Gislaine Aparecida Rojas

RA: 002319-1

Análise de Intrusões através de Honeypots e Honeynets

Americana – SP

Segundo Semestre de 2003

Gislaine Aparecida Rojas

RA: 002319-1

Análise de Intrusões através de Honeypots e Honeynets

Trabalho de graduação apresentado à Faculdade de Tecnologia de Americana, como parte dos requisitos para obtenção do título de Tecnólogo em Processamento de Dados.

Orientador:

Marcos Antonio de Almeida Corá

Americana – SP

Segundo Semestre de 2003

Dedico este trabalho aos meus pais Elvira e Honofre, minha irmã Gisele e a todos aqueles que colaboraram para concretização de mais essa fase.

Agradecimentos

A Deus pela oportunidade da vida, e por todas as bênçãos que me concede a cada amanhecer.

Aos meus pais Elvira e Honofre, pela dedicação e apoio familiar. A minha irmã Gisele pelo carinho e excessivas colaborações.

As minhas amigas Fabiana, Joseane e Mariluce, que me ajudaram em todos os sentidos.

Aos colegas da FATEC, que estiveram presentes durante esses anos na faculdade e ao Edgar, pela ajuda na escolha desse tema.

Aos professores que me deram oportunidades de novos conhecimentos, e em especial ao Professor Marcos Corá, pela orientação fornecida durante o desenvolvimento desse trabalho.

Enfim, a todos que direta ou indiretamente colaboraram para concretização desse trabalho de graduação.

Sumário

Índice de Figuras

Lista de Abreviaturas

DMZ	Demilitarized Zone
DNS	Domain Name Server
DoS	Denial of Services
FTP	File Transfer Protocol
HTTP	HiperText Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IMAP	Internet Message Access Protocol
INPE	Instituto Nacional de Pesquisas Espaciais
IP	Internet Protocol
IRC	Internet Relay Chat
MAC	Modify / Access / Change
MCT	Ministério da Ciência e Tecnologia
NBSO	NIC BR Security Office
POP	Post Office Protocol
RPC	Remote Procedure Call Protocol
SMTP	Simple Mail Transmission Protocol
SO	Sistema Operacional
SSH	Secure Shell
TCP	Transmission Control Protocol
TELNET	Network Terminal Protocol
ToS	Type of Service
TTL	Time To Live
UDP	User Datagrama Protocol

Resumo

Rojas, Gislaine (2003). Análise de Intrusões através de Honeypots e Honeynets. Americana, 2003. 66 p. Dissertação (Graduação) – FATEC – Americana – SP.

A internet, um dos meios mais importantes de comunicação, é utilizada para realização de constantes invasões. Muitos procedimentos são usados para proteger informações importantes de empresas e usuários domésticos, mas não são totalmente seguros, pois novas táticas de invasão são descobertas e criadas a todo instante.

Honeypots e Honeynets são recursos de segurança utilizados para serem sondados, atacados e comprometidos; para observação do comportamento das invasões, detecção das tendências e também permitir desenvolver novas técnicas de segurança.

Palavras Chave: Rede de Computadores, Segurança, Intrusão, Honeypot, Honeynet.

Abstract

Rojas, Gislaine (2003). Analysis of Intrusions through Honeypots and Honeynets. Americana, 2003. 66 p. Dissertation (Graduation). FATEC – Americana – SP.

Internet, one of the most important ways of communication, is used to accomplishment of constant invasions. Many procedures are used to protect important information of companies and domestic users, but they aren't totally safe, because new tactics of invasion are discovered and created the all instant.

Honeypots and Honeynets are resources of security used to be probed, attacked and compromised; for observation of the behavior of the invasions, detection of the tendency and also to allow to develop new technologies of security.

Key Works: Computers Network, Security, Intrusion, Honeypot, Honeynet.

1. Introdução

A internet proporciona grande comodidade, permitindo que pessoas troquem informações de forma eficiente; isso explica o extraordinário crescimento observado nos últimos anos no número de sites, de serviços, de pessoas e companhias conectadas.

A expansão das conexões dos computadores proporcionou acréscimo em nossas vulnerabilidades, tornando as redes mais propensas a ataques. Informações privadas e importantes podem ser invadidas a qualquer instante.

Antes as invasões eram provenientes de pessoas com grandes conhecimentos técnicos, comumente chamados de hackers; hoje com as ferramentas e manuais para invasão de redes disponibilizados em vários sites, o perfil do atacante mudou, pois pessoas sem conhecimentos profundos em informática podem atacar sistemas desprotegidos.

Como a informação é uma arma importante em todos os segmentos, cada vez mais as empresas estão se conscientizando da necessidade de uma política de segurança, já que é sinônimo de credibilidade, agregando valores aos negócios.

No entanto, política de segurança não previne totalmente os ataques, pois novas técnicas e falhas são observadas diariamente após a efetivação das atividades maliciosas, ou seja, somente após o prejuízo, que muitas vezes refere-se a valores significativos.

A comunidade de segurança se baseava na detecção do ataque e em mecanismos de reação, e com o tempo percebeu a necessidade de conhecer o inimigo, seus métodos, ferramentas e táticas de ataque; o conceito de *honeypot* surgiu dessa necessidade.

Honeypots são utilizados para monitoração de ataques, colecionando informações importantes sobre tendências e permitindo aprimoramento na segurança das redes.

1.1. Hackers

Originalmente hacker é um indivíduo que possui conhecimentos técnicos para explorar sistemas de computadores, mas com a crescente publicação sobre invasões de sistemas associadas a esse termo, a palavra passou a ter uma conotação negativa.

O termo geral hacker pode ser dividido em muitas categorias relacionadas a motivos e comportamentos. A categoria *Cracker* / *Hacker BlackHat* será o enfoque dessa pesquisa, que caracteriza aqueles indivíduos que utilizam seus conhecimentos para cometer crimes.

Cada hacker possui sua própria metodologia de trabalho e cada sistema possui seus pontos fortes e fracos, mas a maioria dos ataques segue um padrão:

- reunir informações técnicas e gerais, incluindo nomes da equipe, sistema operacional, senhas, números de discagem por acesso remoto;
- obter acesso inicial ao sistema;
- explorar os pontos fracos do sistema para aumentar os privilégios e expandir seu acesso;

- executar a finalidade do ataque;
- instalar porta dos fundos, que é uma modificação no sistema pra criar uma entrada fácil para possíveis retornos;
- cobrir os rastros e sair, que envolve modificação dos arquivos de log que registram o acesso e as modificações no sistema.

1.2. Motivações para efetivação de um ataque

A identificação dos inúmeros motivos que levam algumas pessoas a atacarem sistemas de computador é uma estratégia muito interessante, seguem alguns [49]:

- ganhos financeiros: com freqüência, os intrusos são funcionários que obtêm acesso a sistemas financeiros para roubar dinheiro;
- vingança: por parte de funcionários insatisfeitos;
- necessidade de aceitação ou respeito: muitos intrusos se dedicam a atividades ilegais envolvendo o uso de computador devido à necessidade de aceitação e/ou respeito de outras pessoas; membros de clubes de crackers ganham aceitação ao cometerem atos de intrusão;
- idealismo: alguns intrusos atacam sistemas por razões idealistas, se portando como heróis protegendo o mundo de operações clandestinas de coleta de dados por parte do governo;
- curiosidade ou busca de emoção: alguns intrusos possuem apenas a necessidade de saber o que o sistema possui;
- anarquia: os anarquistas penetram nos sistemas simplesmente para produzirem discórdia;
- aprendizado: pequena parte daqueles que violam sistemas fazem isso para aprimorar seus conhecimentos;
- ignorância: não têm consciência de que suas ações são ilegais;

- espionagem industrial: empresa ou organização que se dedica a atividades ilegais contra outra.
- espionagem nacional: é semelhante à espionagem industrial, exceto pelo fato de que um país começa a atacar os recursos de informática de outro.

1.3. Entidades mais vulneráveis

As entidades mais vulneráveis a um ataque em grande escala são:

- instituições financeiras e bancos, que são testados e atacados para execução de fraudes, como desvio de dinheiro e transferências de fundos, e que normalmente não são levados ao conhecimento público;
- provedores de internet, pois são facilmente acessados através da internet e podem possuir acesso a conexões rápidas, utilizadas para transferência de grandes quantidades de dados, além do cadastro dos seus clientes;
- companhias farmacêuticas, buscando resultados de pesquisas e desenvolvimentos de novos medicamentos;
- governo e agências de defesa, devido ao baixo orçamento destinado às políticas de segurança;
- empresas multinacionais, que são as principais vítimas de tentativas de espionagem industrial.

1.4. Pontos fracos na segurança da rede

Alguns hackers são sofisticados, explorando novos bugs no software, outros utilizam como porta de entrada, falhas conhecidas que não foram atualizadas pelos administradores dos sistemas ou usuários.

