs en regardant les programmes légitimes appelés « hôtes », comme les virus organiques. Cela peut avoir des conséquences graves sur le fonctionnement de l'ordinateur infecté. Le virus se propage par tous les moyens d'échange de données numériques, comme les réseaux informatiques ou les dispositifs de stockage externes (clés USB, disques durs). **[02]**

Un virus informatique est composé de 3 parties.

- **Le mécanisme** de transmission est comment le virus se propage où il se propage. Un virus est généralement une « routine de recherche » qui localise de nouveaux fichiers ou lecteurs pouvant être infectés. **[12]**

• **Le déclencheur** spécifie l'événement ou la condition dans lesquels la charge utile doit être exécutée (comme à tout moment) dans un autre programme, afin que la capacité du disque dépasse un certain seuil ou un double clic pour ouvrir un fichier particulier. **[12]**

• **La charge** utile est le symbole qui atteint la cible du virus nuisible.

6.4.2. Vers

Le ver est un logiciel disponible sur le disque dur, contrairement aux virus qui se cachent sous forme de virus dans les fichiers, ou un code de fichiers exécutable dans le secteur d'amorçage. Cependant, très peu de ces données sont enregistrées sur le disque et sont donc stockées. Le ver peut être connecté directement au réseau par le biais d'un port ouvert, mais la méthode traditionnelle est d'être une pièce jointe. **[12]**

6.4.3. Cheval de Troie

Ce terme désigne actuellement tout logiciel qui s'auto-rétablit de manière frauduleuse (souvent par courrier électronique ou une page Web piégée) pour exécuter des actions hostiles sans que l'utilisateur en soit informé. Les fonctions malveillantes peuvent être des espions électroniques, des envois de courriers en masse et l'ouverture d'accès aux pirates.

6.4.4. Les bombes logiques

Une bombe logique est un logiciel qui persiste dans le système hôte jusqu'à ce qu'un moment, un événement ou une circonstance se produise et entraîne des effets dévastateurs dans le système hôte. **[15]**

6.4.5. Logiciel espion

Un logiciel espion (en anglais spyware) est un logiciel malveillant utilisé sur un autre ordinateur ou appareil mobile pour collecter et transmettre des informations sur l'environnement dans lequel il se trouve le plus souvent, à l'insu de l'utilisateur. **[15]**

6.4.6. Spam

Un courriel indésirable ou un e-mail est un e-mail qui n'est pas exigé principalement par le courriel. Ces envois sont généralement importants à des fins de publicité. **[15]**

7. Outils de sécurité

Nous présentons ci-dessous un ensemble non exhaustif d'outils de sécurité :

7.1. Pare-feu (firewall)

Un pare-feu qui définit le trafic ou le réseau de données à risque fonctionne lorsqu'un ordinateur est connecté à un réseau externe ou à Internet. Le principal avantage de ce système est de filtrer les éléments dangereux et fiables. **[11]** Il s'agit d'une porte de filtrage composée des interfaces réseau suivantes :

- Une interface pour le réseau à protéger (réseau interne).
- Une interface pour le réseau externe. **[16]**

Le tableau ci-dessous donne des exemples de règles de pare-feu :

Règle	Action	IP source	IP dest	Protocol	Port source	Por dest
1	**Allow**	**192.168.10.20**	**194.154.192.3**	**tcp**	**Any**	**25**
2	**Allow**	**any**	**192.168.10.3**	**tcp**	**Any**	**80**
3	**Allow**	**192.168.10.0/24**	**Any**	**tcp**	**Any**	**80**
4	**Deny**	**any**	**Any**	**any**	**Any**	**any**

Tableau 1.01 : Règles du pare-feu En général

Il existe 3 types de pare-feu :

- Les systèmes à filtrage de paquets sans état (firewall stateless)
- Les systèmes à filtrage de paquets avec état (firewall stateful)
- Les firewalls de type proxy

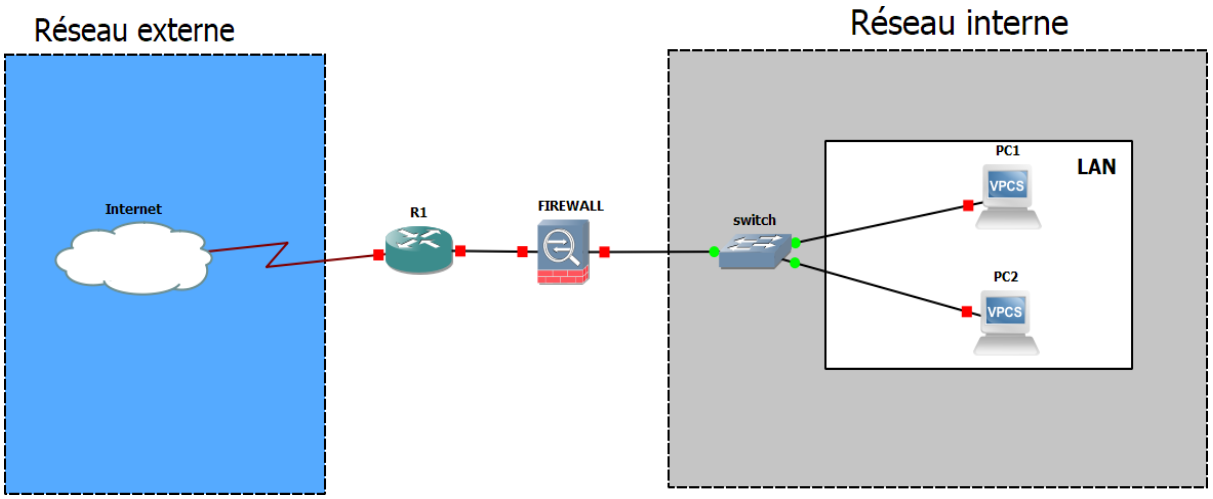

Figure 1.02 : Schéma de fonctionnement d'un pare-feu

7.2. Antivirus

La protection contre les virus analyse les fichiers internes (fichiers téléchargés ou courriers électroniques), la mémoire RAM, les périphériques de stockage comme les disques durs internes et externes, les disques USB et les cartes mémoire Flash. [12]

7.3. Réseau privé virtuel (VPN)

Un réseau privé virtuel (Virtual Privat Network) est un tunnel sécurisé au sein d'un réseau. Il permet l'échange sécurisé et anonyme d'informations en utilisant une adresse IP différente de l'adresse de votre ordinateur. **[12]** VPN consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. **[15]**

7.4. Cryptographies

Le chiffrement est habituellement une technique d'écriture, par laquelle un message chiffré est écrit avec des codes secrets ou des clés cryptographiques. Le cryptage est principalement utilisé pour protéger un message considéré comme confidentiel. **[6]**

8. Les systèmes de détection et de prévention d'intrusion IDS/IPS

Le système de prévention des intrusions (IPS) est une forme de sécurité réseau qui détecte et prévient les menaces identifiées. Les IPS surveillent en permanence votre

réseau à la recherche d'informations ou d'éventuels actes de sabotage. **[17]**

8.1. Les systèmes de détection d'intrusions (IDS)

Les premiers systèmes de détection d'intrusion (IDS) ont été développés par l'armée américaine mais plus tard, des projets open sources ont été lancés dont certains d'entre eux ont connu un grand succès dont : Snort ou Prelude. Ces logiciels sont capables de réagir dans le cas où ils détectent des flux de données suspects d'où leur nom. IDS s'agit d'un ensemble de composants logiciels et matériels dont la mission est de détecter et d'analyser toute tentative d'intrusion dans les politiques de sécurité d'un réseau. On dit aussi qu'il existe différentes approches de détection utilisée par les IDS : Statistique ; Motifs ; Règles ; États ; Heuristique. **[16]**

8.2. Les systèmes de détection d'intrusions réseaux (NIDS)

Le NIDS est un système d'information de base qui surveille le trafic réseau en faisant face aux paquets détectés d'une série de signatures ou de règles. En cas de violation des règles, l'indice de sécurité nationale enregistre l'incident comme une attaque. Les fonctions du NIDS sont divisées en trois taches distinctes : (La capture ; L'analyse des signatures ; Les alertes). **[16]**

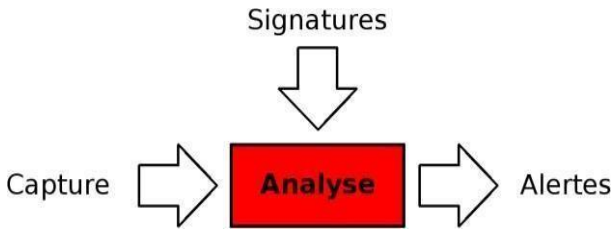

Figure 1.03 : Technique utilisée par un NIDS.

8.3. Host Basé Intrusion Détection System (HIDS)

Une machine peut être surveillée de différentes manières :

- Contrôle les activités de la machine : Nombre de listes de processus, d'utilisateur et de consommables...
- Contrôle des activités de l'utilisateur : Durée et heure des appels, commandes

d'utilisation, messages, logiciels possibles.

- Contrôle des activités malicieuses d'un vers, virus ou cheval de Troie.

Il existe un autre type d'HIDS qui est (kernel). Ils sont appelés KIDS (Kernel Intrusion Détection System).

L'avantage du KIDS c'est qu'il agit plus rapidement par rapport aux autres IDS. **[16]**

8.4. Les systèmes de détection d'intrusions hybrides

Et il collecte des informations des différents sons du réseau. Le terme « hybride » est issu des capacités à collecter des informations à partir des systèmes HIDS et NIDS. **[16]**

L'architecture simplifiée d'un IDS hybride est représentée par la figure 1.04 :

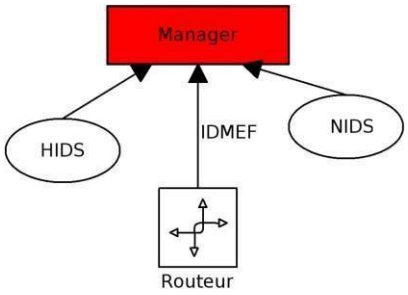

Figure 1.04 : Schéma simplifié d'un IDS hybride.

8.5. Les systèmes de prévention d'intrusions (IPS)

Il existe plusieurs stratégies de prévention des intrusions :

- Mémoire et opérations de protection de base : Surveille et tue les opérations qui semblent dangereuses.
- Session d'opposition/session de Sniping : Annulation d'une session TCP à l'aide de la commande TCP : RST. Il est utilisé dans le système d'intrusion du réseau.
- Ouverture de session : Si le système NIPS est placé comme routeur, il prévient le trafic. Sinon, ils envoient des messages à d'autres destinataires pour modifier leur liste d'accès. **[16]**

9. La segmentation

La partition d'un réseau est une approche architecturale divisant une grille en plusieurs parties ou sous-réseaux, pour chacun des filets qui agissent comme des petits en eux-mêmes. Permet aux administrateurs de contrôler les flux de trafic entre ces sous-réseaux en fonction de règles spécifiques. **[18]** Cette technique peut aussi être utilisée pour augmenter la sécurité d'un réseau. **[16]**

Il existe plusieurs façons de segmenter un réseau :

- La segmentation physique.
- La segmentation par VLANs.
- La segmentation en utilisant un DMZ.
- La segmentation en fonction des services .

