Honeypots & Honeynets

Definição de Honeypots

- O nome deriva dos potes de mel e está redefinido pelo projeto Honeynet (www.honeynet.org).
- Definição do projeto:
  "*Um recurso de segurança cujo o valor está em sua capacidade de ser varrido, atacado e invadido*"
- Tudo que chega até ele é considerado varredura, ataque ou invasão.
- 2 tipos: baixa interatividade e alta interatividade

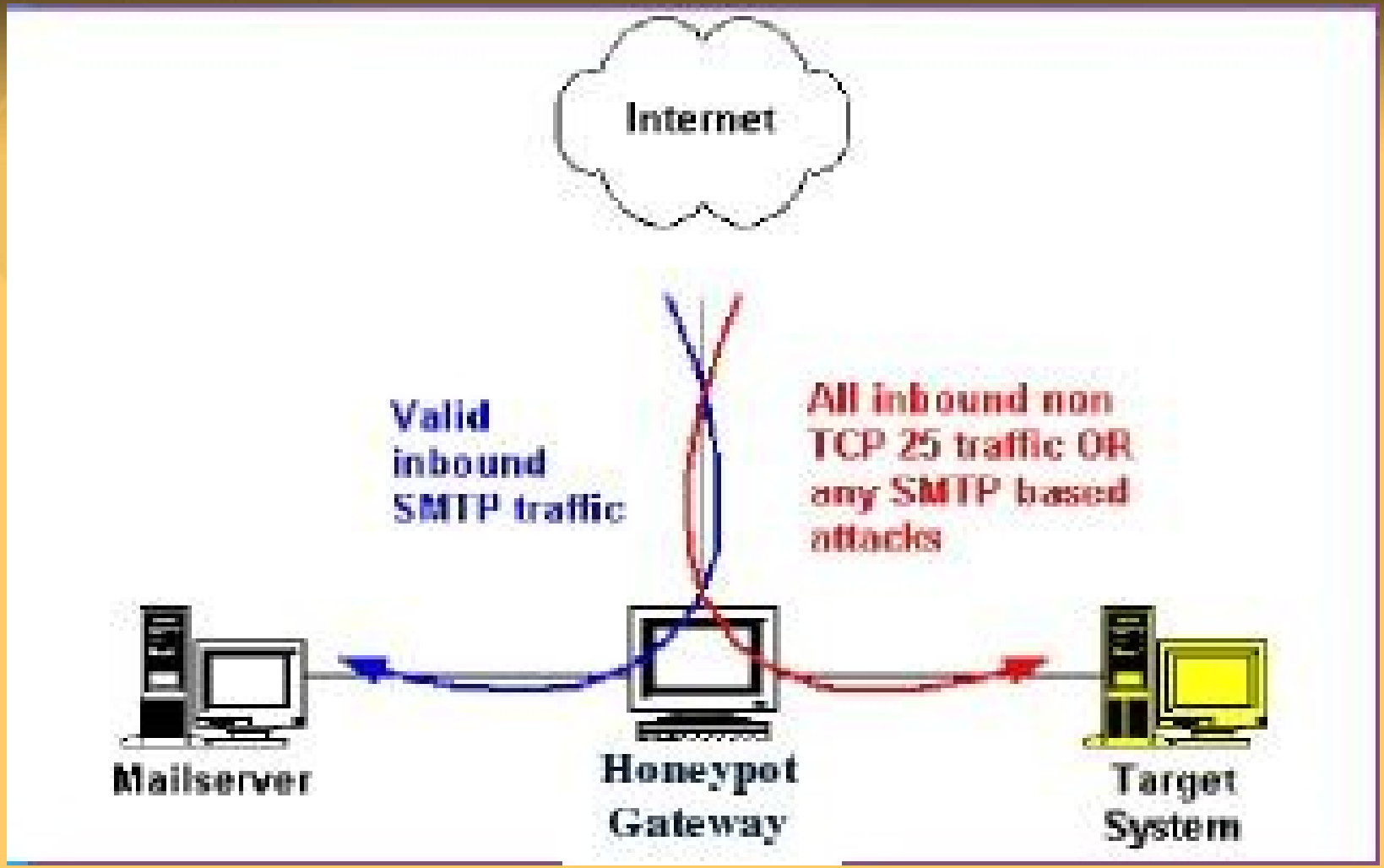
Histórico dos Honeypots

- Sistemas reais invadidos em 1990.
  Não existia a idéia de criar sistemas falsos
  Tudo era feito no mundo real
- Honeypots virtuais
  Simulações de serviços de rede
  Sistemas virtuais
- Sistemas de honeypots reais sendo monitorados e controlados em 2000.
  Mais captura de dados, análise e ferramentas de controle
  Começa a trabalhar com o esquema da honeynet

Redirecionamento

- Conceito básico dos honeypots
- Atividades maliciosas e/ou não autorizadas devem ser redirecionadas para honeypot
- O honeypot deve chamar a atenção do cracker
- Deve usar alvo de sistemas já existentes

Redirecionamento



Conteúdo da Honeypot

- Deve ser o máximo realista possível.
- Deve usar os mesmos dados e aplicações do sistema real – com limitações
- So assim poderemos monitorar cada passo dos atacantes em um sistema altamente controlado

Dados do Honeypots

- Trabalha com o conceito de que o atacante não busca um sistema em si, mais sim uma informação.
- Itens que podem ser utilizados;
  - Sistemas operacionais reais e virtuais
  - Bancos de dados
  - Servidor web, servidor FTP, ssh entre outros.

Tipos de Honeypots

- Objetivo
  - Buscam atingir determinados objetivos dentro de uma organização;
    - Produção
    - Pesquisa

Tipos de Honeypots

- Interação;
  - Busca definir um nível de interação que os atacantes terão ao acessarem os honeypots;
    - Baixa-Interação
    - Alta-Interação

Honeypots de Produção

- Tem o objetivo de proteger a organização;
  - Previnindo
  - Detectando
  - Ajudando a responder a ataques.