1.4.1. Bugs de Software

Os softwares normalmente são colocados no mercado com erros ou com partes do código que não executam o esperado, mas as empresas de softwares mantêm sites dedicados a questão de segurança, contendo emendas que corrigem os problemas. A visita constante nesses sites permite as atualizações necessárias, dificultando o trabalho dos atacantes.

1.4.2. Problemas de configuração do sistema

Configurações default

Muitos sistemas são instalados com configurações default, devendo ser alteradas imediatamente pelo administrador da rede, pois os hackers possuem ferramentas de busca dessas configurações vulneráveis.

Programas vulneráveis

A maioria dos softwares possui diferentes níveis de segurança, sendo necessário revisar algumas configurações para se obter um nível de segurança mínimo.

Atalhos administrativos

Na configuração de um sistema novo, nunca deve ser reutilizada a senha dos sistemas antigos, nem utilizar senhas simples ou em branco.

Relacionamento de confiança

O relacionamento de confiança entre hosts da rede local deve ser muito bem estudado, pois se todas as máquinas confiarem uma na outra, uma máquina desprotegida pode comprometer a rede inteira em uma invasão, já que não é necessário nenhum tipo de autenticação nesses relacionamentos.

Verificação de senha

A autenticação por senha é uma ótima ferramenta para o controle de acesso a contas e sistemas, o seu uso incorreto é o mesmo que não utilizar autenticação nenhuma. As senhas devem ser longas com combinação de letras e números, não devem possuir palavras do dicionário, não usar nomes de pessoas próximas ou dados pessoais, alterar constantemente, nunca escrevê-las em papel ou informar por telefone.

Uso de sniffers em redes desprotegidas

Sniffer é uma ferramenta de software que registra o tráfego da rede e remete a quem instalou. Um sniffer pode ser instalado por um hacker para obter senha das contas.

Computadores remotos desprotegidos

Pessoas que acessam a rede da empresa de forma remota devem possuir computadores protegidos com um firewall pessoal e antivírus no mínimo, pois um invasor pode penetrar no computador doméstico e ter acesso fácil a intranet.

1.5. Organização da Dissertação

O capítulo 1 apresenta o conceito de hacker e como ele pode prejudicar instituições, explorando os pontos fracos em uma rede.

O capítulo 2 evidencia o histórico, as definições e os tipos mais comuns de honeypots e honeynets; como é o funcionamento e as técnicas de controle, captura e análise dos dados.

No capítulo 3 serão apresentadas algumas organizações espalhadas pelo mundo.

O capítulo 4 menciona os principais honeypots encontrados no mercado.

O capítulo 5 apresenta outros níveis existentes de honeypots.

O capítulo 6 faz uma conclusão da pesquisa efetuada nessa dissertação e propõe alguns trabalhos futuros.

2. Ambientes de Análise de Intrusões

2.1. Histórico

As primeiras experiências sobre análise de intrusões são de 1988, quando o especialista Clifford Stoll faz um relato completo sobre a história de invasão nos sistemas do Lawrence Berkeley Laboratory.

Quatro anos depois, em 1992, foi a vez do especialista Bill Cheswick expor no artigo "An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied" os resultados do acompanhamento de invasões em um dos sistemas da AT&T, projetado especialmente para este fim.

O termo *honeypot* surgiu em 1998 após o desenvolvimento da ferramenta Detection Toolkit por Fred Cohen, utilizada para emular diversas vulnerabilidades e coletar informações sobre os ataques sofridos.

Em 1999, o conceito de *honeynets* ganha repercussão mundial através do lançamento do *Honeynet Project*, demonstrando a importância do estudo do comportamento dos invasores de uma rede para o desenvolvimento de novas ferramentas e sistemas de defesa [6].

2.2. Honeypots

Honeypots [1,9] são recursos de segurança criados para serem sondados, atacados ou comprometidos por um atacante; podem ser utilizados para

distrair atividade maliciosa de máquinas valiosas da rede ou como mecanismo de alerta (honeypots de produção); ou podem ser utilizados para monitoração de um ataque (honeypots de pesquisa).

Tradicionalmente *honeypot* é um único sistema conectado a uma rede de produção.

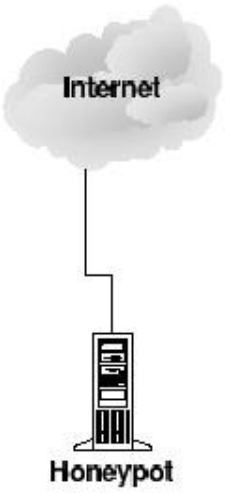

Figura 1 – Honeypot [10]

2.2.1. Vantagens e Desvantagens

Vantagens:

- como o *honeypot* é isolado, o fluxo de informações para análise é pequeno se comparado a uma rede de produção, tornando esse processo menos exaustivo e mais barato;
- acaba com os falsos positivos gerados pelos sistemas de detecção de intrusos; esses sistemas, pela grande quantidade de fluxo de informações, geram muitos alertas falsos, fazendo com que os administradores passem a ignorá-los; no *honeypot* todo tráfego é não autorizado, não ocorrendo esse tipo de erro;

- o IDS (Sistema de Detecção de Intrusos) e o firewall não são sobrecarregados com grande tráfego, porque a geração de logs é pequena e precisa;
- exigência de recursos mínimos;
- captura tráfego criptografado, diferente da maior parte de tecnologias de segurança;
- descoberta de novas ferramentas e táticas dos hackers, não apresentando o problema de falsos negativos das tecnologias IDS, que não detectam atividades desconhecidas.

Desvantagens:

- visão limitada ao tráfego de dentro do *honeypot*;
- risco de ser invadido e utilizado para prejudicar outros sistemas;
- ausência de tráfego implica em gastos sem retorno, já que nada foi monitorado.

2.2.2. Níveis de Interação

A interação define o nível de atividade que o *honeypot* permite ao atacante, podendo ser de duas categorias:

Honeypots de baixa interação

Apenas emulam serviços e sistemas operacionais, não permitindo que o atacante interaja com o sistema. É de fácil instalação; riscos mínimos porque os serviços emulados controlam o que é permitido; quantias de capturas de informações limitadas; fácil descoberta por hackers qualificados. Exemplos: Specter, Honeyd e KFSensor.

Honeypots de alta interação

São compostos por sistemas operacionais e serviços reais e permitem que o atacante interaja com o sistema. Essa interação permite capturar mais

informações, inclusive novas ferramentas e comunicações; a instalação é mais complexa; risco maior, pois os atacantes podem usar o sistema operacional real para atacar outros sistemas. Exemplo: Mantrap

Os *honeypots* de produção normalmente têm um nível baixo de interação, e de pesquisas têm um alto nível.

2.2.3. Localização de um Honeypot

O *honeypot* pode ser instalado na intranet ou na internet, de acordo com as perspectivas do administrador da rede, podendo ser localizado:

Em frente ao firewall

Com a disposição do *honeypot* em frente ao firewall, ou seja, fora da rede, não existe risco para rede interna e também não é gerado logs do firewall e do IDS. Em caso de domínio do sistema pelos atacantes, não é possível controlar o tráfego, podendo colocar em risco outras redes.

Atrás do firewall (intranet)

Normalmente implementado para descoberta de atacantes internos ou detectar configuração vulnerável de firewall. Se o *honeypot* for comprometido por um atacante externo, este terá acesso a toda rede, sem bloqueios do firewall.

DMZ (Demilitarized Zone)

É a rede adicionada entre uma rede interna e uma rede externa a fim de prover uma camada adicional de segurança, fazendo utilização de firewall para controlar todo tráfego de entrada / saída e isolando o *honeypot* da rede de produção. Pode ser chamada de rede de perímetro.

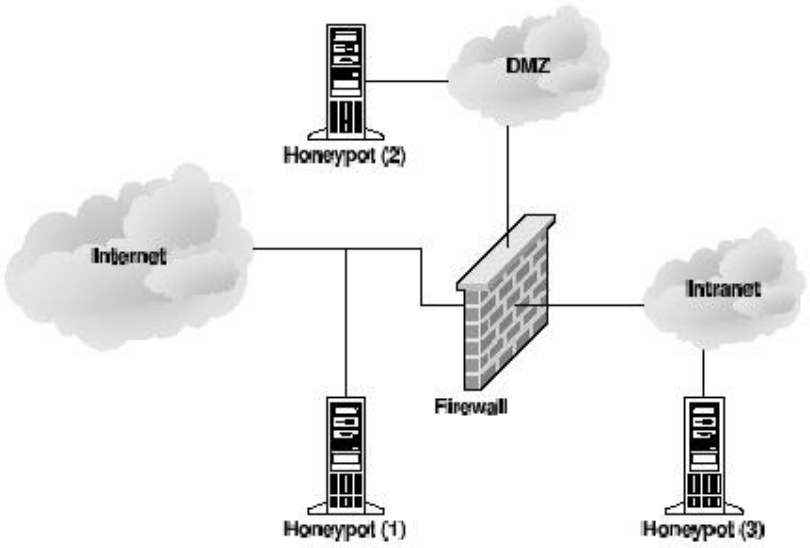

Figura 2 – Localizações permitidas aos honeypots [8]

2.2.4. Legalidade dos Honeypots

Quando o assunto é legalidade dos *honeypots*, é necessário considerar três aspectos: armadilha, privacidade e responsabilidade.