9.1. La segmentation physique

La séparation physique des sous-réseaux est peut-être la méthode la plus sécurisée, mais c'est aussi la plus coûteuse en termes de cartes réseau, d'infrastructure mobile supplémentaire et de gestion. **[16]**

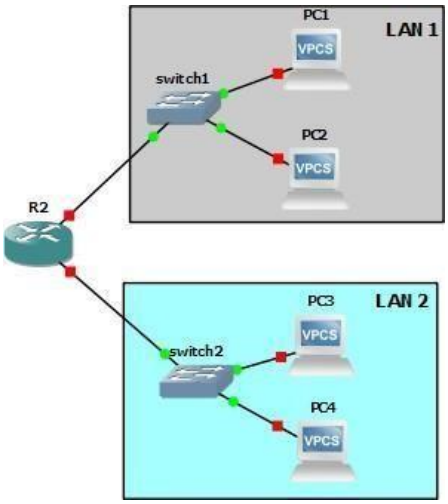

Figure 1.05 : Exemple de segmentation physique

9.2. La segmentation par VLANs

Un VLAN (Virtual Local Area Network ou Réseau Local Virtuel) est un réseau local qui rassemble un groupe d'appareils de manière logique plutôt que physique. C'est un

appareil de couche 2 (liaison de données) qui fait ce que font les VPN au niveau de la couche 3 (le réseau). Le trafic au sein d'un VLAN ne peut pas en croiser un autre sans passer par un routeur. Cela permet de diviser le réseau sans infrastructures supplémentaires. Cependant, la configuration des commutateurs (switchs) qui relient les différents segments est d'une importance primordiale car la sécurité d'un VLAN dépend en partie de l'allocation des ports pour ces commutateurs. **[16]**

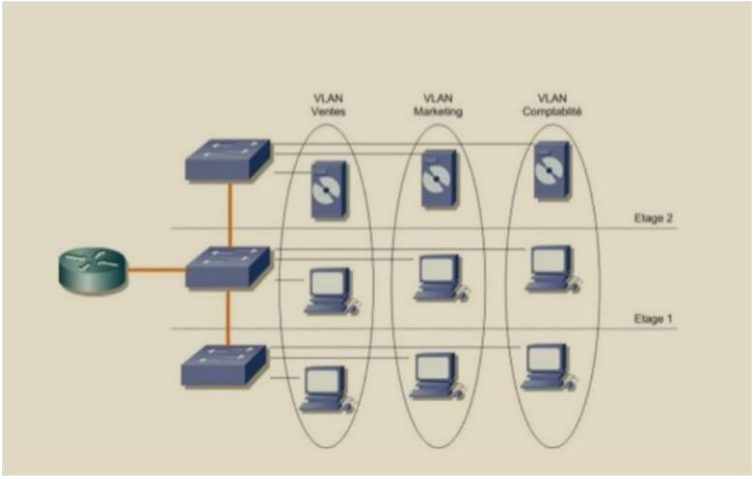

Figure 1.06 : Exemple de segmentation par VLAN

9.3. La segmentation en utilisant une DMZ

La DMZ définit un tampon réseau entre elle et l'Internet externe en général. Il s'agit d'un réseau intermédiaire protégé à la fois contre le réseau externe et interne. L'objectif est de pouvoir mutualiser les ressources du réseau qui fournissent des services accessibles aussi bien en interne qu'en externe pour éviter toute connexion directe au réseau. **[16]**

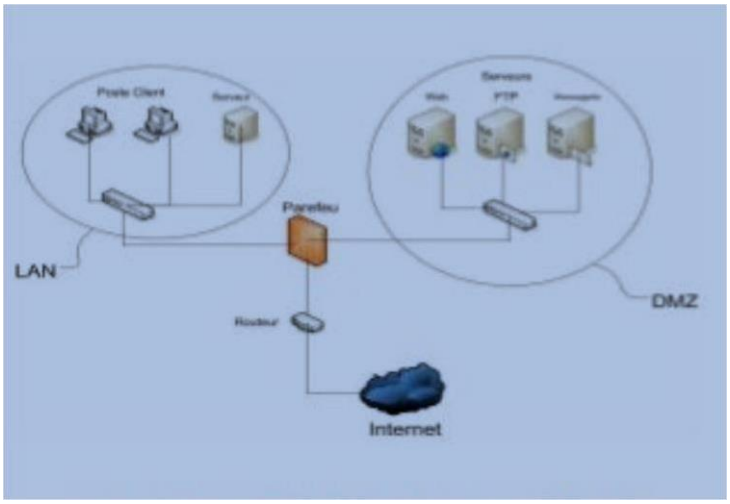

Figure 1.07 : Schéma simplifié d'un réseau segmenté avec un DMZ

9.4. Segmentation en fonction des services

Une autre approche de la segmentation consiste à examiner les services offerts par différentes ressources et à segmenter le réseau en conséquence. Puis chaque partie est sélectionnée en fonction du service rendu par ses ressources. Cette approche permet un contrôle très étroit entre différents segments de réseau. Cela nécessite également des dispositifs de sécurité supplémentaires. **[16]**

10. Conclusion

Au final, la sécurité informatique est un vaste domaine, et les attaques sont d'une diversité accrue. Pour faire face à ces attaques il existe aussi plusieurs techniques et technologies, on a essayé de les voir brièvement dans ce chapitre, alors qu'on va se consacrer à un seul type, et qui est justement le sujet de notre étude.

CHAPITRE II

LES HONEYPOTS

1. Introduction

Pour ce chapitre, nous avons décidé de vous présenter le pot de miel, qui est l'une des solutions pour protéger les réseaux des attaques de pirates, car nous aborderons en détail leurs types puis leurs classifications jusqu'à atteindre leur emplacement depuis un réseau, Tout ça pour comprendre comment gérer un honeypot.

2. Etat de l'art

2.1. Historique

Les « Honeypots » n'ont fait leur apparition au sein de l'entreprise qu'aux alentours de 2002, même si le concept daterait lui plutôt des années 90, avec un hacker intercepté par Bill Cheswick « Un cracker, croyant avoir découvert le fameux trou de sécurité utilisant la commande DEBUG d'envoyer un mail sur notre passerelle Internet a tenté d'obtenir une copie de notre fichier password. Je l'ai lui ai envoyé. » Ainsi commence l'histoire des « pots de miel », Bill Cheswick a laissé travailler ce pirate pendant plusieurs mois, apprenant ainsi ses techniques pour mieux les combattre. Les « pots de miel » profitent désormais de la mise en commun des données pour renseigner un maximum d'informations, on peut par exemple trouver sur le projet « pot de miel » une page web avec la liste des adresses IP de robots de spammeurs de site web. **[13]**

2.2. Un tour du développement des honeypots

Essayons de faire un tour du développement des honeypots depuis leur apparition pour mieux comprendre notre thème de recherche

- Lorsque le projet Honeynet s'est formé en 1999 et a commencé à rechercher des attaques contre les réseaux informatiques, on savait très peu de choses sur nos ennemis, leurs motivations ou les outils et techniques qu'ils utilisaient. Au cours des premières années de la recherche sur les réseaux de miel, nous avons développé une gamme d'outils de pots de miel pour nous aider à collecter et à analyser les données provenant d'attaques contre des systèmes réels déployés dans la nature. Bien que courante maintenant, à l'époque, c'était une activité

assez nouvelle et régulièrement présentée dans des présentations telles que BlackHat 2002 et BlackHat 2003. L'un des premiers défis auxquels nous avons été confrontés était d'équilibrer les compromis entre les données de haute qualité qui pourraient potentiellement être obtenues grâce à une instrumentation de plus en plus complexe de systèmes informatiques réels, par rapport au risque de dommages potentiels et de responsabilité qui pourraient éventuellement être causés par des attaquants abusant d'un pot de miel compromis. Systèmes. Cela a toujours été une préoccupation majeure pour les opérateurs de pots de miel, et le reste aujourd'hui.

- Une solution potentielle à ce problème était le développement de pots de miel émulés, qui tentaient d'imiter divers services en réseau sans exposer réellement un système d'exploitation complet à l'attaquant. Ces pots de miel émulés à « faible interaction » pourraient être conçus pour répondre au moins de manière basique aux entrées réseaux potentiellement malveillants, permettant aux attaques d'être enregistrées tout en réduisant considérablement les risques, les efforts, le déploiement et la complexité de gestion associée.

  Les pots de miel à faible interaction ont commencé comme des outils d'émulation de réseau relativement simples tels que Honeyd (2003), qui, une fois déployés, attendaient les connexions réseau entrantes et n'offraient qu'une émulation de service limitée. Mais au fil du temps, ces outils ont évolué vers des solutions plus performantes, telles que Nepenthes pour la collecte de logiciels malveillants sur le réseau Windows, et éventuellement Dionaea. Des pots de miel spéciaux à faible interaction ont également été créés, tels que Glastopf pour les attaques Web et Conpot pour les systèmes SCADA/ICS, ou Thug en tant que pot de miel client à faible interaction conçu pour explorer et évaluer activement les sites Web potentiellement malveillants.

Bien que les pots de miel complets du système d'exploitation ("haute interaction") fournissaient toujours des données de la plus haute qualité et étaient toujours essentiels pour observer les attaquants humains qualifiés, les

pots de miel à faible interaction se sont définitivement avérés utiles dans certains scénarios de déploiement : des déploiements à faible coût à grande échelle ; pour minimiser l'effort de gestion et réduire la surface d'attaque potentielle, le risque d'exploitation et la responsabilité ; détecter l'analyse de masse du réseau ou les hôtes internes compromis ; suivi de la propagation des logiciels malveillants sur le réseau (vers) ; étudier les menaces à l'échelle d'Internet au niveau macro ou fournir des alertes en temps réel pour les attaques hautement automatisées avec peu d'intervention humaine initiale (force brute, scanners, etc.). Une ancienne présentation de Blackhat Federal 2003 donne toujours un assez bon aperçu des principales différences entre les pots de miel à faible et à forte interaction et leurs problèmes associés. Bien que les technologies et les attaquants aient changé, les concepts restent les mêmes.

Étant donné que cette recherche innovait et que les outils étaient tous open source, nos développeurs étaient régulièrement confrontés à des efforts pour identifier, détecter, attaquer ou contourner nos outils de réseau de miel. Nous nous attendions toujours à ce que cela vienne de la communauté black hat, mais parfois nous avons également été surpris (et mis au défi) par des recherches publiées par des universitaires ou des chercheurs en sécurité white hat. Au fil des ans, il y a eu de nombreux cycles réguliers dans la course aux armements entre les attaquants et les défenseurs du système. Par exemple :

- La détection et l'exploitation des pots de miel étaient des fonctionnalités régulières du magazine Phrack en 2003 (par exemple p62-0x07.txt et p63-0x09.txt), les attaquants cherchant des moyens de détecter ou de vaincre les pots de miel.
- BlackHat 2004 – NoSEBrEak – Defeating Honeynets a présenté des étudiants allemands enthousiastes montrant comment potentiellement détecter et vaincre le composant rootkit Sebek de notre pot de miel à haute interaction de la génération actuelle. Les auteurs ont ensuite rejoint le projet Honeynet, aidé à améliorer les technologies du réseau de miel (avec l'aide de collègues français) et ont finalement écrit l'un des principaux livres sur les pots de miel. Le projet GSOC 2020 et par rapport à la crise mondiale du

covid_19 a essayé de faire parvenir du nouveau en essayant de transformer n'importe quel appareil Android en un honeypot.

