INSTALAÇÃO E USO DE HONEYPOT DE BAIXA INTERATIVIDADE

Lucio Henrique Franco, Luiz Gustavo C. Barbato e Antonio Montes

{lucio.franco,gustavo.barbato,antonio.montes}@cenpra.gov.br.

Centro de Pesquisas Renato Archer - CenPRA/MCT

Rodovia Dom Pedro I, km 143,6

Bairro: Amarais - Campinas - SP - Brasil

Objetivo

Este curso visa apresentar as armadilhas para invasores de sistemas, conhecidas como honeypots, e seu uso como ferramenta de pesquisa. As discussões vão se centrar em honeypots de baixa interatividade, sua origem, finalidade, vantagens e desvantagens das soluções mais conhecidas. Baseado na ferramenta honeyd, será mostrado como instalar e configurar um honeypot, como monitorar e acompanhar os logs gerados, como criar novos emuladores e utilizar algumas das ferramentas de apoio e análise desenvolvidas para esta solução.

Roteiro

- Histórico sobre Honeypots e Honeynets
- Taxonomia dos Honeypots
- Honeypots de Baixa Interatividade
- Arquitetura do Honeyd
- Criação de Listeners e o uso deles no Honeyd
- Instalação e Configuração do Sistema
- Monitoração do Honeyd
- A Ferramenta Honeydsum
- HOACD
- Resultados obtidos

Ferramentas de Pesquisas

- *Honeypots*

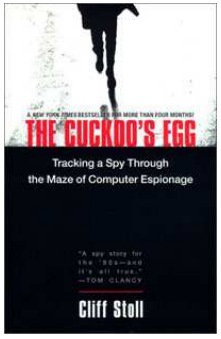
  - *São recursos computacionais dedicados a serem sondados, atacados ou comprometidos, num ambiente que permita o registro e controle dessas atividades.*

- *Honeynets*

  - *São redes compostas de uma sub-rede de administração e de uma sub-rede de honeypots*

Breve histórico sobre Honeypots

- Clifford Stoll (1988)

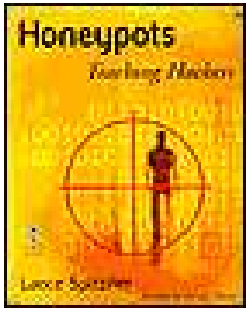


  - *The Cuckoo's Egg*
  - LBL - Lawrence Berkeley Laboratory
  - Monitoração das atividades do invasor

- Bill Cheswick (1992) / Steven M. Bellovin (1992)
  - *Gateway* preparado para ser comprometido
  - Bell Labs - AT&T
  - Aplicações Falsas (FTP, Telnet, SMTP, Finger ...)

Breve histórico sobre Honeypots (cont.)

- Lance Spitzner (2002)

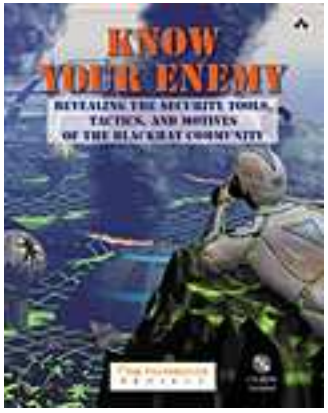


  - *"Um recurso de segurança preparado para ser sondado, atacado ou comprometido"*

- Marty Roesch (2003)
  - *Honeypots de produção: diminuir os riscos e ajudar a proteger as redes das organizações;*
  - *Honeypots de pesquisa: estudar e obter informações da comunidade dos atacantes.*

Breve histórico sobre Honeynets

- *The Honeynet Project* (2001)



  - Aprender com os atacantes
  - Ambiente para capturar os dados
  - Ferramenta de pesquisa
- A **contenção de dados**: impedir que os atacantes, após invadirem a *honeynet*, a utilize para atacar outras redes;
- A **captura de dados**: coletar o maior número possível de informações, com o objetivo de promover um estudo detalhado dos passos dos atacantes.

`http://www.honeynet.org`

Breve histórico sobre Honeynets (cont.)

- *Honeynet Research Alliance*
  - Instituições envolvidas com pesquisa de *honeynets*
- *Honeynet.BR* (2002)
  - Atividades maliciosas na Internet brasileira

`http://www.honeynet.org.br`

Finalidades dos Honeypots

- Coleta de códigos maliciosos
- Identificar varreduras e ataques automatizados
- Acompanhamento das vulnerabilidades
- Motivação dos atacantes
- Correlação de informações com outras fontes
- Auxílio aos sistemas de detecção de intrusão
- Manter atacantes afastados de sistemas importantes

Honeypots

Os *honeypots* podem ser considerados de baixa e alta interatividade, indo desde serviços falsos (baixa interatividade) até máquinas com serviços reais (alta interatividade), onde os atacantes podem obter acesso total ao sistema.

- **Baixa Interatividade:** Back Officer Friendly, Deception Toolkit(DTK), Specter, Honeyd, Labrea, Tarpit
- **Alta Interatividade:** UML, VMware, Mantrap, sistemas e aplicativos reais; instalação padrão de sistemas operacionais; artifícios de monitoração das atividades dos atacantes*(LKM, patches)*.

Taxonomia dos Honeypots

Baixa Interatividade	**Alta Interatividade**
Emulam sistemas e serviços	Executam as versões reais
Simples. Fácil gerenciamento	Cuidados na instalação e configuração. Co leta de artefatos
Atacante não tem controle	Controle total
Ações limitadas, captura de tráfego e *malware*	Captura de ma is informações, incluindo ferramentas e comandos
Difíceis de iludir atacantes avançados/determinados	Difícil de desti nguir de um sistema de produção

Honeypots de Baixa Interatividade

Fonte: `http://www.tracking-hackers.com/solutions/`

Specter

Plataforma	Licensa	Informações
Win32	**Comercial**	**`http://www.specter.com`**

- Pode monitorar até quatorze portas de TCP (sete de armadilhas e sete de serviços)
- Armadilhas bloqueiam e registram as tentativas de ataques
  - DNS, IMAP4, SUN-RPC, SSH, SUB-7, BOK2 e genérica
- As portas de serviços interagem com o invasor
  - FTP, TELNET, SMTP, FINGER, HTTP, NETBUS e POP3