Armadilha: coagir ou induzir alguém a fazer algo que normalmente não faria, ou seja, instigar a prática de um delito, pode acarretar processo judicial. A discussão é intensa sobre esse aspecto, mas na maioria dos casos não poderia ser caracterizado crime pelas seguintes razões:

- *honeypot* não induz ninguém, até porque muitas vezes é emulação do sistema de produção da empresa;
- os ataques são por iniciativa do invasor;
- os *honeypots* não estão sendo usados para processar ninguém, e sim como meio para novas descobertas.

Privacidade: o sistema que o atacante está usando não pertence a ele, portanto toda monitoração realizada no sistema não pode caracterizar quebra de privacidade.

Responsabilidade: se o *honeypot* for comprometido e utilizado para prejudicar outras redes pode acarretar processo civil.

2.3. Honeynets

Honeynet [1] não é um sistema único, mas sim uma rede de sistemas e aplicativos múltiplos, projetada para ser comprometida e observada. *Honeynet* é um tipo de *honeypot* de alta interação, utilizada principalmente para pesquisa.

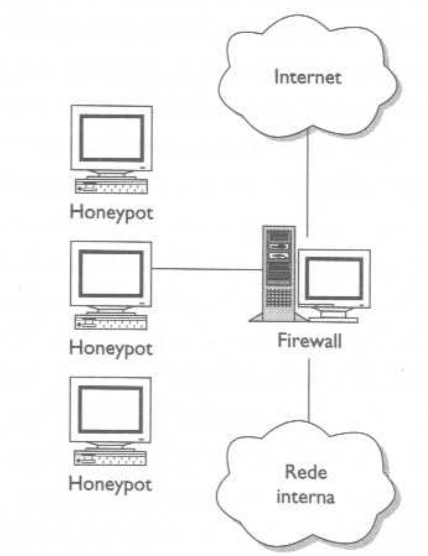

Figura 3: Uma Honeynet [1]

É criado um ambiente que reflete uma rede de produção real, assim os riscos e vulnerabilidades descobertos serão os mesmos que existem em organizações comuns. Nada é emulado e nada é feito para tornar os sistemas inseguros. Tendo sistemas diferentes, como servidor DNS sobre plataforma Linux, um webserver IIS sobre Windows, e um servidor de Banco

de dados sobre Unix Solaris, é possível aprender sobre ferramentas e táticas diferentes, podendo também melhor prever as tendências específicas dos invasores. Essa rede é altamente contida para que todo tráfego de entrada e saída seja analisado [3].

2.3.1. Funcionamento de uma Honeynet

Após a definição e instalação da *honeynet*, pode-se adicionar contas de usuários, enviar e-mails entre eles, forjar documentos em alguns diretórios, estabelecer conexões como TELNET ou FTP, executar alguns comandos que serão armazenados no histórico; tornando a rede aparentemente ativa certamente atrairá mais atenção dos atacantes.

Após, o controle e a captura dos dados são elementos críticos no funcionamento de uma *honeynet*.

2.3.1.1. Controle de Dados

Depois do comprometimento de uma *honeynet*, o fluxo de tráfego deve ser controlado, pois é necessário garantir que esta não será utilizada para prover meios de ataques para outros sistemas. O controle de acesso é obtido com a utilização de um dispositivo de contenção de fluxo de dados, como um firewall invisível [51,52], que separa a *honeynet* da Internet e das redes de produção.

Como o firewall controla o fluxo de tráfego dessas três redes distintas, é necessário definir que qualquer conexão da Internet para a *honeynet* é autorizada, que toda conexão de um *honeypot* para Internet é controlada para não permitir ataques através dele e que a *honeynet* e a rede administrativa não possuem nenhum tipo de comunicação direta. Essas

regras podem ser mudadas, podendo utilizar o mesmo sistema de filtragem utilizada nos sistemas de produção da empresa, ou qualquer outra regra resultante de sua aprendizagem.

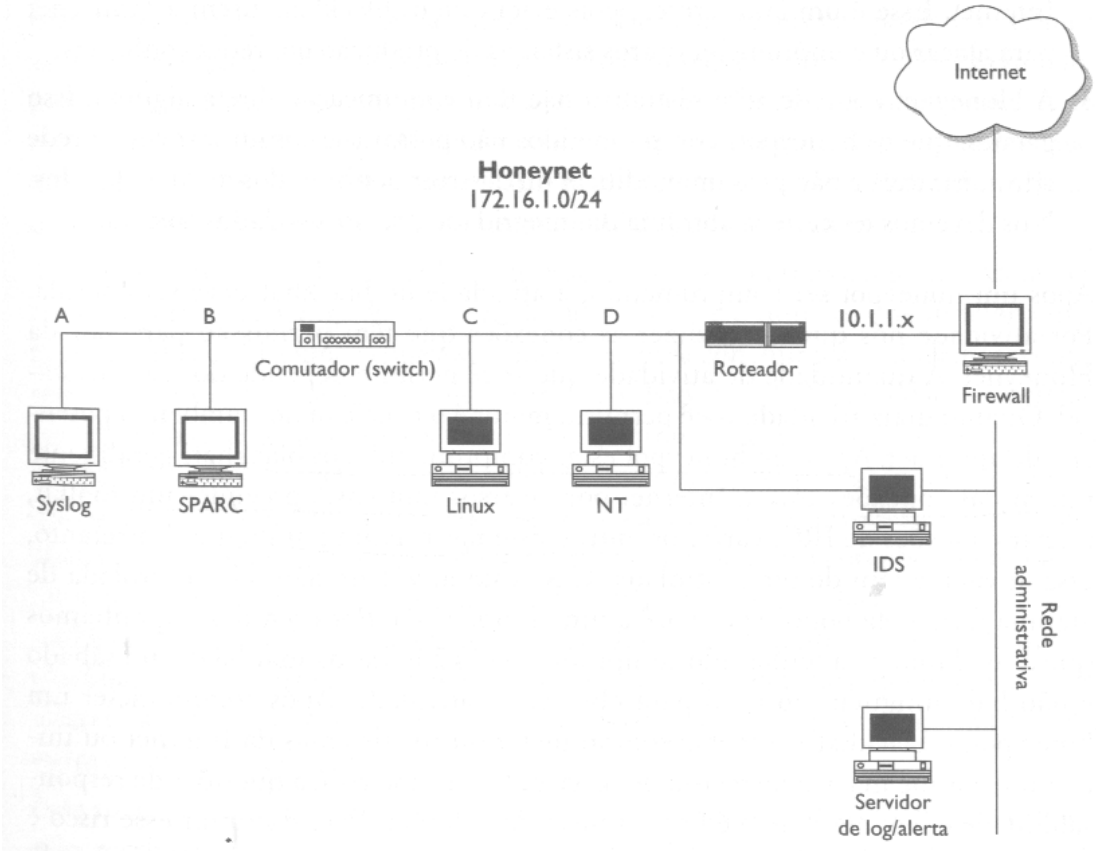

Figura 4: Honeynet e seu projeto de controle de dados [1]

“A quantidade de atividade que você permite depende do risco aceitável. Quanto mais atividade você permitir, maior é o risco e maior é também o potencial de aprender”. [1]

Não podemos ilimitar as conexões por aspectos de responsabilidade em casos de ataques a outros sistemas; não podemos limitar totalmente porque os invasores vão desconfiar e quase nada será aprendido, pois logo descartarão a rede projetada. A organização Honeynet Project (seção 3.1.),

órgão mais conhecido nesse tipo de pesquisa, permite de cinco a dez conexões ao dia.

O controle de acesso da *honeynet* para a Internet deve ser através de meio automatizado, pois o ataque pode ocorrer a qualquer hora e dia da semana, e nesses casos, a intervenção manual pode ser um grande risco: os alertas podem não ser enviados por alguma falha de DNS, ou mesmo não lidos durante a noite. Essa regra deve ser controlada através de um script específico que bloqueia as conexões quando o limite definido é atingido, podendo mesmo assim enviar avisos para o administrador da rede.

A *honeynet* deve conter também um sistema antispoofing adequado, permitindo a saída apenas de pacotes válidos, diminuindo o risco de uso da rede para ataques de recusa de serviço (DoS).

Um roteador fixado entre o firewall e a *honeynet* pode ser utilizado para mascarar o firewall; controlar antispoofing, atuando como uma segunda camada de controle de acesso; atuar como backup caso ocorra falha no firewall; e bloquear grande parte do tráfego inválido, melhorando o desempenho.

2.3.1.2. Captura de Dados

Todas as atividades dos atacantes na *honeynet* devem ser registradas e capturadas para posterior análise.

Uma única camada de captação é muito arriscada, pois falhas podem ocorrer, e a junção das informações provenientes das várias camadas pode melhor alinhar a aprendizagem.