Host âge est un pot de miel mobile à faible interaction pour les appareils Android. L'idée est d'avoir un pot de miel rapide et mobile qui émule la plupart des protocoles modernes. Otage est déjà mature, et ce projet va se concentrer sur son amélioration (par exemple, prise en charge du protocole IoT, visualisations, fonctionnalités de sécurité, etc.).

2.3. Pourquoi avons-nous besoin d'un Honeypot ?

Honeypot a la capacité de générer des informations précieuses qui ne peuvent être générées par aucun type de système de prévention ou de détection d'intrusion disponible sur le marché. Les administrateurs réseau peuvent enregistrer des alertes en fonction des informations qu'ils obtiennent, et les administrateurs peuvent se méfier des attaques potentielles des attaquants. Par conséquent, les administrateurs peuvent avoir beaucoup de temps jusqu'à ce que le mécanisme de défense du système soit renforcé.

2.4. Type des « Honeypots »

Il existe deux grands types d'utilisation des « honeypots » :

2.4.1. « Honeypots » de production

Les entreprises peuvent les utiliser pour détourner les pirates de leurs réseaux utiles, et créer une version facilement accessible en utilisant de fausses données. **[13]** Un « pot de miel » de production est utilisé pour sécuriser un réseau opérationnel. Il détourne les attaques dirigées vers les différents services de production du système, en les attirant vers eux, ce qui permet de réduire les risques, en renforçant la sécurité que d'autres mécanismes de sécurité tels que les pares-feux. Les « pots de miel » de production imitent essentiellement certains services et parfois des systèmes d'exploitation pour attirer les attaquants. **[16]**

2.4.2. « Honeypots » de recherche

Les pots de miel peuvent également être utilisée dans le contexte de la recherche. Le serveur est alors envoyé aux pirates pour étudier les différentes techniques utilisées.

[13] Ces des outils complexes qui visent à recueillir de nombreuses informations sur les attaquants et leurs méthodes. Ils ne sont pas directement chargés de défendre l'entreprise, mais plutôt de découvrir les risques auxquels l'entreprise peut et devra faire face à l'avenir. **[16]**

3. Définition

3.1. Définition 01

Un « Honeypot » est une méthode de défense active consistant à attirer, sur des ressources (serveur, programme, service), des adversaires déclarés ou potentiels afin de les identifierait éventuellement les neutraliser. **[02]**

3.2. Définition 02

Un « Honeypot » est une ressource pour l'ingénierie de sécurité et a pour but de s'approprier la personnalité d'une cible réelle pour être examinée, attaquée ou pénétrée. Pour faire simple, les « pots de miel » sont des machines de production conçues pour attirer les pirates. Ceux-ci, convaincus qu'ils ont infiltré le réseau, ont vu toute leur activité surveillée.

4. Honeypots et sécurité

En décompose la sécurité en trois domaines distincts : la prévention, la détection et la réaction. « 'Bruce Schneier' expert en cryptographie ».

4.1. La prévention d'intrusion

N'est pas le domaine privilégié des pièges d'attraction, dans cette zone ils ne permettent que la collecte d'informations pour prévenir l'intrus s'il tente de s'infiltrer.

4.2. Côté détection

Grand intérêt, IDS a plus de mal à détecter les infiltrés quand ils voient beaucoup de trafic, et les infiltrés ont une technologie connue pour maintenir IDS occupé en leur envoyant beaucoup d'alertes, alors IDS a plus de mal à détecter les véritables demandes d'attaques, donc elle peut créer de fausses alertes et permettre le passage des attaques. En revanche, en ce qui concerne le lieu d'attraction, le trafic entrant et sortant est de nature suspecte, puisqu'il n'existe aucun service de production, l'analyse est donc beaucoup plus simple et la IDS est moins sensible à l'augmentation du trafic.

4.3. La Réaction

C'est le champ « honeypots » caractéristique, où il y a peu d'intérêt à détecter les failles du système si nous n'y réagissons pas. **[13]**

5. Classification des Honeypots

5.1. Basé sur le niveau d'interaction

5.1.1. Pot De Miel À Faible Interaction

Il se caractérise par une interaction minimale avec le pirate et simule certains faux services. Il n'y a pas de systèmes d'exploitation ou de services réels en cours d'exécution sur eux, ce ne sont que des simulations exécutées au-dessus de la couche du système d'exploitation. L'interaction de l'attaquant avec ce système est limitée et limitée dans le temps, de sorte que l'attaquant ne peut pas interférer avec le système. Les meilleurs exemples de ce type d'attraction sont « Honeyd », Glastopf et « KFSensor ». **[14]**

C'est simplement un programme qui imite les services d'un vrai système grâce à l'installation, par exemple, des sockets d'écoute sur chaque port de service, et ces sockets enregistrent seulement les différents paquets qu'ils reçoivent comme illustré dans la figure :

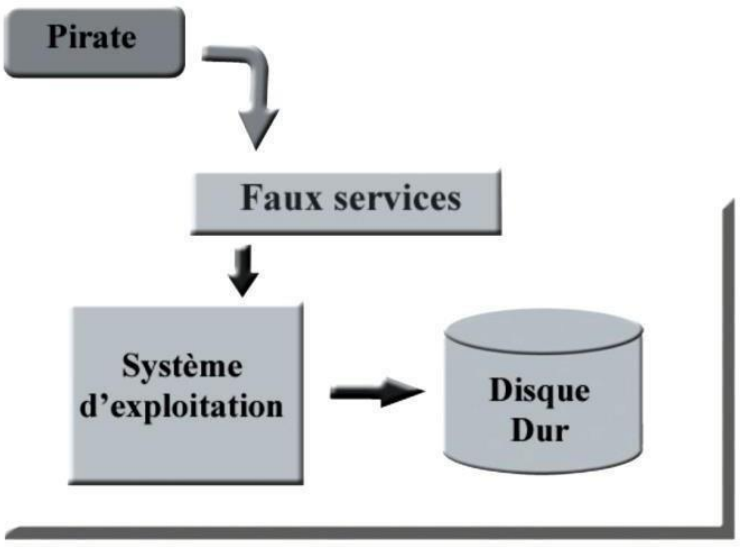

Figure 2.01 : Fonctionnement d'un « pot de miel » à faible interaction.

L'objectif est de détecter les tentatives d'ouverture de session non autorisée. C'est l'espèce la plus utilisée dans le pot de miel de production.

a) Avantages

- La mise en place est très simple.
- La gestion complexe des journaux système est éliminée.
- Maintenir la sécurité du système, mais uniquement s'il est correctement configuré.

b) Inconvénients

- Facilement détecté par les attaquants.
- Peu d'informations sont obtenues sur l'attaquant.

5.1.2. Pot De Miel À Interaction Moyenne

Un « pot de miel » a moyenne interaction est une position de type pseudo-virtuelle qui offrant une meilleure imitation des services du système par rapport à la simulation offerte « pot de miel » à faible interaction, ce qui ajoute la capacité à renvoyer des réponses aux prédateurs, et ces réactions sont généralement fausses. **[16]**

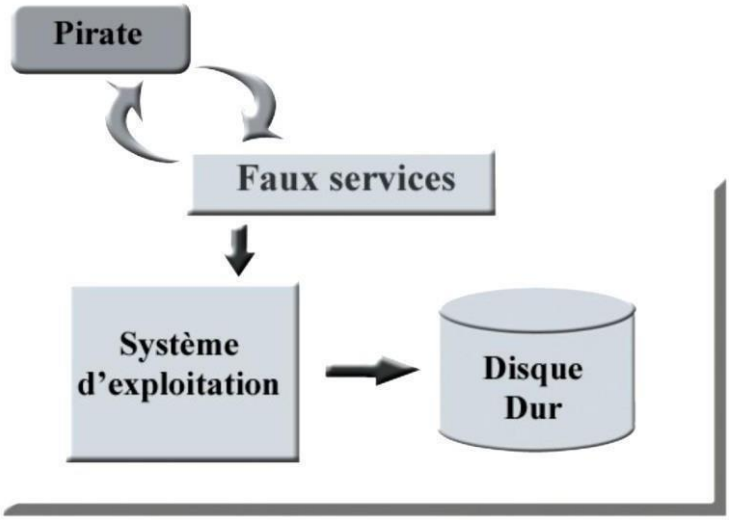

Figure 2.02 : Fonctionnement d'un « pot de miel » à moyenne interaction

a) Avantages

- La gestion des enregistrements du système est facile par rapport aux pots de miel à forte interaction et quelque peu difficile par rapport aux attractions à faible engagement.
- Il fournit des informations plus intéressantes pour l'analyse, compte tenu de la variété des attaques proposées aux pirates.

b) Inconvénients

- Il est très difficile à mettre en œuvre en termes de développement.
- Connaissance complète des protocoles de chaque faux service pour prévenir toute faille de sécurité.
- La sécurité du système est difficile à maîtriser lorsque la complexité de la position de traction augmente.

5.1.3. Pot De Miel À Interaction Élevée

High Interaction « pot de miel » alimente des systèmes et des services réels et fournit aux attaquants des systèmes d'exploitation complets, des applications entièrement fonctionnelles et des services avec lesquels interagir. Cela nécessite un niveau de connaissances plus élevé pour le déploiement et la maintenance. Il capture d'énormes quantités d'informations, Il est donc utilisé spécifiquement à des fins de recherche. **[14]**

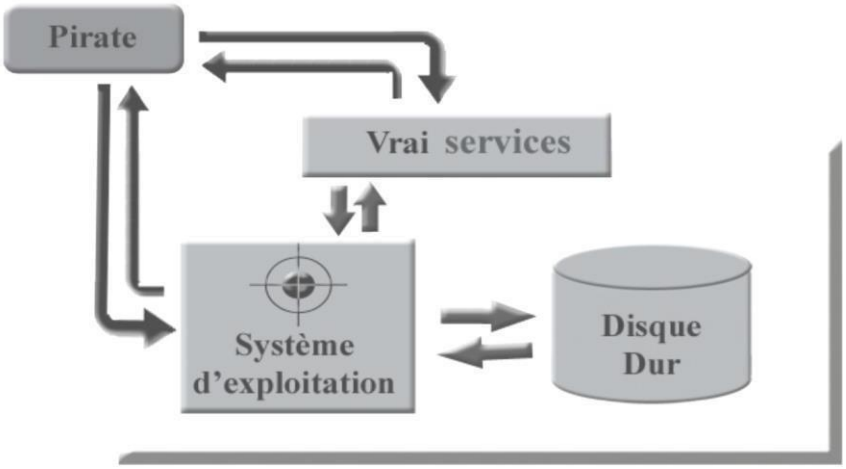

Figure 2.03 : Fonctionnement d'un « pot de miel » à forte interaction

Le but est alors de contrôler les actions et les gestes du pirate sans se faire détecter.

a) Avantages

- Très difficile à détecter par les pirates.
- Fournit beaucoup d'informations sur les activités du pirate.

b) Inconvénients

- Il présente de grands risques pour le système hôte, car le pirate pénètre complètement librement dans le système réel, ce qui peut entraîner une réinstallation périodique du système.
- La réactivité du monitoring est un facteur de complexité important.
- La gestion des logs est très compliquée. **[16]**

5.2. Fondé sur l'adaptabilité

5.2.1. Pot De Miel Statique

Le nombre et la position du pot de miel sont constants. Les pots de miel statiques ont du mal à apprendre de manière dynamique dans des environnements réseau en constante évolution. De plus, les positions " pot de miel " fixes ne peuvent pas cartographier et répondre intelligemment à notre environnement. **[14]**

5.2.2. Pot de miel dynamique

Un pot de miel dynamique est un pot de miel autonome qui est capable de s'adapter dans un environnement de réseau dynamique et en constante évolution. Nous pouvons simplement le brancher et le jouer sans avoir à le tenir à jour. Il devrait être capable d'identifier automatiquement les informations du réseau de production et de publier des pots de miel en fonction de ces informations. **[14]**

5.3. Basé sur le déploiement matériel

5.3.1. Pot de miel physique

Ce type pot de miel est effectué sur un périphérique unique avec un système d'exploitation et des services réels.

