Estudo de ferramentas para honeypots instaláveis em máquinas virtuais perfazendo uma honeynet virtual

Sidney Simões e Silva Filho

Curso de Redes e Segurança de Sistemas
Pontifícia Universidade Católica do Paraná

Curitiba, outubro de 2009

Resumo

A invasão de redes e sistemas ligados a internet é uma realidade. A cada dia surgem novas ameaças. Firewalls, roteadores, filtros e outros bloqueios são necessários. São soluções passivas. Potes de mel (honeypots) são iscas para fisgar atacantes e invasores de redes. Estimula-se a invasão para que se possa aprender com ela. Com os computadores atuais e softwares de virtualização é possível montar um conjunto de honeypots com firewall integrado em apenas um equipamento. .

1. Introdução

Quando o assunto é relativo a segurança de redes e de sistemas existem atitudes passivas e ativas. Roteadores, firewall, filtros, bloqueios, são atitudes passivas. Atitudes ativas são possíveis como por exemplo: sistemas para prevenir intrusos (IPS). Mas estes sistemas não são perfeitos já que sistemas possuem falhas que quando descobertas podem ser exploradas no mesmo dia.

Para conhecer melhor o invasor surgiu então a idéia de criar algo atraente para os invasores. Um pote-de-mel que estando sobre o controle do administrador, permite que se observe e se aprenda como os invasores de redes e sistemas agem.

Ao colocar um pote-de-mel em sua rede o administrador passa a ser pró-ativo em relação ao problema de segurança. Passa a conhecer melhor como atuam e a motivação do inimigo. Com isto os invasores podem combatidos de forma mais eficiente.

Mas apenas um pote-de-mel não é o suficiente, o ideal é termos vários sabores, ou seja, vários computadores em diversos sistemas operacionais em uma rede heterogênea. E é fundamental que estes equipamentos estejam sob controle do administrador.

Uma possibilidade para fazer isto de forma eficiente é usando a virtualização, onde um só computador simularia diversas máquinas.

2. Honeypots & Honeynet, Virtualização

2.1 Honeypot

O honeypot ou pote-de-mel é uma "armadilha destinada a atrair intrusos que tentam invadir um sistema. Consiste em configurar um computador de modo a deixá-lo vulnerável a invasões." [1].

O verbete pote-de-mel não aparece no dicionário Houaiss. Neste trabalho a opção será pelos termos: honeypot (pote de mel), honeynet (rede de potes de mel) e honeywall (firewall da rede de potes de mel). O dicionário de inglês Webster define honeypot como "algo que atrai ou que é desejável", sendo o termo usado 1924.

A idéia de atrair o "inimigo" ou o "invasor" para uma armadilha sempre foi um recurso

utilizado na história da humanidade, principalmente nas guerras. Nos século V a.C. Sun-Tzu já escrevia em seu texto, a Arte da Guerra.

"Uma guerra também é engodo. Quando você for capaz, finja incapacidade, Quando você for bom deslocando unidades finja que é incapaz. Quando você estiver perto finja estar longe, Quando você estiver longe, finja estar perto." no capítulo 1 parágrafo 18. [4]

O conceito de honeypot foi introduzido por Cliff Stoll no livro de 1990 "The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage" (O ovo do cuco, rastreando um espião pelo labirinto da espionagem de computadores) e também por Bill Cheswick em 1991 no texto "An Evening With Berferd, in which a Hacker is Lured, Endured, and Studied" (Uma tarde com Berferd em que um hacker é enganado por uma isca, tolerado e estudado). [14]

Um honeypot então é basicamente uma isca, um engodo. Serve para atrair invasores de computadores de todos os tipos: hackers, crackers, script kiddies (garotos que usam programas prontos), curiosos e até outros administradores de sistemas que estão cruzando os limites legais ao fazerem "testes" nas redes alheias.

Um honeypot então tem que parecer bastante atraente para o atacante. Segundo Provos, [2] uma honeypot é proativa e o seu valor pode ser medido pela quantidade de informações que podem ser obtidas com ela.

As honeypot podem ser classificadas em níveis em que cada um permite um certo grau de interatividade com o sistema.

- Baixa interação: simula apenas parte do sistema, como por exemplo, alguns protocolos de rede e alguns comandos. Com isto o usuário é enganado ao pensar que está se conectando a um sistema de verdade

- Alta interação: é um sistema operacional completo rodando os sistemas de produção

Alguns autores como Spitzner [8] fazem referência também a honeypots de média interação que se situa entre a baixa e a alta interação.

A tabela a seguir mostra uma comparação entre os níveis de interação possíveis em uma honeypot

Nível de interação	Trabalho para instalar e configurar	Trabalho para ativar e manter	Coleta de informações	Nível de risco
Baixo	Fácil	Fácil	Limitada	Baixo
Médio	Mediano	Mediano	Variável	Médio
Alto	Difícil	Difícil	Extensa	Alto

Tabela 1 - Níveis de interação, Spitzner, L., 2002

Mas como existe uma variedade de sistemas operacionais e uma variedade de sistemas de produção, um honeypot sozinho pode não ser atraente para os atacantes. São necessárias então algumas máquinas que não podem apenas serem instaladas e deixadas a própria sorte. Certos cuidados têm que observados:

- A máquina tem que ser monitorada
- As atividades do invasor devem ser capturadas e analisadas
- A máquina não pode servir de base para ataques a outros computadores
- O intruso não deve notar que está sendo enganado e monitorado

Surge então o conceito de honeynet, ou seja, uma rede de honeypots que estejam sob um ambiente controlado.

2.2 Honeynet

O conceito de honeynet iniciou em 1999 quando Lance Spitzner, fundador do *Honeynet Project* publicou um trabalho "To Build a Honeypot". O intuito era aprender com as ferramentas usadas, as táticas e a motivação dos atacantes.

Uma honeynet é formada por um conjunto de honeypots que simulam uma rede de produção. É uma rede verdadeira mas é configurada para que as suas atividades possam ser monitoradas, gravadas, e em certo grau, controladas. É uma rede arquitetada para ser invadida onde se houver tráfego é provavelmente feito pelos invasores [3]

O Projeto Honeynet iniciou informalmente em abril de 1999 liderado por Spitzner. Hoje é um projeto internacional (ver apêndice A) destinado a desenvolver e analisar dados de honeynets e honeypots, promovendo a pesquisa sobre como os invasores agem. É uma organização sem fins lucrativos.

Segundo os estudos do Projeto Honeynet, uma honeynet para ser bem sucedida tem que lidar com dois requisitos críticos: o controle e a captura dos dados.

O controle dos dados é o controle de toda a atividade do invasor. Este controle pode ser feito de forma automática ou com a intervenção do administrador.

A captura dos dados é o armazenamento de todas as informações geradas pelo invasor. Com o controle e a captura dos dados, aprende-se sobre o invasor.