Os dados capturados não devem ser armazenados localmente, devem ser enviados para um sistema que os atacantes não têm acesso. Se o atacante detectar dados de seu acesso no *honeypot*, a rede pode ser comprometida e eles poderão ser modificados ou apagados.

Camada de Controle de Acesso

Todas as atividades para dentro ou para fora da *honeynet* devem passar por dispositivos de controle de acesso, como o firewall ou roteador, que registram as ocorrências (logs) que, nesse caso, são sempre suspeitas.

O firewall, além do já citado envio de e-mail alerta para os administradores, pode armazenar informações sobre as varreduras em um banco de dados, e posteriormente confrontados com os logs do IDS. Mas o firewall só registra o tráfego que passa por ele, sendo necessário outros meios de monitoração.

Camada de Rede

Outra camada é relacionada à captura e análise dos pacotes que trafegam na rede, um IDS pode identificar e capturar toda carga útil (payload) dos pacotes na rede, alertar o administrador sobre assinaturas suspeitas, capturar todos os pressionamentos de teclas dos atacantes. É importante ressaltar que essas informações devem ser armazenadas de forma a facilitar a análise e não o contrário.

Camada de Sistema

É necessário capturar também a atividade dos sistemas, porque o invasor pode estar fazendo uso de criptografia, impossibilitando a monitoração dos pressionamentos de teclas através da rede; devem ser armazenados remotamente, pois são os primeiros a serem apagados após um ataque. Todos os modos de acessos são enviados a um servidor de logs, que

mesmo que seja comprometido não afetará no processo de aprendizagem, já que o IDS capturou os logs que trafegaram até o servidor.

Camada Off-line

Os sistemas normalmente são colocados em modo off-line ou as imagens dos sistemas são copiadas após o comprometimento, para análise das modificações.

Tripwire [29] é um utilitário muito usado em *honeynets*; é uma ferramenta que verifica alterações não autorizadas na assinatura de arquivos e diretórios de todo o sistema.

2.3.1.3. Análise

A análise é a parte mais difícil e demorada de uma *honeynet*, pois é necessário a transformação das informações capturadas em dados úteis.

Logs de Firewall

O firewall, como já mencionado, pode ser configurado para enviar e-mails de alertas sobre tentativas de invasão, minimizando o trabalho do processo de coleta de dados para análise, já que os logs serão arquivados para análise detalhada.

Em um sistema IDS de uma empresa comum, o número de acessos é gigantesco, mas na *honeynet*, como todo tráfego é suspeito e direcionado a ataques, o número de acessos não é muito grande, por isso, não sobrecarregará o número de alertas enviados.

Um alerta pode evidenciar o que está ocorrendo na rede, podendo direcionar a análise mais detalhada no tráfego que o sniffer do IDS capturou. É interessante manter arquivados os endereços IP e as atividades manifestadas em um ataque, a fim de definir as tendências e direcionar a segurança na rede administrativa.

Análise do IDS

Os alertas enviados pelo IDS também são armazenados em um banco de dados; os pacotes podem ser armazenados em um arquivo de log binário; e acumula os logs de ASCII detectados na carga útil dos pacotes, como os pressionamentos de teclas, por exemplo.

Parece redundante enviar novamente alerta para os administradores da rede, mas o firewall, no alerta, pode informar somente a tentativa de conexão, já o do IDS, relata o que o invasor está executando, através de um banco de dados que contém informações de como é um ataque e de como ele é detectado, dando informações que permitem a definição de análise mais detalhada nos arquivos de log binário.

Como já afirmado, é imprescindível a captura de dados em camadas, pois o firewall pode dar um alerta de conexão para fora da *honeynet* e não ser identificado nenhum alerta proveniente do IDS, pois pode não estar armazenado informações sobre esse tipo de comportamento em seu banco de dados de assinatura.

Se o atacante não estiver fazendo uso de criptografia, a análise do arquivo de log ASCII pode ser bastante útil, já que mostra os pressionamentos de tecla que originaram uma determinada situação.

Muitas vezes, após o comprometimento da rede, os invasores iniciam comunicações entre sua comunidade, através do IRC (Relay Chat da

Internet), por exemplo, que também são capturadas no log binário do IDS. Muitas informações valiosas podem ser conseguidas nessas conversas.

Logs de Sistema

Os logs do sistema identificam as assinaturas dos ataques, registram o caminho do invasor pelos sistemas e também as reinicializações realizadas.

Muitas vezes, os logs do sistema são apagados pelo atacante, por isso é necessário fazer uma comparação do que foi armazenado remotamente no servidor e no arquivo de logs do *honeypot* comprometido, identificando realmente o que o invasor modificou.

2.3.2. Técnicas Adicionais de análise

2.3.2.1. Obtenção Passiva de Impressões Digitais

Obtenção de Impressões digitais [33] é uma técnica utilizada para identificar diferenças entre sistemas operacionais que, tradicionalmente, é feita através de ferramentas ativas, como Queso e Nmap [32].

Toda pilha IP e todos os aplicativos do sistema operacional possuem particularidades, que são exploradas pela ferramenta. Cada sistema operacional responde de forma diferente para diversos tipos de pacotes, fazendo utilização de um banco de dados é possível fazer uma comparação com os resultados obtidos, descobrindo a identificação do sistema utilizado, dos serviços e muitas vezes até o aplicativo utilizado pelo atacante.

Em *honeynets*, essa ferramenta pode ser utilizada de modo passivo, através dos rastros do sniffer gerados pelo sistema remoto. A *honeynet* captura todos os pacotes que trafegam, tornando possível essa análise sem que o atacante perceba.

A obtenção passiva de impressões digitais não é perfeita, pois alguns aplicativos não produzem a mesma assinatura do sistema operacional, e essas informações podem ser alteradas facilmente. Em compensação, permiti agir em todas as camadas do TCP/IP, podendo ser detectado em tempo de operação.

Características da Pilha de Protocolos TCP/IP

Exemplos de características que podem ser observadas para determinar o sistema operacional [1]:

TCP/IP (Protocolo de Controle de Transmissão / Protocolo da Internet)

- TTL (time-to-live) – tempo de vida de um pacote, ou seja, número de saltos de roteamento permitidos até seu destino.
- Tamanho da Janela – medida de controle de fluxo de dados interno, que varia de um S.O. para outro.
- DF – bit "Don't Fragment" (não fragmentar) do IP

ICMP (Protocolo de Controle de Mensagens da Internet)
O ICMP relata informações de controle e de erros ocorridos na comunicação, enviando mensagens de controle quando necessário.

O *ping,* muito usado pelos invasores, leva à identificação clara do S.O.; a mensagem gerada pelo ICMP via ping em S.O. da Microsoft é de aproximadamente 60 bytes, para os semelhantes a UNIX é de 84 bytes de comprimento, por exemplo.

As características relacionadas a ICMP podem trazer informações como:

- tamanho do retorno da solicitação;
- conteúdo da carga útil de dados do retorno;
- número de identificação usada;
- números de seqüência.

2.3.2.2. Análise de Argumentação

O processo de argumentação pode recuperar processos, arquivos ou ferramentas utilizadas pelos invasores, recriando seus passos. É uma técnica muito complexa.

As unidades de disco devem ser totalmente limpas, eliminando todos os registros de instalações anteriores. Os dados de cada *honeypot* são copiados antes da instalação, para permitir comparação com o sistema comprometido. Antes da análise também é feita outra cópia, para garantir que um erro não modifique os dados originais. Essas cópias devem ser precisas, byte a byte.

Para sistemas UNIX, a ferramenta The Coroner's Toolkit disponibiliza muitos recursos úteis, como coleta de dados automatizada, recuperação de arquivos excluídos e reconstrução de eventos baseados nos horários de MAC (Modify / Access / Change).

2.3.3. Tipos de Honeynets

2.3.3.1. Honeynet Clássica

É composta por sistemas reais (físicos), com instalações específicas; podendo utilizar sistemas operacionais variados e independentes.

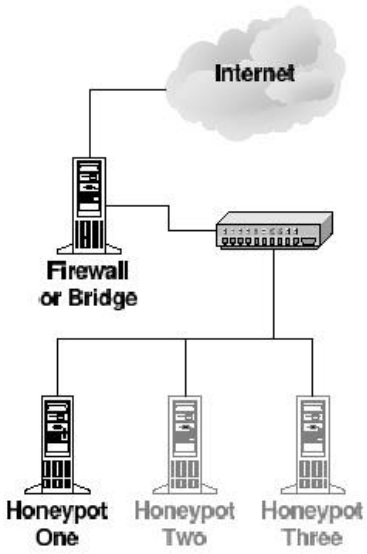

Figura 5 – Honeynet Clássica [10]

Vantagens:

- dispositivos reais;
- mais segurança pela descentralização dos *honeypots*.

Desvantagens:

- custo elevado;
- dificuldades na instalação e administração;
- complexidade para manutenção;
- espaço alocado muito grande.

