Honeypots

Ferramentas de estudo de segurança

Projeto HoneyPotBR

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/)
- Palestrante no:
  - IV Fórum Internacional de SL (Porto Alegre – 2003)
  - Conferência Internacional de SL (Curitiba - 2003)

Tópicos

- O que é um Honeypot
- A história dos Honeypots
- Tipos e Níveis de Honeypots
- Projeto HoneypotBR
- Contato
- Perguntas e Respostas
- Links

O que é um Honeypot ?

- Honeypot = Pote de Mel

- Ferramenta de estudos 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 um Honeypot ?

"Um honeypot é um recurso de rede cuja função é de ser atacado e compremetido (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 um HoneyPot ?

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

A história dos Honeypots

- “The Cuckoo's Egg” de Cliford Stool
  - Durante 10 meses (1986/87) localizou e encurralou o hacker Hunter.
- “An evening with Berferd” de Bill Cheswick
  - Durante meses estudos as técnicas e criou armadilhas para o hacker Berferd.

A história dos Honeypots

- DTK – Deception Toolkit
  - 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)
  - Utilizado em ambiente Windows NT
  - Simulava uma rede inteira
  - Emitia respostas falsas para os atacantes simulando diversos ambientes operacionais

A história dos Honeypots

- Projeto Honeynet (1999)
  - Lance Spitzner e mais 30 especialistas
  - Desenvolveu metodologias
  - Tornou-se referência

A história dos Honeypots

- Captura de Worms (2001 / 2002)
  - CodeRed II e W32/LeavesWorm
  - Dtspcd (CDE Subprocess Control Service Server)

- Honeyd – 2002
  - Niels Povos
  - Honeypot Open Source

Tipos e Níveis de Honeypots

- Honeypots de pesquisa
  - Acumular o máximo de informações dos atacantes e suas ferramentas
  - Grau alto de comprometimento
  - Redes externas ou sem ligação com rede principal

Tipos e Níveis de Honeypots

- Honeypots de produção
  - Diminuir risco
  - Elemento de distração ou dispersão

Tipos e Níveis de Honeypots

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

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

Tipos e Níveis de Honeypots

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

Tipos e Níveis de Honeypots

- Alta Interatividade
  - SO com serviços comprometidos
  - Não perceptível ao atacante
  - Estudo melhor das técnicas utilizadas
  - Vários riscos:
    - Utilização como trampolim
    - Repositório de informações roubadas

Projeto HoneypotBR

- Surgiu através de um grupos de especialistas em segurança e pesquisadores independentes

- Inspirado no Projeto Honeynet de Lance Spitzner

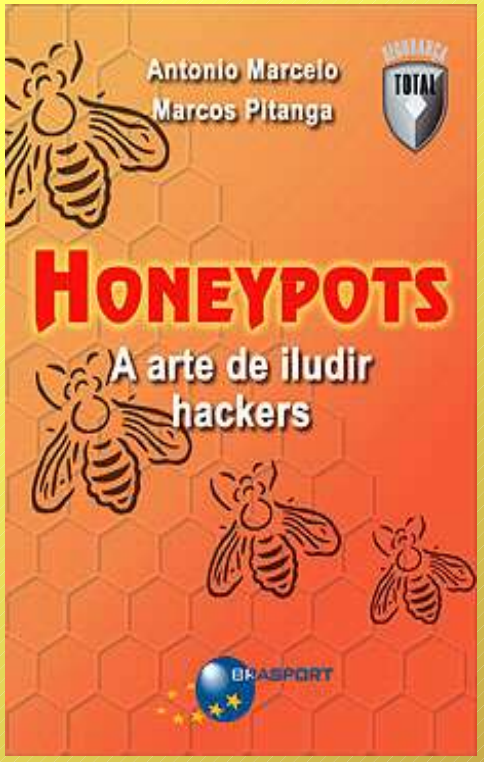
Projeto HoneypotBR

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

Projeto HoneypotBR

Honeypots – A arte de iludir hackers

Antonio Marcelo e Marcos Pitanga



Projeto HoneypotBR

- Logs FakeHttpd

Tue Sep 30 20:04:35 2003 fakehttpd log - Connection from 200.195.95.66:4154

GET /
default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090%
u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%
u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%
u53ff%u0078%u0000%u00=a HTTP/1.0 : Ataque WEB !
Tentativa de execucao de comando

Projeto HoneypotBR

- Logs FakeSmtp

Thu Oct 2 16:48:58 2003 fakesmtp log - Connection from 200.195.139.30:2541
POST / HTTP/1.0 :
Content-Type: application/octet-stream :
Content-Length: 698 :
Via: 1.1 portal.redexsol.com:3128 (Squid/2.4.STABLE7) :
X-Forwarded-For: 64.216.218.32 :
Host: 200.200.200.200:
Cache-Control: max-age=259200 :
Connection: keep-alive :
HELO 200.195.147.185 :
MAIL FROM:<annieb1980@yahoo.com> :
RCPT TO: <jimrant@flashmail.com> :
RCPT TO: <brucert@acmemail.net> :
RCPT TO: <tupperhorse3@aol.com> :
RCPT TO: <leroydert@swbell.net> :
RCPT TO: <garyhottie@hotmail.com> :
RCPT TO: <bobbiepmcginnis@gofree.co.uk> :
RCPT TO: <tupperhorse3@yahoo.com> :
DATA :
QUIT :

Projeto HoneypotBR

- Logs FakeSmtp

Message-ID:
<05004804804604905705304604905705204605405 7@200.195.194.69>
To: <cybershark55@hotpop.com>
From: crystalalpinekid@yahoo.com
Subject: Information for you
Date: Mon, 08 Sep 2003 14:18:24 -1900
MIME-Version: 1.0
Content-Type: text/plain; charset="Windows-1252"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.3018.1300
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.3018.1300
052046051056046049048056046049056058078079084058054048054058049058

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

  http://www.honeynet.org

  http://www.honeypots.net

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