Honeypot

29 langues

Cet article ne cite pas suffisamment ses sources (mars 2019).

Si vous disposez d'ouvrages ou d'articles de référence ou si vous connaissez des sites web de qualité traitant du thème abordé ici, merci de compléter l'article en donnant les **références utiles à sa vérifiabilité** et en les liant à la section « Notes et références ».

En pratique : Quelles sources sont attendues ? Comment ajouter mes sources ?

Dans le jargon de la sécurité informatique, un **honeypot** (en français, au sens propre « **pot de miel**[1] », et au sens figuré « **leurre** ») est une méthode de défense active qui consiste à attirer, sur des ressources (serveur, programme, service), des adversaires déclarés ou potentiels afin de les identifier et éventuellement de les neutraliser.

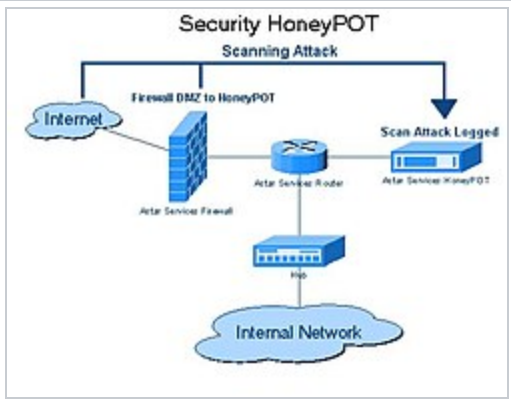

Schéma de principe d'un honeypot.

Le terme désigne à l'origine des dispositifs informatiques spécialement conçus pour susciter des attaques informatiques. Son usage s'est étendu à des techniques relevant de l'ingénierie sociale et du renseignement humain[2,3,4].

Principes de fonctionnement [modifier | modifier le code]

Le but de ce leurre est de faire croire à l'intrus qu'il peut prendre le contrôle d'une véritable machine de production, ce qui va permettre à l'administrateur d'observer les moyens de compromission des attaquants, de se prémunir contre de nouvelles attaques et lui laisser ainsi plus de temps pour réagir.

Une utilisation correcte d'un pot de miel repose essentiellement sur la résolution et la mise en parallèle de trois problématiques[5] :

- la surveillance ;
- la collecte d'information ;
- l'analyse d'information.

Surveillance [modifier | modifier le code]

Il faut partir du principe que toute information circulant sur le réseau à destination ou non du pot de miel est importante. De ce fait, la surveillance doit absolument être constante et doit porter aussi bien au niveau local

qu’au niveau distant. Cette surveillance de tous les instants repose sur :

- l'analyse du trafic réseau ;
- l'analyse pré compromission ;
- la journalisation des événements.

Collecte d'informations [modifier | modifier le code]

La collecte d’informations est possible grâce à des outils appelés renifleurs qui étudient les paquets présents sur le réseau et stockent les événements dans des bases de données. On peut également collecter des informations brutes grâce à des analyseurs de trames.

Analyse d'informations [modifier | modifier le code]

C'est grâce à l'analyse des informations recueillies que l'on va pouvoir découvrir les défaillances du réseau à protéger et les motivations des attaquants.

Différents types de pot de miel [modifier | modifier le code]

On compte deux types de pots de miel qui ont des buts et des fonctionnalités bien distincts :

- les pots de miel à faible interaction ;
- les pots de miel à forte interaction.

Pots de miel à faible interaction [modifier | modifier le code]

Ils sont les plus simples de la famille des pots de miel. Leur but est de recueillir un maximum d’informations tout en limitant les risques en offrant un minimum de privilèges aux attaquants.

On peut ranger, par exemple, la commande netcat dans cette catégorie. Netcat peut écouter un port particulier et enregistrer dans un journal toutes les connexions, ainsi que les commandes entrées. Ce programme permet donc d'écrire dans un fichier toutes les commandes entrées par des agresseurs. Cependant, ce type d’écoute reste très limité car il faut exécuter la commande pour chaque port que l'on souhaite observer.

Dans la même famille, on peut citer :

- *Honeyd* (en), de Niels Provos (en), qui est un pot de miel virtuel capable d’émuler des machines ou un réseau virtuel dans le but de leurrer les hackers. C’est l’un des pots de miel à faible interaction qui offre le plus de possibilités. Cependant, il ne permet pas de simuler tous les paramètres du système, ce qui le rend facilement repérable[6].
- *Specter*, qui permet d’émuler des services classiques (web, FTP, etc.). Il ne permet pas à l’attaquant l'accès total à un système d’exploitation, ce qui limite son intérêt.

Pots de miel à forte interaction [modifier | modifier le code]

Ce type de pot de miel peut être considéré comme le côté extrême du sujet puisqu'il repose sur le principe de l'accès à de véritables services sur une machine du réseau plus ou moins sécurisée.

Les risques sont beaucoup plus importants que pour les pots de miel à faible interaction. Il apparaît donc nécessaire de sécuriser au maximum l'architecture du réseau pour que l'attaquant ne puisse pas rebondir et s'en prendre à d'autres machines.