Inicialmente o projeto honeynet sugeriu a seguinte arquitetura conhecida como geração um ou GEN I como é a sigla usada pelo Projeto Honeynet. Esta rede é projetada para que se tenha o controle e a captura dos dados.

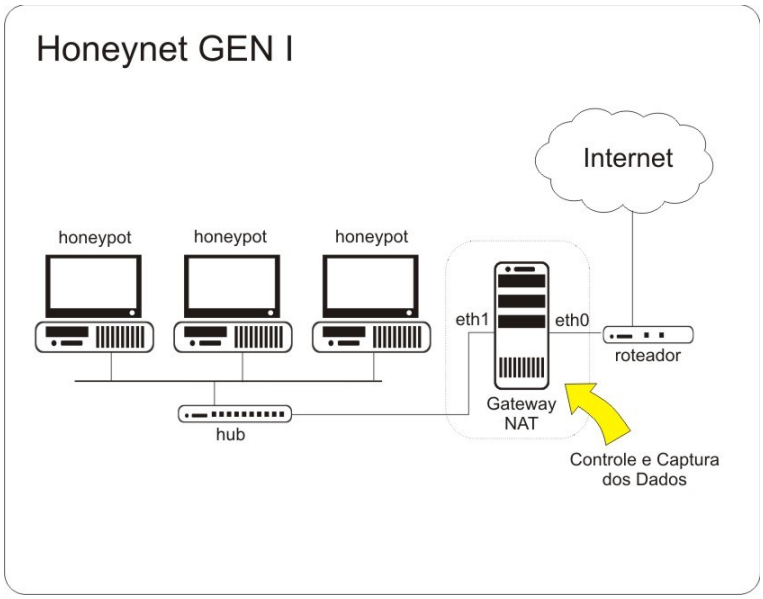


Figura 1 – Uma honeynet geração I

Um roteador isola a rede de produção. Um firewall de camada 3 (do modelo OSI) é o gateway entre a internet e a rede dos computadores honeypot. O firewall faz NAT e controla todas as conexões que entram e saem. Ele permite todas as conexões de entrada, mas limita a conexões de saída. É mantido um log de todas as conexões que o atacante faz.

Segundo Levine, [7] a arquitetura de geração 1 é de certa forma limitada no requisito captura de dados e controle de dados. Ela é muito efetiva em detectar ataques automáticos ou ataques feitos por iniciantes. Suas limitações no controle de dados permitem que os atacantes saibam que estão em uma honeynet.

Em 2002 então o Projeto Honeynet sugeriu uma nova arquitetura, chamada de GEN II.

Foi feita uma mudança e ao invés do gateway usar a NAT, passou-se a usar também a camada 2 (do modelo OSI). A máquina passou a atuar como um gateway bridge.

Com esta técnica ficou mais difícil para o atacante detectar que está em uma honeynet. E os endereços IP podem até ser da mesma faixa da rede de produção. Assim como na GEN I, todo o tráfego que entra e sai da Honeynet tem que passar pelo Gateway.

O controle dos dados foi melhorado, desta forma um filtro de pacotes é usado para determinar o bloqueio, a passagem ou a modificação do pacote (neste caso um pacote maligno para a ser benigno).

Introduziu-se também uma VPN (com endereços IP próprios) entre a máquina gateway, para que outra máquina pudesse gerenciar e receber dados da honeynet.

Como esta máquina funciona como uma parede (wall) de proteção, o projeto Honeynet nomeou a mesma de Honeywall.

Com o aumento da complexidade uma honeynet Gen II era mais difícil de ser instalada e mantida.

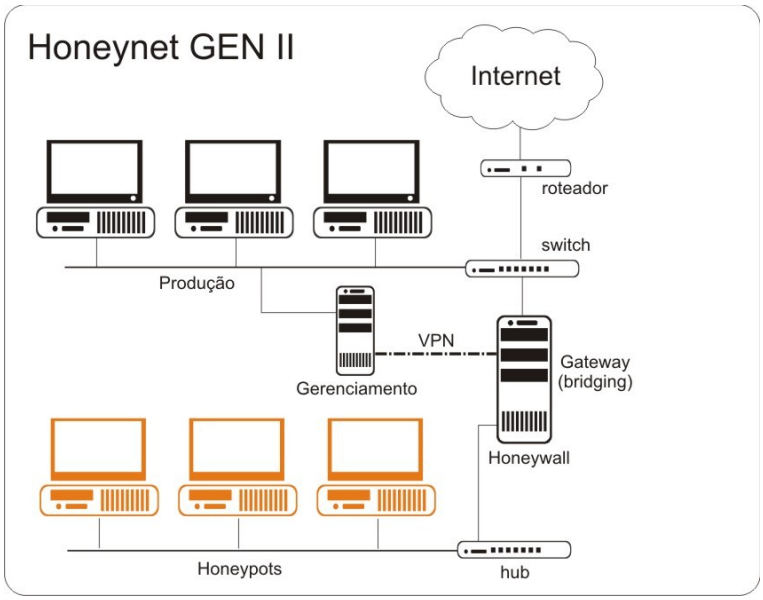


Figura 2 – Uma honeynet geração II

Com a geração II obteve-se uma rede ligada a rede de produção. É feita para ser analisada, atacada e explorada. Ao receber os ataques ela protege os sistemas de produção que queremos que não sejam atacados.

Esta arquitetura trouxe as seguintes vantagens:

- Poucos dados, mas muito valiosos
- Redução do falso positivo - alarme quando não existe um ataque
- Reduz falso negativo - falta de alarme quando tem um ataque verdadeiro
- Recursos pré definidos - não há impacto na rede dos sistemas de produção
- Conexões criptografadas são registradas
- Os ataques IPv6, muito usados pelos invasores, podem ser registrados

Mas algumas desvantagens também vieram, a arquitetura é mais complexa, e há a necessidade de instalar e configurar diversas máquinas. Além disto, depois de um ataque as máquinas teriam que voltar a seu estado inicial, para ficarem pronta para o próximo ataque.

E não se poderia ter erros de configuração, pois neste caso os invasores saberiam que estavam em uma armadilha e fugiriam. Se o sistema nunca for atacado é inútil, não serve para nada.

Em seu livro de 2002, Provos [2] comenta que é praticamente impossível colocar

honeypots físicas para cada endereço IP, neste caso necessitamos de um honeypot virtual.

Com o constante avanço da computação temos hoje em dia processadores rápidos. Nestes equipamentos pode-se colocar um sistema de virtualização, e em apenas um computador executar várias honeypots virtuais formando uma honeynet.