Honeypots de Produção

- Geralmente não precisa de algo muito elaborado do ponto de vista técnico para funcionar.
- Alguns exemplos de honepots de produção comerciais;
  - KFSensor
  - Specter

Honeypots de Pesquisa

- Normalmente desenvolvidos para capturar ataques de Crackers
- Evoluídos para;
  - Aprender o que eles estão fazendo
  - Estudar seus métodos de invasão
  - Capturar cada comando digitado

Honeypots de Baixa-Interação

- Trabalha com emulação de serviços e sistemas operacionais
- Por não ser um sistema operacional real, captura informações mais limitadas
- Mais facil de ser desenvolvido e o risco é minimo.
- Exemplos: Honeyd

Honeypots de Alta-Interação

- Captura informações mais detalhadas
- Trabalha com sistemas operacionais e serviços gerais
- Difícil implementação
- Maior risco pois os ataques serão mais serios.

Vantagens Honeypot

- Como Honeypot é isolado, o fluxo de informações para análise é pequeno comparado com a uma rede de produção;
- Redução de alertas falsos;
- Exigência de recursos mínimos;
- Ajuda manter atacantes afastados de sistemas importantes
- Descoberta de novas ferramentas e táticas dos hackers

Desvantagens Honeypot

- Visão limitada de tráfego;
- Risco de ser invadido e utilizado para prejudicar outros sistemas;
- Ausência de tráfego implica em gastos sem retorno, já que nada foi monitorado;

Riscos Envolvidos

- Os crackers mais avançados sabem as características de honeypot e sabem que sistemas devem evitar
- Informação muito valiosa disponibilizada no honeypot
- Ataque real ao sistema

Riscos Envolvidos

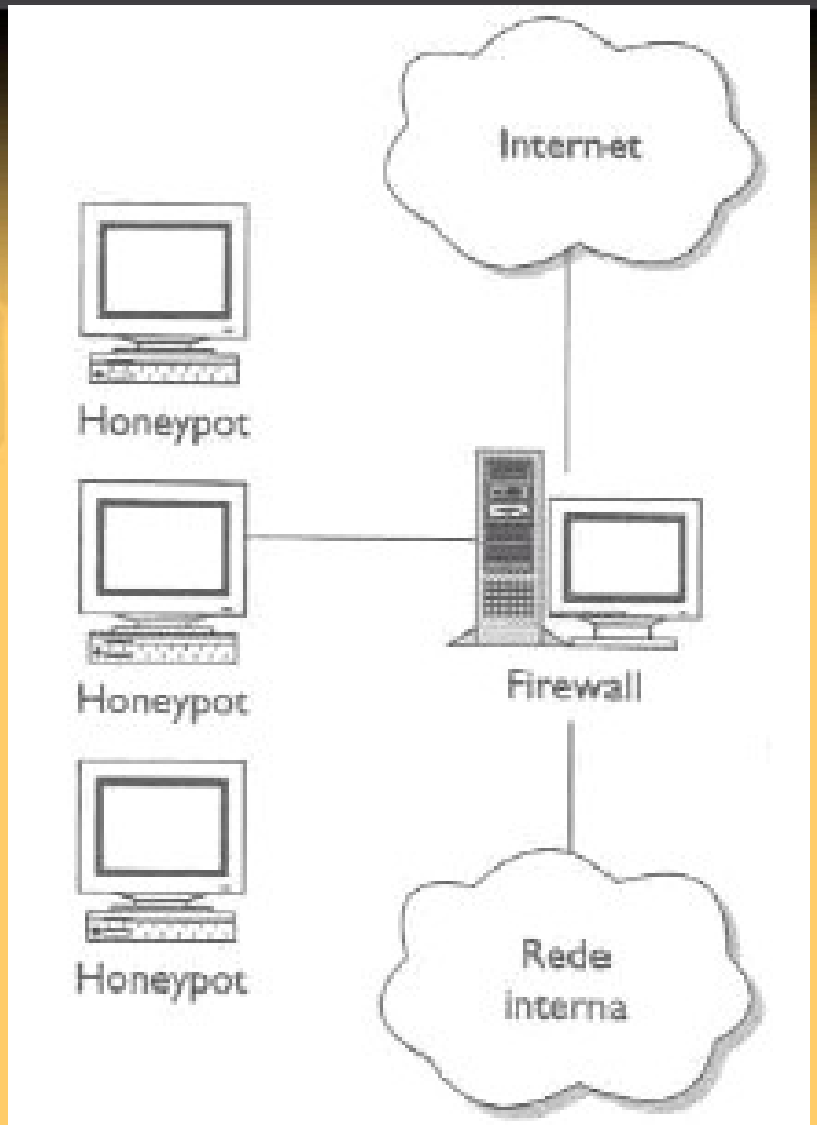
- Inerente – É esperado do atacante a tomada total do honeypot

- Utilizar o honeypot para atacar outros sistemas
  - Seja como hospedeiro de ataques
  - Seja como escada para outros sistemas ou até para sistema principal através de brechas deixadas

Honeynet

- É uma rede altamente controlada onde todo pacote que entra ou deixa a honeynet é monitorado, capturado, e analisado.
- Qualquer tráfego que entra ou deixa a Honeynet é suspeito por natureza.
- *Honeynet* é um tipo de *honeypot* de alta interação, utilizada principalmente para pesquisa.

