Honeypot

Constantin Yamkoudougou

28 décembre 2005

Table des matières

1 Définition

Pour se prémunir des attaques sur Internet, les entreprises déploient des pare-feu, des sondes de détection d'intrusion et des techniques d'authentification dont la complexité varie du simple mot de passe à des systèmes biométriques. En dépit de toutes ces protections de nombreuses entreprises se font toujours piratées. Afin de mieux comprendre les techniques et les motivations profondes des attaquants, la communauté des professionnels de la sécurité utilise entre autres stratégies, les systèmes de pot de miel encore connus sous l'anglicisme "honeypot" . Un pot de miel est un système informatique qui a vocation à être attaqué et corrompu.

2 Typologies de honeypots ?

Il existe differentes catégories de honeypot selon le niveau d'interaction que l'on souhaite offrir aux attaquants. Lance Spitzner [ref7] les classe selon trois catégories : les honeypot de faible interaction, ceux de moyenne interaction et enfin ceux de grande interactivité.

- Les honeypots de très faible interaction se contentent de simuler certains services notoirement connus tels que l'activité apparente d'un serveur web, d'un serveur de messagerie, d'un serveur de transfert de fichier, etc. L'objectif de ce type de honeypot est par exemple d'identifier les adresses sources de pirates et aussi et surtout les premières commandes de base. Ce type de honeypot n'apporte guère d'information précise sur les procédés et les méthodes d'attaque.

- Les honeypots de moyenne interactivité fournissent un ensemble de services élaborés à l'attaquant. Ce type de honeypot est souvent déployé sur un poste hôte.

- Les honeypots de très grande interactivité fournissent des systèmes d'exploitation ou un réseau tout entier à l'attaquant. Ce dernier type de honeypot est souvent dédiés à la recherche comportementale et psychologique pour le profilage des pirates.

3 où peut-on se procurer des systèmes à utiliser dans la conception de pots de miel ?

Parmi les types de honeypot du marché, il existe une mosaique importante de systèmes qui peuvent être repartis en système de logiciels libres et

de logiciels sous licence privée. Parmi les plus connus, on peut citer :

- BackOfficer Friendly [ref0] est considéré aujourd'hui comme primaire et peut être installé sur un poste à domicile. Il permet de configurer simplement un petit nombre de services que l'on souhaite simuler et d'en recevoir une alerte en cas d'attaque distante.

- Specter [ref1] qui est un outils commercialisé par la société suisse SPECTER. En Avril 2003 il était à sa huitième version.

- ManTrap [ref2] qui est un pot de miel de très haute interactivité commercialisée par la société Recourse Technologies et permettant de simuler un véritable environnement virtuel pour les attaquants. Aux dernières nouvelles, la société Recourse aurait été acheté par l'éditeur Symantec.

- Honeyd [ref 3] est une technologie disponible en libre et qui permet de simuler des services ou une machine sur un système d'exploitation hôte. Honeyd est un projet initié par Niels Provos de l'université du Michigan. La première version de ce logiciel est publiée en avril 2002. Honeynet

- User Mode Linux [ref4] [ref5] est un une très bonne simulation d'un système Linux qui s'installe sur un autre système Linux hôte. Cette technologie permet de mettre en cage un attaquant sur un système non compromis.

- Vmware est un émulateur de PC en environnement Windows, Linux, Netware ou Solaris commercialisé par la société Vmware [ref6].

- Xen [ref8], technologie d'infrastructure de réseau virtuel bâtit à partir d'un projet libre

Malheureusement, la plupart des systèmes décrits sont reconnaissables par les attaquants. Chaque système possède une emprunte particulière qui est reconnue quand on interroge par exemple les interfaces réseaux, le processeur, la mémoire ou certains fichiers particuliers. La meilleure façon de déployer un honeypot est certainement d'utiliser de vraies machines avec un dimensionnement adéquat des services que l'on souhaite faire compromettre et surtout de trouver le moyen permettant d'éviter les attaques par rebond.