2.3 Virtualização

A virtualização existe há mais de 40 anos, sendo que a pioneira neste campo foi a IBM com o sistema VM usado inicialmente em sua linha de computadores IBM/370. No mundo dos microcomputadores a virtualização voltou a ser importante no ano de 1999 quando a empresa americana VMWare introduziu o seu primeiro produto para virtualização o "VMware Virtual Platform", baseado nas pesquisas de seus fundadores na Universidade de Stanford [6]

Atualmente a virtualização é tão importante que nos processadores mais novos ela tem apoio por hardware como nas tecnologias AMD-V e a Intel-VT. Estes recursos trazem um desempenho superior para as máquinas virtuais.

Ainda assim uma máquina mais simples como, por exemplo, um Pentium IV é capaz de rodar alguns sistemas operacionais em conjunto bastando que tenha memória RAM suficiente para as máquinas virtuais.

3 Criando a honeynet virtual

3.1 O sistema de virtualização

O computador onde a honetnet ficará hospedada roda o sistema operacional Linux distribição Fedora 11. Testes indicam que para virtualização o Linux é superior ao Windows.

Para as máquinas virtuais tínhamos algumas opções pagas no mercado como a linha de produtos para virtualização da VMWare (que possui produtos gratuitos e pagos). Na linha de produtos para Microsoft Windows tínhamos o Virtual PC, o Virtual Server e o Hyper-V.

Na área de sistemas abertos temos o QEMU, o KVM (Kernel-based Virtual Machine) e o Virtualbox de Sun Microsystems (que baseou sua parte do seu código no QEMU, mas atualmente é um sistema completo de virtualização).

Outro sistema que vem sido muito utilizado é o Xen que trabalhava com paravirtualização (no modo paravirtualizado o sistema operacional deve ser modificado, pois algumas instruções podem dar problema durante a execução) [12], mas em sua versão 3.0 consegue fazer uma virtualização total se o processador Intel tiver a tecnologia VT.

O escolhido foi o Virtualbox da Sun. Ele mostrou ser o mais adequado na máquina disponível para os testes (Pentium IV com 2GB de memória) e possuir os modos de rede necessários para os testes (na versão 3.0.8)

Com isto temos a base para instalar os honeypots, criar a honeynet e também o colocar o honeywall virtualizado, todos na mesma máquina.

3.3 O Honeywall

O projeto Honeynet disponibiliza um CD-ROM [9] com um sistema honeywall completo, é um sistema Linux modificado a partir da distribuição CentOS (que é derivado direto o RedHat Enterprise Linux). No site existe uma imagem ISO que pode ser gravada em um CD. O sistema foi testado e a versão Roo-2008 rodou com sucesso dentro do Virtualbox.

O CD vem com todas as ferramentas e sugere uma arquitetura mais avançada ainda do que a honeynet de geração 2. Nesta nova arquitetura o honeywall tem um analisador de pacotes, o Snort-In-Line, derivado do programa Snort de detecção de intrusão (IDS). O

Snort-in-line não só detecta mas rejeita ou modifica pacotes de acordo com regras pré-determinadas. É considerado um IPS (Intrusion Prevention System) "Sistema de Prevenção de Intrusos". O Snort IDS e o Snort IPS foram desenvolvidos pela Sourcefire é são projetos de código aberto. [13]

O sistema usa Iptables no modo bridge, que é fundamental na configuração do gateway da honeywall. E o sistema Linux CentOS foi modificado para ter apenas os serviços essenciais e necessários para o funcionamento da honeywall.

3.4 Honeypot da família Windows

Qualquer sistema operacional da família Windows consegue rodar dentro do Virtualbox, no nosso teste o Windows 2000 foi instalado com sucesso e também o XP. Não foram testados outros sistemas (Vista, 2003, 2008), mas teoricamente não há empecilho uma vez que todo o conjunto das instruções do microprocessador está disponível para o sistema operacional.

Como o Windows trabalha com pacotes periódicos de atualização, é possível então criar versões desprotegidas do Windows como, por exemplo, um Windows XP que tenha sido atualizado até o service pack 2, não tendo sido instalada o 3. A mesma técnica pode ser aplicado em toda a família de sistemas operacionais.

3.5 Honeypot da família Linux

Todas as distribuições Linux podem ser colocadas para rodar dentro do Virtualbox, neste presente trabalho optamos pelo Dan Small Linux, um pequena distribuição Linux, compatível com a memória da máquina de testes.

3.6 Honeyd um programa daemon que simula baixa interatividade

Uma forma de simular máquinas em uma honeynet é usar um programa daemon que simula alguns sistemas operacionais. Um programa muito utilizado é o Honeyd.

Ele consiste em um programa daemon que junto com scripts que simula diversos sistemas operacionais. Foi desenvolvido por Niel Pavos da Universidade de Michigan. Conta atualmente com versões Unix e Windows. [15]

O honeyd é configurável pode se escolher as portas tcp e udp abertas, ligar scripts nas portas, ajustado qual sistema operacional irá aparecer para invasor criando IPs virtuais. Ele é uma opção para um honeypot de baixa interatividade, ou seja, o usuário é limitado nos comandos que pode executar.

Uma utilização possível do honeyd na honeynet virtual seria criar várias máquinas falsas em uma máquina virtual, simulando vários sistemas operacionais, sem gastar muito os recursos (memória, CPU), do computador principal onde se hospeda a honeynet.

O Honeyd possui o arquivo honey.conf, no quadro abaixo parte do script de configuração onde se simula uma máquina 2000 dentro de um XP.

```
### Standard Windows 2000 computer
create win2k
set win2k personality "Windows 2000 server SP2"
set win2k default tcp action reset
set win2k default udp action reset
set win2k default icmp action block
set win2k uptime 3567
set win2k droprate in 13
dd win2k tcp port 21 "sh scripts/win32/win2k/msftp.sh $ipsrc $sport $ipdst $dport"
add win2k tcp port 25 "sh scripts/win32/win2k/exchange-smtp.sh $ipsrc $sport $ipdst $dport"
# This will redirect incomming windows-filesharing back to the source
```

```
add win2k udp port 137 proxy $ipsrc:137
add win2k udp port 138 proxy $ipsrc:138
add win2k udp port 445 proxy $ipsrc:445
add win2k tcp port 137 proxy $ipsrc:137
add win2k tcp port 138 proxy $ipsrc:138
add win2k tcp port 139 proxy $ipsrc:139
add win2k tcp port 445 proxy $ipsrc:445
bind 10.1.1.56 win2k
```

Tabela 2 – Exemplo de script para o honeyd

3.7 Sebex – modificando o núcleo dos sistemas operacionais

Tanto nas arquiteturas da geração I como na geração II as honeypots devem ter possuir sistemas de coleta das atividades do invasor. Esta captura dos dados é feita com programas especiais que mandam esta informação para o honeywall. São programas que modificam o núcleo dos sistemas operacionais e permitem a captura do que o invasor está teclando na honeypot sendo invadida. Esta captura tem que ser feita de forma invisível ao invasor.

