Honeypots

Définition

- La définition d’un honeypot comme a été défini par Lance Spitzner est: "Un honeypot est une ressource système dont la seule utilité est de se faire attaquer ou compromettre", autrement dit, un honeypot est un ordinateur ou un programme volontairement vulnérable destiné à attirer et à piéger les pirates informatiques.

Types de "honeypots"

- Selon ce qu’on attend des honeypots, nous pouvons distinguer deux principaux types : honeypots de production et honeypots de recherche

Types de "honeypots"

1- "Honeypots" de production (production Honeypots)

- Un honeypot de production est utilisé pour sécuriser un réseau opérationnel. Il déroute les attaques orientées vers les différents services de production du système, en les attirant vers lui, ce qui permet de réduire le risque, en renforçant la sécurité qui est assurée par les autres mécanismes de sécurité comme les firewalls, les IDS (Systèmes de Détections d'Intrusions), etc.
- Comme il peut aussi détecter des attaques grâce à ses fichiers d'audit, qui peuvent être aussi utilisés pour corriger les vulnérabilités.

Types de "honeypots"

1- "Honeypots" de production (production Honeypots) :

- Son rôle dans la protection du système: Un honeypot de production joue un rôle important dans une ou plusieurs composantes de la sécurité du système de production telles que :

– La prévention : Laisser le hacker jouer sur le honeypot au lieu de jouer sur les systèmes de production.

– La détection : Toute connexion établie avec un honeypot de production est considérée comme tentative d'intrusion au système, il élimine ainsi toutes les fausses alertes (positives et négatives).

– Le recouvrement : Le rôle des honeypots de production dans le recouvrement se traduit par les deux points suivants :

– Ils permettent une continuité des services après une attaque produite en leur sein, en les mettant simplement hors service.

– L'information enregistrée par les honeypots de production sera d'un apport considérable pour le recouvrement du système.

Types de "honeypots"

2- "Honeypots" de recherche (research Honeypots)

- Le souci de ce type de honeypots n'est pas de sécuriser un système particulier, mais c'est de s'introduire dans un environnement de recherche pour comprendre et étudier comment la communauté Black Hat évolue, quelles sont les techniques que cette communauté utilise et qui appartient à cette communauté.
- Les honeypots de recherche sont plus complets que les honeypots de production.
- C'est en général le système en entier qui peut être attaqué (et non pas seulement un seul service), ce qui en fait des systèmes sensibles dans leur gestion et complexes pour l'analyse de leurs résultats.

Types de "honeypots"

2- "Honeypots" de recherche (research Honeypots)

- Son rôle dans la protection du système : Les honeypots de recherche ne servent pas la sécurité des systèmes (prévention, détection et recouvrement) d'une manière directe, mais ils offrent des renseignements précieux sur les attaquants et leur comportement.
- Ces informations permettent une meilleure connaissance de la communauté des hackers, ce qui aide les professionnels de la sécurité informatique dans l'amélioration de méthodes et mécanismes de protection.

Classification des "honeypots"

- L’implémentation d’un honeypot est reposée principalement sur le niveau d’interaction "level of involvment" du honeypot utilisé.
- Ainsi, nous pouvons distinguer trois classes différentes de honeypots : les honeypots à faible interaction, les honeypots à moyenne interaction et les honeypots à haute interaction.

Classification des "honeypots"

1- "Honeypots" à faible interaction

- Un honeypot à faible interaction est un honeypot virtuel fournit comme le montre son nom une interaction limitée (faible) avec le pirate, il est tout simplement un programme qui simule les services d'un système réel par la mise en place par exemple des Sockets d'écoute sur chaque port d'un service, ces sockets ne font que logger les différents paquets qu'elle reçoit.

Classification des "honeypots"

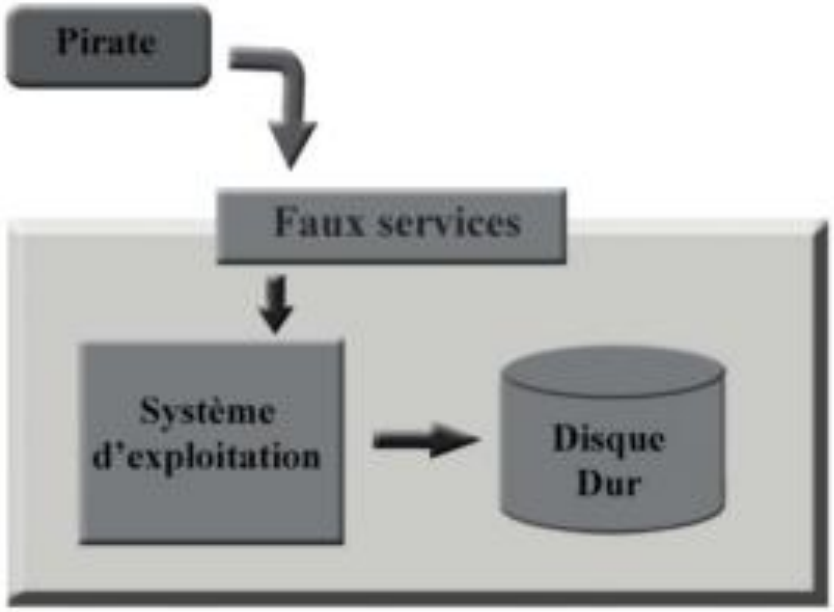

FIG. 1.1 – Schéma d'une interaction faible

Classification des "honeypots"

1- "Honeypots" à faible interaction

- Les avantages et les inconvénients principaux de ce type de honeypots sont :

– Avantages :

– La mise en place est très simple.

