Honey, devine qui vient butiner ce soir?

par tAd pour le Jack

HoneyWut ?

« Un honeypot (pot de miel) 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. » **Wikipédia**

HoneyPot SSH

Basé sur Kippo/Cowrie:

But : émuler un shell tout en restant « en cage ».

.Fonctionnel
.Facile à administrer
.Facile d'installation

(git, quelques paramètres à éditer, password list, une règle de NAT)

/!\ dédier le matériel utilisé pour ce genre de jeu!

HoneyPot? Pourquoi?

.Pour le fun, ~~la gloire et l'argent~~!
.L'analyse de menaces (récupération de binaires/scripts)
.L'analyse de déroulés d'attaques
.Sensibilisation
.Essayer de profiler de potentiels attaquants

→ Apprendre

Approche « HaaH »
(Honeypot as a Hobby)

HoneyPot? Comment?

.Choix de login/password ciblés (en fonction de ce que l'on cherche)

.Rendre le système émulé le plus original possible (fingerprint SSH, hostname, users déclarés, …)

HoneyPot? Quoi?

Récupération de:

.liste de logins / mots de passe

(~34.000 paires sur 14 mois)

```
1220 [root/!@]
1150 [admin/admin]
1000 [root/root]
 900 [root/password]
 892 [root/123456]
 806 [root/admin]
 772 [root/1234]
 770 [root/12345]
 767 [root/wubao]
 764 [root/123]
 745 [root/p@ssw0rd]
 738 [root/1]
 725 [root/jiamima]
 716 [root/root123]
 713 [root/test]
 701 [root/!]
 695 [root/!q@w]
 667 [root/!qaz@wsx]
 665 [root/idc!@]
```

```
661 [root/admin!@]
445 [admin/12345]
424 [admin/1234567890]
264 [admin/aaaaaa]
208 [admin/password]
167 [admin/root]
153 [admin/Saint]
152 [admin/default]
149 [root/]
143 [admin/123456]
130 [ftpuser/asteriskftp]
127 [admin/Paris]
125 [admin/Sauvelade]
122 [admin/Unknown]
115 [admin/123456789]
115 [admin/password1]
100 [guest/guest]
 90 [ubnt/ubnt]
 84 [root/-]
 80 [root/qwerty]
```

```
78 [root/123456789]
74 [root/12345678]
74 [test/test]
72 [a/a]
70 [admin/1234]
70 [root/1234567890]
64 [oracle/oracle]
64 [root/toor]
60 failed
60 [pi/raspberry]
60 [root/123123]
57 [admin/admin123]
57 [root/abc123]
57 [root/changeme]
57 [root/q1w2e3r4]
56 [admin/]
56 [root/111111]
56 [root/1234567]
```

HoneyPot? Quoi?

Récupération de:

.binaires/scripts d'exploitation (DDoS, Bruteforcers, …)

(155 samples différents sur 14 mois)

```
 37  ASCII text
  1  ASCII text, with CRLF line terminators
  1  a /usr/bin/perl  script executable (binary data)
  6  a /usr/bin/perl script executable (binary data)
 17  Bourne-Again shell script, ASCII text executable
  1  C source, ASCII text, with very long lines, with CRLF line terminators
  1  data
  1  ELF 32-bit LSB executable, ARM, EABI4 version 1 (SYSV), statically linked, not stripped
  2  ELF 32-bit LSB executable, ARM, EABI5 version 1 (GNU/Linux), statically linked, stripped
  2  ELF 32-bit LSB executable, ARM, EABI5 version 1 (SYSV), statically linked, for GNU/Linux 2.6.16, not stripped
  2  ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, not stripped
  4  ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, for GNU/Linux 2.6.18, not stripped
  1  ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, for GNU/Linux 2.6.26, BuildID[sha1]=a83831b8b3c28d
  4  ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, stripped
  1  ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.32,
 15  ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.2.5, not stripped
  1  ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.2.5, not stripped, too many notes (256)
 14  ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped
  3  ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, not stripped
```

HoneyPot? Qui?

Plusieurs profils:

.Outils de bruteforce: connexion OK, déconnexion.

.Robots: connexion, déroulé de scénario, déconnexion.

.Humain: connexion, tentatives parfois (très) maladroites de déroulé de scénario, déconnexion.

HoneyPot? Qui?

Plusieurs profils:

(Démos playlog Cowrie)

HoneyPot? Donc?

On peut en tirer plein de savoir:

.On ne laisse pas accessible quelque équipement que ce soit, accessible sur un réseau, sans un mot de passe correct…

.On peut apprendre des modes d'opération:

- **Détection d'un honeypot**
- **Effacer efficacement ses traces (ou presque)**

.Pour qui cherche, on doit pouvoir remonter des parties de botnets, les analyser, les fliquer, ...

Merci :)