O Sebek é um modulo para ser instalado nos honeypots de alta interatividade com o propósito de coletar dados extensivamente. Permite que o administrador colete informações sobre as atividades no sistema como o que foi teclado, mesmo em ambientes criptografados. Atualmente tem versões para Windows e para Linux.

Ele possui duas partes o modulo para instalar nos clientes e o módulo do servidor. No CD Roo-2008 o módulo servidor é instalado automaticamente.

Para instalar no Windows o Sebek foi baixado direto do site do Projeto Honeynet [10].

O Sebek se instala de forma escondida (tal como um rootkit) tanto no Windows como no Linux. As telas de configuração abaixo mostram que pode ser configurado o endereço MAC (falso, de preferência o do próximo nó), o IP (falso, de preferência o do próximo nó) e a porta do servidor para onde os dados capturados serão enviados.

Existe também o numero mágico que modifica os pacotes de forma que ele seja criptografado e possa ser decodificado pelo Sebex no servidor. Todas as máquinas na honeynet que usam Sebek devem usar o mesmo numero mágico.

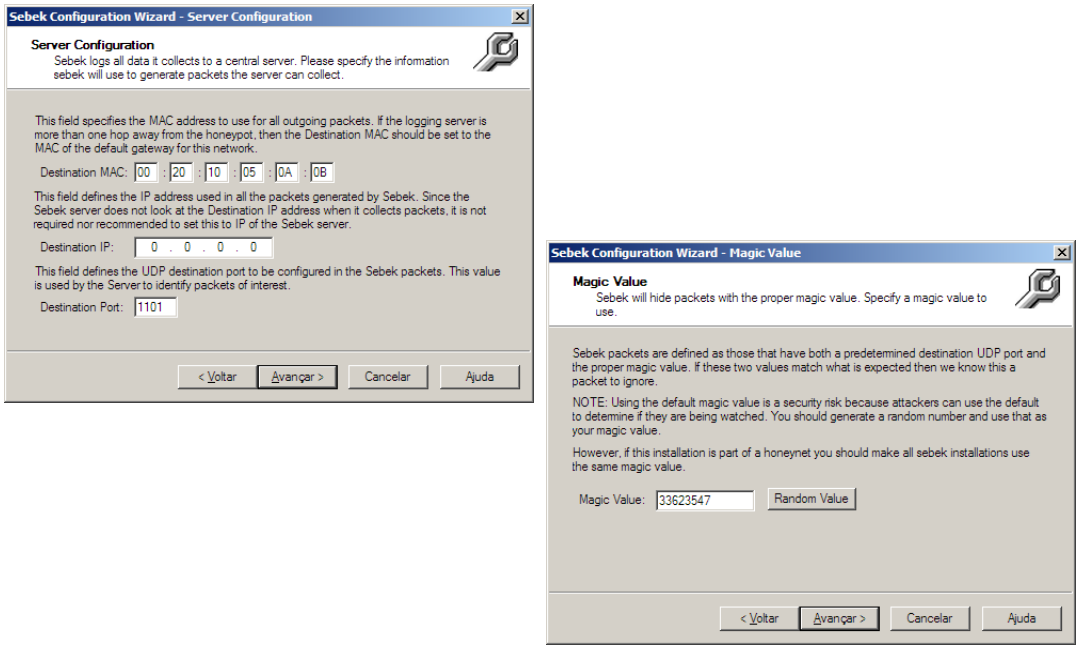


Figura 3 – telas de instalação do Sebek no Windows

3.7 A arquitetura da honeynet virtual

A arquitetura da honeynet ficou como na figura 5. Os honeypots agora passam a ser virtuais. A honeywall também roda em uma máquina virtual.

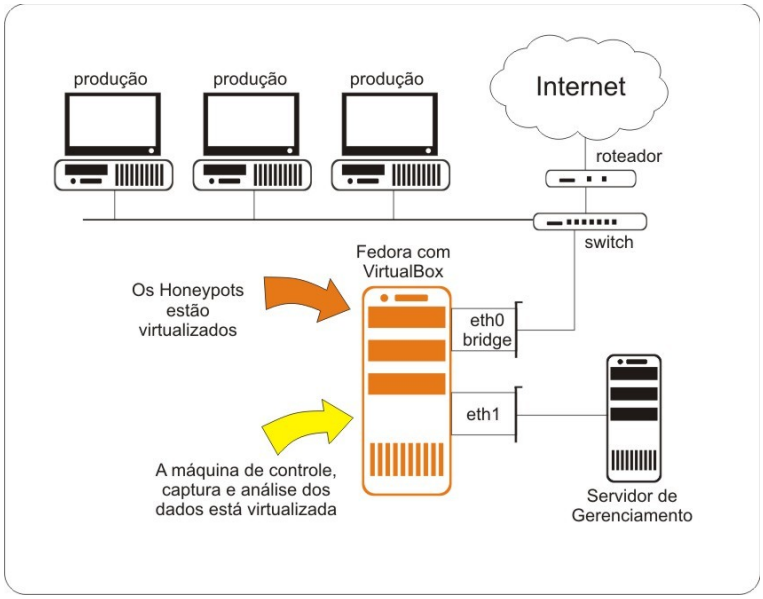


Figura 4 – Diagrama de uma configuração de honeynet virtualizada

A máquina tem duas placas de rede reais. Uma placa é usada para ligar-se ao roteador e a outro é usada para se conectar de modo segura ao sistema de gerenciamento.

Para se entender melhor a arquitetura da honeynet a figura abaixo mostra o fluxo da informação separado em tráfego da produção (azul), tráfego dos ataques (vermelho) e tráfego do gerenciamento (verde)

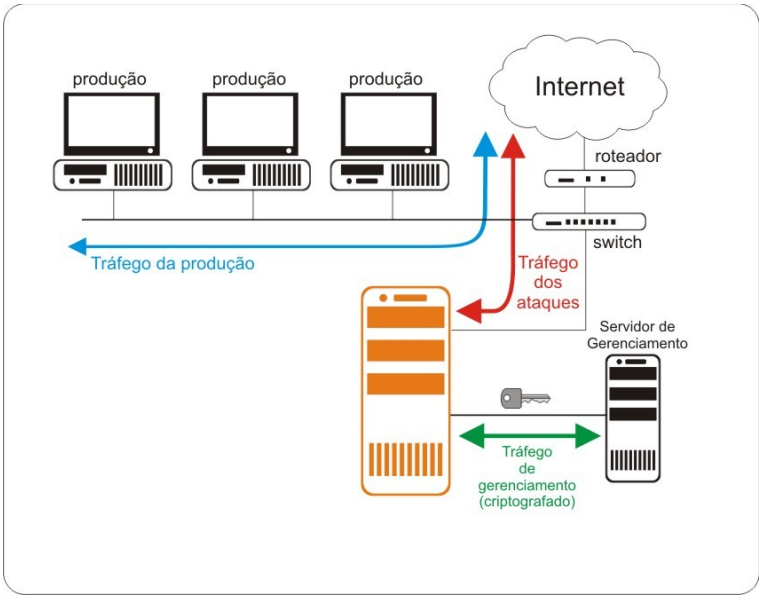


Figura 5 – Setas indicam o fluxo da informação

Dentro do computador as máquinas virtuais ficaram da seguinte forma, são quatro máquinas virtuais. A virtual 1, é a Honeywall, responsável pelo controle, captura e análise dos dados (filtrando os pacotes quando necessário).