– La gestion complexe des logs du système est éliminée.

– La sécurité du système est conservée (mais uniquement s'il est bien configuré et que les faux services implémentés ne possèdent pas eux même un trou de sécurité).

Classification des "honeypots"

1- "Honeypots" à faible interaction

– Inconvénients :

– Sont faciles à détecter par les attaquants à cause d'absence de réponses attendues dues à l'implémentation incomplète des services.

– Peu d'informations sur l'attaquant sont dérivées (le temps et la date d'attaque, adresse IP (Internet Protocol) source et adresse IP destination de la connexion, port source et port destination de la connexion), car le honeypot n'offre aucune possibilité au pirate de s'introduire dans le système.

- Le but principal de ce type de honeypots est la détection des tentatives de connexions non autorisées. Donc ce type est sans doute le plus utilisé dans les honeypots de production.
- Les honeypots à faible interaction les plus connus sont :Honeyd, Specter.

Classification des "honeypots"

2- "Honeypots" à moyenne interaction

- Un honeypot à moyenne interaction est un honeypot semi-virtuel qui assure une simulation améliorée des services d'un système par rapport à la simulation fournie par les honeypots à faible interaction, en lui ajoutant la possibilité de renvoi des réponses aux attaquants, ces réponses sont généralement fausses de façon à leur donner des pistes ou à les dérouter sans forcément les intriguer, comme le montre la figure Fig.1.2.
- En plus des services simulés, il offre aussi quelques services réels, mais sans donner la possibilité au pirate de prendre un contrôle total du système.

Classification des "honeypots"

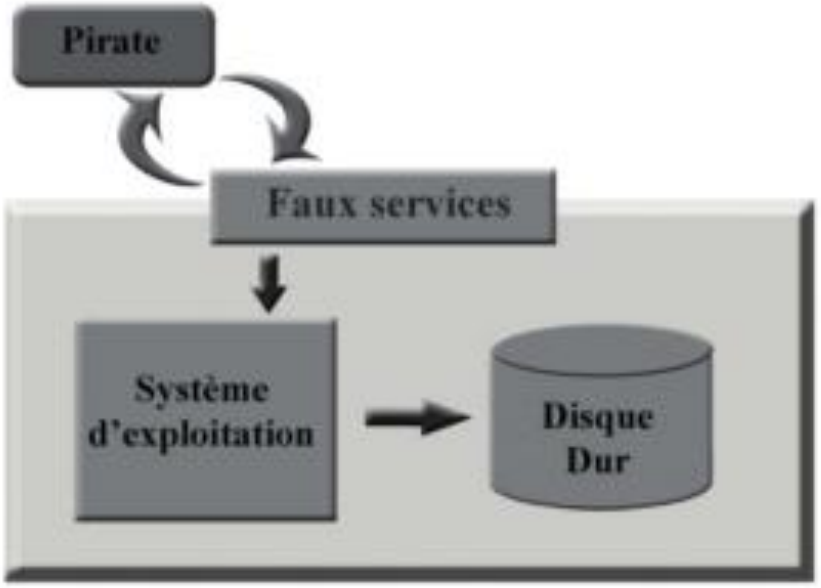

FIG. 1.2 – Schéma d'une interaction moyenne

Classification des "honeypots"

2- "Honeypots" à moyenne interaction

- Les avantages et les inconvénients principaux de ce type de honeypots sont :

– Avantages :

– La gestion des logs du système est facile par rapport à celle des honeypots à haute interaction et un peu difficile par rapport à celle des honeypots à faible interaction.

– Fournit beaucoup plus d'informations intéressantes à analyser, à cause de variété d'attaques proposées aux pirates ce qui s'avère plus intéressant pour eux.

Classification des "honeypots"

2- "Honeypots" à moyenne interaction

– Inconvénients :

– Très dur à implémenter en terme de développement, car la fourniture d'un leurre parfait implique une parfaite connaissance des protocoles de chaque faux service pour bannir toute faille de sécurité.

– Sécurité du système difficile à contrôler, du fait que, plus le niveau de complexité d'un honeypot augmente plus il y a de chance qu'il contienne lui même un trou de sécurité qui peut être exploité par le pirate.

- Les honeypots les plus connus de ce type sont: homemade honeypots, Deception Toolkit.