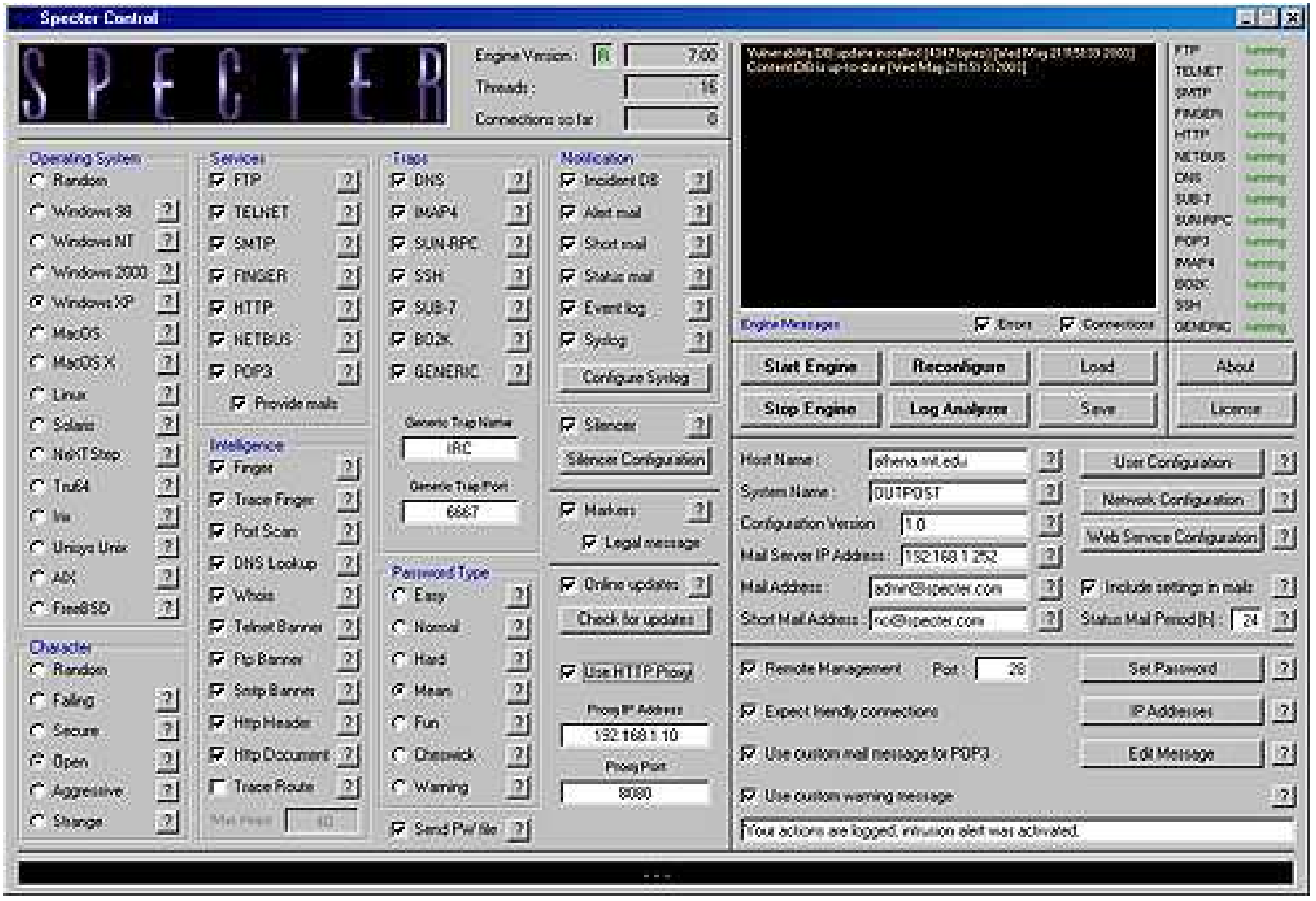
Honeypots de Baixa Interatividade

Specter

- Pode emular até quatorze sistemas operacionais diferentes
  - Windows 98, Windows NT, Windows 2000, Windows XP, Linux, Solaris, Tru64 (Digital Unix), NeXTStep, Irix, Unisys Unix, AIX, Maços, MacOS X, FreeBSD
- Não consegue emular na pilha IP
- Possui grande variedade de configuração
- Características de notificação
- Banco de dados dos incidentes
- Facilidade no uso

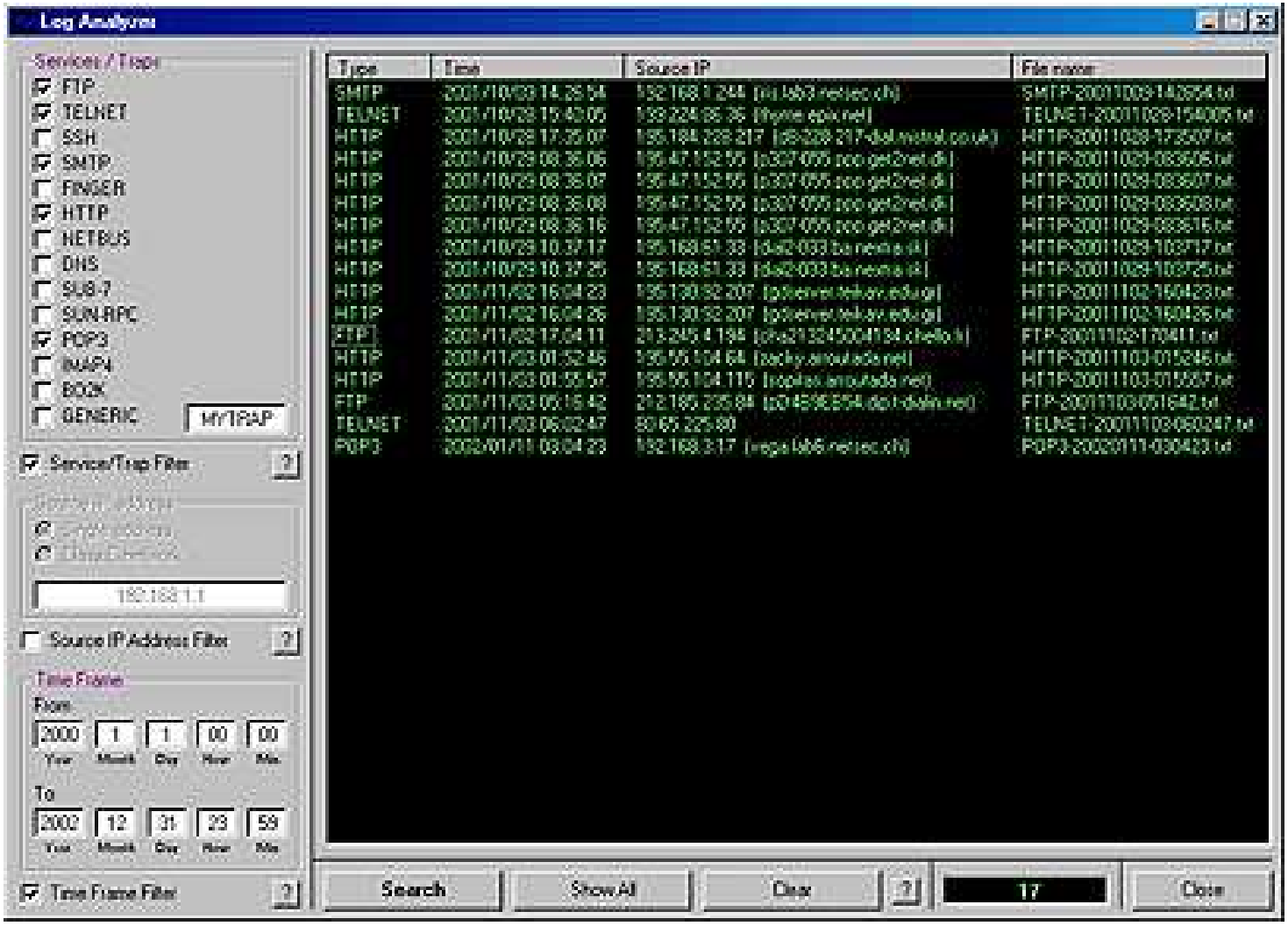
Honeypots de Baixa Interatividade

Specter



Honeypots de Baixa Interatividade

Specter



Honeypots de Baixa Interatividade

Smoke Detector

Plataforma	Licensa	Informações
Win32	**Comercial**	**`http://palisadesys.com/products/smokedetector`**