As máquinas virtuais restantes fazem parte da rede de honeypots, rodando Win2000, e uma distribuição do Linux.

A figura 7 mostra como fica a configuração dentro da máquina virtual. A placa de rede eth0 é mapeada em forma de bridge para a rede virtual vboxeth0 (10.0.0.0/24), a placa de rede real eth1 é mapeada em forma de bridge para a vbox-eth2 com endereço distinto (10.10.10.0/24)

Para a rede virtual dentro da máquina o Virtualbox disponibiliza a forma "host interface" (suportado nativamente). Com isto é possível colocar qualquer endereço nas máquinas virtuais honeypot.

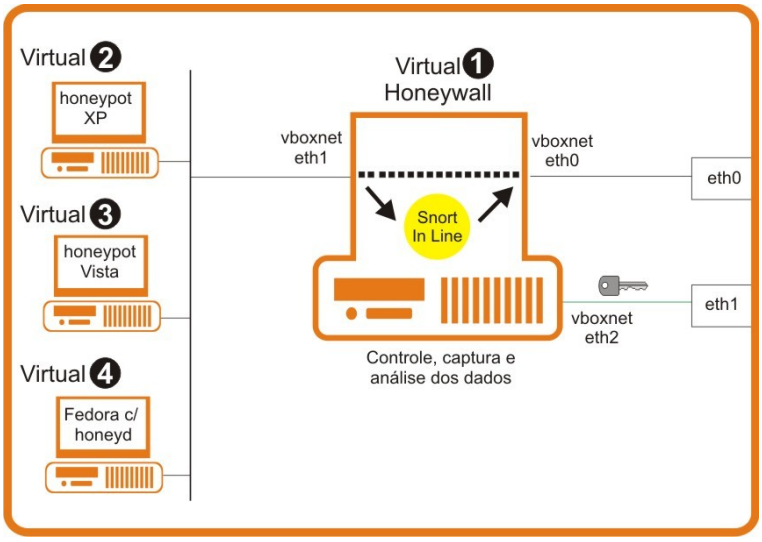


Figura 6 – Estruturas das máquinas virtuais

3.8 Configurando as máquinas

O Virtualbox é instalado no Fedora pelo Yum. Aqui temos a tela já com os sistemas operacionais usados para teste.

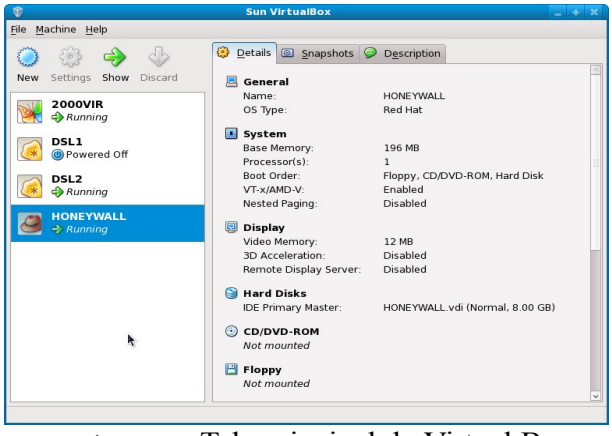


Figura 7 – Tela principal do Virtual Box

O modo de rede utilizado na entrada na honeywall é o modo bridge, que nesta versão do Virtualbox é oferecido nativamente. Este modo permite que a entrada tenha o IP da honeywall.

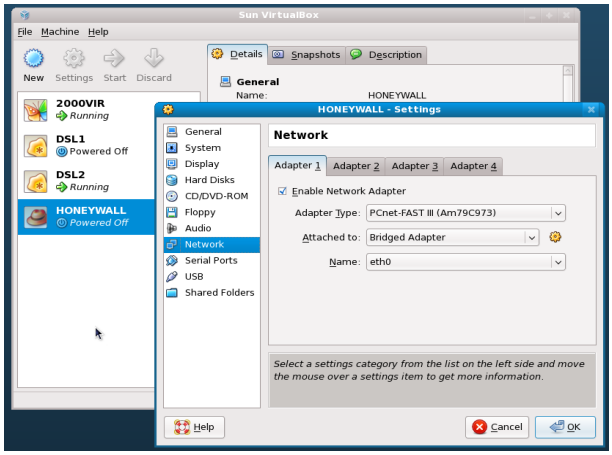


Figura 8 – Tela do modo de rede da honeywall

A instalação se dá montando o ISO ou botando com o CD Roo-2008 da Honeynet que já inicia o processo de instalação automaticamente. Este CD é projetado para uma rápida recuperação da honeywall, podendo ler um arquivo de configuração de uma instalação anterior.

Em uma instalação padrão entra-se como usuário: roo, senha: honey. Usa-se o modo “interview” (entrevista) que irá configurar por meio de perguntas, todos os parâmetros da honeywall.

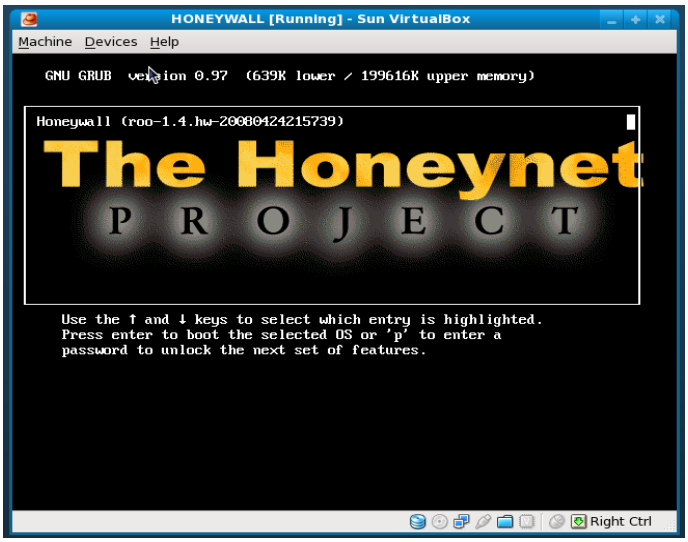


Figura 9 – Tela de inicialização

O script de instalação configura todas às opções. Endereços IP , acesso remoto a interface web, limite de conexões tcp e udp, permissão de acesso aos DNS, alerta por email, ativação do snort-in-line, lista permitida e lista proibida (blacklist, whitelist), modo "fence list" (que restringe a faixa de IPs que as honeypots podem ver), modo Roachmode Motel (armadilha de baratas, o ataque fica restrito a honeywall), o receptor de dados Sebek e ainda o Snort.