ref0 http ://www.nfr.com/resource/downloads/back-officer-friendly.tar

ref1 http ://www.specter.ch/introduction50.shtml

ref2 http ://www.tracking-hackers.com/solutions/

ref3 http ://www.honeyd.org/

ref4 http ://usermodelinux.org/

ref5 http ://user-mode-linux.sourceforge.net/

ref6 http ://www.vmware.com/

ref7 http ://www.spitzner.net/

ref8 http ://www.xensource.com/

4 Pour ou contre l'idée que l'on peut protéger des réseaux d'entreprise par un pot de miel ?

Dans le domaine des honeypots, il existe classiquement deux écoles. Ceux qui pensent que le déploiement de ces systèmes est très dangereux et favorise la compromission d'autres systèmes notamment par les attaques par rebonds. On comprend ces détracteurs de honeypots dans la mesure où cela engage la responsabilité civile des entreprises voire la responsabilité pénale du personnel ayant déployé le honeypot. La seconde école pense qu'ils aident à une meilleure protection de l'infrastructure de réseau. Ce second point de vue suppose implicitement une excellente maîtrise de la technologie mise en oeuvre pour couver et garder les activités malveillantes hors du périmètre de sécurité de l'entreprise. En fait, un honeypot peut aider à la protection d'un réseau s'il est reconnu comme tel par un attaquant qui penserait alors qu'on lui tend un piège. Il s'agit dans ce cas de mettre en exergue le rôle dissuasif du honeypot au service de la protection. Cependant, ce cas de figure ne tient pas compte de la majorité des attaques sur internet qui sont conduites par des non spécialistes et qui restent encore aveugles en utilisant des robots qui ne font pas la part des choses entre Honeypot et système ordinaire.

Pour les entreprises traquant véritablement les pirates, le honeypot n'est efficace que s'il n'est pas détectable. Ce type de honeypot capture le trafic illégime qui était destiné a priori à des environnements de production. L'analyse de ce trafic permet de renforcer la protection des serveurs de production si ceux-ci ne sont pas encore corrompus.

Certains types de honeypots comme le LaBrea Tarpit [ref 1] ont la possibilité de ralentir certaines attaques telles que la propagation de vers. Il s'agit là d'un honeypot qui concoure directement à la protection des réseaux.

Enfin, dans tous les cas, un honeypot à lui tout seul ne saurait assurer la protection d'une infrastructure de réseau. La meilleure protection contre les attaques demeure donc la mise à jour de pare-feu, l'application de patches de sécurité, l'application et le suivi d'une bonne politique de sécurité dans l'entreprise.
Le honeypot est un outil complémentaire qui permet de mieux comprendre les methodes et les mobiles des attaquant pour mieux anticiper la protection d'un réseau.

ref 1 http ://labrea.sourceforge.net/

5 Peut on utiliser les pots de miel comme systèmes de détection d'intrusion ?

Il existe classiquement deux types de systèmes de détection d'intrusion pour les réseaux. Les systèmes à fonctionnement statistique et ceux qui reposent sur les d'attaques dont la signature est connue. Les systèmes statistiques reposent sur l'apprentissage du comportement statistique du réseau : moyenne de paquets, typologie des paquets et des services à des moments déterminés. La plupart du temps il faut une longue période d'apprentissage à ce type de système pour être opérationnel. Les systèmes à base de signature fonctionnent comme les anti-virus, ils ont constamment besoins d'être mis à jour face à de nouvelles attaques. Le moindre manquement de mise à jour peut être fatal à une entreprise qui risquerait d'être victime des attaques les plus récentes. Quelle que soit la typologie du système de détection d'intrusion les écueils les plus recurents sont l'existence d'un taux de faux positifs et de faux négatifs que chaque administrateur tente de réduire désespérément. Les faux positifs sont des alertes d'attaques non réels. Plus il y a de faux positifs générés par un système de détection d'intrusion plus la vigilance s'estompe en matière de surveillance à cause de l'effet d'accoutumance que cela crée au sein du personnel d'administration. Les faux négatifs sont de véritables attaques que le système de détection d'intrusion considère comme du trafic licite. Aujourd'hui, il existe quantité d'outils qui permettent de débrider certaines attaques même notoire pour les rendre indecélables par un système de détection d'intrusion. Par exemple ADMmutate [ref1] en est un. Il permet de modifier la signature de certaines attaques afin de les rendre imperceptible par le système de détection.
Quel rôle un système de pot de miel peut - il donc apporter dans dans un environnement de système de détection d'intrusion ?

