

Utilizando Honeypots como Ferramenta de Segurança



Humberto Sartini
<http://web.onda.com.br/humberto>

Palestrante

Humberto Sartini

- Analista de Segurança do Provedor Onda S/A
- Participante dos projetos:
 - Rau-Tu Linux (<http://www.rau-tu.unicamp.br/linux/>)
 - HoneypotBR (<http://www.honeypot.com.br/>)
 - RootCheck (<http://www.ossec.net/rootcheck/>)
- Palestrante no:
 - IV e V Fórum Internacional de SL
 - Conferência Internacional de SL (Curitiba - 2003)

Tópicos

- O que é Honeyypot
- A história dos Honeyypots
- Tipos de Honeyypots
- Níveis de Interação
- Honeyynet - Conceito
- Projeto HoneyypotBR
- Logs Honeyypot
- Instalação

O que é Honeypot ?

- Honeypot = Pote de Mel
- Ferramenta de estudo de segurança, onde sua função principal é colher informações do atacante
- Elemento atraente para o invasor, ou melhor, uma iguaria para um hacker

O que é Honeypot ?

“Um honeypot é um recurso de rede cuja função é de ser atacado e comprometido (invadido). Significa dizer que um Honeypot poderá ser testado, atacado e invadido. Os honeypots não fazem nenhum tipo de prevenção, os mesmos fornecem informações adicionais de valor inestimável”

Lance Spitzner - 2003

O que é Honeyypot ?

É um sistema que possui falhas de segurança, reais ou virtuais, colocadas de maneira proposital, a fim de que seja invadido e que o fruto desta invasão possa ser estudado

A história dos Honeyypots

- “The Cuckoo's Egg” de Clifford Stool
 - Durante 10 meses (1986/87)
localizou e encurralou o hacker
Hunter
 - Técnicas utilizadas são as
precuroras dos Honeyypots atuais

A história dos Honeypots

- “An evening with Berferd” de Bill Cheswick (1991)
 - Durante meses estudou as técnicas e criou armadilhas para o hacker Berferd, que utilizava-se de um bug do Sendmail
 - Primeiro “paper” com grande teor técnico e metodologia

A história dos Honeypots

- DTK – Deception Toolkit
 - Primeiro Honeypot “real”
 - Criado por Fred Cohen (1997)
 - Scripts em Perl e C que simulam vários servidores
 - Software Livre
 - Utilizado nos dias de hoje

A história dos Honeypots

- Sting – Cybercop (NAI)
 - Primeiro produto comercial
 - Utilizado em ambiente Windows NT
 - Simulava uma rede inteira
 - Emitia respostas falsas para os atacantes simulando diversos ambientes operacionais

A história dos Honeyypots

- Projeto Honeyynet (1999)
 - Lance Spitzner (ex-militar) e mais 30 especialistas
 - Desenvolveu metodologias
 - Tornou-se referência
 - Autor de “Know Your Enemy” - “Conheça o seu Inimigo”

A história dos Honeypots

- Captura de Worms (2001 / 2002)
 - CodeRed II e W32/LeavesWorm
- Captura do primeiro exploit desconhecido (2002)
 - Dtspcd (CDE Subprocess Control Service Server)
 - Vulnerabilidade reportada pelo CERT em 2001

A história dos Honeypots

- Honeyd – 2002
 - Niels Povos
 - Suporta hosts virtuais
 - Simula SO em nível de pilha TCP/IP, dificultando descoberta de SO remotamente
 - Suporta TCP, UDP e ICMP
 - Simula redes (arpd)

Tipos de Honeyypots

- Honeyypots de pesquisa
 - Acumular o máximo de informações dos atacantes e suas ferramentas
 - Alto grau de comprometimento
 - Redes externas ou sem ligação com rede principal

Tipos de Honeyypots

- Honeyypots de produção
 - Ferramenta para diminuição de riscos
 - Elemento de distração ou dispersão
 - Não adiciona nenhum tipo de vantagem à estrutura de segurança

Níveis de Interação

- Baixa Interatividade
 - Serviços Falsos
 - Listener TCP/UDP
 - Respostas Falsas

```
nc -l -p 80 > /var/log/honey80.log
```


Níveis de Interação

- Média Interatividade
 - Ambiente falso
 - Cria uma ilusão de domínio da máquina
 - Estudo melhor das técnicas utilizadas
 - Invadir o sistema realmente !!