Lorsque la position de la cible est connectée à l'et est accessible par une adresse IP unique. Les Pots de miel physiques sont toujours liés à l'idée de sites d'attraction à forte interaction et sont moins fréquentes dans les scénarios du monde réel en raison de la visibilité limitée d'une adresse IP unique et du coût élevé de la maintenance d'une ferme de miel physique. **[14]**

5.3.2. Pot de miel virtuel

Il est généralement appliqué sur machine. L'hôte qui a plusieurs ventes de miel par défaut. La surveillance du protocole Internet (IP) à grande échelle et la taille de la zone d'adressage IP sont les plus populaires. **[14]**

- **Avantages**

  - Un seul système physique peut simuler de nombreux pots de miel virtuelles.
  - Ils peuvent émuler de nombreux systèmes d'exploitation et simuler différentes adresses IP.
  - Un aimant virtuel nécessite beaucoup moins de ressources informatiques et réseau qu'un aimant physique.
  - Il offre également une plus grande flexibilité dans l'émulation de différents systèmes d'exploitation.

6. Architecture des « pot de miel »

6.1. Au niveau système

Il existe deux possibilités d'architecture des « pots de miel » au niveau du système

6.1.1. Honeypot purement virtuel

Utilisation d'un seul système de « honeypot » sur un seul appareil physique.

a) Avantage

- Une administration simplifiée.

b) Inconvénients

- Si plusieurs « honeypots » alors plusieurs machines physiques.
- Contraintes de monitoring système sans se faire repérer par le pirate.
- Contraintes de réinstallation du système, fréquentes pour un « honeypot ».

6.1.2. Honeypot virtuel hybride

Utilisation d'un système « honeypot » sur une machine virtuelle permettant d'avoir plusieurs « honeypots » sur une même machine physique : **[13]**

a) Avantages

- Sécurité de la machine virtuelle.
- Économie de machines physiques.
- Possibilité de monitoring en temps réel des disques virtuels.

- Facilité de réinstallation par sauvegarde des disques virtuels.
- Le système hébergeant les systèmes virtuels est rendu invisible pour le pirate.

b) Inconvénients

- Charge importante du système hébergeant les machines virtuelles.
- Le choix du système virtuel est restreint à ceux qui sont compatibles.

6.2. Au niveau réseau

Il existe plusieurs solutions d'architecture du « pot de miel » en fonction du type de « honeypot », de l'environnement réseau de l'utilisateur et de ce qu'il désire collecter comme information.

6.3. La mise en place des Pots de miel

La mise en place d'un « pot de miel » nécessite une infrastructure lourde qui s'appuie sur un ou plusieurs serveurs. Où nous devons nous assurer de deux choses principales lors de la mise en place d'une honeypot. **[13]**

a) Le contrôle des données

S'assurer que le pirate n'utilise pas le « pot de miel » pour scanner ou attaquer le reste de l'infrastructure ou d'autres entités de l'utilisateur.

b) La capture des données

Enregistrez toutes les actions et gestes du pirate sans les soupçonner afin qu'il puisse les étudier et ainsi connaître ses outils et méthodes.

- Lors de la publication d'emplacements de « honeypot ». Nous dépendons savoir sile système est destiné à surveiller les attaques externes ou internes. Il y a trois fonctions possibles pour installer des « honeypot ». **[16]**

  - Devant un pare-feu (ou "firewall").
  - Dans une zone démilitarisée (DMZ).
  - Derrière le pare-feu.

6.3.1. Devant un pare-feu (ou "firewall")

Un « honeypot » connecté à un pare-feu (firewall) transparent permet la conception de ce qu'est un « honeynet » simple. **[13]** Cette situation n'augmente pas le risque de pénétration du réseau interne. **[16]**

a) Avantages

- Avec cette architecture il est possible de contrôler les agissements d'un éventuel pirate sur le réseau.
- Il n'y a aucun changement à faire au niveau des règles de filtrages du pare-feu qui protège le réseau interne.
- Cette localisation n'introduit pas de nouveaux risques pour les machines du réseau interne.

b) Inconvénient

- Ne permet pas de détecter les attaques menées depuis l'intérieur du réseau puisque généralement les flux sortant sont bloqués par le pare-feu.

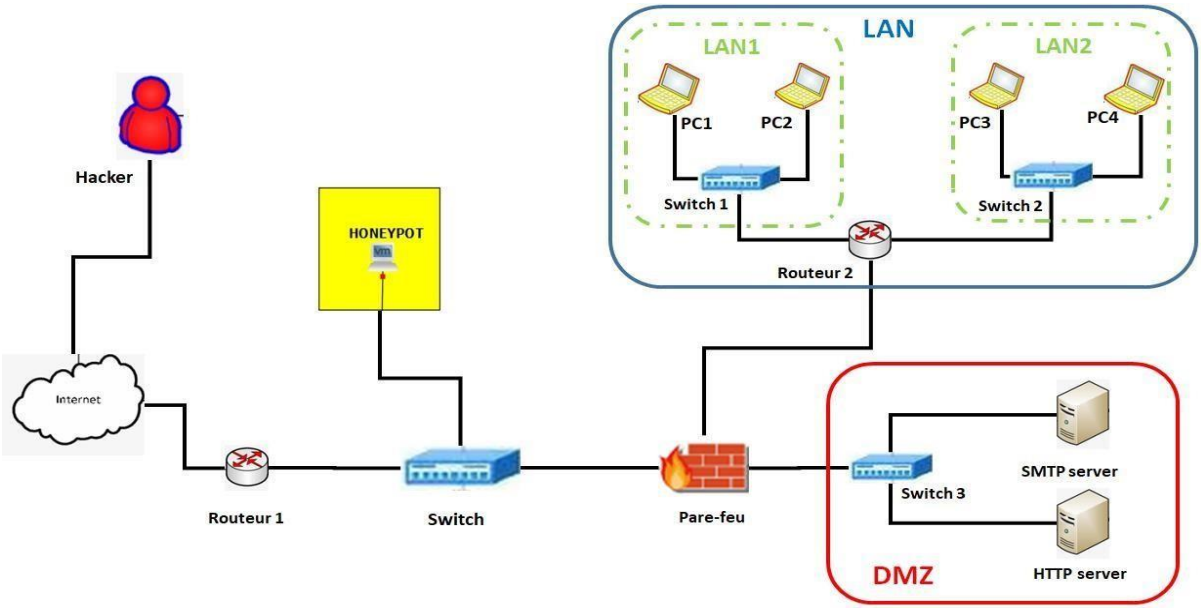

Figure 2.04 : « Honeypot » installé devant le pare-feu

6.3.2. Dans une zone démilitarisée (DMZ)

Considérons un environnement de production simplifié composé des 3 serveurs.

- Elle consiste à placer un « Honeypot » dans une zone démilitarisée
- Le rôle de la DMZ est que le pirate ne peut pas rebondir vers Internet, vers un appareil sensible de la passerelle d'accès, ou vers le réseau interne.
- Un système de détection d'intrusion permet de monitorer le réseau et d'espionner le pirate.
- Le « serveur de logs » empêchera le pirate de modifier les logs.

- La surveillance doit être constante lorsque le système vulnérable est accessible depuis Internet.

➢ **Avantages**

- Permet de pallier le défaut de la première position.
- Cette dernière sera configurée de façon à ce qu'elle ne soit pas accessible par le pirate, ne soit en ne lui donnant pas accès au réseau, soit en la masquant grâce au firewall le plus proche.

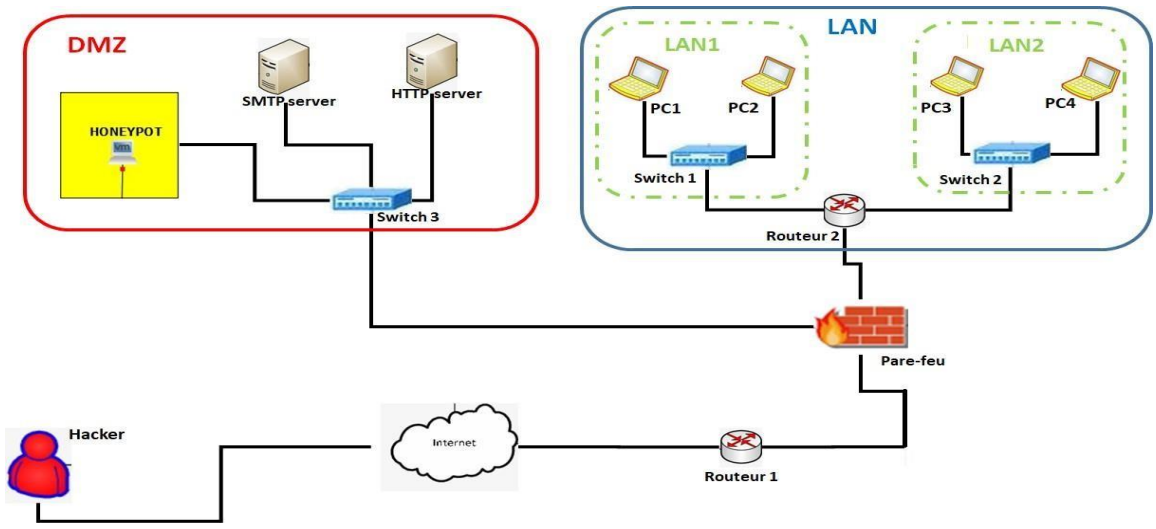

Figure 2.05 : « Honeypot » installé dans une DMZ

6.3.2.1.Première stratégie

a) Avantages

- Intégration facile du « Honeypot » au niveau du Firewall.
- Permet au « Honeypot » d'implémenter tous les services souhaités.
- Le risque de faux positifs est nul.
- Le trafic qui arrive sur le « Honeypot » est forcément suspect Néanmoins.

b) Inconvénient

- Utiliser une (ou plusieurs) adresse(s) publique(s) dédiée(s).