Exemplo de Honeynet

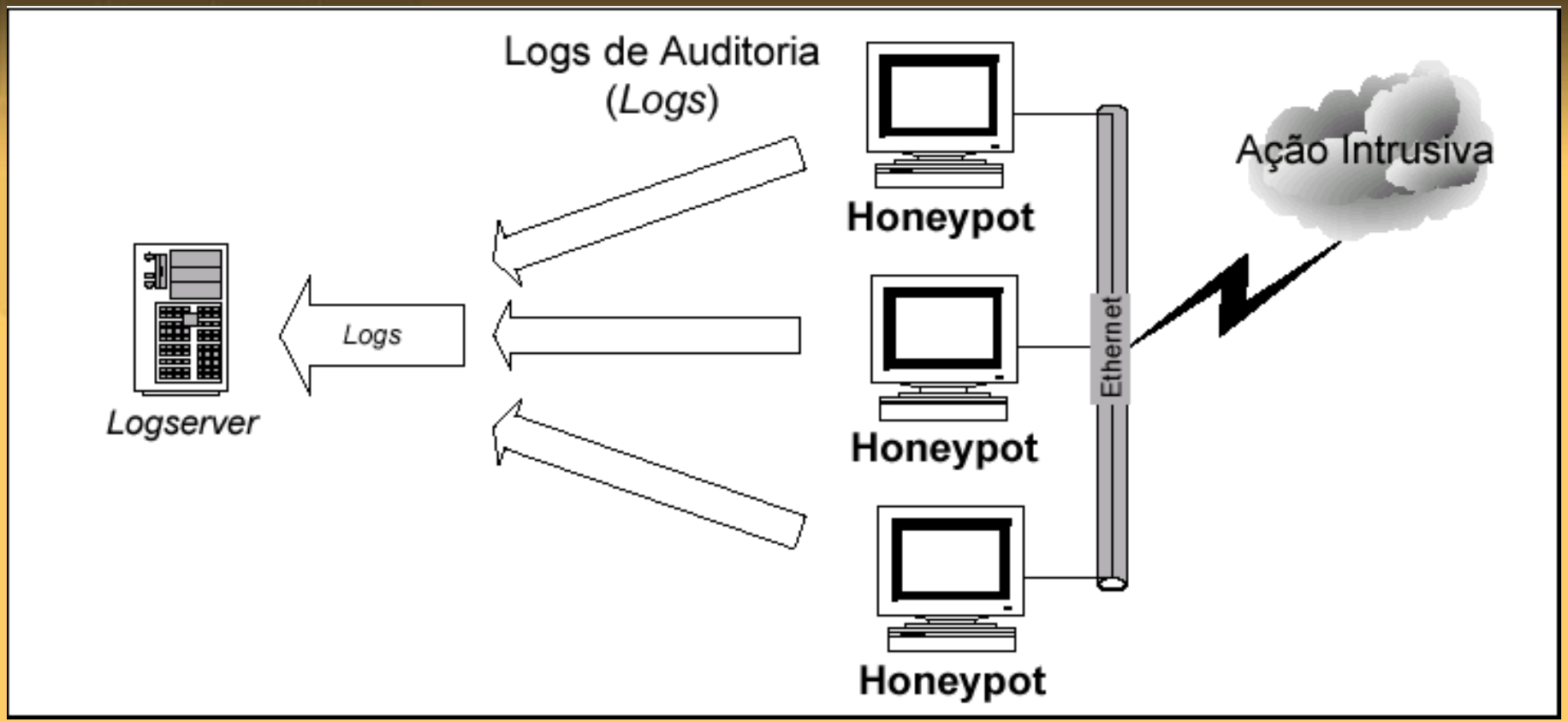


- É criado um ambiente que reflete uma rede de produção real;

Componentes de uma Honeynet

- Formada por diversos elementos, que podem ser divididos em:
  - Componentes alvos: são os honeypots;
  - Componentes de interconexão e contenção de fluxo para controle de dados (roteador,firewall);
  - Componentes de captura, armazenamento e análise (SDI, LogServer)

Componentes de uma Honeynet

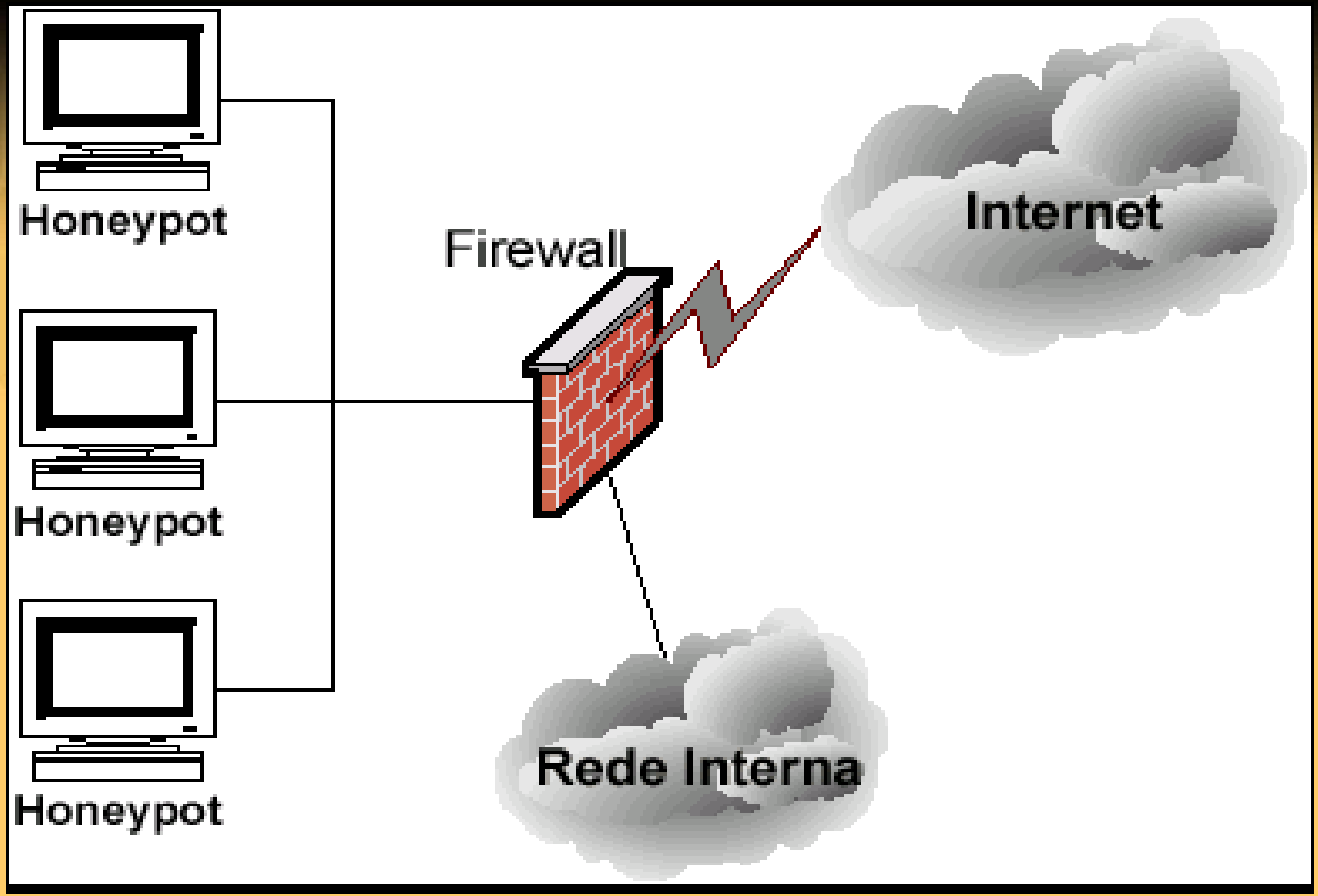


Os Logs não devem ser armazenados localmente.