- Emula até dezenove sistemas operacionais por máquina entre:
  - Linux, Solaris8, HP-UX, AIX4, FreeBSD4, AS400, WindowsNT4 e Windows2000
- Pode enviar alertas de tentativas de invasão ao administrador da rede

Honeypots de Baixa Interatividade

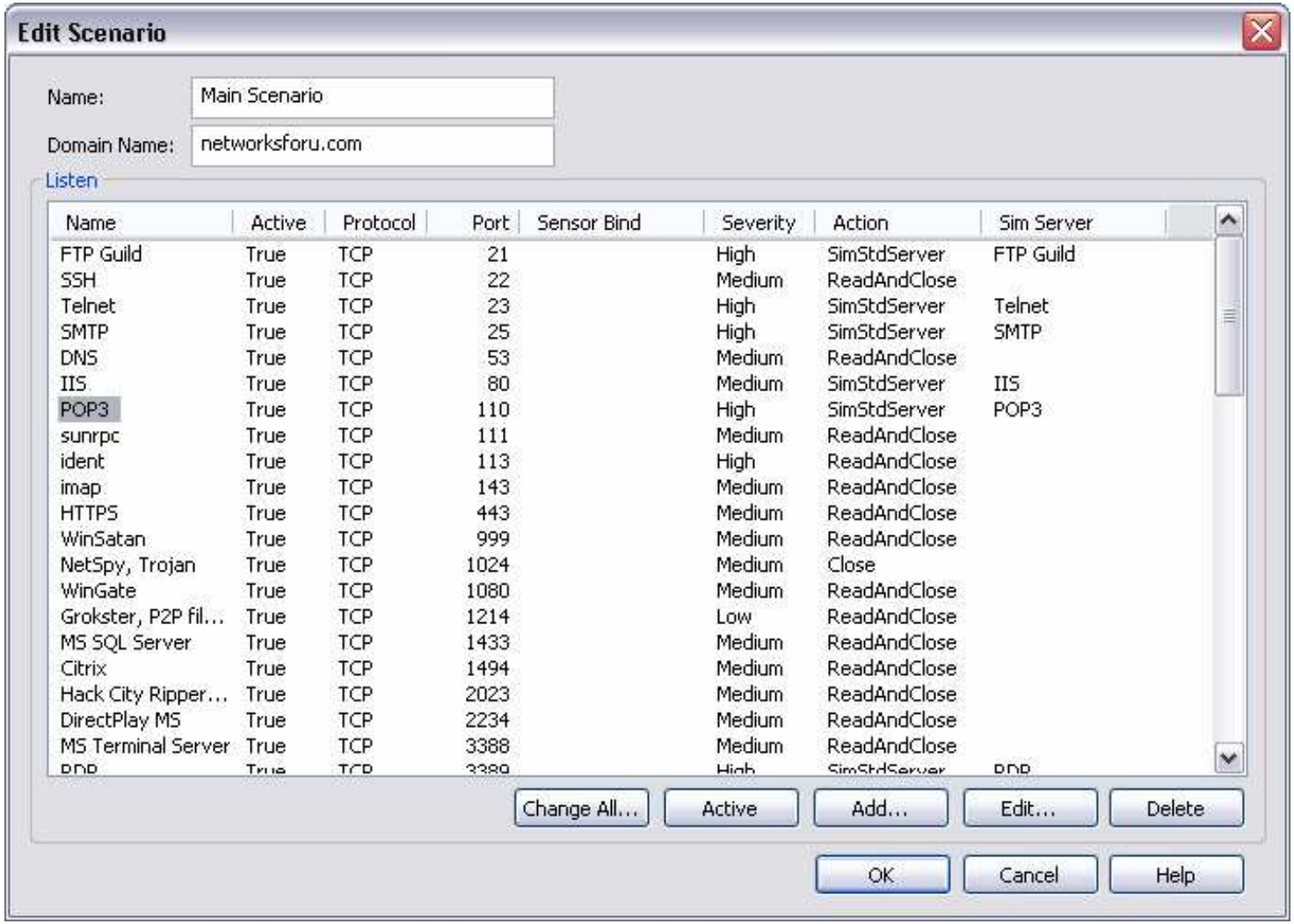
KFSensor

Plataforma	Licensa	Informações
Win32	**Comercial**	**`http://www.keyfocus.net`**

- Registra os logs e permite aplicar filtros
- Possui simulação de NetBIOS, SMB, FTP, POP3, HTTP, Telnet, SMTP e SOCKS
- Interopera com scripts do Honeyd
- Há cópias para avaliação