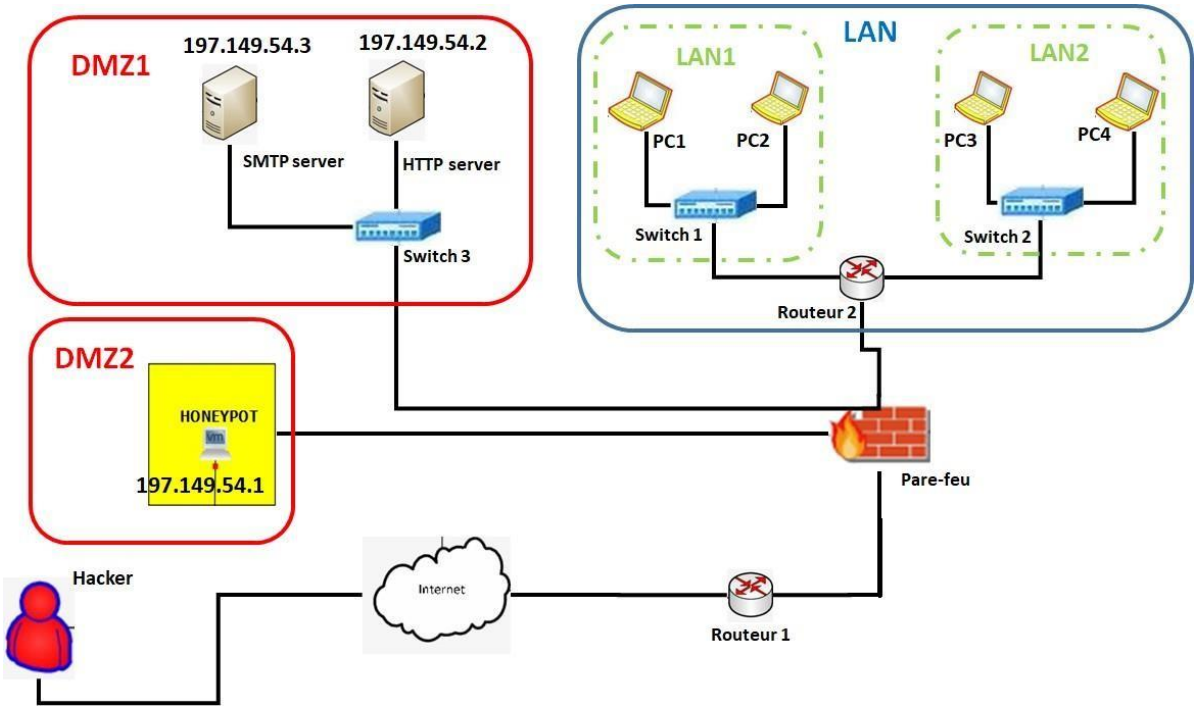

Figure 2.06 : « Honeypot » installé dans une DMZ dédiée – adressage publique

6.3.2.2. Deuxième stratégie

a) Avantages

- Cette stratégie partage les mêmes avantages avec la première, tout en évitant le gaspillage d'adresse(s) IP.

b) Inconvénients

- Le « Honeypot » n'est utilisé que pour certains types de services.
- Intégration plus compliquée.

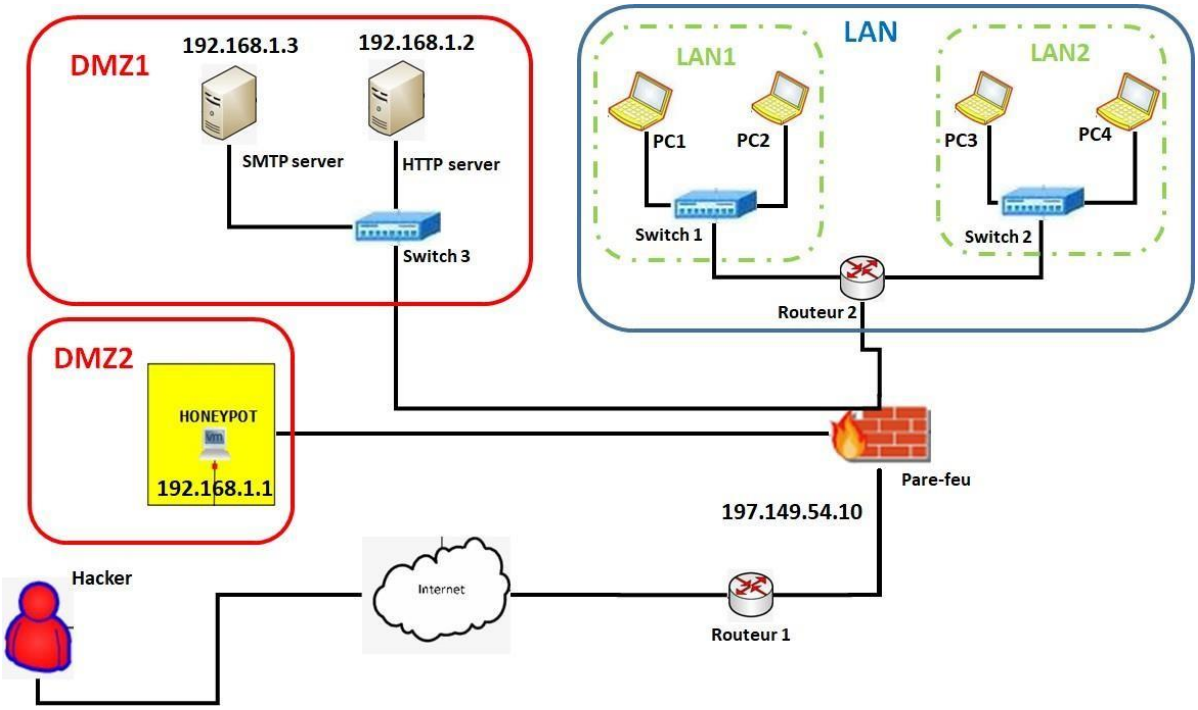

Figure 2.07 : « Honeypot » installé dans une DMZ dédiée – adressage privé

Une autre alternative à cette stratégie est de placer un IDS et de rediriger les flux « Suspects » par IDS vers le « Honeypot » via la règle NAT sur le pare-feu. Une adresse IP publique est attribuée à l'interface externe du pare-feu / IDS. **[16]**

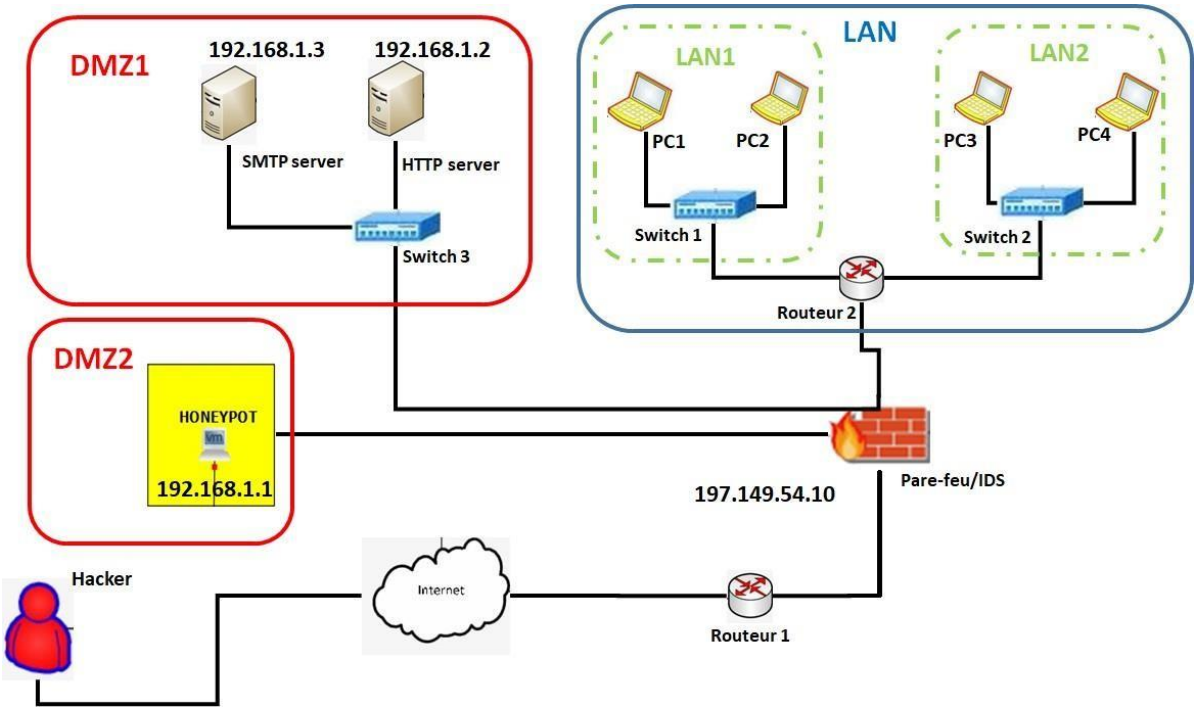

Figure 2.08 : « Honeypot » installé dans une DMZ dédiée derrière un IDS

6.3.3. Derrière le pare-feu

La position du pot de miel se trouve derrière le pare-feu dans le réseau interne. Si un système Honeypot est utilisé pour détecter des attaques externes, cela peut entraîner un risque accru de vulnérabilités car une fois compromis, un attaquant peut utiliser le Honeypot pour lancer d'autres attaques sur le réseau interne. **[16]**

a) Avantages

Un pare-feu est qu'il peut détecter les attaques des utilisateurs au sein de l'organisation sur les services internes ou détecter une mauvaise configuration du pare-feu.

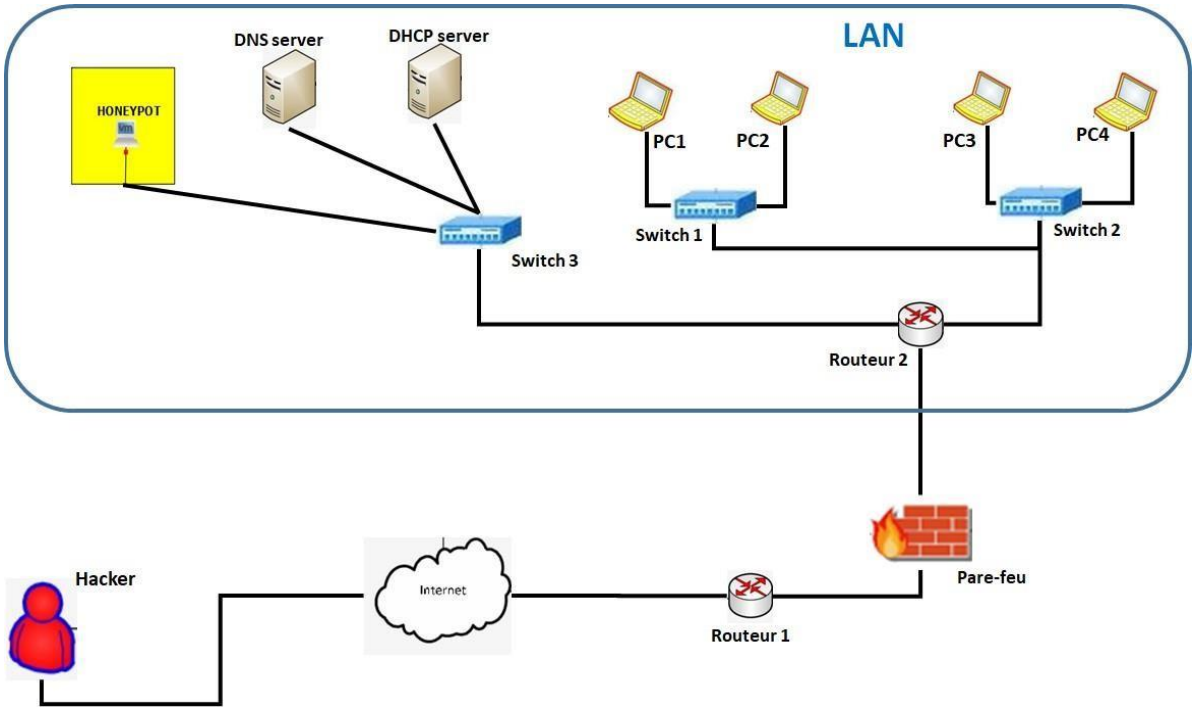

Figure 2.09 : « Honeypot » installé derrière un pare-feu

7. Honeynet

7.1. Définition

Un « Honeynet » est un réseau de systèmes « Honeypots » accompagné d'un ensemble de mécanismes de sécurité tels que des pares-feux, des identifiants pour les systèmes de contrôle (IDS) et des serveurs de logs. Il est utilisé comme appât pour leurrer

les attaquants, de sorte que sa structure en réseau permet d'obtenir des informations sur les connexions entre les attaquants et leurs méthodes de coopération. **[19]**

7.2. Principe du fonctionnement des « Honeynets »

Le fonctionnement du « honeynet » doit assurer les trois opérations principales suivantes : le contrôle des données, la capture et la collection des données et l'analyse des données.