Níveis de Interação

- Alta Interatividade
 - SO com serviços comprometidos (isca)
 - Não perceptível ao atacante
 - Estudo melhor das técnicas utilizadas
 - Vários riscos:
 - Utilização como trampolim
 - Repositório de informações roubadas
 - Entrada para rede real do Honeypot

Honeynet - Conceito

Rede altamente controlada, formada por Honeypots “reais” ou “virtuais” com o intuito de monitorar, capturar e analisar todas as atividades registradas. Geralmente executam sistemas operacionais e aplicativos idênticos aos sistemas de produção

Honeynet - Conceito

Composta por:

- Honeypots
- Equipamentos de interconexão e contenção de fluxo (Roteador, Switch, Firewall, etc)
- Componentes de captura, armazenamento e análise de dados (Servidor de Log, Scripts, etc)

Honeynet - Conceito

- Honeynet Real
 - Honeypots reais (várias máquinas reais)
 - Ficam descentralizados
 - Necessita de muito espaço físico e grande tempo de instalação e manutenção dos sistemas

Honeynet - Conceito

- Honeynet Virtual
 - Honeypots virtuais (única máquina com emulador)
 - Pouco espaço físico e instalação rápida
 - Grande carga, necessita de máquina mais robusta, um único ponto de acesso

Projeto HoneyPotBR

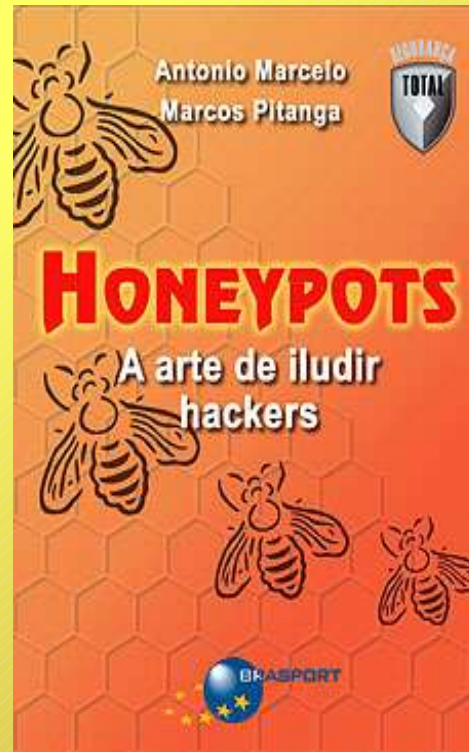
- Surgiu através de um grupo de especialistas em segurança e pesquisadores independentes
- Inspirado no Projeto HoneyNet de Lance Spitzner

Projeto HoneyPotBR

- Ferramentas
 - Fake Echo – Daniel B. Cid
 - Fake Ftp – Fabio Henrique
 - Fake Http – Adriano Carvalho
 - Fake Pit – Antonio Marcelo
 - Fake Pop3 – Humberto Sartini
 - Fake Smtip – Daniel B. Cid
 - Fake Squid – Antonio Marcelo

Projeto HoneyPotBR

Honeypots – A arte de iludir hackers
Antonio Marcelo e Marcos Pitanga



Logs Honeypot

- Logs FakeEcho

Fri Feb 6 04:51:20 2004 fakeecho log -
Connection from 200.175.243.28:1467

Fri Feb 6 04:52:49 2004 fakeecho log -
Connection from 200.175.243.28:1469

Logs Honeypot

- Logs FakeHttpd

Fri May 28 11:13:16 2004 fakehttpd log -
Connection from 222.40.48.77:2678

GET

http://dc.tickerbar.net:42857/tld/pxy.m?nc=1
7093090 HTTP/1.0 : Ataque WEB ! Tentativa
de execucao de comando

Logs Honeypot

- Logs FakeHttpd

Fri Feb 20 00:20:40 2004 fakehttpd log -
Connection from 203.115.20.2:3283

GET /scripts/nsiislog.dll : Ataque WEB ! Tentativa
de execucao de comando

Fri Feb 20 10:30:42 2004 fakehttpd log -
Connection from 200.190.217.51:59954

GET /scripts/..%255c255c../winnt/system32/
cmd.exe?/c+dir : Ataque WEB ! Tentativa de
execucao de comando

Logs Honeyypot

- Logs FakeSmtplib

Thu May 13 10:29:06 2004 fakesmtp log -
Connection from 218.18.41.186:4084

HELO 200.200.200.200 :

MAIL FROM:<smtp2001soho@yahoo.com> :

RCPT TO:<popo.gigi@msa.hinet.net> :

DATA :

QUIT :

Logs Honeypot

- Logs FakeSmtplib

Received: from g83r.lnimp.net (HELO uvgr)
[115.23.107.44] by 200.200.200.200 with SMTP for
<wjuuberich@yahoo.com.tw>; Thu, 15 Apr 2004
19:20:40 +0600

Message-ID: <uj57y-j13x0-8@thmtl3>

From: "" <jas@ms9.hinet.net>

To: <wjuuberich@yahoo.com.tw>

Subject: BC_200.200.200.200

Date: Thu, 15 Apr 04 19:20:40 GMT

Logs Honeypot

- Logs FakeSquid

Wed Feb 18 05:02:44 2004 fakesquid log -
Connection from 64.222.144.163:1031

GET http://www.yahoo.com/ HTTP/1.1 : Ataque WEB !
Tentativa de execucao de comando

Wed Feb 18 10:32:22 2004 fakesquid log -
Connection from 200.217.90.207:3707

CONNECT irc.brasnet.org:6667 HTTP/1.0 :

Wed Feb 18 10:33:35 2004 fakesquid log -
Connection from 200.217.90.207:3780

CONNECT irc.brasnet.org:6667 HTTP/1.0 :