2.3.3.2. Honeynet Virtual

É uma máquina que executa sistemas operacionais múltiplos ao mesmo tempo, executados através do uso de emuladores, criando uma rede virtual.

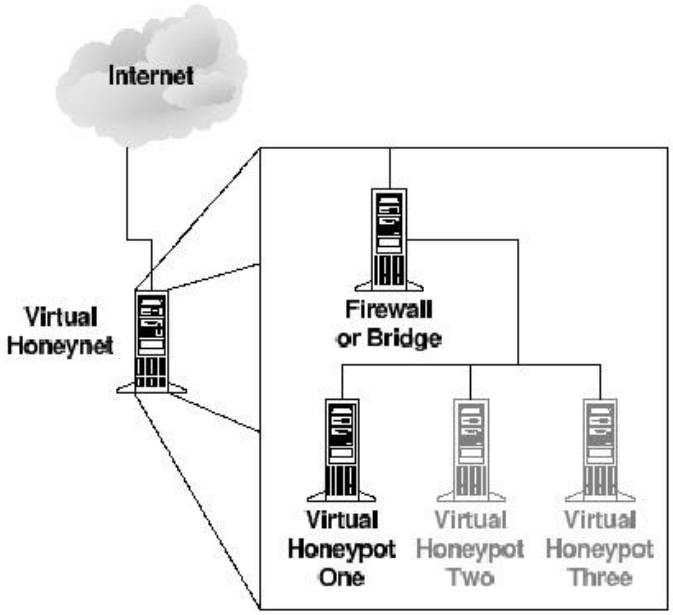

Figura 6 – Honeynet Virtual [10]

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. A maioria dos softwares é baseada na arquitetura dos chips Intel X86;
- possibilidade de comprometimento do software de virtualização, levando o invasor a controlar todos os sistemas e até mesmo determinar os sistemas operacionais que serão executados pelo ambiente virtual;
- instabilidade pelo uso exaustivo de memória.

2.3.4. Importância de uma Honeynet

A segurança de informações sempre foi de origem defensiva; as falhas e vulnerabilidades são detectadas para então depois reagir a essas imperfeições.

O propósito de uma *honeynet* é colecionar informações para revelar as ameaças existentes, proporcionando a descoberta de novas ferramentas, determinando os padrões de ataque e motivos do invasor estudado. Assim, as organizações podem parar um ataque ou corrigir falhas antes que algo errado aconteça.

Honeynets também podem conter os mesmos sistemas e aplicativos que uma empresa esteja utilizando em seu ambiente de produção, que esteja querendo testar ou distribuir, identificando seus reais riscos.

Em uma *honeynet*, todo o tráfego é suspeito, qualquer conexão efetuada deve ser monitorada, caracterizando intrusão, assim a detecção de riscos é facilitada, pois não há uma sobrecarga de dados ocasionada pelo tráfego normal da rede.

Essas redes projetadas melhoram a capacidade de detecção, reação, recuperação e análise dos sistemas que foram comprometidos, pois a cada ataque há um aperfeiçoamento das técnicas utilizadas. Ocorre uma aprendizagem sobre os invasores e sobre os próprios recursos de segurança disponíveis como logs, IDS, análise de tráfego de rede, fortalecimento de sistemas, entre outros [3].

3. Projetos

3.1. Honeynet Project

O *Honeynet Project* é uma organização de pesquisa não lucrativa de profissionais da área de segurança de informação, dedicado a aprender as ferramentas, táticas e motivos dos atacantes, compartilhando todas as lições aprendidas.

Esse projeto teve início no ano de 1999, com listas de e-mail de um grupo informal, evoluindo em junho de 2000, para o oficial *Honeynet Project*.

O projeto é composto de trinta membros de diversos países, empenhados em desenvolver a tecnologia de *honeynet* através de seus próprios recursos.

Em 2002, surgiu a *Honeynet Research Aliance* que adicionou organizações de vários países ao projeto, inclusive o Brasil; essa inclusão aumentou drasticamente a possibilidade de pesquisa e de resultados em âmbito global.

Organizações Ativas :

- Florida Honeynet Project
- Paladion Networks Honeynet Project - India
- Internet Systematics Lab Honeynet Project - Greece
- AT&T Mexico Honeynet
- 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

Essas organizações pretendem conscientizar das ameaças e das vulnerabilidades existentes na Internet; prover informações para assegurar a segurança dos sistemas; e fornecer essa mesma tecnologia desenvolvida para entidades interessadas.

3.1.1. Fases do Projeto

O *Honeynet Project* é dividido em quatro fases:

Fase I (1999 - 2001)

A finalidade do projeto na Fase I foi identificar e divulgar as ameaças mais comuns às instalações. Implementam controle e captura de dados simples, mas efetivos.

A rede foi dividida em três partes: *Honeynet*, Internet e Rede Administrativa; todos os pacotes trafegam através do firewall e roteador. A tecnologia empregada na *honeynet* fase I foi citada na definição do funcionamento de uma *honeynet*.

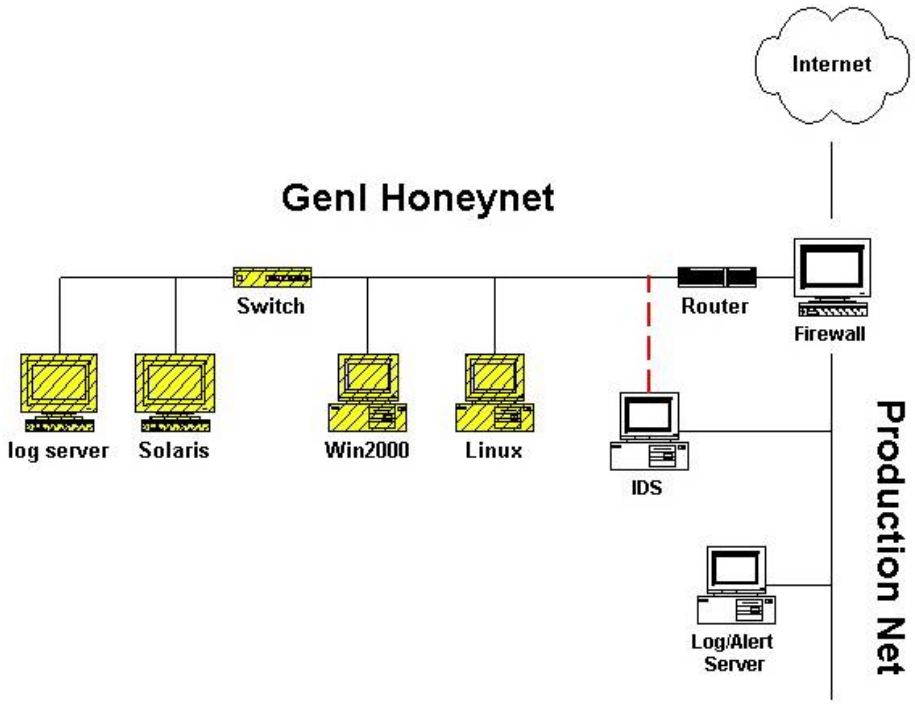

Figura 7 – Honeynet Fase I [3]

Fase II (2002 - 2003)

Essa fase visa a melhoria e simplificação da tecnologia empregada em *honeynets,* apresentando métodos mais avançados para controlar as atividades dos invasores e tornando mais difícil a descoberta do monitoramento, além da redução no risco de ataques a outras redes. Foi dado mais flexibilidade aos atacantes, proporcionado maior aprendizagem.

O processo de controle, captura e coleção dos dados são feitos em um único dispositivo, tornando a *honeynet* de mais fácil administração. O gateway, dispositivo que separa as redes, é denominado Honeywall; possui uma camada com duas bridge, permitindo integração e verificação de ameaças também nas redes internas.