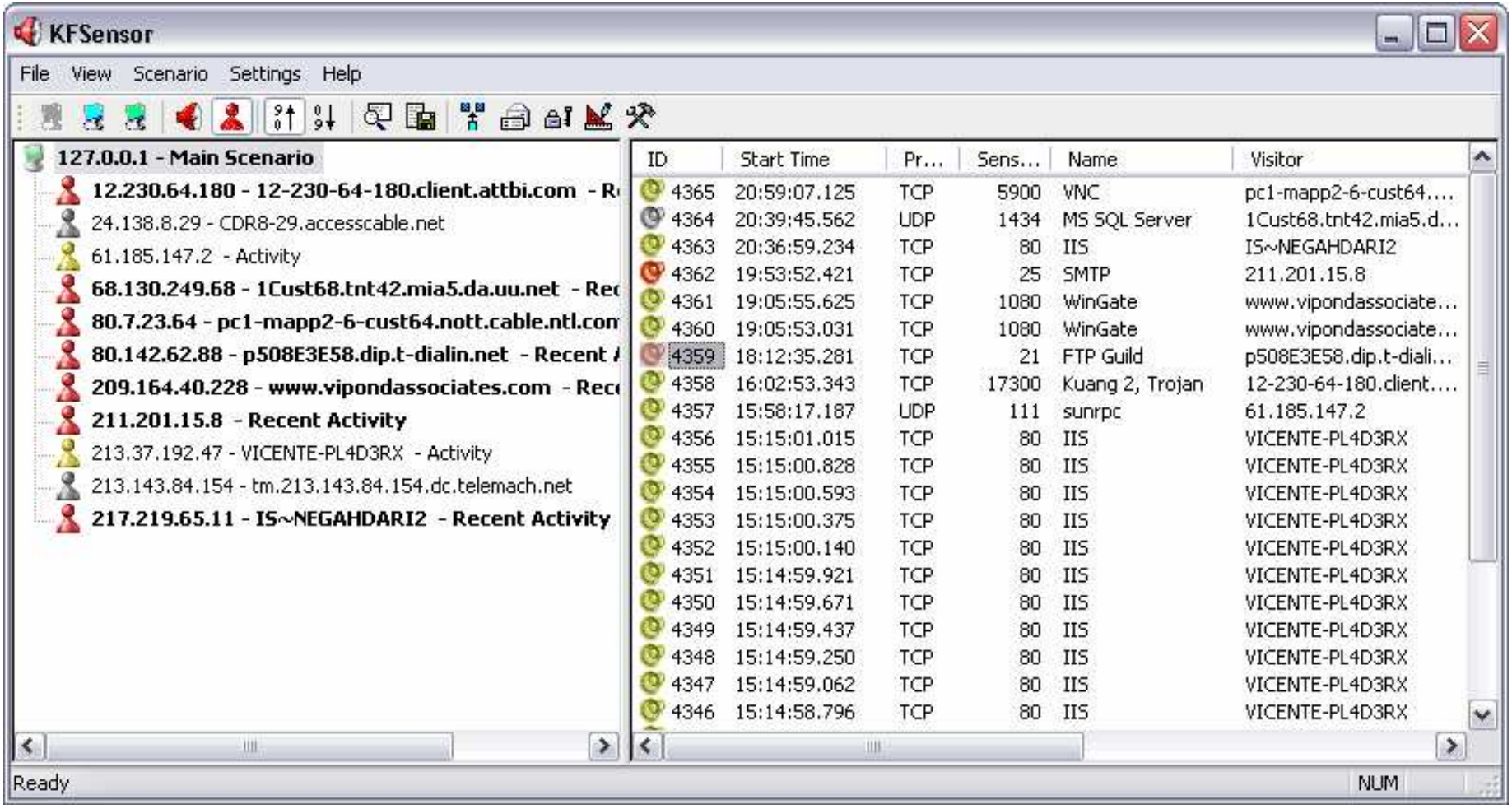
Honeypots de Baixa Interatividade

KFSensor



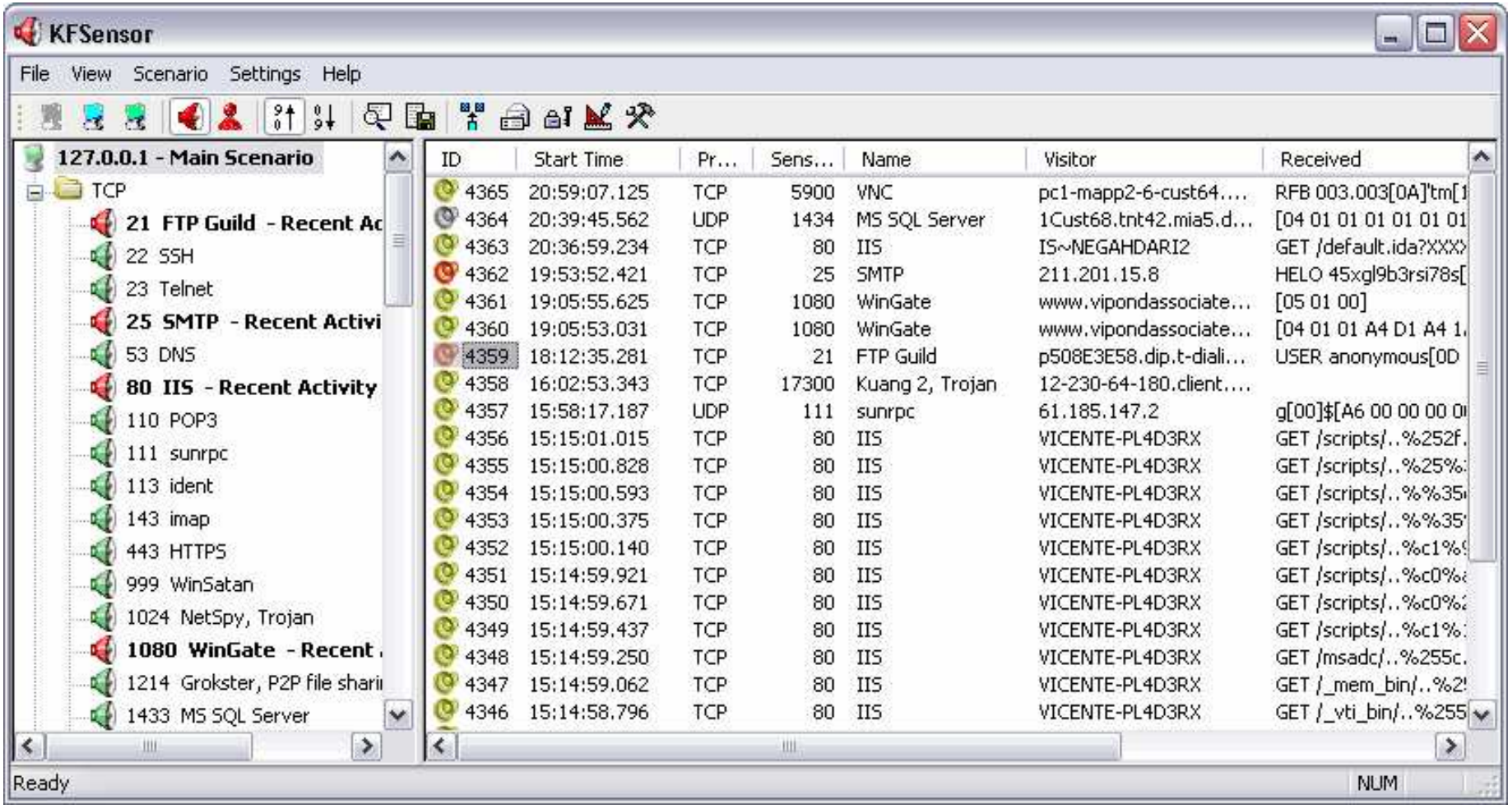
Honeypots de Baixa Interatividade

KFSensor



Honeypots de Baixa Interatividade

KFSensor



Honeypots de Baixa Interatividade

Symantec Decoy Server

Plataforma	Licensa	Informações
Solaris	**Comercial**	**`http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=157`**

- Simula tráfego de e-mail
- Possui mecanismos de respostas baseados nas atividades dos invasores, como desligar o sistema
- Detecção de intrusão baseada em host e em rede
- Gerenciamento centralizado - p/ Windows

Honeypots de Baixa Interatividade

Deception ToolKit

Plataforma	Licensa	Informações
UNIX	**Código Aberto**	**`http://www.all.net/dtk/dtk.html`**

- Simula sistemas com grande número de vulnerabilidades
- Atende as requisições e fornece respostas personalizadas falsas

Honeypots de Baixa Interatividade

Tiny Honeypot

Plataforma	Licensa	Informações
UNIX	**Código Aberto**	**`http://www.alpinista.org/thp/`**

- Escrito em Perl
- Simula serviços de HTTP e FTP
- O honeypot monitora todas as portas e provê uma série de respostas falsas

Honeypots de Baixa Interatividade

BackOfficer Friendly

Plataforma	Licensa	Informações
Win32	**Comercial, mas, Livre**	**`http://www.nfr.com/resource/backOfficer.php`**

- Emula serviços básicos como TELNET, FTP, SMTP, POP3
- Consegue monitorar sete portas por vez
- Indicado para iniciantes que desejam verificar o funcionamento de um honeypot

Honeypots de Baixa Interatividade

LaBrea Tarpit

Plataforma	Licensa	Informações
UNIX e Win32	**Código Aberto**	**`http://scans.bizsystems.net/paged_report.plx`**

- Assume endereços IP novos em uma rede
- Trabalha observando requisições ARP
- Somente aceita a conexão

Honeypots de Baixa Interatividade

Honeyd

Plataforma	Licensa	Informações
UNIX e Win32	**Código Aberto**	**`http://www.honeyd.org/`**

- Um dos principais aplicativos utilizados na construção de honeypots
- Emula centenas de sistemas operacionais
- Simula aplicações no espaço de endereços IP não utilizados
- Responde as requisições e registra os ataques

Honeypots de Baixa Interatividade

- Pode monitorar todas as portas baseadas em UDP e TCP
- Grande facilidade de configuração
- Permite o desenvolvimento de novos módulos
- Gerenciamento via console*
- Emulação de Ethernet*

* - Características implementadas a partir da versão 0.8a

Por que utilizar o honeyd?