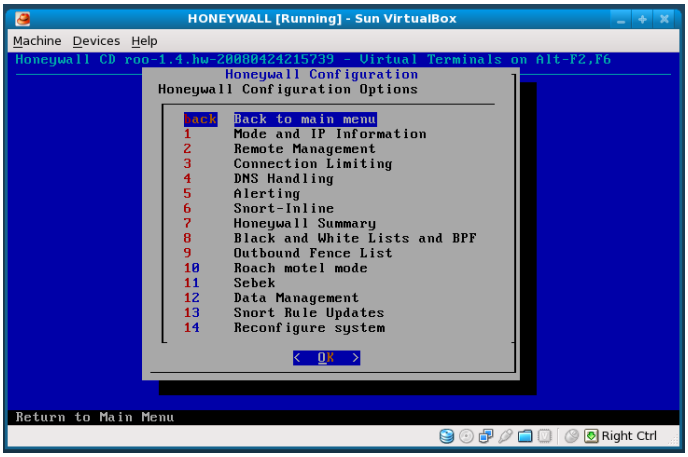


Figura 10 – Menu de configuração do honeywall

Na penúltima opção, as regras do sistema IPS (intrusion detection system) Snort podem ser atualizadas. Se cadastrando no site do Snort é possível receber as atualizações das regras de filtragem/bloqueio utilizadas pela honeywall [13]

3.9 Rodando a honeynet

Com as honeypots instaladas virtualmente (Linux e Windows), foi feita a execução de toda a honeynet. Aqui temos três máquinas virtuais rodando ao mesmo tempo. A tela da máquina honeywall está no menu principal de administração.

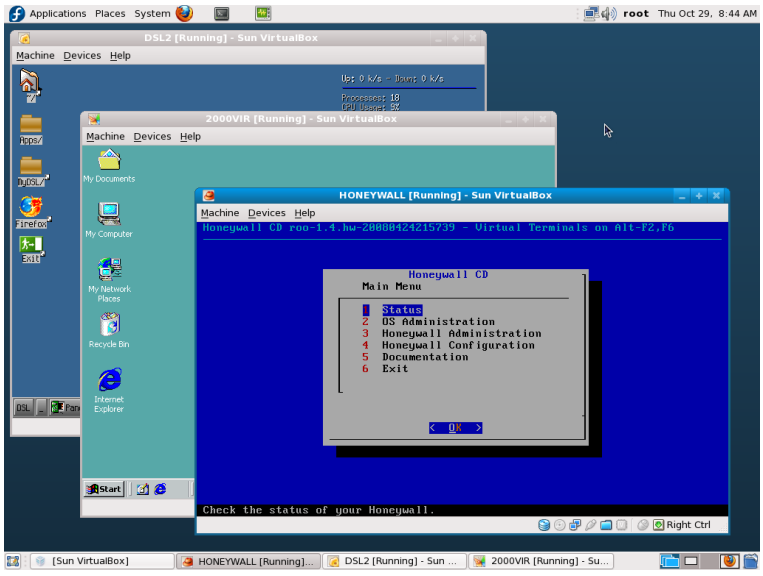


Figura 11 – Máquinas virtuais no Fedora 11

Desta forma o honeywall pode ser administrado diretamente pelos menus na honeywall virtual ou pelo Walleye.

O Walleye é um sistema completo de configuração controle e análise dos dados, acessado pela máquina de gerenciamento.

Ao se entrar no sistema a mudança de senha é obrigatória. A conexão é feita via SSL e a configuração do honeywall permite restringir os IPs que podem acessar a conexão via web.

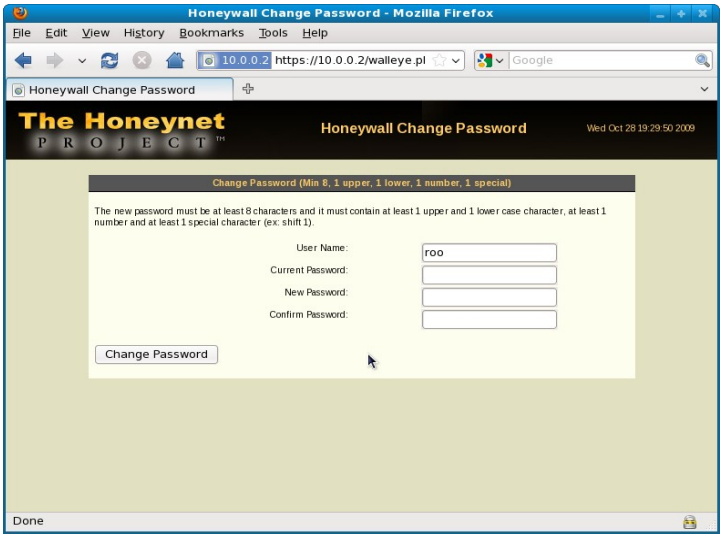


Figura 12 – Segurança nativa da entrada do Walleye

Praticamente toda a configuração da honeywall pode modificada pelos menus do Walleye. Aqui vemos as interfaces de rede.

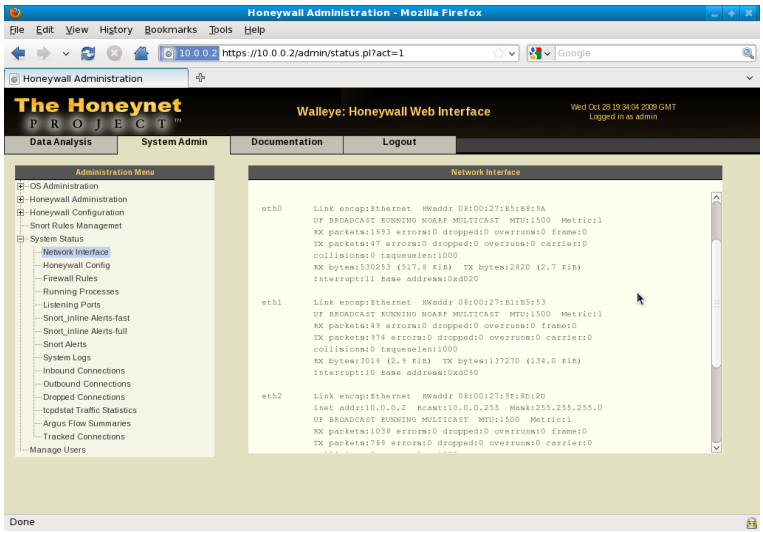
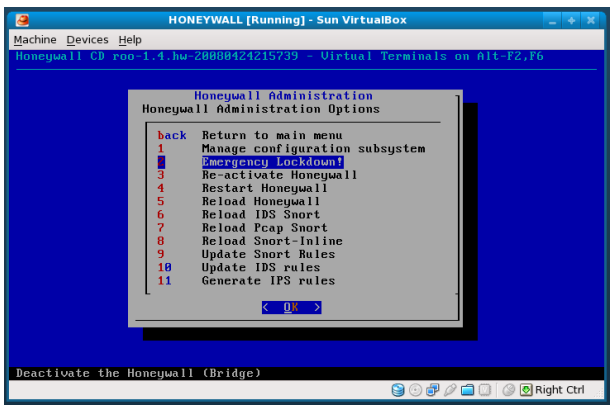


Figura13 – Administração pelos menus do Walleye

Em caso de emergência, ambas as interfaces permitem interromper imediatamente o funcionamento da honeynet.