Tipos de Honeynets

- **Clássica:**
  - Composta por sistemas reais (físicos)
  - Instalações específicas;
  - Sistemas operacionais variados e independentes

Honeynet Clássica



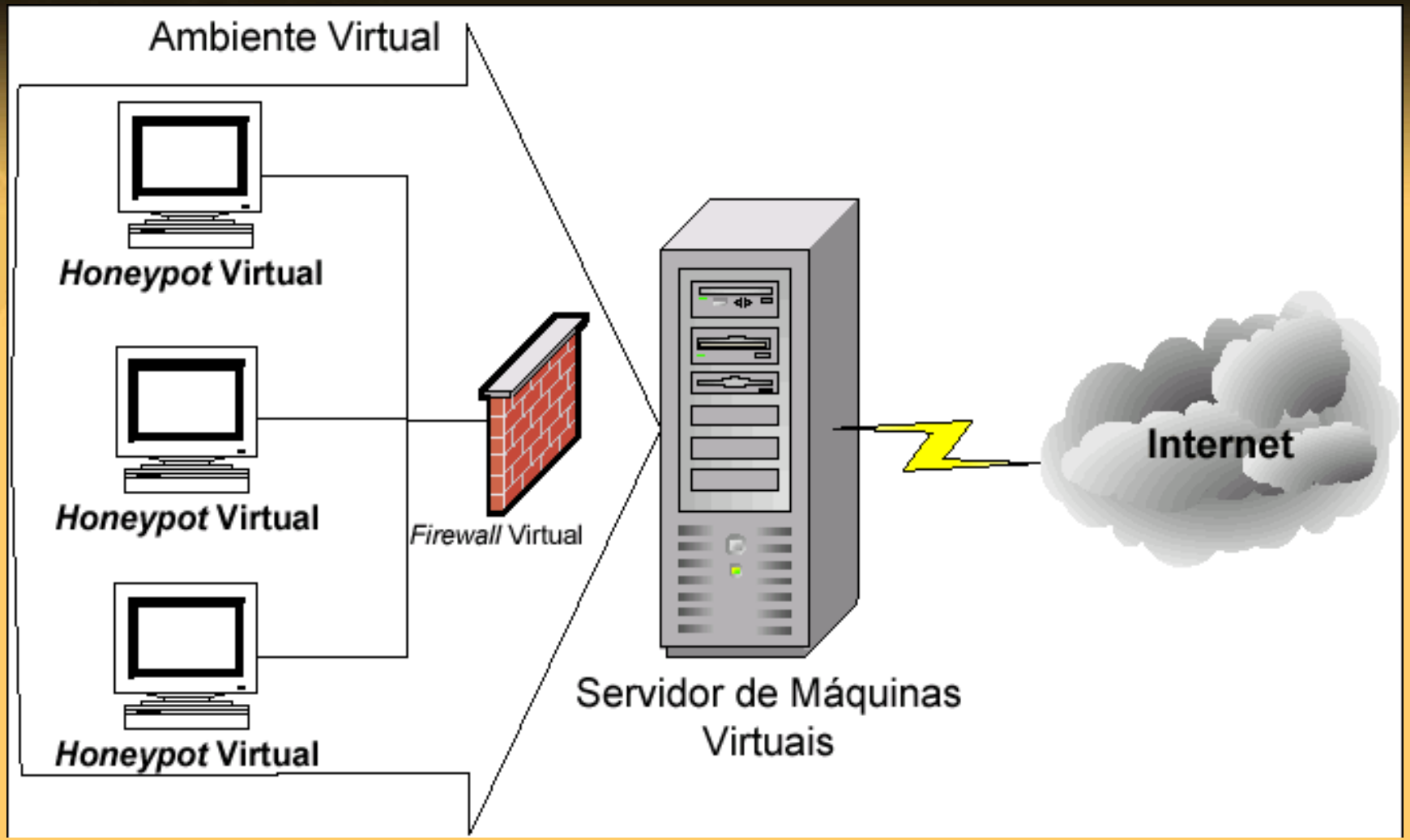
Honeynet Clássica

- **Vantagens:**
  - Dispositivos reais;
  - Mais segurança pela descentralização dos honeypots
- **Desvantagens:**
  - Custo elevado;
  - Dificuldades na instalação e administração;
  - Complexidade para manutenção;
  - Espaço alocado muito grande;

Tipos de Honeynets

- **Virtual:**
  - Composta por Honeypots virtuais (máquinas virtuais);
  - Uso de *emuladores;
  - Todo ambiente composto por uma única máquina (sistemas operacionais emulados)

Honeynet Virtual



Honeynet Virtual

- 2 categorias:
- Auto-conteção
  - *Todos os componetes em um único computador*
- Híbridas
  - *Sistema de log, geração de alertas separado do honeypot*

Honeynet Virtual

- **Vantagens:**
  - custo reduzido;
  - gerenciamento facilitado;
  - facilidade na instalação e administração;
  - menor gasto de energia elétrica, devido à menor quantidade de máquinas utilizadas

- **Desvantagens:**
  - limitação nos tipos de sistemas operacionais oferecidos pelos softwares de virtualização;
  - possibilidade de comprometimento do software de virtualização, ponto único de falha;
  - instabilidade pelo uso exaustivo de memória

Evolução da Honeynet

Ano de 1988

- Chifford Stoll, torna pública a invasão do Sistema do Lawrence Derkely Laboratory (LBL).

Ano de 1992

- Bil Cheswick publicou um artigo descrevendo o acompanhamento de uma invasão em um dos Sistemas da AT & T.