- Simula sistemas, executando em espaços de endereçamento não alocados
- Simula diversos hosts virtuais ao mesmo tempo
- Simula um SO no nível de pilha do TCP/IP
  - Engana o *nmap* e o *xprobe*
- Suporta redirecionamento de um serviço
- Suporta somente os protocolos TCP, UDP e ICMP

Por que utilizar o honeyd? (cont.)

- Recebe o tráfego de rede:
  - Utilizando proxy ARP (arpd)
  - Através de roteamento específico para os endereços IP virtuais
- Nenhum *socket* é alocado no sistema operacional
  - Nada aparece no comando *netstat*
  - Implementa sua própria máquina de estado TCP
  - libpcap+libdnet

Por que utilizar o honeyd? (cont.)

- Transparência no desenvolvimento de *listeners*(emuladores de serviço)
  - Os *listeners* não precisam se preocupar com detalhes de comunicação de rede
- Redirecionamento de *file descriptors*
  - Ler da rede (STDIN)
  - Enviar para a rede (STDOUT)
  - Registro de logs (STDERR)
- Não necessariamente é preciso associar um *listener* a uma porta

Por que utilizar o honeyd? (cont.)

- Utilização de subsistemas
  - Personalidade
  - Serviços
  - Endereço de rede

```
create mail
set mail personality "Linux kernel 2.2.13"
add mail tcp port 25 "perl scripts/qmail.pl"
add mail tcp port 22 "sh scripts/test.sh $ipsrc $dport"
bind 192.168.50.13 mail
```

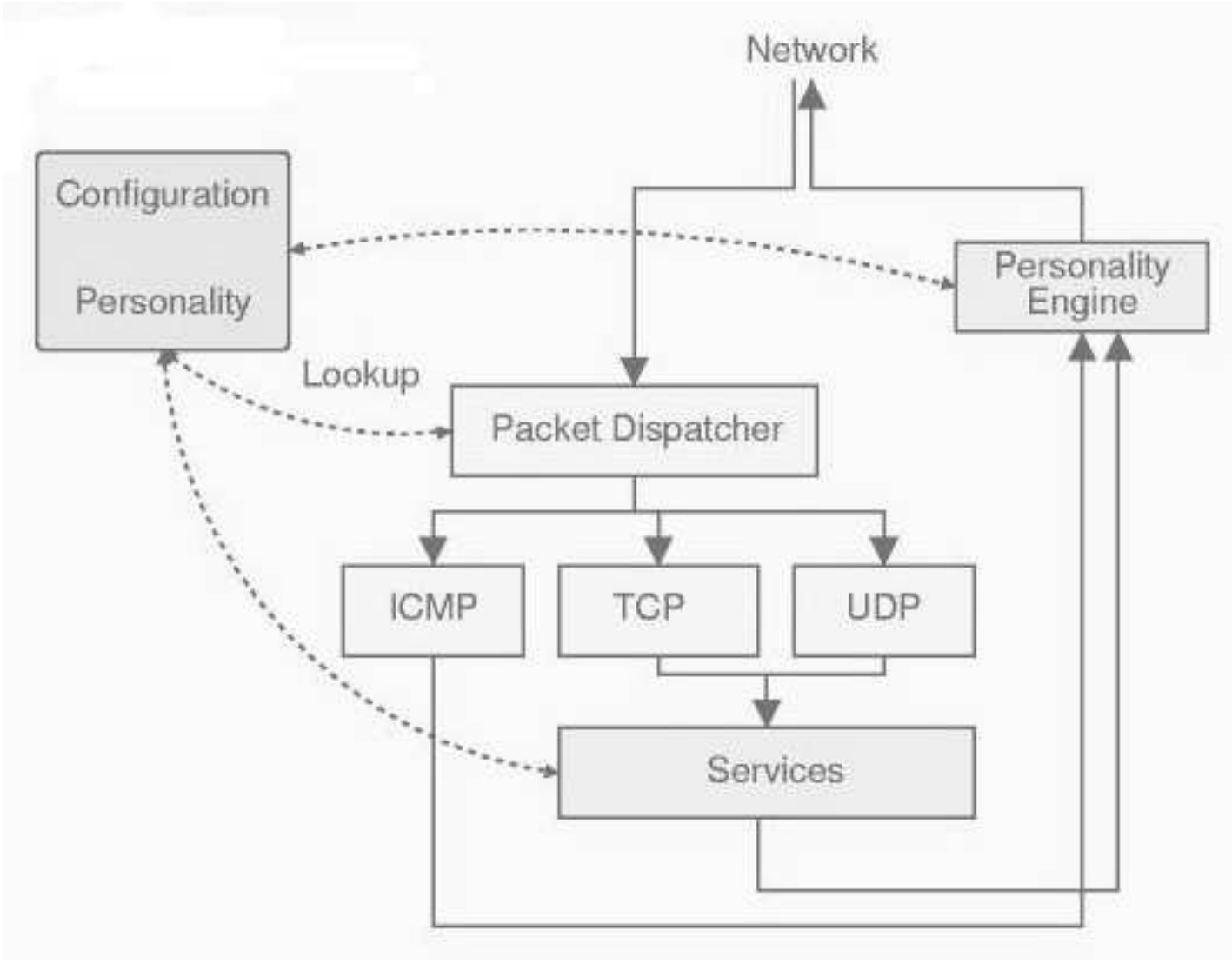
Por que utilizar o honeyd? (cont.)

- Segurança no *honeyd*
  - Roda com baixo privilégio
    - *Default: nodoby*
    - -u (UID)
- Permite Systrace
  - Ações limitadas
- Se o honeyd ou algum *listener* for comprometido, o atacante conseguirá somente alguns privilégios de *nobody*, restritos pelo *systrace*

Por que utilizar o honeyd? (cont.)