7.2.1. Le contrôle des données

Ceci est garanti, par exemple, par un pare-feu caché derrière le routeur qui utilise de nombreuses technologies, comme le maintien du trafic après un nombre limitées connexions.

7.2.2. La capture et la collection des données

Ce travail se fait à trois niveaux : Pare-feu d'application des règles (UPS), des systèmes d'inventaire (IDS) et les systèmes honeypots eux même. Toutes les informations recueillies à ces trois niveaux doivent être collectées et stockées dans une structure centrale, à l'abri de tout risque potentiel, afin d'éviter leur suppression par l'attaquant.

7.2.3. L'analyse des données

Ce processus est effectué à l'aide d'un ou plusieurs instruments graphiques ou non graphiques. « Honeynet » utilise ces outils pour afficher et passer en revue toutes les informations recueillies de manière lisible et simple. **[19]**

7.3. Honeynet virtuel

C'est un réseau, alors qu'il ressemble à un réseau physique, c'est une image virtuelle d'un réseau qui est sur un seul serveur. En l'absence d'un système réseau, les analystes de la sécurité de l'ordinateur ne doivent pas perdre leur temps à examiner les utilisateurs légitimes des réseaux du monde réel.

Il y a toujours un risque que l'attaquant se déplace horizontalement du réseau de la famille vers le secteur du réseau de production pour pénétrer le vrai réseau. Parce que le réseau d'abeilles ne peut pas détecter d'attaques sur les systèmes légitimes, il est donc préférable d'isoler et de surveiller le réseau « Honeynet » de façon proactive afin de réduire les risques. **[19]**

8. Conclusion

En projetant nos recherches sur les honeypots, nous avons essayé de les définir, parler de leurs types et leurs architectures ainsi que leur principe de fonctionnement. Cependant, les honeypots n'ont pas cessé d'évoluer chaque année.

Et pour en faire un peu le tour au but de se faire éclaircir les idées, nous nous sommes focalisé sur ce que les dernières recherches scientifiques ont abouti comme nouvelles techniques d'honeypots.

CHAPITRE III

PROJET « GLASTOPF » COMME HONEYPOT A FAIBLE INTERACTION

1. Introduction

Après avoir mentionné précédemment ce qu'est un pot de miel et énuméré ses types et statuts possibles dans le réseau, nous avons choisi un type de pot de miel open source qui est Glastopf développé par Lukas Rist. Où dans cette partie du mémoire nous allons faire de la modélisation sur le système honeypot puis dans la deuxième partie du troisième chapitre nous discutons le code open source pour glastopf.

2. Présentation

Glastopf est une honeypot d'application web phyton dont la fonction principale est de simuler le type de vulnérabilité plutôt que la vulnérabilité en soi. Glastopf est un honeypot à faible interaction qui émule un serveur Web vulnérable hébergeant de nombreuses pages Web et applications Web avec des milliers de vulnérabilités. Il est facile à configurer et une fois indexé par les moteurs de recherche, les attaques afflueront par milliers chaque jour.

2.1. Stations d'amélioration honeypot Glastopf

- Base de données centrale optimisée contenant les données collectées à partir d'un petit nombre de nœuds Glastopf (Lucas Rist, mai 2009)
- Nouvelles fonctionnalités implémentées :
    - LFI (fichiers locaux inclus)
    - Module d'enregistrement IRC : il s'agit d'une requête/réponse de bot. La requête est traduite en une requête MySQL dont les résultats sont répondus au demandeur.
    - Le module Twitter est désormais intégré à Glastopf.

Le Glastopf Vulnerability Simulator est l'un des éléments centraux face aux attaques. J'ai amélioré le concept et la première version est terminée et sera implémentée dans les prochaines semaines.

- Le nombre d'attaques sur le Web Honeypot a doublé, l'analyseur a donc été amélioré et les changements à venir dans les modèles d'attaque sont réduits. (Lucas

Rist, juillet 2009)

Voici un exemple simple :

- ***Fichier injecté***

```
$un =php_uname();
echo "uname -a : $un
" ;
?
```

- **Analyste**

```
for line in file:
pattern = "uname"
if re.search(pattern, line):
uname = "Linux debian 2.6.8... "
response = "uname -a: " + uname + " "
return response
```

- Collectez beaucoup d'attaques. En fait, nous avons environ 1,27 million d'adresses IP d'attaquants uniques et les groupes de vulnérabilités requis dans notre base de données. Au total, nous avons plus de 14 millions de visites sur les trois capteurs déployés. Des vulnérabilités, lancées par l'attaquant, ont également été collectées. (Lucas Rist, Août 2009)
- Exécutez l'application Web de pot de miel Glastopf de nouvelle génération, alias GlastopfNG (Lucas Rist, octobre 2010)

  GlastopfNG : une attraction spécialisée dans l'émulation d'un serveur/d'une application Web vulnérable pour devenir la cible d'attaques automatisées et même manuelles. Au lieu d'essayer d'empêcher ces attaques, GlastopfNG essaie d'obtenir autant d'informations que possible sur l'attaquant et l'attaque qui s'est utilisée. Il n'a plus aucun défaut dans le Glastopf original, ce qui en fait le site d'attraction d'attaques Web le plus avancé.
- Dans l'ensemble, GlastopfNG est désormais l'une des attractions les plus flexibles disponibles.

- En mai 2012, la troisième version de l'application Web Honeypot Glastopf est sortie et elle est livrée avec de nouvelles fonctionnalités très puissantes :
  Un bac à sable PHP intégré pour l'émulation d'injection de code, nous permettant de porter la simulation de vulnérabilité à un nouveau niveau connecté à notre système de flux de données public HPFeeds pour la collecte de données centralisée, une intégration étroite dans notre bac à sable et une implémentation standard de notre système de surveillance de serveur Web.
- Nombre d'alertes pour la période : **1325919** durant le mois d'avril (Michael Kerry, juillet 2014)
  Les noms de fichiers (RFI)-3 les plus courants au fil du temps :
  - b8cbfe520d4c2d8961de557ae7211cd2 (**1072** mouvement)
  - 3cc11c8fa7e3e36f0164bdcae9de78ec (**998** mouvement)
  - 7de0bcb903eaba7881c6d03a8c7769a8 (**682** mouvement)

➢ Ping back

pingback.ping, une fonctionnalité WordPress légitime, est utilisée à mauvais escient par les victimes DoS utilisant des sites WordPress légitimes.

➢ Méthode

```
pingback.pinghttp://victime.com
www.anywordpresssite.com/postchosenparam> '
```

- Nombre d'alertes pour la période : 1859863 durant le mois de mai (Michael Kerry, août 2014)
  Noms de fichiers (RFI) - Les plus populaires au fil du temps :
  - 48101bbdd897877cc62b8704a293a436 (**2425** instantanés)
  - 4997ed27142837860014e946eed96124 (**2050** mouvements)
  - d070c4cccf556b9da81da1e2de3cba54 (**644** résultats)

➢ **Méthode**

```
pingback.pinghttp://victim.comwww.anywordpresssite.com/postchosen'
```

3. Modélisation d'un système honeypot

3.1. Diagramme de contexte

- Le pirate essaie d'envoyer des paquets croyant tester des failles, le firewall les intercepté et connecte l'honeypot qui les transmet à son tour au système de détection d'intrusion.

  L'IDS crée de fausses données et les envois au pirate. L'honeypot enregistre les données du pirate qui peuvent être plus tard consultées par l'administrateur.

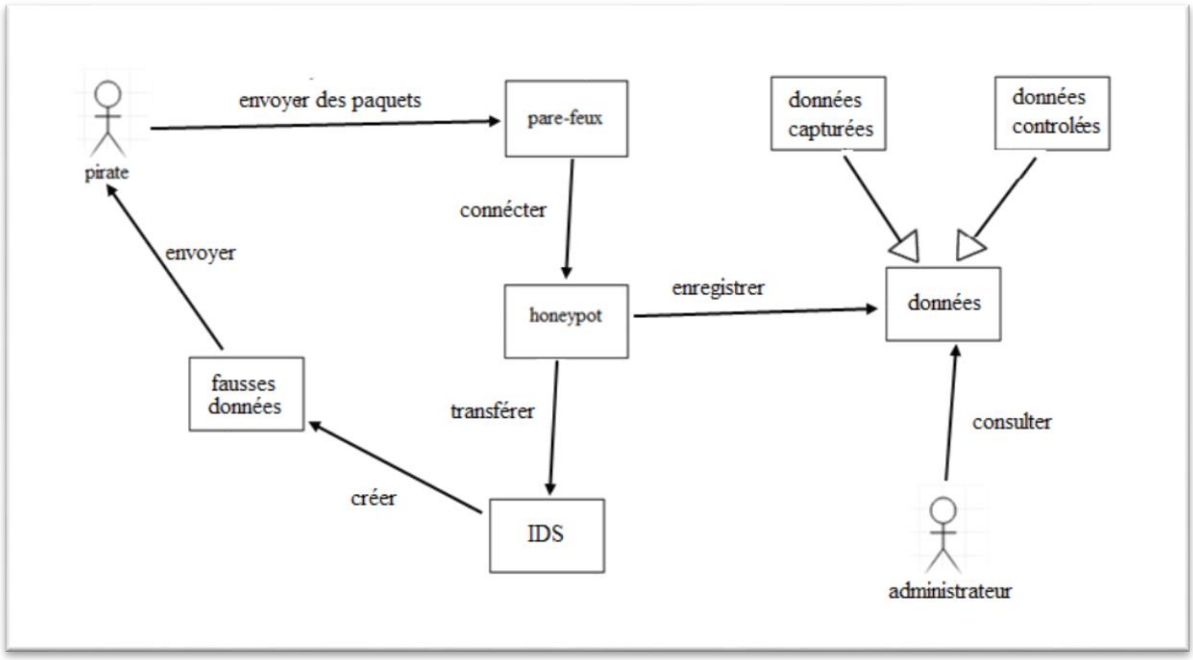

Figure 3.01 : Diagramme de contexte du système

- Le firewall filtre le trafic envoyé au serveur, si le trafic est suspect il est transféré à l'honeypot, si le trafic est normal il obtient un laisser passer directement au serveur.