Evolução da Honeynet

- Ano de 1998
  - Fred Cohen desenvolveu o Deception Toolkit

- Ano de 1999
  - Criação do Honeynet Project
  - Criação da Honeynet Research Alliance

- Março de 2002
  - Entra em operação o projeto Honeynet.BR

Honeynet Project

- O projeto de Honeynet:
  - Organização sem fins lucrativos
  - Liderada pelo americano (Lance Spitzner)
  - É uma organização internacional

- Composição
  - Membros Ativos; e
  - Membros Especiais

Objetivos

- Melhorar a segurança da internet
  - Capiturando Ataques;
  - Compartilhando das lições aprendidas; e
  - Estimular a comunidade a se defender.

- Manerias
  - Consciência;
  - Informação
  - Ferramentas.

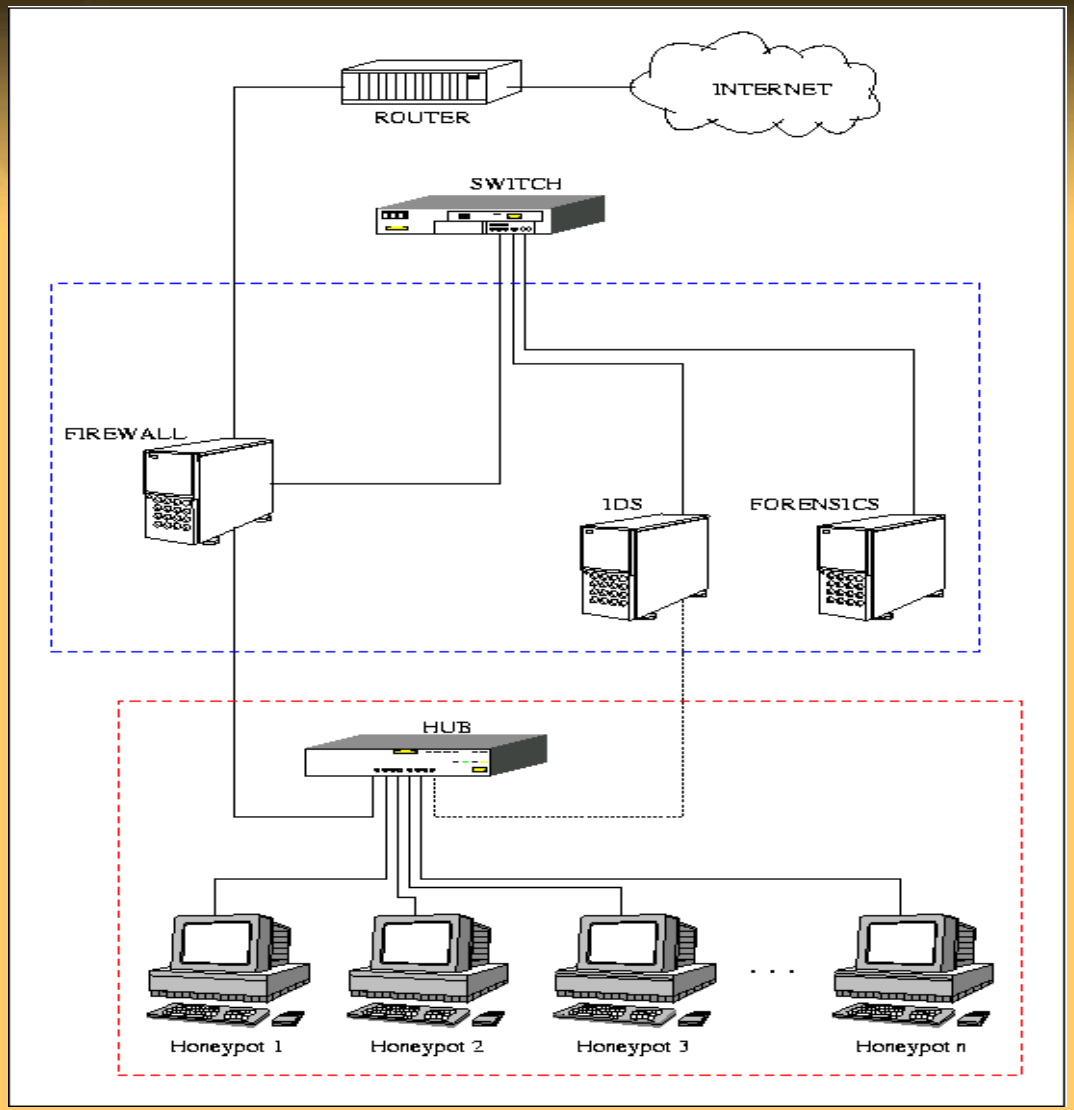
Principais colaboradores

- Christine Kilger, sustentação gráfica
- Microsoft Suporte com as ferramentas do software e de desenvolvimento, including subscrições a MSDN.
- VMware com software.