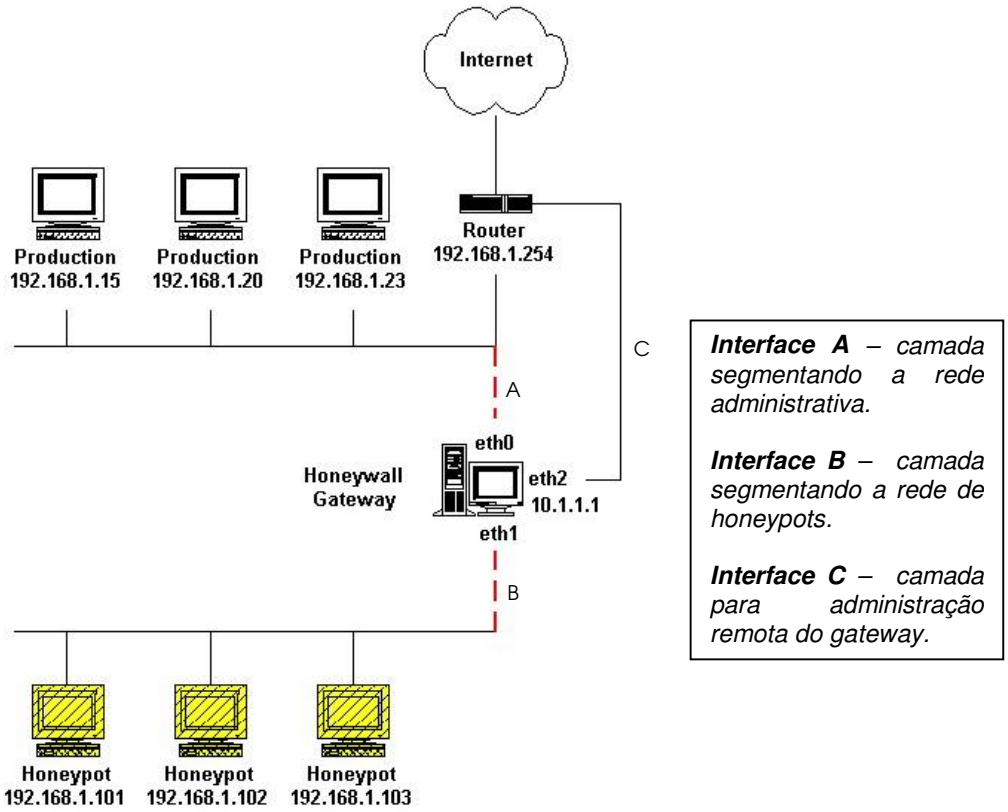

Figura 8 – Honeynet Fase II [3]

Como as interfaces interna e externa (A e B) são através da bridge, não possuem endereço IP atribuído; já a interface C, contém pilha de IP atribuída a ela (10.1.1.1.).

As conexões não são mais bloqueadas quando alcançam o número preestabelecido, é feito um monitoramento inteligente, identificando a atividade e analisando o que deve ser realmente impedido.

Essa arquitetura permite modificar bits do código enviado pelo atacante, desativando sua funcionalidade e retornando alguns pacotes. A emissão de respostas forjadas faz com que o atacante não desconfie do motivo do

insucesso de seu ataque a uma rede externa, continuando a fornecer dados para a pesquisa.

A captura de dados também sofreu alterações para reter dados criptografados, capturando dados do kernel.

Fase III – Começando em 2003

O objetivo dessa fase é o desenvolvimento de um CD-ROM de boot, contendo a tecnologia adotada na Fase II. As organizações devem inicializar o CD-ROM e colocar seus sistemas atrás do gateway; os registros poderão ser enviados para um sistema central e depois disponibilizados publicamente. Isso padronizará as *honeynets* e permitirá o desenvolvimento de sistemas distribuídos.

Fase IV – Início estimado para 2004

A expectativa é desenvolver um sistema de coleta de dados centralizado para captar os resultados das *honeynets* distribuídas.

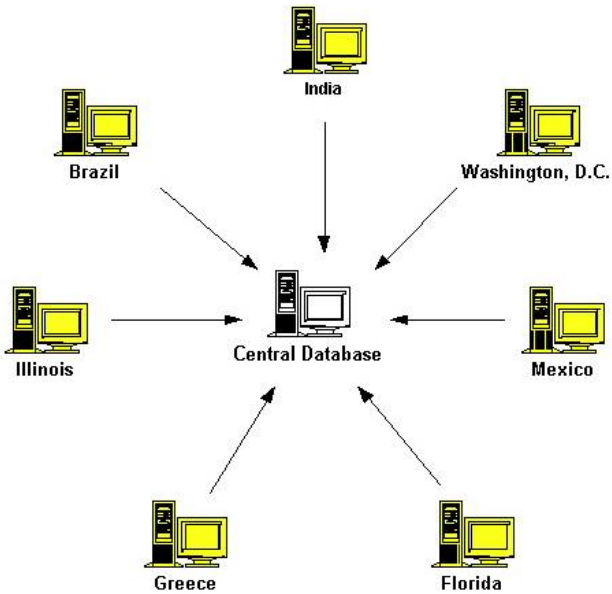

Figura 9 – Honeynet Fase IV [5]

Pretendem criar interfaces para o usuário, permitindo análise dos ataques em tempo real, com análise do tráfego e extração da carga útil dos pacotes; e análise dos dados de várias *honeynets*, armazenados em um banco de dados único, permitindo verificação das tendências.

3.2. Honeynet.BR

A *Honeynet.BR*, organização mantida por especialistas do INPE e pelo NBSO, teve sua fase de projeto iniciada em dezembro de 2001, entrando em operação em março de 2002.

O projeto começou como um laboratório do curso de Pós-graduação em Segurança de Sistemas de Informação do INPE, migrando para um projeto maior, envolvendo alunos de mestrado e doutorado no desenvolvimento de pesquisas.

Em junho de 2002, três meses após seu início, o projeto *Honeynet.BR* foi adicionado a *Honeynet Research Alliance*, pelo engajamento em pesquisas relacionadas a *honeynets*.

O projeto brasileiro começou com equipamentos doados pelo INPE, de membros do projeto e do Ministério da Ciência e Tecnologia (MCT).

3.2.1. Diferenciais do Honeynet.BR

O sistema operacional utilizado pelo projeto brasileiro é o OpenBSD, pela segurança, por possuir filtro de pacotes de qualidade e suporte para a implementação de uma bridge transparente. O filtro de pacotes utilizado possui implementação de regras de tráfego de entrada e saída, descartando o tráfego malicioso de saída; clareza na especificação de regras complexas;

normalização de tráfego; e limitação de banda para inibir ataques externos fora de controle.

Alguns tipos de ataques utilizam sobreposição, ordem inválida de fragmentos ou conjuntos inválidos de flags de TCP para enganar o IDS e o firewall. O filtro de tráfego normaliza o fluxo, remontando os fragmentos e descartando código malicioso.

Os principais mecanismos de contenção e geração de alertas foram desenvolvidos por membros do projeto, como sessionlimit, mecanismos de alerta e sistema de monitoração de atividades.

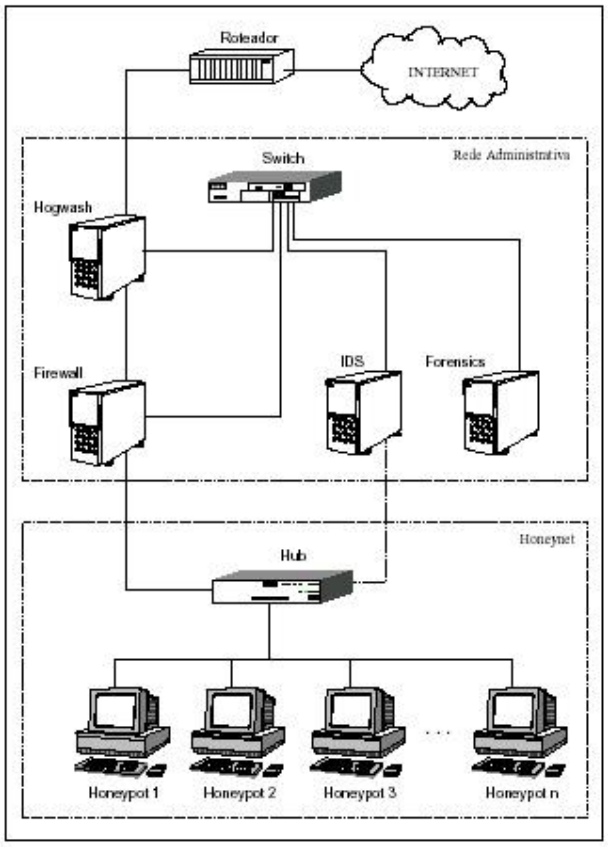

Figura 10 – Topologia da Honeynet.BR [6]

Segundo STEDING-JESSEN, do NBSO, o sessionlimit foi desenvolvido para interagir com o filtro de pacotes, inserindo e retirando regras de filtragem conforme necessário. Essa ferramenta demonstrou-se muito útil em barrar seletivamente ataques e tentativas de DoS contra outras redes, sem interferir, contudo, em outras atividades dos invasores, como download de ferramentas e troca de informações. [13]

Utilizam também uma ferramenta chamada hogwash, que descarta pacotes com assinaturas de ataques já conhecidos.

3.2.2. Resultados

O projeto detectou que grande parte do número de ataques foi executado através de worms automatizados, normalmente destinados a servidores Web; e grande procura por servidores de e-mail com configurações vulneráveis para serem utilizados para envio de spam.

Foi reafirmado de que cada vez mais o uso de código criptografado é utilizado em ataques, dificultando a coleta de informações e a atualização de ferramentas de segurança.

3.3. Wireless Honeynet Project

Uma rede sem fio (wireless) é um conjunto de sistemas que estabelecem comunicação com a utilização de portadoras de rádio ou infravermelho; os dados são modulados e transmitidos através de ondas eletromagnéticas.

As redes sem fio estão se difundindo rapidamente por todo o mundo, pela extrema facilidade de instalação e uso. O ponto de acesso recebe o sinal e

retransmite aos demais aparelhos, assim as máquinas ganham mobilidade podendo se conectar a rede de qualquer ponto no alcance da antena.