- Sistema de *logging* já desenvolvido
  - *Fingerprinting* passivo
    - Tenta identificar o SO do atacante
    - Usa a base de dados do pf (pf.os)
    - Não é limitado ao OpenBSD
  - Não registra o contéudo dos pacotes
    - Utilizar de *logs* de *firewall*
    - Ferramentas de captura de tráfego de rede (tcpdump)

Arquitetura do Honeyd



http://niels.xtdnet.nl/papers/honeyd-dfn/mgp00010.html

Listeners

- Propósito:
  - fechar o *three-way handshake*
  - registrar as atividades
- Basicamente dois tipos:
  - apenas estabelecem a conexão
  - entendem o protocolo (http, ftp, etc)
- Podem ser executados *standalone* ou via *honeyd*

Exemplo de Listeners simples

Blaster

- Explora o DCOM RPC

  `http://www.kb.cert.org/vuls/id/568148`

  - nc -l 135
  - Instalará um *backdoor*

- Acesso ao *Backdoor*

  - socket -s 4444
  - Shell para executar comandos

`http://www.cert.org/advisories/CA-2003-20.html`

Criação de Listeners

- Na maioria dos casos não adianta somente deixar uma porta em estado de OPEN, pois os *malware* esperam por determinadas respostas para continuar o ataque.
- Basicamente duas formas de criação:
  - Quando conhecemos o serviço
  - Ataques novos, *malware* desconhecidos

Criação de Listeners - Serviços Conhecidos

- Ter em mãos as aplicações (cliente e servidora) do serviço a ser emulado;
  - Caso não seja possível, procurar por documentação sobre o protocolo, como as RFCs ou artigos.
- Coletar o tráfego de rede entre essas aplicações, se possível;
- Desenvolver aplicações servidoras simples que permitam o registro dos dados recebidos (*listener standalone*);

Criação de Listeners - Serviços Conhecidos (cont.)

- Analisar o comportamento (tráfego de rede/protocolo) da aplicação servidora do serviço e implementar no *listener* as mesmas respostas que são enviadas para o cliente;
  - Se receber A então envie B senão envie C
- Ferramentas de apoio
  - Tcpdump, Ethereal, nc e principalmente o VI

Criação de Listeners - Malware desconhecidos

- Conheço a porta que é atacada mas não sei qual é o serviço
- Criar um *listener* para atuar nesta porta e habilitar o tcpdump para capturar todo o tráfego de rede
- Analisar o tráfego capturado
  - O *malware* enviou algum dado ou ficou esperando uma resposta?
  - Qual o SO da máquina de origem?
  - As informações dos cabelhaços podem ser bastante úteis

Criação de Listeners - Malware desconhecidos (cont.)

- Procurar pelos possíveis serviços que podem atuar nessa porta
  - Que respostas estes serviços enviam para os clientes?
    * Implemente e reze para o *malware* gostar da resposta
    * Se sim continue a "conversa"para ver até onde ele quer chegar
    * NÃO?????

Criação de Listeners - Malware desconhecidos (cont.)

- Procurar pelos *malware* conhecidos e verificar o que eles esperam receber
  - Pode ser uma variante que utilize um protocolo de outro *malware*
  - Implemente e dobre a oração

Criação de Listeners - Malware desconhecidos (cont.)

- Se a "conversa" inicial for positiva procure pelo protocolo que este *malware* utiliza
  - Se não for encontrado, procure por códigos fontes ou binários
  - No caso de binários, aplique técnicas de engenharia reversa para tentar encontrar a utilização do protocolo.
    * Analisar as *strings* do binários pode ajudar
    * Desassembly

Criação de Listeners - Malware desconhecidos (cont.)

- Se em último caso, tudo que você tentar não der certo, desista, deve ser o seu vizinho chato te atormentando.
  - PARE PARANÓIA!!!!, pois apenas uma conexão estabelecida pode te levar ao hospício.

Por que eu desenvolveria Listeners?

- Entender os *malware*
- Entender as ameaças e vulnerabilidades
- Didático
  - Conhecer protocolos de rede
  - Aprender a programar em ambientes cliente/servidor
- Conhecer os detalhes dos sistemas
- Aprender técnicas de programação segura
- **Encontrar *bugs* nas ferramentas dos atacantes**

Listeners no Honeyd

- Algoritmo principal:
  - Devido ao redirecionamento de *file descriptors*:
    - *Read STDIN*
    - *Write STDOUT*

Listeners no Honeyd (cont.)

- Variáveis de Ambiente:
  - HONEYD_IP_SRC
  - HONEYD_IP_DST
  - HONEYD_SRC_PORT
  - HONEYD_DST_PORT
  - HONEYD_PERSONALITY
- Receber essa informações por linha de comando
- Alterar o comportamento do *Listener* de acordo com a personalidade do subsistema

Listeners no Honeyd (cont.)

Exemplo com o subsistema Linux kernel 2.2.13:

```
create mail
set mail personality "Linux kernel 2.2.13"
add mail tcp port 22 "sh scripts/test.sh $ipsrc $dport"
add mail tcp port 25 "perl scripts/qmail.pl"
bind 192.168.50.13 mail
```

Listeners no Honeyd (cont.)

test.sh:

```
DATE=`date`
echo "$DATE: Started From $1 Port $2" >> /tmp/log
echo SSH-1.5-2.40
while read name
do
        echo "$name" >> /tmp/log
        echo "$name"
done
```

Listeners no Honeyd (cont.)

qmail.pl:

```
syswrite ( STDOUT, "220 $name ESMTP\n" );
while (<STDIN>) {
  if ( /^(helo.*)/i ) {
    syswrite ( STDOUT, "250 $name\n" );
  } elsif ( /^(mail.*)/i ) {
    syswrite ( STDOUT, "250 ok\n" );
  } elsif ( /^(rcpt.*)/i ) {
    syswrite ( STDOUT, "250 ok\n" );
  } elsif ( /^(data)$/i ) {
    syswrite ( STDOUT, "354 go ahead\n" );
  } elsif ( /^(\.)$/i ) {
    syswrite ( STDOUT, "250 ok 1076685260 qp 68536\n" );
  }
}
```

Personalidades

- Simular a pilha TCP/IP de um SO
- Enganar ferramentas de *fingerprinting*
  - Xprobe, Nmap
  - OPENBSD RODANDO IIS??????
- Utiliza as bases de dados de personalidade do Nmap para TCP e UDP e do Xprobe para ICMP

Personalidades - Exemplo (nmap.prints)

```
Fingerprint Linux kernel 2.2.13
Class Linux | Linux | 2.2.X | general purpose
TSeq(Class=RI%gcd=<6%SI=<E5F68C&>24CA0)
T1(DF=Y%W=7F53%ACK=S++%Flags=AS%Ops=MENNTNW)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=7F53%ACK=S++%Flags=AS%Ops=MENNTNW)
T4(DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(DF=N%TOS=C0|A0|0%IPLEN=164%RIPTL=148%RID=E
                    %RIPCK=E%UCK=F%ULEN=134%DAT=E)
```

http://www.insecure.org/nmap/nmap-fingerprinting-article.html

Personalidades - Criando novas

- Passar o nmap com a opção -O contra novo sistema a ser criado a personalidade

```
# nmap -sS -p 80 -O -v <host>
```

- Se o nmap não conseguir identificar o SO, ele retornará o resultados dos testes com mostrado no *slide* anterior
- Acrescentar essa saída no arquivo *nmap.prints*

Personalidades - Criando novas (cont.)