Honeynets.BR

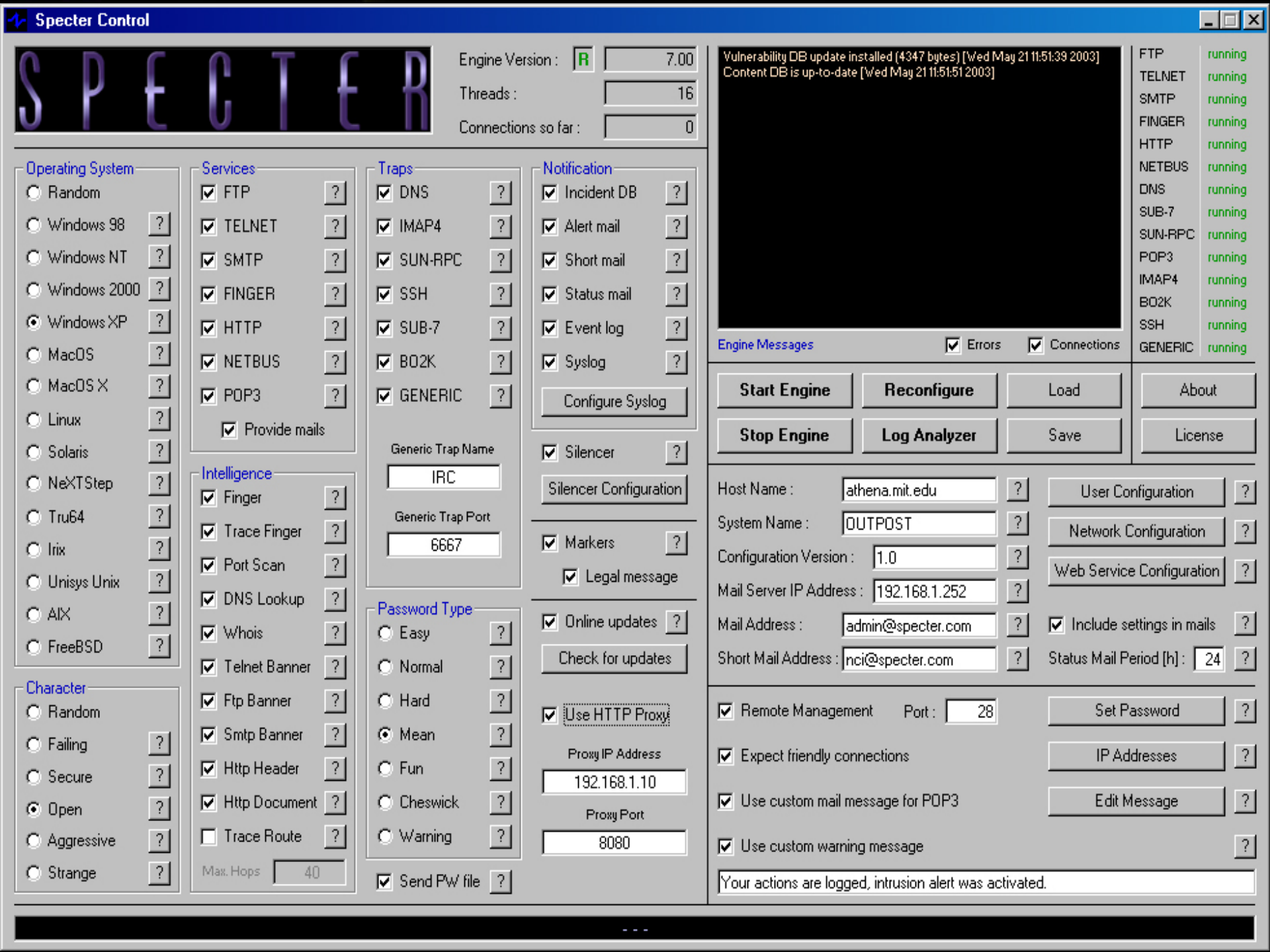
- Iniciou-se a partir de uma Palestra do Lance Sptzner – 2000
- Criada e Mantida INPE e NBSO – 2001
- Tornou-se membro da Honeynet Research Alliance- 2002.