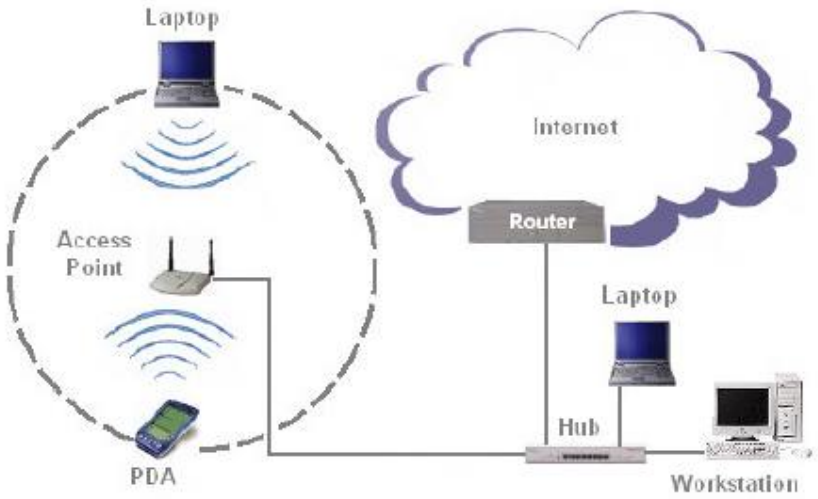

Figura 11 – Exemplo de uma rede wireless [39]

Existem questões de segurança importantes relacionadas com as redes wireless; um laptop, uma placa wireless e uma antena são suficientes para a detecção de redes sem fios com brechas, podendo ser utilizada para meio de navegação ou mesmo para atividade maliciosa.

Uma *honeynet* pode ser projetada para capturar e controlar toda atividade wireless existente. Essas informações podem ser analisadas para a detecção das táticas, técnicas e motivos dos atacantes de redes sem fio, possibilitando desenvolvimento de procedimentos mais eficientes de segurança.

Os nós são conectados através de pontos de acessos comercias e residenciais de redes sem fio, interligados a fim de criar uma área de controle grande para o gerenciamento remoto.

O enfoque é o desenvolvimento de resposta a incidentes, detecção de intrusão, e metodologias de análise para assegurar as redes sem fio, elaborando também estatísticas dos acessos acidentais e intencionais.

3.3.1. Fases do Projeto

O Projeto da *honeynet* sem fio segue os padrões do projeto *honeynet* convencional:

Fase I

Honeynet usa computadores múltiplos para imitar uma rede para o atacante.

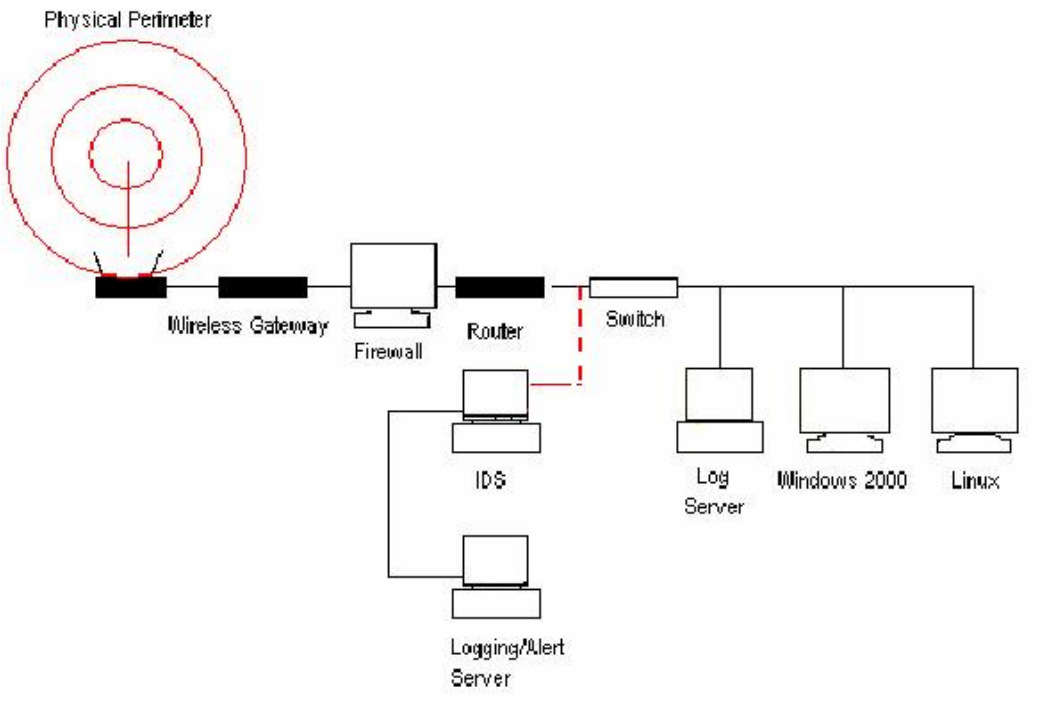

Figura 12 – Wireless Honeynet Fase I [38]

Fase II

Honeynet usa os mesmos componentes de uma *honeynet* padrão, mas sendo capaz de executar sistemas operacionais virtuais.

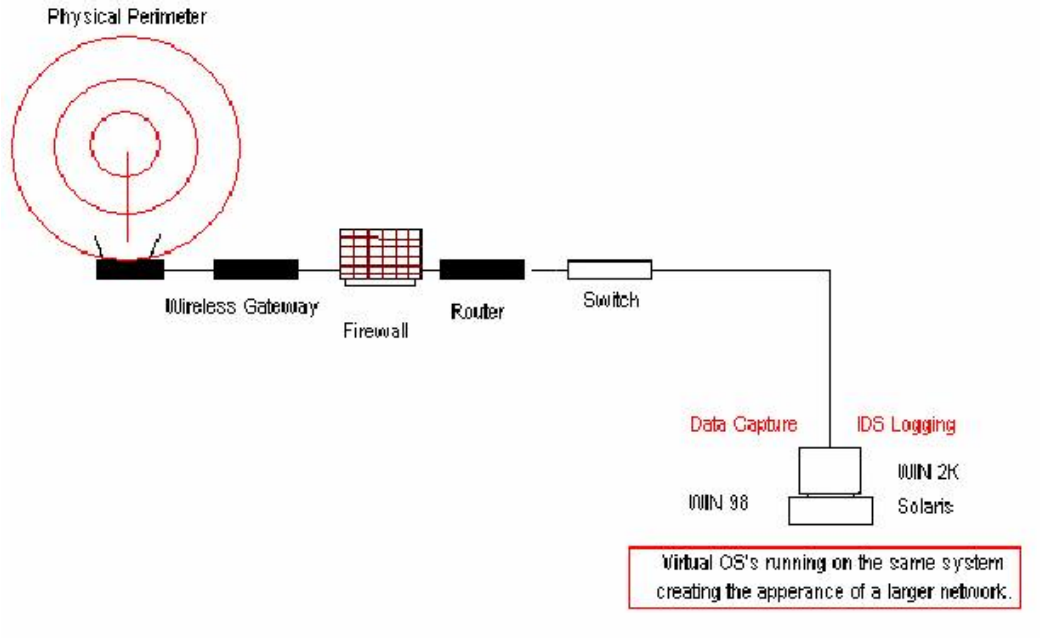

Figura 13 – Wireless Honeynet Fase II [38]

4. Alguns Honeypots disponíveis

4.1. Honeypots Comerciais

4.1.1. Mantrap [36]

Mantrap é um sistema comercial desenvolvido para atuar na plataforma Solaris, sendo utilizado tanto para segurança externa quanto interna.

Ele cria quatro ambientes, chamados de jaulas, podendo assim suportar até quatro sistemas operacionais. Com apenas uma máquina são criados quatro sistemas visíveis na rede, cada um com sua própria interface, podendo emular qualquer aplicativo compatível com o sistema operacional da jaula. O Mantrap somente limita aqueles aplicativos que interagem como o kernel.

Os ambientes são isolados, sendo personalizados distintamente. O módulo de geração de conteúdo gera, por exemplo, mensagens de e-mail utilizando nomes conhecidos da instituição, diferentes para cada ambiente criado.

Cada instalação deve possuir uma interface de rede administrativa, a fim de não permitir que o fluxo de dados seja visível aos atacantes que estão concentrados dentro das jaulas.

Todas as atividades relevantes ocorridas dentro de cada jaula são armazenadas localmente ou no servidor remoto de logs, além de possuir uma ferramenta gráfica de análise de eventos.

Classificação: alta interação / pesquisa

4.1.2. Specter [35]

Specter é projetado para ambiente Windows, para organizações comerciais de pequeno e grande porte. Pode monitorar até quatorze portas de TCP, sendo sete de armadilhas e sete de serviços. As armadilhas bloqueiam e registram as tentativas de ataques; as portas de serviços interagem com o invasor, emulando o aplicativo de acordo com o serviço utilizado.