Classification des "honeypots"

3- "Honeypots" à haute interaction

- Contrairement aux honeypots à faible et à moyenne interaction, un honeypot à haute interaction ne se base pas sur l'émulation d'un service, mais plutôt sur un vrai système d'exploitation, ce qui offre une grande interactivité avec l'attaquant, puisque il s'agit bien des systèmes réels avec des failles de sécurité qu'il peut exploiter, comme le montre la figure Fig.1.3.
- Ce type de honeypots est orienté plus à la recherche dont on souhaite qu'un pirate pénètre un système pour l'observer.

Classification des "honeypots"

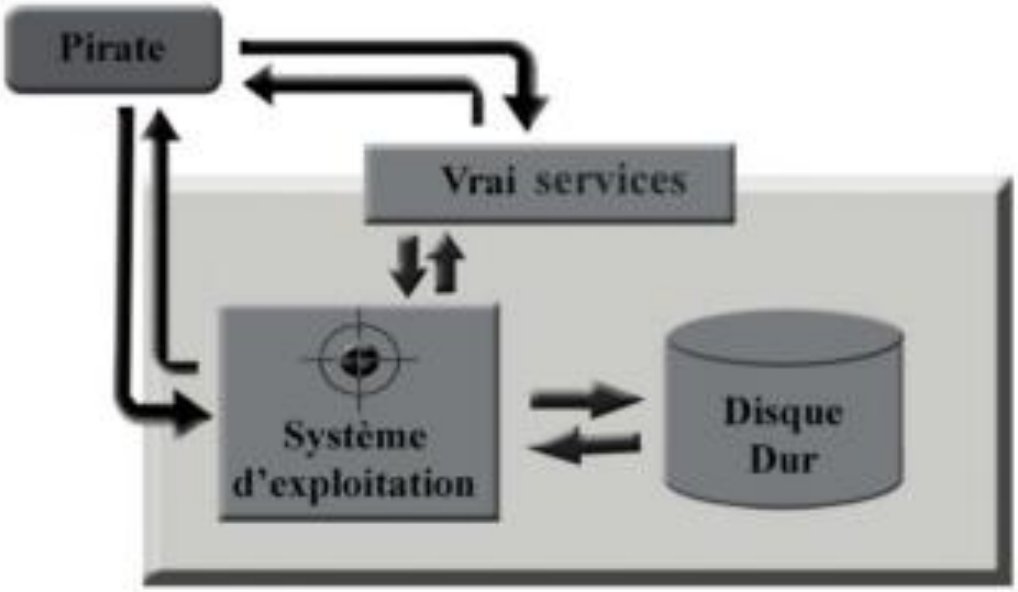

FIG. 1.3 – Schéma d'une interaction forte

Classification des "honeypots"

3- "Honeypots" à haute interaction

- Les avantages et les inconvénients principaux de ce type de honeypots sont :

– Avantages :

– Très difficile à détecter par les pirates.

– Fournir beaucoup d’informations sur les activités du pirate.

Classification des "honeypots"

3- "Honeypots" à haute interaction

– Inconvénients :

– Introduire un grand risque dans le système hôte, à cause de la pénétration du pirate au système réel avec une liberté totale, ce qui puisse engendrer une réinstallation périodique du système.

– La réactivité du monitoring est un facteur de complexité important.

– La gestion des logs est très compliquée (transférer les informations capturées sur le pirate à un log distant sans se faire repérer par les attaquants).

- Les honeypots à haute interaction les plus connus sont : Honeynet CDROM ROO, ManTrap.

Architecture des "honeypots"

- L’architecture d’un honeypot est définie par la nature du système qui l’héberge, qui peut être réel ou virtuel

Architecture des "honeypots"

1- Architecture réelle

- Dans cette architecture, chaque honeypot est installé sur sa propre machine physique, c'est-à-dire chaque honeypot est représenté par un système réel.
- Les avantages et les inconvénients de cette architecture sont :

– Avantages :

  – Administration simplifiée.

– Inconvénients :

  – Si plusieurs honeypots alors plusieurs machines physiques.

  – Le monitoring système sans se faire repérer par le pirate est compliqué.

  – Réinstallation fréquente du système pour chaque honeypot.

Architecture des "honeypots"

2- Architecture virtuelle

- Dans cette architecture, le honeypot est installé sur une machine virtuelle. La création des machines virtuelles est assurée par des outils de virtualisation de systèmes comme : VMWare sous Linux et Windows, UML (User-Mode-Linux) sous Linux, et Jail sous Unix BSD.
- Ces outils peuvent émuler un ou plusieurs systèmes sur une seule machine, donc il est possible d'installer plusieurs honeypots virtuels sur une seule machine.
- De plus, VMWare peut émuler plusieurs systèmes de natures différentes (windows, linux , ...etc), on peut alors proposer plusieurs honeypots de plusieurs systèmes d'exploitation virtuels sur la même machine physique.

Architecture des "honeypots"

2- Architecture virtuelle

- Les avantages et les inconvénients de cette architecture sont résumés dans :

– Avantages :
  – Sécurité de la machine virtuelle.
  – Economie 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.
– Inconvénients :
  – Charge importante du système hébergeant les machines virtuelles.
  – Le choix du système virtuel est restreint à ceux qui sont compatibles.