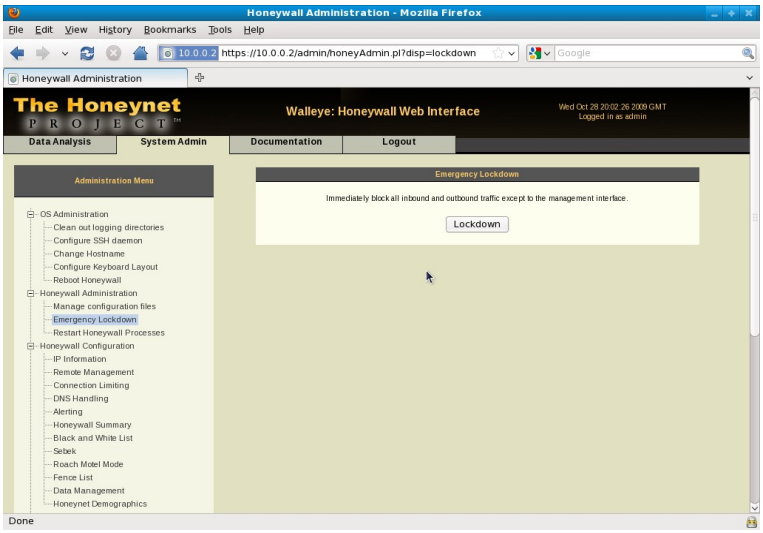


Figura 14 – Opções de interrupção emergencial

O menu de análise dos dados (Data Analysis) permite ao administrador ver um panorama geral da honeynet. Qualquer atividade detectada é mostrada neste painel principal.

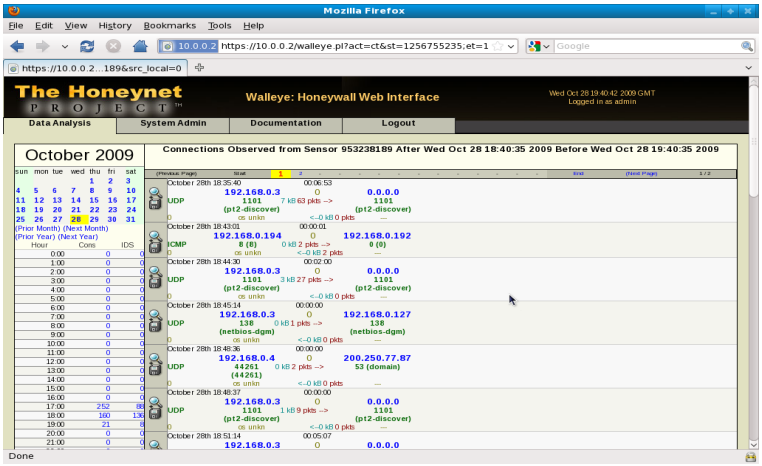


Figura 15 – Análise de dados no Walleye

Na tela de análise de dados as conexões detectadas pelo IDS podem ser inspecionadas detalhadamente. Bastando clicar na lupa ao lado do registro da conexão.

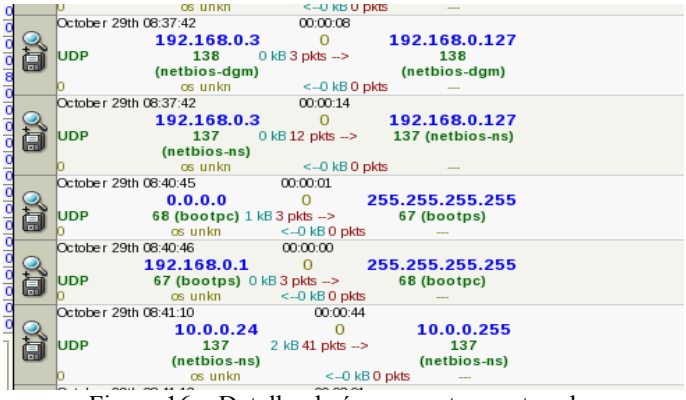


Figura 16 – Detalhe da área pacotes capturados

Na situação abaixo foi feito um acesso a honeypot Windows 2000, usando o netcat acessar a porta 135 (Windows RPC) . A honeywall detectou e registrou os pacotes usados pela conexão.

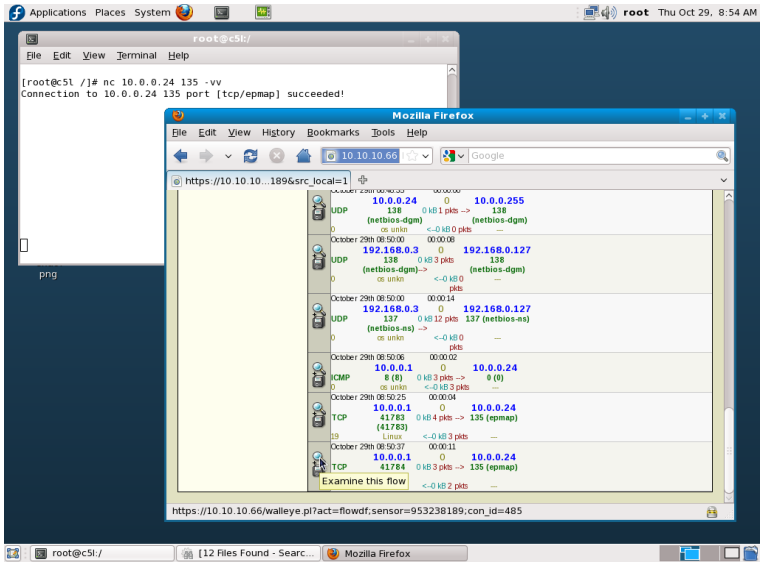


Figura 17 – Pacotes capturados de um acesso feito ao honeypot

Usando a opção "Examine this flow" o pacote é decodificado.