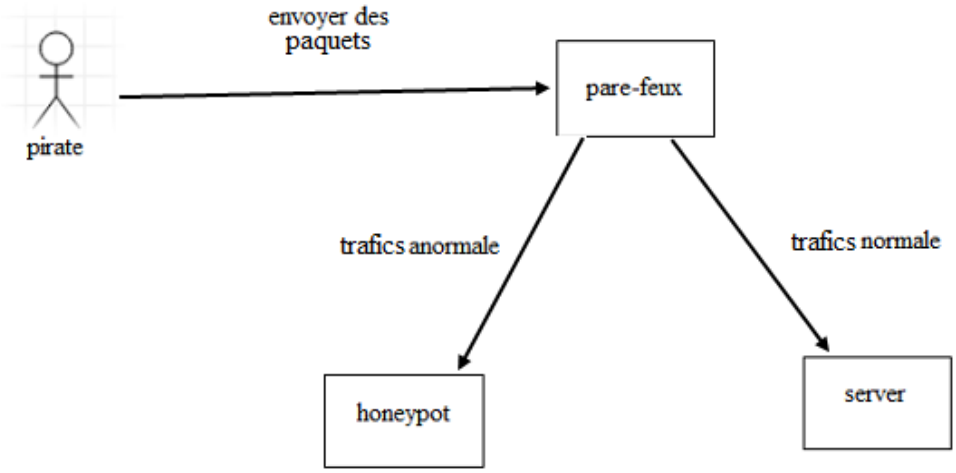

Figure 3.02 : Diagramme de contexte du réseau

3.2. Diagramme de cas d'utilisation

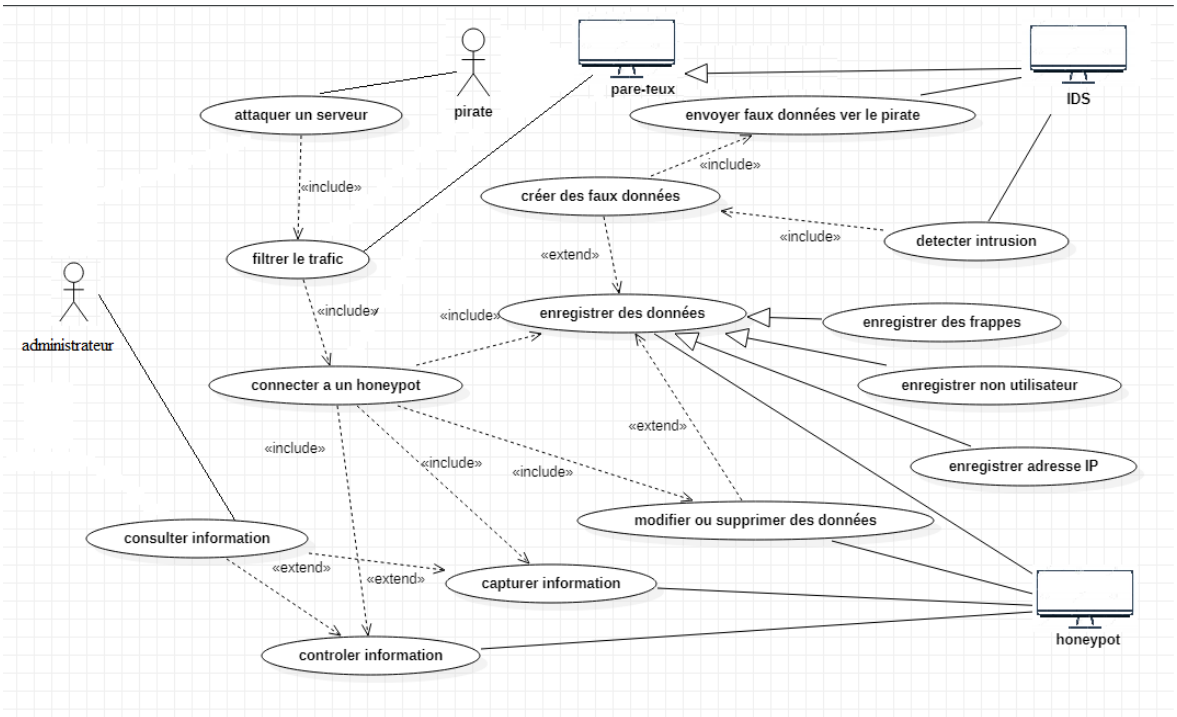

Figure 3.03 : Diagramme de cas d'utilisation du système

3.2.1. Description des acteurs

- **Acteur principale**
  - **Administrateur :** L'administrateur système surveille, installe et assure le bon fonctionnement de l'infrastructure système et réseau.
- **Acteur secondaire :**
  - **Le pirate :** Il s'introduit dans votre système informatique pour voler des données, modifier des informations à des fins illégales.
  - **Pare feux :** permettant de faire respecter la politique de sécurité du réseau.
  - **Ids :** sont seulement protégés par un chiffrement
  - **Honeypot :** composé d'applications et de données destiné à servir d'appât pour piéger les pirates.

3.2.2. Description textuelle des cas d'utilisations :

a) Attaquer un serveur

Titre	Attaquer un serveur
Acteurs	Le pirate
Type	Secondaire
Objectif	Controller le serveur
Scenario nominal	Le Pirate envoyer des paquets ver le server, puis le pare feux repousse l'attaque et affiche les données malveillante

Tableau 3.01 : descriptions textuelles de cas attaquer un serveur

b) Filtrer le trafic

Titre	**Filtrer le trafic**
Acteurs	Pare feux
Type	Secondaire
Objectif	Déterminer tous les protocoles requis utilisés
Scenario nominal	Une menace à détecter Le pare feux commence à vérifier protocole entrant

Tableau 3.02 : descriptions textuelles de cas filtrer le trafic

c) Connecter à un honeypot

Titre	Connecter à un honeypot
Acteurs	Pare feux
Type	Secondaire
Objectif	Pour transférer les trafics si elle menacé le serveur
Scenario nominal	Après détecter une menace au sein pare feux ce dernière déclenche avec l'honeypot et puis transférer le trafic

Tableau 3.03 : descriptions textuelles de cas connecter à un honeypot

d) Enregistrer des données

Titre	Enregistrer des données
Acteurs	Honeypot
Type	Secondaire
Objectif	Pour la capaciter de la création des fausses données et contrôler mieux mes données
Scenario nominal	Le honeypot se déclenche après telle opération fait l'enregistrement des données

Tableau 3.04 : descriptions textuelles de cas enregistrer des données

e) Détecter intrusion

Titre	Détecter intrusion
Acteurs	IDS
Type	Secondaire
Objectif	Pour protéger mon système puis en a fait la réponse nécessaire

Tableau 3.05 : descriptions textuelles de cas détecter intrusion

f) Créer fausses données

Titre	Créer fausses données
Acteurs	IDS
Type	Secondaire
Objectif	Pour envoyer ver l'attaquant

Tableau 3.06 : descriptions textuelles de cas créer fausses données

g) Envoyer fausses des données

Titre	Envoyer fausses des données
Acteurs	IDS
Type	Secondaire
Objectif	Placer l'attaquant dans de fausses données, croyant ainsi qu'il a atteint ce qui est requis.

Tableau 3.07 : descriptions textuelles de cas envoyer fausses données

h) Consulter information

Titre	Consulter information
Acteurs	Administrateur
Type	Principale
Objectif	Définir les vulnérabilité et son type puis en reconnu l'intrusion

Tableau 3.08 : descriptions textuelles de cas consulter information

i) Contrôler information

Titre	Contrôler information
Acteurs	Honeypot
Type	Secondaire
Objectif	Pour connaitre les données de l'attaquant et de la capacité de manipulation des informations

Tableau 3.09 : descriptions textuelles de cas contrôler information

j) Capturer information

Titre	Capturer information
Acteurs	Honeypot
Type	Secondaire
Objectif	Pour connaitre les données de l'attaquant et de la capacité de manipulation des informations

Tableau 03.10 : descriptions textuelles de cas capturer information

k) Modifier ou supprimer des données

Titre	Modifier ou supprimer des données
Acteurs	Honeypot
Type	Secondaire
Objectif	La fiabilité du système

Tableau 03.11 : descriptions textuelles de cas modifier ou supprimer des données

l) Enregistrer des frappes

Titre	Enregistrer des frappes
Acteurs	Honeypot
Type	Secondaire
Objectif	Pour répondre et sauvegarder

Tableau 3.12: descriptions textuelles de cas enregistrer des frappes

3.3. Diagramme de séquence

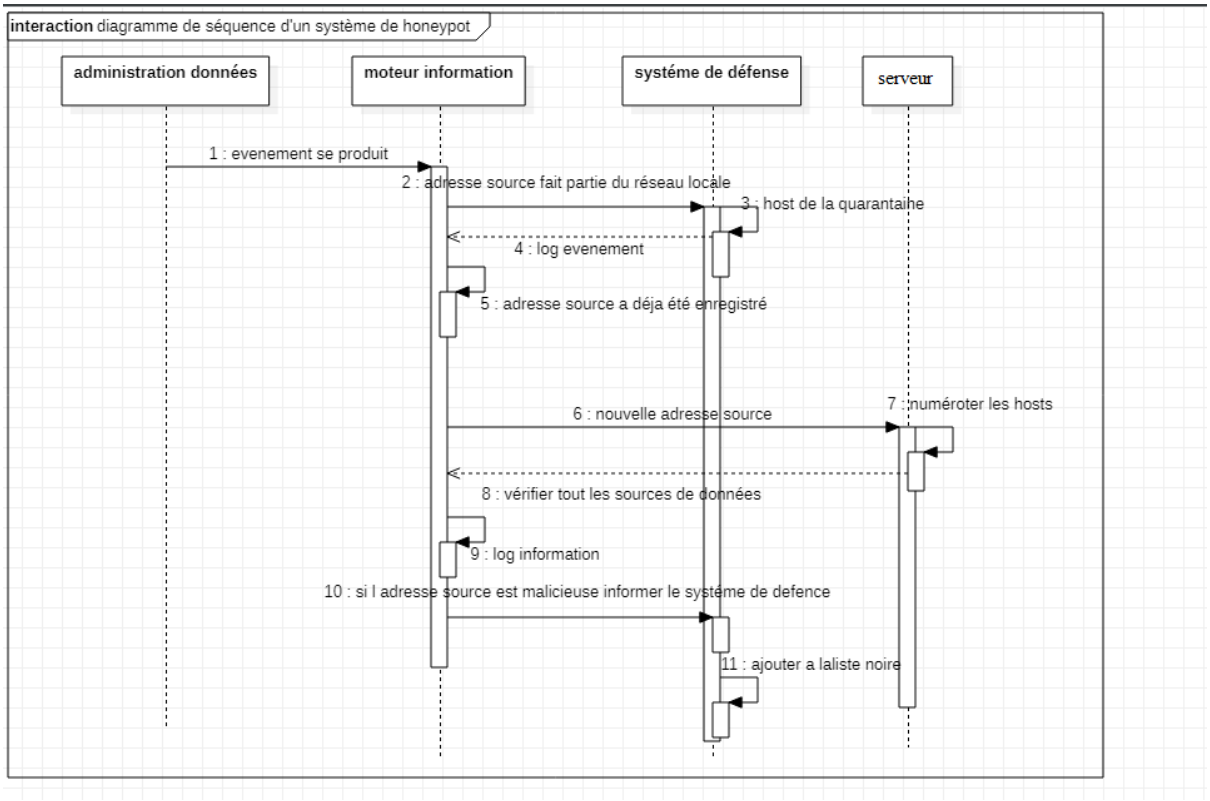

Figure 3.04 : Diagramme de séquence du système

Un mécanisme honeypot peut être décortiqué en plusieurs séquences :

- Une administration de données sur laquelle l'évènement se produit.
- Un moteur d'information qui classe et vérifié et enregistre les adresses sources
- Un système de défense qui met en quarantaine les adresses sources malicieuses signalées et les ajoute à la liste noire puis nous avons le serveur qui ne reçois que le résultat final du travail. (Hosts après identification, classement et filtrage).