On peut par exemple mettre en place dans une zone démilitarisée des systèmes de pot de miel dont on ne renseigne pas les adresses de réseaux dans les serveurs de noms afin d'éviter toute corrélation avec les serveurs officiels de production. Compte tenu de l'ignorance des adresses dédiées au système de pot de miel par le système de noms d'Internet, tous trafic reçu par ce type de pot de miel est nécessairement illicite. Par conséquent, toute alerte d'attaque sur un service ciblé sur le pot de miel vaudra alors pour les services du même type en environnement de production. Cela permet au moins au personnel de sécurité de mieux investiguer ce type d'attaque qui ne sont pas de faux positifs.

Les systèmes de pot de miel ne remplaceront certainement jamais les systèmes de détection d'intrusion qui sont destinés à fonctionner en environnement de production mais sont un outils complémentaire voire indispensable dans certains cas à une politique d'analyse et de détection d'intrusion.

ref1 http ://www.ktwo.ca/security.html

6 Risques encourus par une entreprise utilisant des pots de miel ?

Les pots de miel ne sont pas sans risque. Les attaquants sont toujours à la recherche de système de rebond afin de cacher au mieux les traces qu'ils laissent sur internet. La prise en main d'un honeypot peut alors devenir avantageuse dans ce cas pour prendre le contrôle d'autres systèmes. Ce risque est plus ou moins important selon la typologie des honeypots déployés. Il est mineur voire quasiment impossible pour les systèmes de faible interaction tels que Back Officer friendly, Specter ou le projet open source Honeyd. Le risque est vraiment sérieux pour des systèmes tels que Vmware, ManTrap et systèmes d'exploitation tout entier dédiés aux attaquants. Les honeypots posent également un certain nombre de risques juridiques. A-t-on le droit capturer et d'analyser des trafic tiers fussent-ils des attaques. A-t-on le droit de déployer des systèmes expressément vulnérables pour les faire compromettre ? quels sont les risques encourus en matière de cyber criminalité par l'entreprise ou le particulier dans un scénario d'attaque par rebond ? A-t-on le droit d'enregistrer des communications de pirates sur canal IRC par exemple ? Selon les pays, les droits des pirates varie, ce qui peut entraver une traque sérieuse. Il importe donc de s'enquérir des responsabilités juridiques et des risques encourus avant de déployer des honeypot de très grande interaction.

7 Peut-on utiliser les pots de miels en tant qu'outils de collecte de preuve recevable devant un tribunal ?

Lorsqu'une attaque réussie est détectée, il est nécessaire de se doter d'une possibilité de répondre au niveau technique et juridique à cet événement. La poursuite judiciaire d'un attaquant suppose la constitution de preuve légale devant les tribunaux. Les traces laissées par un attaquant sur un honeypot sont - elles utilisables comme preuve légale ?. Ne peut-on pas évoquer en faveur du pirate, le motif de provocation et de consentement de la victime lors de la compromission d'un honeypot. De plus, toujours en la faveur de l'attaquant, ne peut-on pas qualifier l'acte de transmission de données du système compromis vers son ordinateur de délit d'intrusion sur son poste. D'une manière générale, pour qu'une infraction soit reconnue il faut qu'elle soit réprimée par un texte, que l'auteur ait eu l'intention de la commettre et qu'il ait réalisé matériellement cette infraction [ref 1]. La saisine d'un tribunal est donc loin d'être triviale en cas de cyber compromission puisse qu'il faut prouver qu'on n'a non seulement été victime d'une attaque mais aussi que telle était la véritable intention de l'attaquant. Sur le plan technique, les honeypots peuvent aider à la constitution de preuves matérielles à condition que celles-ci soient récoltées par des spécialistes de la cybercriminalité : les fameux "foreinsics". La saisie du poste de l'attaquant et l'analyse des fichiers est également nécessaire pour corroborer les événements d'une attaque. En France, sur le plan moral et légal l'article 323-1 [ref 2] du code pénal réprime la pénétration frauduleuse d'un réseau. Reste à prouver l'intention de celui avec de bon avocats pour gagner un procès. Pour ne pas porter atteinte à leur image par des procès médiatiques, les entreprises ne portent pratiquement jamais plainte et de ce fait il n'existe pratiquement aucun chiffre fiable sur les entreprises compromises ni de retour d'expérience après compromission, ce qui est fort dommage !

ref 1 confère article Misc 11, page 8, Elisabeth STELLA, Thierry MARTINEAU.

ref 2 http ://www.celog.fr/cpi/codepenal.htm

8 Références complémentaires

http ://www.tracking-hackers.com/papers/honeypots.html

http ://www.projecthoneypot.org/

http ://www.honeypots.net/

http ://www.lucidic.net/