- Importante destacar que não adianta somente acrescentar a saída neste arquivo, se a base de dados da ferramenta utilizada não for atualizada também.
  - Neste caso somente a pilha TCP/IP do subsistema se comportará como o novo sistema
- O *nmap.prints* do honeyd deve ser constantemente atualizado com a base de dados das novas versões da ferramenta nmap.

Instalação e Conf. do Sist. OpenBSD

Os passos que serão aqui apresentados fazem parte dos procedimentos de configuração de um honeypot de baixa interatividade do Consórcio Brasileiro de Honeypots Distribuídos.

`http://www.honeypots-alliance.org.br`

Instalação e Conf. do Sist. OpenBSD

- Recursos necessários:
  1. Sistema Operacional OpenBSD

     (`http://www.openbsd.org`)
  2. Honeyd (`http://www.honeyd.org`)
  3. Arpd

     (`http://www.citi.umich.edu/u/provos/honeyd/`)
  4. Libevent

     (`http://www.monkey.org/~provos/libevent-0.8.tar.gz`)
  5. Libdnet (`http://libdnet.sourceforge.net/`)

Instalação e Conf. do Sist. OpenBSD

- Zerar o disco, ex:
  1. boot pela mídia
  2. # dd if=/dev/zero of=/dev/wd0c bs=1m
- Sugestões de particionamento:

```
/         100MB
swap      2 * RAM
/home     512MB
/usr      3GB
/tmp      512MB
/var      restante do disco
```

Instalação e Conf. do Sist. OpenBSD

- ***NÃO* instale o sistema todo em uma única partição.**
- Informações sobre `disklabel` podem ser obtidas em:

  `http://www.openbsd.org/faq/faq4.html#Disks`

- Procedimentos de instalação:

  `http://www.openbsd.org/faq/faq4.html#Install`

- Sugestões de instalação:
  - Nao instalar X11 e nem games
  - Escolher um timezone e empregá-lo a todos os honeypots

Instalação e Conf. do Sist. OpenBSD

- Personalizando a instalação:
  - Crie as regras do firewall(pf) no arquivo /etc/pf.conf. Mais informações em:

    `http://www.openbsd.org/faq/pf/index.html`
- Crie e insira no arquivo /etc/rc.conf.local as informações abaixo:

```
portmap=NO
inetd=NO
check_quotas=NO
ntpd=YES
pf=YES
```

Instalação e Conf. do Sist. OpenBSD

- Configure o sistema de rotacionamento de logs em /etc/newsyslog.conf
- Ative o sistema de accounting que será habilitado no próximo reboot

```
# touch /var/account/acct
```

- Instale a árvore atualizada dos fontes, conforme os comandos abaixo:

```
# export CVS_RSH="/usr/bin/ssh"
# CVSROOT=anoncvs@anoncvs.ca.openbsd.org:/cvs
```

Instalação e Conf. do Sist. OpenBSD

```
# export CVSROOT
# CVS_IGNORE_REMOTE_ROOT=1
# export CVS_IGNORE_REMOTE_ROOT
# cd /usr/src
# cvs -d ${CVSROOT} up -rOPENBSD_3_4 -Pd
```

Mais informações sobre o sistema CVS em:

`http://www.openbsd.org/faq/faq8.html#CVS`

Instalação e Conf. do Sist. OpenBSD

- Instale a árvore atualizada dos ports, conforme os comandos:

```
# export CVS_RSH="/usr/bin/ssh"
# CVSROOT=anoncvs@anoncvs.ca.openbsd.org:/cvs
# export CVSROOT
# export CVS_IGNORE_REMOTE_ROOT=1
# cd /usr
# cvs up -rOPENBSD_3_4 -Pd ports
```

Mais informacoes sobre a árvore de ports em:

`http://www.openbsd.org/faq/faq8.html#Ports`

Instalação e Conf. do Sist. OpenBSD

- Instalação do sistema de sincronização de tempo via ports

```
# cd /usr/ports/net/ntp/stable
# make && make install && make clean
```

- Configuração desse sistema através do arquivo /etc/ntp.conf

```
server ENDEREÇO DO SEU SERVIDOR DE NTP
authenticate no
logconfig all
logfile /var/log/ntp.log
restrict default noquery
```

Instalação e Conf. do Sist. OpenBSD

- Crie, compile e instale um kernel compatível com o seu hardware. Os passos necessários se encontram em:

  `http://www.openbsd.org/faq/faq5.html#Building`

- Procure adicionar e/ou manter as linhas:

  ```
  option DUMMY_NOPS
  option NMBCLUSTERS=8192
  ```

- Recompile todo o sistema, conforme descrito em:

  `http://www.openbsd.org/faq/upgrade-minifaq.html#1.5`

- **É conveniente utilizar o `mergemaster` para verificar arquivos de configuração que foram alterados**

Instalação e Conf. do Sist. OpenBSD

- Altere as linhas correspondentes no arquivo /etc/ssh/sshd_config para refletir a alteração abaixo:

```
Port 22
Protocol 2
ListenAddress 0.0.0.0
ServerKeyBits 1664
PermitRootLogin no
PasswordAuthentication yes
PermitEmptyPasswords no
```

- Para o sistema ser administrado remotamente, crie um usuário através do comando:

```
# adduser
```

Instalação e Conf. do Sist. OpenBSD

- Crie um alias de mail do usuário root dessa máquina para um e-mail válido, através da alteração da linha correspondente no arquivo /etc/mail/aliases
- Para ativar a mudança, execute:

```
# newaliases
```

- Reinicialize o sistema:

```
# shutdown -r now
```

Instalação e Configuração do Honeyd

- Bibliotecas utilizadas pelo honeyd
- **libdnet e libevent**
  1. Baixe-as dos respectivos sites
  2. Siga o roteiro:
     (a) `# tar xzvf nome-da-biblioteca`
     (b) `# cd diretorio-da-bibliteca`
     (c) `# ./configure && make && make install`

Instalação e Configuração do Honeyd

- Arpd
  - Responde qualquer *ARP request* para um intervalo de endereços IPs que coincidem com a rede especificada

1. Baixe a última versão do site citado anteriormente
2. Siga o roteiro:
   (a) `# tar xzvf arquivo-do-arpd`
   (b) `# cd diretorio-do-arpd`
   (c) `# ./configure && make && make install`

Instalação e Configuração do Honeyd

- Honeyd
  1. Baixe a última versão do site citado anteriormente
  2. Siga o roteiro:
     (a) `# tar xzvf arquivo-do-honeyd`
     (b) `# cd diretorio-do-honeyd`
     (c) `# ./configure && make && make install`

Instalação e Configuração do Honeyd

- Copie os arquivos de configuração do Honeyd para um diretório adequado
  1. `# mkdir -p /var/log/honeyd/conf /var/log/honeyd/log /var/log/honeyd/scripts`
  2. `# chown -R nobody:nobody /var/log/honeyd/log /var/log/honeyd/scripts`
  3. `# cd /var/log/honeyd/conf`
  4. `# cp /usr/local/share/honeyd/nmap* .`
  5. `# cp /usr/local/share/honeyd/xprobe2.conf .`