Logs Honeypot

- Logs FakeSquid

Mon May 10 09:44:24 2004 fakesquid log -
Connection from 218.27.4.199:38332

GET http://www.ebay.com/ HTTP/1.1 : Ataque
WEB ! Tentativa de execucao de comando

Mon May 10 12:56:36 2004 fakesquid log -
Connection from 200.222.197.254:3258

GET http://www.hellabs.com.ua/cgi-bin/
textenv.pl?3128 HTTP/1.0 : Ataque WEB !
Tentativa de execucao de comando

Logs Honeypot

- Logs FakeSquid

Wed Feb 18 05:02:44 2004 fakesquid log -
Connection from 64.222.144.163:1031

GET http://www.yahoo.com/ HTTP/1.1 : Ataque WEB !
Tentativa de execucao de comando

Wed Feb 18 10:32:22 2004 fakesquid log -
Connection from 200.217.90.207:3707

CONNECT irc.brasnet.org:6667 HTTP/1.0 :

Wed Feb 18 10:33:35 2004 fakesquid log -
Connection from 200.217.90.207:3780

CONNECT irc.brasnet.org:6667 HTTP/1.0 :

Instalação

1) Configuração do Sistema

```
groupadd honeypot
```

```
adduser -g honeypot -s /bin/false  
-d /home/honeypot honeypot
```

Instalação

2) Instalação do Honeyperl

Fonte: <http://web.onda.com.br/humberto/arquivo/honeyperl-0.0.7.tar.gz>

```
cd /home/honeypot
tar xzvpf honeyperl-0.0.7.tar.gz
mv honeyperl-0.0.7/* .
rm -rf honeyperl-0.0.7/
chown -R fake:fake *
chmod -R 600 *

find . -type d -exec chmod 700 {} \;
find . -iname '*.pl' -exec chmod 700 {} \;
```

Instalação

3) Módulos Perl

Execute o programa abaixo para verificar se existem os módulos do Perl:

```
./verify.pl
```

Caso não exista algum módulo, execute o comando referente ao módulo a ser instalado:

```
perl -MCPAN -e 'install strict'
```

```
perl -MCPAN -e 'install IO::Socket'
```

```
perl -MCPAN -e 'install Term::ANSIColor'
```

Instalação

4) Estrutura do Honeyperl

conf -> Arquivos de Configuração

docs -> Documentação

fakes -> Código dos servidores e respostas

firewall -> Scripts do Firewall

honeyperl.pl -> Programa principal

logs -> Diretório de Logs

modules -> Diretório de Módulos

verify.pl -> Checa módulos do Perl

Instalação

4) Editando o honeypert.pl

- Poucos parâmetros devem ser alterados, somente se houver necessidade, entre eles:

Formato dos Logs:

```
#$logfile="logs/$diames-$mes-$ano($hor:$min:$seg).log";  
$logfile="logs/$ano$mes$diames.log";
```

Instalação

4) Editando o honeypperl.pl

```
$server = IO::Socket::INET->new (  
  Proto => 'tcp',  
  ## Caso o servidor tenha mais de um IP e seja  
  necessario rodar em um especifico  
  LocalAddr => 'ENDERECO_IP';  
  LocalPort => $porta,  
  Listen => SOMAXCONN,  
  Timeout => 60,  
  ReuseAddr => 1) or die "Falha ao iniciar o  
$fake $!" unless $server;
```

Instalação

5) Editando o conf/honeyperl.conf

dominio=dominio.com.br

email=usuario@dominio.com.br

usuario=honeygot

terminal=sim/nao

Instalação

5) Editando o conf/honeyperl.conf

→ Caso queira desabilitar alguma FAKE é necessário adicionar "#" no inicio da linha correspondente:

```
# ECHO
```

```
fakeecho:echo::7:Echo emul
```

```
# FTP
```

```
fakeftp:ftp:conf/fakeftp.conf:21:Ftp emul
```

```
# HTTP
```

```
fakehttpd:httpd:conf/httpd.conf:80:Httpd emul
```

```
# PIT - Generico
```

```
fakemit:pit::20001:Pit emul
```

```
# POP3
```

```
fakemop3:pop3:conf/pop3.conf:110:Pop3 emul
```

```
# SQUID
```

```
fakesquid:squid:conf/fakesquid.conf:3128:Squid Emul
```

```
# SMTP
```

```
fakesmtp:smtp:conf/fakesmtp.conf:25:Smt emul
```

Instalação

6) Arquivos dos FAKES

→ Os outros arquivos do diretório "conf" servem para configurar qual a versão do software irá rodar e arquivos de logs.

Configuracao do FAKE POP3:

conf/pop3.conf

→ Altere a variavel "\$serveremul" para teapop, qpopper ou pop3

Agradecimentos



<http://www.onda.com.br>

Contato

- Através do site ou e-mail

<http://web.onda.com.br/humberto>

humberto@onda.com.br

Perguntas e Respostas

Espaço aberto para
perguntas e dúvidas !!!

Obrigado !

Links

- Projeto HoneyPotBR

<http://www.honeypot.com.br>

- Outros HoneyPots e Documentos

<http://www.honeynet.org>

<http://www.honeypots.net>

<http://www.lac.inpe.br/security/honeynet>