Les deux grands principes d'un tel pot de miel sont :

- le contrôle de données : pour observer le maximum d'attaques, le pot de miel à forte interaction doit accepter toutes les connexions entrantes et au contraire limiter les connexions sortantes pour éviter tout débordement. Cependant, il ne faut en aucun cas interdire toutes les connexions sortantes pour ne pas alerter l'attaquant. Un bon compromis entre sécurité et risque de découverte du leurre est donc nécessaire.
- la capture des données : avec un pare-feu ou un système de détection d'intrusion (SDI).
  - le pare-feu permet de *loguer* et de rediriger toutes les tentatives d'attaque aussi bien internes qu'externes.
  - le SDI permet d'enregistrer tous les paquets circulant pour pouvoir reconstruire la séquence d'attaque. Il peut permettre également, grâce aux iptables, de rediriger les paquets compromis vers le pot de miel. Il vient donc en complément d'un pare-feu et sert également de sauvegarde au cas où celui-ci tomberait.
  - les informations générées seront redirigées vers une machine distante et non stockées sur la machine compromise en raison du risque de compromission de ces données.

Il faut également relever l'existence de pots de miel plus spécifiques comme les pots de miel anti-spam ou anti-virus.

Projets en cours [modifier | modifier le code]

Un grand nombre de projets sur les pots de miel ont vu le jour pour collecter des informations sur les outils utilisés par les attaquants, leurs méthodes d'attaque et les failles de sécurité qu'ils exploitent, mais aussi et surtout leurs motivations.

The Honeypot Project [modifier | modifier le code]

The Honeypot Project[7] a pour objectifs :

- de faire prendre conscience de la réalité des menaces provenant d'Internet ;
- de donner toutes les informations nécessaires pour améliorer la protection des ressources ;
- de diffuser ses outils et stimuler la recherche pour accroître leur potentiel de recherche.

Autres projets [modifier | modifier le code]

On notera aussi d'autres projets intéressants :

- *HOSUS (HOneypot SUrveillance System)*, de Lance Spitzner ;

- *Honeypots : Monitoring and Forensics*, de Ryan Barnet ;
- *Florida Honeynet Project* ;
- (en) *Network of Affined Honeypots (NoAH) Project* [archive].
- Le projet MHN (Modern Honey Network [archive]) permet de déployer et gérer plusieurs solutions de pot de miel. Il est distribué sous licence GNU GPL.
- Le projet T-Pot ((Deutsche Telekom AG Honeypot Project) [archive]) permet de déployer et gérer plusieurs solutions de pot de miel. Il s'intègre avec Elasticsearch, Logstash, Kibana.

Notes et références [modifier | modifier le code]

1. ↑ « pot de miel [archive] », *Grand Dictionnaire terminologique*, Office québécois de la langue française (consulté le 14 mai 2020).
2. ↑ (en) David Dittrich, *The Ethics of Social Honeypots*, University of Washington, 4 décembre 2012, texte intégral [archive]
3. ↑ (en) Hugh Pickens, US Military Shuts Down CIA's Terrorist Honey Pot [archive], *Slashdot*, 19 mars 2010, consulté le 18 octobre 2013.
4. ↑ (en) Bruce Schneier, Highway Honeypot [archive], *Schneier on Security*, 15 septembre 2010, consulté le 18 octobre 2013.
5. ↑ Charline Zeitoun, « Virus et malwares : les chercheurs contre-attaquent [archive] », sur *CNRS Le journal*, 7 mars 2016 (consulté le 15 mai 2017)
6. ↑ « Qu'est-ce qu'un honeypot? [archive] », sur *IONOS Digitalguide* (consulté le 23 mars 2022)
7. ↑ Page d'accueil du *Project Honey Pot* [archive]

Voir aussi [modifier | modifier le code]

Articles connexes [modifier | modifier le code]

- Compagnonnage (botanique) : le même concept est utilisé en horticulture pour éviter que certaines plantes ne soient la cible de parasites en les attirant vers d'autres plantées à cet effet et ayant un effet toxique.

Liens externes [modifier | modifier le code]

- (en) *The Honeynet Project* [archive]
- (en) The Modern Honey Network project [archive]

v · m **Fuite d'information ou de données personnelles** [masquer]

Crimes et délits financiers	*Bahamas Leaks* · *CumEx Files* · *Football Leaks* · *FinCEN Files* · *Implant Files* · *Luxembourg Leaks* · *Malta Files* · *Mauritius Leaks* · *Offshore Leaks* · *OpenLux* · *Panama Papers* (personnes citées) · *Pandora Papers* (personnes citées (en)) · *Paradise Papers* (personnes citées) · *Suisse secrets* · *SwissLeaks*
Autres fuites	*BlueLeaks* · *Fuite des photos de personnalités d'août 2014* · *MacronLeaks* · *Uber Files*
Contre-mesures	Piège à canaris · **Honeypot**

v · m **Renseignement d'origine humaine** [masquer]

Acteurs	Agent · Agent dormant · Agent double · Agent clandestin · Agent de pénétration · Agent provocateur · Chef de poste · Agent d'influence · Analyste · Officier traitant · Honorable correspondant/Collaborateur officieux/Indicateur · Transfuge · *Walk-in*
Techniques	Traitement d'agent · Boîte aux lettres morte · Coupe-circuit · Stéganographie · Interrogatoire · **Honeypot** · Honey trapping · Couverture · Surveillance/Surveillance ciblée · Offuscation · Filature/Piquetage · Ingénierie sociale · Station de nombres · Kompromat/Provocation policière · Piège à canaris
Contre-mesures	Contre-espionnage · Harcèlement en réseau
Services de renseignement	Central Intelligence Agency · Direction générale de la Sécurité extérieure · Secret Intelligence Service · Service fédéral de renseignement · Service des renseignements extérieurs de la fédération de Russie · Defense Counterintelligence and Human Intelligence Center

Portail de la sécurité des systèmes d'information

Catégories : Logiciel de sécurité informatique | Matériel de sécurité informatique | Sécurité du réseau informatique | Cybercriminalité [+]