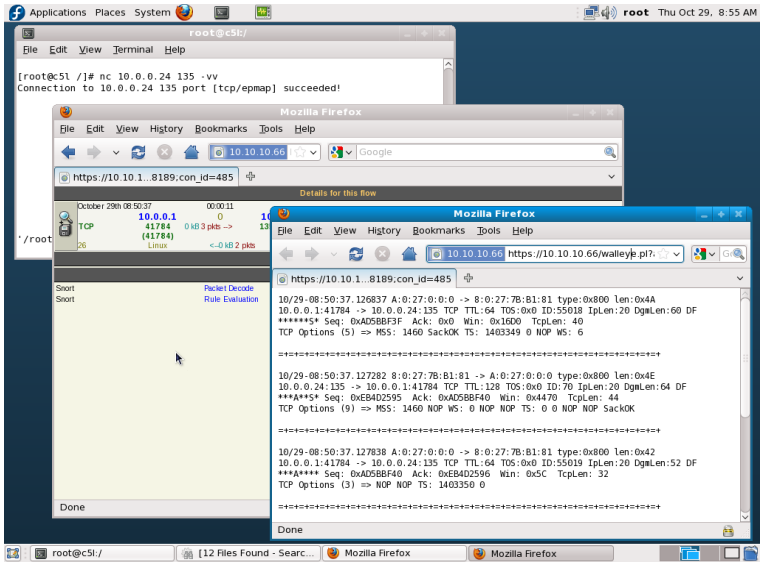


Figura 18 – Decodificando o pacote interceptado

4. Prós e contras de uma honeynet virtual

4.1 Vantagens

O custo de uma honeynet virtualizada é baixo: Estes testes forma realizados em uma máquina simples para os padrões de 2009. Com uma ou duas máquinas mais potente pode-se criar uma honeynet complexa e muito atrativa para os invasores.

A recuperação da rede é rápida: As máquinas virtuais usam discos virtuais que podem ter sua imagem guardada periodicamente. E sendo somente um computador o disco principal pode ter uma cópia em DVD para pronta reinstalação do sistema operacional básico.

A segurança é eficiente: O CD Roo-2008 do projeto do Honeynet possui extensas configurações de segurança, somando-se isto ao fato de estar em uma máquina virtual, que o torna ainda mais seguro, pois está contido dentro de um ambiente onde não há dados importantes (além do isolamento provido pelo roteador).

Muita flexibilidade: Pode-se colocar varias máquinas e diversos sistemas operacionais. O Virtualbox dá suporte a toda a família Windows, as distribuições Linux.

4.2 Desvantagens

A complexidade da configuração: A honeywall é feita para ser transparente para o invasor, qualquer erro de configuração que a torne visível fará com que o atacante descubra onde está e fuja. Tornado a honeynet inútil.

A caducidade dos dados: Ao se usar imagens prontas de sistemas operacionais, as datas de acesso aos arquivos são antigas. Isto pode ser percebido pelo invasor.

Conexões de rede: Se forem usadas as configurações padrão, os endereços MAC das placas virtuais podem ser parecidos, dando pistas de que não é uma rede real (mas isto pode ser modificado na configuração do Virtualbox que permite inclusive alguns modelos de placa de rede).

Bugs:Um bug no sistema operacional ou no Virtualbox pode permitir ao invasor comprometer a máquina, obtendo controle do sistema (por isto é utilizada uma máquina de gerenciamento externa).

5. Conclusão

Este foi um estudo rápido de como se pode montar um honeynet em apenas uma máquina sem que o custo seja muito elevado. Honeynet é uma arquitetura e não um produto, seu desenvolvimento está em constante evolução.

Ferramentas como o CD-ROM Roo da Honeywall facilitam muito a tarefa de criar uma honeynet de forma rápida e com um bom nível de segurança pré-estabelecido. E com muita facilidade na configuração e na monitoração.

A lei de Moore, uma observação feita por Gordon Moore em 1965, que previa que os transistores dobrariam nos chips a cada par de anos ainda é válida [11]. Isto significa cada vez mais poder computacional favorecendo a quantidade e também a qualidade de máquinas virtuais que podemos obter com apenas um computador.

O futuro é virtualização dos sistemas, neste caso é natural que as honeynets sejam virtualizadas o que até facilita a existência das honeynets virtuais, pois os administradores passam a ter experiência na área.

Outro ponto importante é as honeypots não devem ser padronizadas. A virtualização permite muitas configurações de rede e múltiplos sistemas operacionais. O uso de imagens de máquina de produção (sem dados reais) é útil. Máquinas de produção podem ser convertidas em virtuais, ter seus dados sensíveis apagados com segurança, e utilizadas.

Tal como segredos militares onde cada país tem os seus cabe a cada responsável pela honeynet, criar um ambiente atrativo, que permita aprender para proteger a rede corporativa. ,

Estar sempre um passo a frente dos invasores é importante. Com uma Honeynet bem arquitetada e configurada o administrador de segurança estará bem mais preparado para as batalhas do dia a dia.

Apêndice A – Lista dos participantes do Projeto Honeynet

Florida HoneyNet Project
Paladion Networks Honeynet Project - India
Internet Systematics Lab Honeynet Project - Greece
Mexico Honeynet Project
NetForensics Honeynet
Azusa Pacific University Honeynet
Brazilian Honeynet Project
Irish Honeynet Project
Honeynet Project at the University of Texas at Austin
Norwegian Honeynet Project
UK Honeynet Project
West Point Honeynet Project
Pakistan Honeynet Project
Italian Honeynet Project
French Honeynet Project
Ga Tech Honeynet Project

Bibliografia

[1] http://www.dicweb.com/hh.htm acessado em 10/6/2009
[2] Provos, N. and Holz, T., 2008, Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Addison Wesley Professional
[3]http://en.wikipedia.org/wiki/Honeynet acessado em 10/10/2009
[4]http://www.chinese-wiki.com/Sun_Tzu_Art_of_War_Chapter_1 acessado em 8/10/2009
[5]http://www-03.ibm.com/systems/virtualization/news/view/100207.html acessado em 21/10/2009
[6]http://en.wikipedia.org/wiki/X86_virtualization acessado em 21/10/2009
[7]The Use of Honeynets to Detect Exploited Systems Across Large Enterprise Networks John Levine, Richard LaBella e outros. 2003 IEEE Workshop on Information Assurance
[8] Spitzner, L., 2002, Tracking Hackers, Addison Wesley Professional.
[9] https://projects.honeynet.org/honeywall/ acessado em 22/10/2009
[10] http://www.honeynet.org/project/sebek acessado em 07/09/2009
[11] http://techresearch.intel.com/articles/Tera-Scale/1609.htm acessado em 26/10/2009
[12]http://www.vmware.com/interfaces/paravirtualization.htm acessado em 26/10/2009
[13]Informaçõs sobre o Snort, http://www.snort.org/ acessado em 22/10/2009
[14] Paper de Bill Cheswick http://cheswick.com/ches/papers/berferd.pdf acessado em 20/10/2009
[15]Projeto honeyd no Google Source Code http://code.google.com/p/honeyd/