Instalação e Configuração do Honeyd

- Criando subsistemas

  Arquivo (/var/log/honeyd/conf/honeyd.conf)

```
### windows
create windows
set windows personality "Microsoft Windows XP \\
    Professional SP1 or Windows 2000 SP3"
set windows default tcp action reset
set windows default udp action reset
set windows default icmp action open
```

Instalação e Configuração do Honeyd

```
add windows tcp port 135 open
add windows tcp port 137 open
add windows udp port 137 open
add windows tcp port 139 open
add windows tcp port 445 open
add windows udp port 445 open

set windows uptime 323242

bind 10.0.0.5 windows
```

Instalação e Configuração do Honeyd

- Inicialize o Honeyd

```
# /usr/local/bin/honeyd \
   -l /var/log/honeyd/log/honeyd.log.2004-04-14-00:00 \
   -f /var/log/honeyd/conf/honeyd.conf \
   -p /var/log/honeyd/conf/nmap.prints \
   -x /var/log/honeyd/conf/xprobe2.conf \
   -a /var/log/honeyd/conf/nmap.assoc 10.0.0.0/24
```

- Inicialize o Arpd

```
# /usr/local/sbin/arpd 10.0.0.0/24
```

Instalação e Configuração do Honeyd

- Insira no final do arquivo /etc/rc.local as informações abaixo para inicializar o arpd e o honeyd no boot do sistema

```
if [ -x /usr/local/sbin/arpd ]; then
   /usr/local/sbin/arpd 10.0.0.0/24 &
fi

if [ -x /usr/local/bin/honeyd ]; then
   /usr/local/bin/honeyd \
   -l /var/log/honeyd/log/honeyd.log.2004-04-14-00:00 \
   -f /var/log/honeyd/conf/honeyd.conf \
   -p /var/log/honeyd/conf/nmap.prints \
   -x /var/log/honeyd/conf/xprobe2.conf \
   -a /var/log/honeyd/conf/nmap.assoc 10.0.0.0/24 &
fi
```

Monitoração do Honeyd

- Análise do sistema de logs (arquivo honeyd.log*)

Protocolo TCP

2004-01-07-15:26:40.0209 tcp(6) - 244.233.22.102 61891
172.162.8.180 21: 60 S [FreeBSD 5.0-5.1]

2004-01-07-16:48:30.1212 tcp(6) S 92.168.21.135 33395
172.162.8.91 80 [Linux 2.6]

2004-03-11-18:06:41.8778 tcp(6) E 10.173.240.67 61658
192.168.14.178 6588: 65 147

Monitoração do Honeyd

Protocolo UDP

2004-03-11-02:48:58.5614 udp(17) - 192.168.0.1 53 10.0.0.1 53: 46

2004-03-11-12:33:49.8080 udp(17) S 172.162.8.100 53 10.0.1.5 53

2004-03-11-12:34:49.8118 udp(17) E 172.162.8.20 53 10.1.10.50 53:
24 0

Monitoração do Honeyd

Protocolo ICMP

2004-03-11-16:35:04.1317 icmp(1) - 10.50.230.1 192.168.5.5: 11(0): 56

2004-03-11-12:04:53.5659 icmp(1) - 10.222.35.49 192.168.100.100: 8(0): 92

Monitoração do Honeyd

- Utilizando emuladores (serviço FTP)

  http://www.citi.umich.edu/u/provos/honeyd/contrib/mael/ftp.sh

```
### Linux
...
add linux tcp port 21 \
   "sh /var/log/honeyd/scripts/ftp.sh $ipsrc $dport"
```

- Características:
  - Emula WU-FTPD 2.6.0(5)
  - Registra os comandos digitados

```
PASS mozilla@
Mon Apr 12 20:01:27 GMT 2004:  FTP started from
xxx.xxx.xxx.xxx Port xxxxx
```

Monitoração do Honeyd

- Servico HTTP

  http://sourceforge.net/projects/iisemul8/

```
### Windows
...
add windows tcp port 80 \
   "perl /var/log/honeyd/scripts/iisemul8.pl"
```

Monitoração do Honeyd

- Emula IIS 5

```
# iisemul8.pl
GET HEAD HTTP/1.0


HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Thu, 15 Apr 2004 18:44:29 GMT
Content-Type: text/html
Content-Length: 87
<html><head><title>Error</title> \
</head><body>The parameter is incorrect. \
</body></html>
```

Monitoração do Honeyd

- Mydoom

  http://www.honeynet.org.br/tools/

```
### Windows
add windows tcp port 3127 \
  "/var/log/honeyd/scripts/mydoom.pl -d \
   -l /var/log/honeyd/var/mydoom"
```

- Características:
  - Script em Perl que emula o mydoom
  - Armazena os arquivos capturados no formato

    ./10/0/0/1/2749/FILE.14195

Monitoração do Honeyd

- Sistema "spam-bait"

```
### Linux
add linux tcp port 1080 \
   "perl /var/log/honeyd/scripts/proxy.pl \
    /var/log/honeyd/scripts/smtp.pl \
    /var/log/honeyd/var/mail"
```

- Características:
  - "Ilude" spammers - emula proxy aberto

Monitoração do Honeyd

- Armazena os e-mails capturados no formato

```
/path/10/10/27/249/.lock
/path/10/10/27/249/.count
/path/10/10/27/249/d0/1
```

```
Return-Path: <business@xxxxxx.com>
Received: from unspecified (xxx-xxx-xxx-xxx.xxxxx.net [xxx.xxx.xxx.xxx])
        by xxxxxx.xxxxx.com (8.12.9/8.11.3) with ESMTP id i0N3ar55071
        for <business@xxxxxx.com>; Fri, 23 Jan 2004 03:36:50 +0000 (GMT)
From: business@xxxxxx.com
Subject: =?Big5?B?wuCrSLZspfOlRL73tPq41bP4p2k=?=
To: business@xxxxx.com
Content-Type: multipart/alternative; \
   boundary="=_NextPart_2rfkindysadvnqw3nerasdf"
MIME-Version: 1.0
Date: Fri, 23 Jan 2004 11:25:54 +0800
X-Priority: 3
```

A Ferramenta Honeydsum

- Funcionalidades:
  - Escrita em Perl
  - Gera sumários em texto e HTML válido
  - Gera gráficos personalizados
  - Sistema de filtros como, portas, protocolos, endereços IPs e redes, etc.
  - Sanitização dos logs por endereço/rede de origem e/ou destino
  - Correlacionamento de eventos entre diversos honeypots

HOACD

- HOACD = Honeyd+OpenBSD+Arpd in CD.
  - É um honeypot de baixa interatividade que roda directamente do CD
  - Armazena os logs gerados no HD
  - As aplicações nele contidas seguem os padrões de configurações apresentados neste tutorial.
- Instalação e uso

Resultados obtidos

- Projeto Rede Brasileira Distribuída de Honeypots, intituições participantes:
  1. ANSP
  2. CBPF
  3. CenPRA
  4. Fiocruz
  5. INPE
  6. NBSO
  7. RedeRio
  8. UNESP
  9. USP

Resultados obtidos

- Volume de dados (compactados):
  8.7GB em 17/04/2004
- Aproximadamente 38.500.000 linhas de logs (únicas)
- Número de acessos totais à porta 80: 9.668.347

Agradecimentos

Hewlett-Packard Brasil