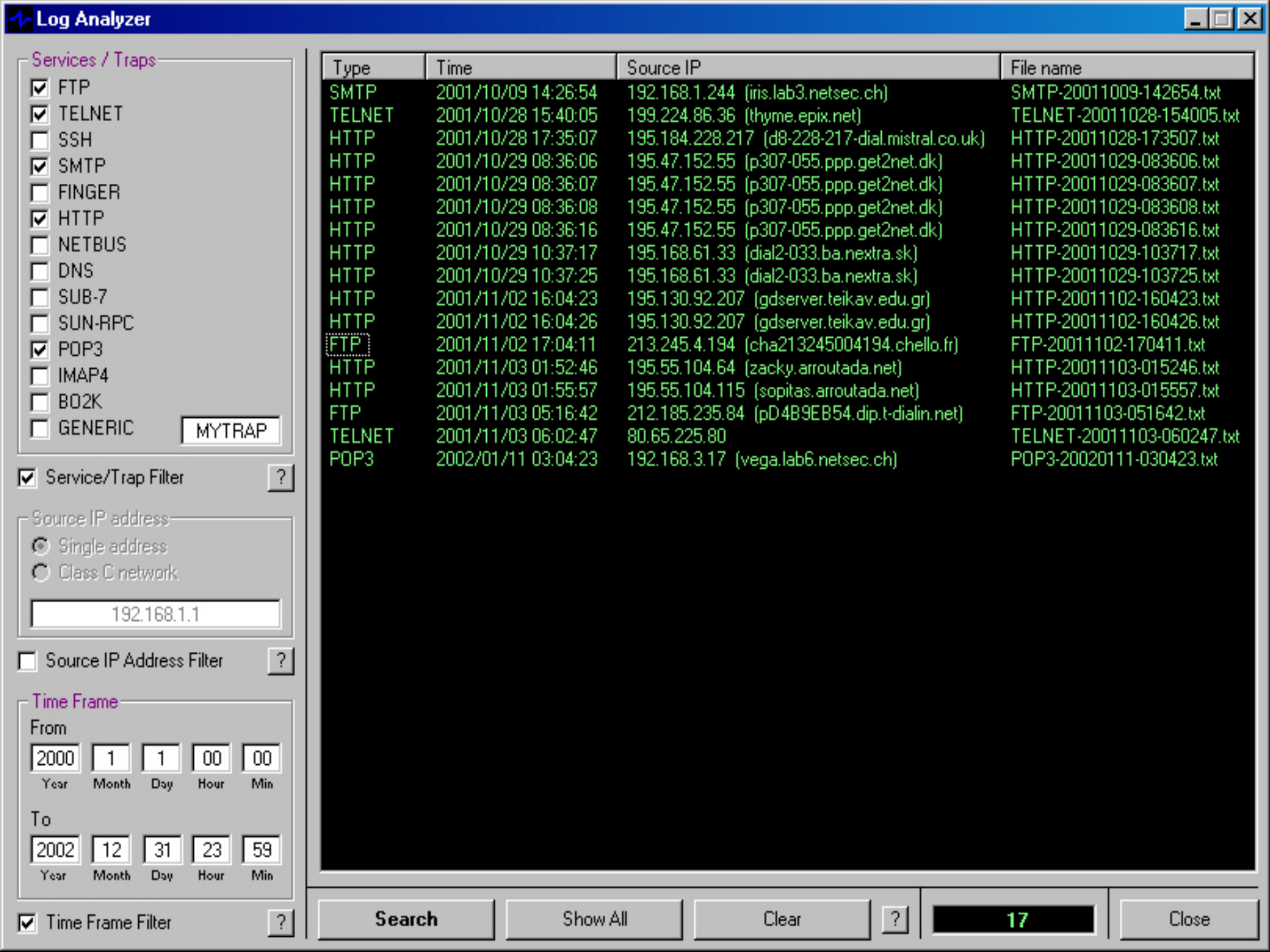
Estrutura do Honeynet

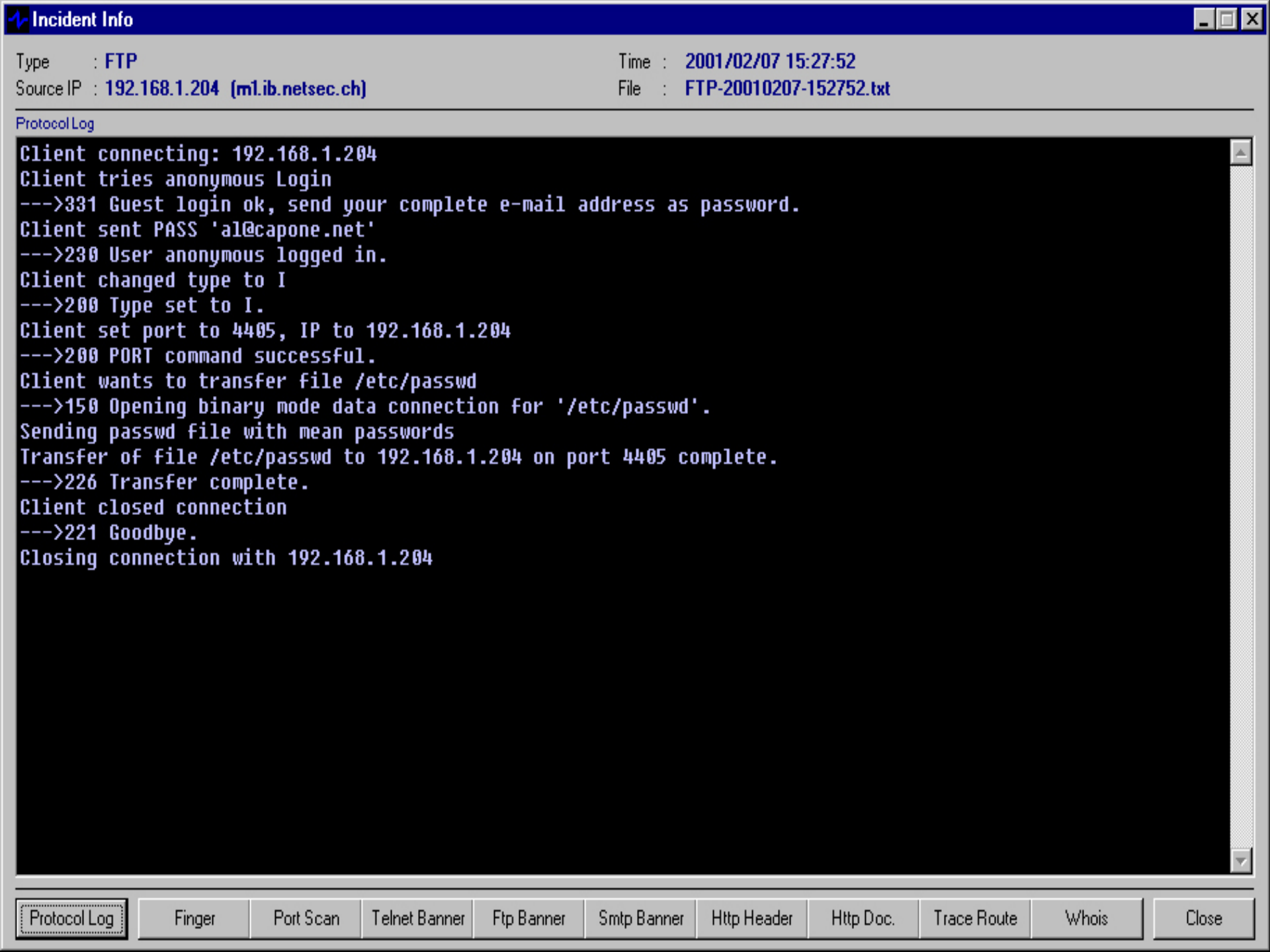


Softwares

- **Honeypots Comerciais**
  - KFSensor (windows)
    - IDS
    - **Standart** (US $199) **/ Professional** (US $199) **/ Enterprise** ?
  - Specter (windows)
    - **IDS**
    - **Emula inúmeros SO´s diferentes**
    - **Research** (US $199) **/ Light** (US $599) **/ Specter** (US $599)


Specter Control
SPECTER
Engine Version : R 7.00
Threads : 16
Connections so far : 0
Vulnerability DB update installed (4347 bytes) [Wed May 21 11:51:39 2003]
Content DB is up-to-date [Wed May 21 11:51:51 2003]
FTP running
TELNET running
SMTP running
FINGER running
HTTP running
NETBUS running
DNS running
SUB-7 running
SUN-RPC running
POP3 running
IMAP4 running
BO2K running
SSH running
GENERIC running
Engine Messages
Errors
Connections
Operating System
Random
Windows 98
Windows NT
Windows 2000
Windows XP
MacOS
MacOS X
Linux
Solaris
NeXTStep
Tru64
Irix
Unisys Unix
AIX
FreeBSD
Services
FTP
TELNET
SMTP
FINGER
HTTP
NETBUS
POP3
Provide mails
Traps
DNS
IMAP4
SUN-RPC
SSH
SUB-7
BO2K
GENERIC
Generic Trap Name
IRC
Generic Trap Port
6667
Notification
Incident DB
Alert mail
Short mail
Status mail
Event log
Syslog
Configure Syslog
Silencer
Silencer Configuration
Markers
Legal message
Online updates
Check for updates
Use HTTP Proxy
Proxy IP Address
192.168.1.10
Proxy Port
8080
Start Engine
Reconfigure
Load
About
Stop Engine
Log Analyzer
Save
License
Host Name : athena.mit.edu
System Name : OUTPOST
Configuration Version : 1.0
Mail Server IP Address : 192.168.1.252
Mail Address : admin@specter.com
Short Mail Address : nci@specter.com
User Configuration
Network Configuration
Web Service Configuration
Include settings in mails
Status Mail Period [h] : 24
Intelligence
Finger
Trace Finger
Port Scan
DNS Lookup
Whois
Telnet Banner
Ftp Banner
Smtp Banner
Http Header
Http Document
Trace Route
Max. Hops 40
Password Type
Easy
Normal
Hard
Mean
Fun
Cheswick
Warning
Send PW file
Remote Management
Port : 28
Set Password
Expect friendly connections
IP Addresses
Use custom mail message for POP3
Edit Message
Use custom warning message
Your actions are logged, intrusion alert was activated.
Character
Random
Failing
Secure
Open
Aggressive
Strange