4. Description du code source

Cette application web Glastops est développer avec le langage python.

- **Définition**

Python est le langage de programmation open source le plus utilisé par les informaticiens. Ce langage a propulsé le sommet de la gestion d'infrastructure, de l'analyse de données ou du développement de logiciels. En fait, parmi ses qualités, Python permet aux développeurs de se concentrer sur ce qu'ils font plutôt que sur la façon dont ils le font. Il a libéré les développeurs des limitations de forme qui tourmentaient leur temps avec les langages plus anciens. Ainsi, développer du code avec Python est plus rapide que d'autres langages.

- Le programmeur commence par importer les bibliothèques et les méthodes essentielles au bon fonctionnement du code.

La ressource système Unix, spécifiquement **usr** qui est le système dans lequel le développement a été fait et le module **sys** fournit également des fonctions et des variables qui permettent l'interaction avec l'interpréteur Python.

Importer toutes les fonctions de **WSGIServer** depuis une bibliothèque **gevent** qui permet de créer en Python des coroutines pour gérer efficacement des problématiques réseau. Un serveur WSGI (Web Server Gateway Interface) exécute du code Python pour créer une application Web.

OpenSSL est une boîte à outils de chiffrement comportant deux bibliothèques, libssl et libcrypto, le module crypto fournit un moyen de gérer les données chiffrées.

Importer la fonctions **wsgi_wrapper** de **GlastopfWSGI** depuis une bibliothèque glastopf, Une fonction wrapper est un programme dont la fonction principale est d'appeler une autre fonction.

Le module de journalisation permet aux applications de configurer différents gestionnaires de journal et d'acheminer les messages de journal vers ces gestionnaires. Cela permet une configuration très flexible qui permet de gérer de nombreux cas d'utilisation différents. Pour écrire un message de journal, un appelant demande un enregistreur nommé. Se logger peut-être utiliser pour écrire des messages formatés en utilisant un niveau de log (DEBUG, INFO, ERROR etc).

La magie est que le ressort transfèrera **logging.path** dans les propriétés système **LOG_PATH**.

La méthode **isdir ()** est utilisée pour vérifier si le chemin spécifié est un répertoire existant ou non si non utilisez **os.makedirs()** pour créer les dossiers intermédiaires.

La fonction de format **(str.format())** est une technique de la catégorie de chaîne qui vous permet d'essayer de faire des substitutions de variables et de formater des données. Il vous permet de concaténer des parties d'une chaîne à des intervalles souhaités grâce à la fonction de format de données ponctuelles **(str. format())** Cette technique de la catégorie de chaîne vous permet d'essayer de faire des substitutions de variables et de formater les données. Il vous permet de concaténer des parties d'une chaîne à des intervalles souhaités via la forme de données ponctuelles

Cela signifie que les noms des enregistreurs suivent la hiérarchie des packages/modules, et il est intuitivement évident où les événements sont enregistrés uniquement à partir du nom de l'enregistreur. Cela ressemble à un bon conseil

Au sommet de la hiérarchie se trouve le root logger, accessible via la journalisation. racine. Cet enregistreur est appelé lorsque des méthodes telles que **logging. debug()** est utilisé. Par défaut, le niveau de journal racine est WARN, donc chaque journal de niveau inférieur (par exemple via logging.info("info")) sera ignoré.

L'activation de la journalisation de la console suit les événements se produisant dans un certain morceau de code lors de son exécution en Python.

Selon la documentation de **TimedRotatingFileHandler** : Le système enregistrera les anciens fichiers journaux en ajoutant des extensions au nom de fichier. Les extensions sont basées sur la date et l'heure,

Contient un tuple de la forme (hôte, port) faisant référence à l'adresse du client.

L'interface de passerelle de serveur Web **(WSGI)** est une interface standard entre le logiciel de serveur Web et les applications Web écrites en Python.

Le protocole **SSL** est une technologie de sécurité standard utilisée pour établir un lien crypté entre un serveur Web et un client Web. SSL facilite la communication réseau sécurisée en identifiant et en authentifiant le serveur ainsi qu'en garantissant la confidentialité et l'intégrité de toutes les données transmises

Ajoutez deux astérisques : avant le nom du paramètre dans la définition de la fonction. De cette façon, la fonction recevra un dictionnaire d'arguments

Un identifiant unique (UID ou Unique Identifier en anglais) est une chaîne numérique ou alphanumérique associée à une seule entité au sein d'un système

L'utilisateur **'nobody'** qui exécute le démon n'a aucun privilège sur la machine. Il est généralement réservé aux démons non approuvés comme httpd, etc.

GID est un sigle qui peut désigner : gestion intégrée des documents, un système pérenne de gestion dont les composantes sont intégrées afin de donner, aux personnes accréditées, accès à toute l'information pertinente portée par un support qui documente les activités d'une organisation.

"nogroup". Essayez de modifier le serveur de messagerie pour exécuter le script en groupe

- **Glastopf Installation - Ubuntu 12.04 LTS**

Install the dependencies:

sudo apt-get update

sudo est une commande informatique utilisée principalement dans les systèmes d'exploitation de type Unix.

sudo pip install --upgrade distribute

sudo pip install probably signifie que vous souhaitez installer un paquet à l'échelle du système. Pour certains packages, tels que virtualenvwrapper, cela pourrait être utile, mais à part cela, j'éviterais d'installer des packages à l'échelle du système et de créer un virtualenv pour chaque application et une installation pip sur ce virtualenv

- **Install glastopf**

Install latest stable release from pip::

sudo pip install glastopf

Or install latest development version from the repository::

cd /opt

```
sudo git clone https://github.com/mushorg/glastopf.git
cd glastopf
sudo python setup.py install
```

- **Configuration**

```
Prepare glastopf environment::
        cd /opt
        sudo mkdir myhoneypot
        cd myhoneypot
        sudo glastopf-runner
A new default glastopf.cfg has been created in *myhoneypot*, which can be customized as required.
```

- **Testing the Honeypot**

```
Start Glastopf (from your 'myhoneypot' directory)::
   sudo glastopf-runner
  2013-03-14 08:34:08,129 (glastopf.glastopf) Initializing Glastopf using "/opt/myhoneypot" as work directory.
        2013-03-14 08:34:08,130 (glastopf.glastopf) Connecting to main database with: sqlite:///db/glastopf.db
```

Définition des instances request_string, client_address et Initialisation server_version, sys_version à la valeur zéro

```
class HTTPHandler(BaseHTTPRequestHandler):
 def __init__(self, request_string, client_address, server_version=None,
sys_version=None):
```

- **Extraire tous les membres de l'archive vers le répertoire de travail actuel**

- Extraire des répertoires avec un mode sans échec.

```
directories.append(tarinfo)
tarinfo = copy.copy(tarinfo)
tarinfo.mode = 448
```

- Répertoires de tri inversé.

```
if sys.version_info < (2, 4):
def sorter(dir1, dir2):
        return cmp(dir1.name, dir2.name)
    directories.sort(sorter)
    directories.reverse()
  else:
    directories.sort(key=operator.attrgetter('name'), reverse=True)
```

- Les arguments positionnels sont ignorés

```
  return options
def main(version=DEFAULT_VERSION):
```

Install or upgrade setuptools and EasyInstall

```
  options = _parse_args()
  tarball = download_setuptools(download_base=options.download_base)
  return _install(tarball, _build_install_args(options))
if __name__ == '__main__':
  sys.exit(main())
```

5. Conclusion

Comme démontré dans ce chapitre qui représente la conception d'un honeypot et étude sur le code source de application web glastopf, il est clair qu'avec une bonne technique de camouflage, ils erait possible de piéger les pirates les plus expérimentés

Conclusion générale

Le meilleur endroit pour déployer Glastopf est près du ou des serveurs de production basés sur le Web (DMZ) ou dans un état séparé protégé par un pare-feu, un pare-feu et le système IDPS (détection et prévention des intrusions). Les journaux créés par Glastopf peuvent aider à détecter les attaques sur les serveurs web dans le réseau de production et aider à rassembler des informations (telles que l'adresse IP, les outils, les technologies, etc.) sur ces attaques. Ces informations peuvent être utilisées pour renforcer la sécurité des serveurs d'applications sur Internet et pour identifier des attaques coordonnées sur des serveurs Web.
Par ailleurs nous avons rencontré quelques contraintes et difficultés durant notre travail.Et cela dû aux modestes ressources que nous avons sous disposition. Il est à prendre en compte qu'une telle simulation pour un honeypot glastopf nécessite des machines avec des caractéristiques physiques haut de gamme, spécialement en matière de processeur et mémoire vive.

Bibliographie

[01] https://www.avast.com/fr-fr/business/resources/future-of-network-security#pc

[02] https://fr.wikipedia.org/wiki/

[03] https://www.cyberjobs.fr/actualites-articles/zoom-sur-les-5-objectifs-de-lasecurite informatique#

[04] https://www.scarg.org/preface-securite-informatique-et-reseaux-3eme-edition?

[05] https://inetdoc.developpez.com/

[06] https://www.oracle.com/fr/security/

[07] https://www.ionos.fr/digitalguide/

[08] https//www.informatique-mania.com/linformatique/session-hijacking/

[09] https://www.inetdoc.net/guides/tutoriel-secu/

[10] https://geekflare.com/fr/web-application-injection-attacks/

[11] https://www.kaspersky.fr/resource-center/definitions/

[12] https://www.futura-sciences.com/tech/definitions/

[13]http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2005/ladrouz- bennouna/

[14] Yonas Kibret, Wang Yong, April 2013. Design and Implementation of Dynamic Hybrid Virtual Honeypot Architecture for Attack Analysis. Université des sciences et de l'ingénierie électroniques de Chine Chengdu, Chine

[15] Bousebsi Amel**,** Boukadoum Meriem**,** A 2018. Méthodes d'ensemble en machine learning pour la détection d'intrusion. Mémoire de master. Université 20 Aout 1955-SKIKDA

[16] Rznotronarison Nomena Arivony, A 2018. Implémentation d'un honeypot pour la sécurisation d'un réseau d'entreprise. Mémoire de master. Université d'Antananarivo

[17] https://www.forcepoint.com/fr/

[18] https://www.paloaltonetworks.fr/cyberpedia/

[19] https://www.rapport-gratuit.com/les-honeynets/

[20] https://www.researchgate.net/publication/

[21] Kamaldeep Sehgal, A 2013. Study on Web application Honeypots. Mémoire de master.

Université de Bedfordshire
[22] http://mushmush.org/
[23] Mphago, B, Mpoeleng, D & Masupe, S 2017, 'Deception in Web Application Honeypots : Case of Glastopf', International Journal of Cyber-Security and Digital Forensics, vol. 6, no. 4, pp. 179-186.
[24] https://github.com/