Log Analyzer
Services / Traps
FTP
TELNET
SSH
SMTP
FINGER
HTTP
NETBUS
DNS
SUB-7
SUN-RPC
POP3
IMAP4
BO2K
GENERIC
MYTRAP
Service/Trap Filter
?
Source IP address
Single address
Class C network
192.168.1.1
Source IP Address Filter
?
Time Frame
From
2000 1 1 00 00
Year Month Day Hour Min
To
2002 12 31 23 59
Year Month Day Hour Min
Time Frame Filter
?
Type | Time | Source IP | File name
SMTP 2001/10/09 14:26:54 192.168.1.244 (iris.lab3.netsec.ch) SMTP-20011009-142654.txt
TELNET 2001/10/28 15:40:05 199.224.86.36 (thyme.epix.net) TELNET-20011028-154005.txt
HTTP 2001/10/28 17:35:07 195.184.228.217 (d8-228-217-dial.mistral.co.uk) HTTP-20011028-173507.txt
HTTP 2001/10/29 08:36:06 195.47.152.55 (p307-055.ppp.get2net.dk) HTTP-20011029-083606.txt
HTTP 2001/10/29 08:36:07 195.47.152.55 (p307-055.ppp.get2net.dk) HTTP-20011029-083607.txt
HTTP 2001/10/29 08:36:08 195.47.152.55 (p307-055.ppp.get2net.dk) HTTP-20011029-083608.txt
HTTP 2001/10/29 08:36:16 195.47.152.55 (p307-055.ppp.get2net.dk) HTTP-20011029-083616.txt
HTTP 2001/10/29 10:37:17 195.168.61.33 (dial2-033.ba.nextra.sk) HTTP-20011029-103717.txt
HTTP 2001/10/29 10:37:25 195.168.61.33 (dial2-033.ba.nextra.sk) HTTP-20011029-103725.txt
HTTP 2001/11/02 16:04:23 195.130.92.207 (gdserver.teikav.edu.gr) HTTP-20011102-160423.txt
HTTP 2001/11/02 16:04:26 195.130.92.207 (gdserver.teikav.edu.gr) HTTP-20011102-160426.txt
FTP 2001/11/02 17:04:11 213.245.4.194 (cha213245004194.chello.fr) FTP-20011102-170411.txt
HTTP 2001/11/03 01:52:46 195.55.104.64 (zacky.arroutada.net) HTTP-20011103-015246.txt
HTTP 2001/11/03 01:55:57 195.55.104.115 (sopitas.arroutada.net) HTTP-20011103-015557.txt
FTP 2001/11/03 05:16:42 212.185.235.84 (pD4B9EB54.dip.t-dialin.net) FTP-20011103-051642.txt
TELNET 2001/11/03 06:02:47 80.65.225.80 TELNET-20011103-060247.txt
POP3 2002/01/11 03:04:23 192.168.3.17 (vega.lab6.netsec.ch) POP3-20020111-030423.txt
Search
Show All
Clear
?
17
Close


Incident Info
Type : FTP
Source IP : 192.168.1.204 (ml.ib.netsec.ch)
Time : 2001/02/07 15:27:52
File : FTP-20010207-152752.txt
Protocol Log
Client connecting: 192.168.1.204
Client tries anonymous Login
--->331 Guest login ok, send your complete e-mail address as password.
Client sent PASS 'al@capone.net'
--->230 User anonymous logged in.
Client changed type to I
--->200 Type set to I.
Client set port to 4405, IP to 192.168.1.204
--->200 PORT command successful.
Client wants to transfer file /etc/passwd
--->150 Opening binary mode data connection for '/etc/passwd'.
Sending passwd file with mean passwords
Transfer of file /etc/passwd to 192.168.1.204 on port 4405 complete.
--->226 Transfer complete.
Client closed connection
--->221 Goodbye.
Closing connection with 192.168.1.204
Protocol Log
Finger
Port Scan
Telnet Banner
Ftp Banner
Smtp Banner
Http Header
Http Doc.
Trace Route
Whois
Close

Softwares

- **Honeypots Livres**
  - Honeyd (autor Niels Provos)
    - Um dos principais aplicativos para construção de honeypots;
    - Pode monitorar todas as portas baseadas em UDP e TCP
    - Emula vários sistemas operacionais;
    - Grande facilidade de configuração (arquivo);
    - OpenSource (permite alteração no código)

Softwares

Honeyd configuration file

Windows computers
create windows
set windows personality "Windows NT 4.0 Server SP5-SP6"
set windows default tcp action reset
set windows default udp action reset
add windows tcp port 80 "perl scripts/iis-0.95/iisemul8.pl"
add windows tcp port 139 open
add windows tcp port 137 open
add windows udp port 137 open
add windows udp port 135 open
set windows uptime 3284460
bind 200.0.0.4 windows

Softwares

Honeyd configuration file

Linux 2.4.x computer
create linux
set linux personality "Linux 2.4.16 - 2.4.18"
set linux default tcp action reset
set linux default udp action reset
add linux tcp port 110 "sh scripts/pop3.sh"
add linux tcp port 25 "sh scripts/smtp.sh"
add linux tcp port 21 "sh scripts/ftp.sh"
set linux uptime 3284460
bind 200.0.0.5 linux

Conclusão

- *Honeypots e Honeynets* são recursos de segurança planejados para serem comprometidos, com o objetivo de estudar os ataques e os atacantes, suas técnicas, motivos e ferramentas utilizadas; podem ser utilizados também para desviar a atenção dos destinos reais.

- Embora sejam de grande valor, os *honeypots e honeynets* não devem substituir nenhuma técnica de segurança ativa na rede de uma empresa.

Referências Bibliográficas

http://www.cert.br/docs/whitepapers/honeypots-honeynets/

http://www.honeynet.org.br

http://www.honeynet.org

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

http://www.keyfocus.net/kfsensor/

http://www.specter.com

http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=408&pagina=1