Armadilhas: DNS, IMAP4, SUN-RPC, SSH, SUB-7, BOK2 e genérica
Serviços: FTP, TELNET, SMTP, HTTP, NETBUS e POP3

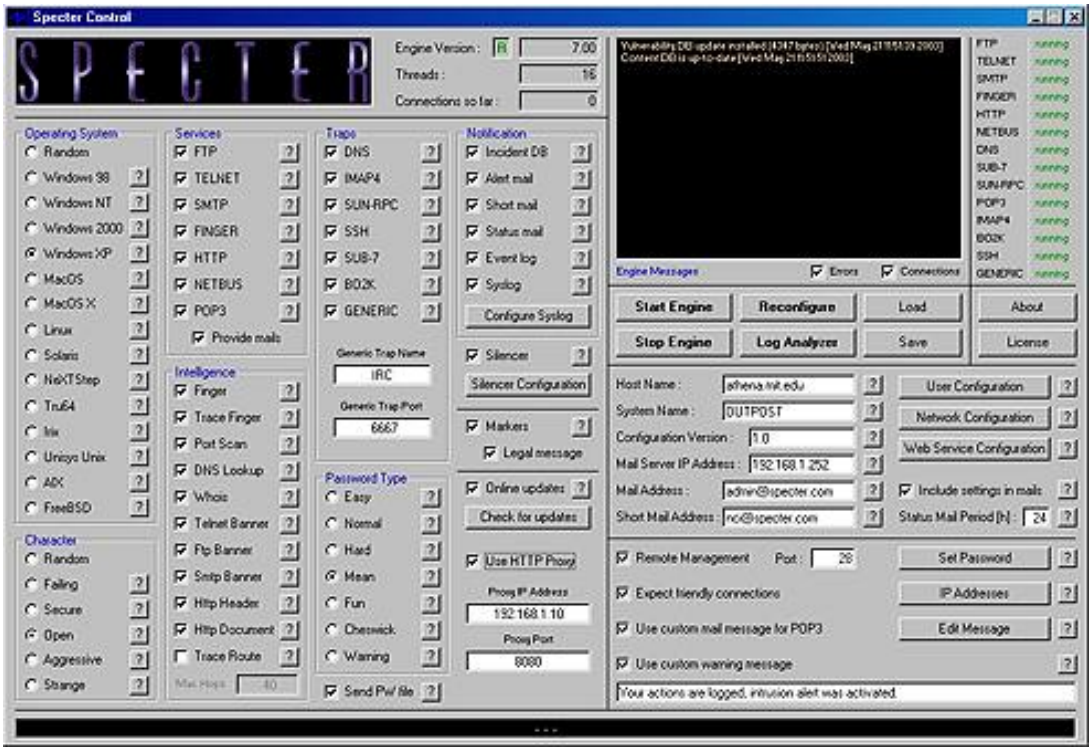

Figura 14 – Tela do Specter [35]

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), mas não consegue emular na pilha IP, assim um atacante fazendo uso de uma

ferramenta de obtenção de impressões digitais ativa pode detectar o *honeypot*.

Possui grande variedade de configuração, características de notificação, banco de dados dos incidentes, além da facilidade no uso.

Classificação: baixa interação / produção

4.1.3. NetBait [44]

NetBait é uma solução de segurança de rede que redireciona ataques contra espaços de IP não utilizados para "fazendas de *honeypots*", anulando o intruso pelo uso da ilusão.

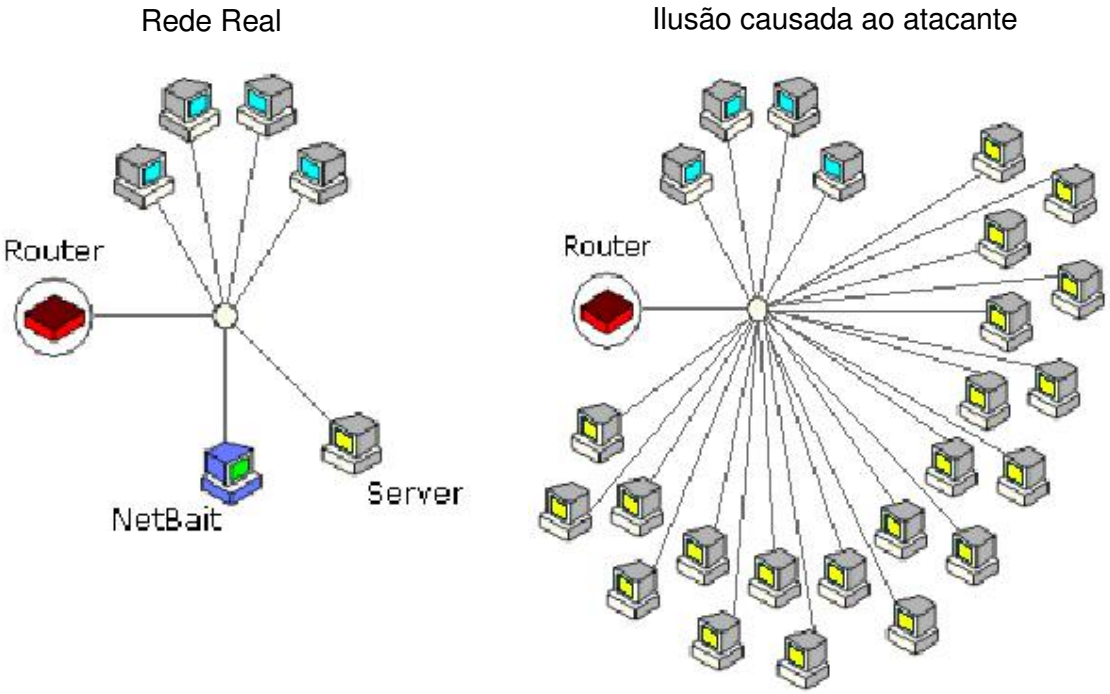

Figura 15 – Ilusão causada pelo NetBait [25]

NetBait cria esses ambientes projetando um desvio da rede real, assim os nós da rede ficam cercados por múltiplos nós falsos; cada nó falso pode ser configurado com qualquer combinação de sistemas operacionais, serviços e aplicativos. Possui gerenciamento remoto centralizado e configuração de comportamento dinâmico.

Classificação: baixa interação / produção

4.1.4. Smoke Detector [47]

Smoke Detector emula até dezenove sistemas operacionais por máquina entre Linux, Solaris8, HP-UX, AIX4, FreeBSD4, AS400, WindowsNT4 e Windows2000, confundindo e estendendo o tempo de resposta ao invasor.

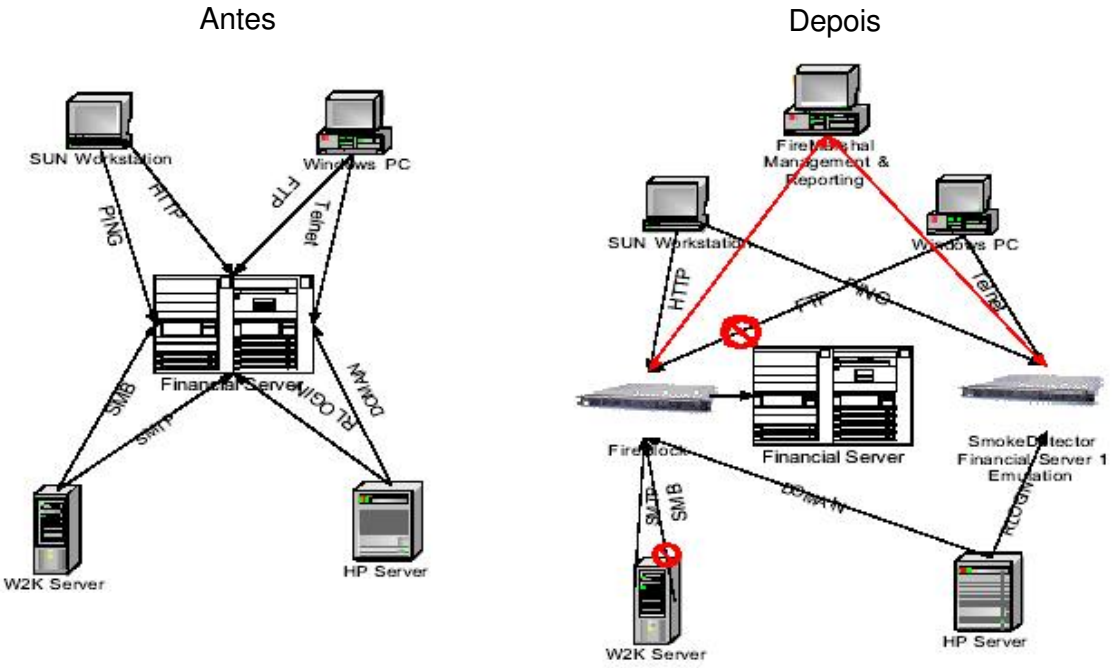

Figura 16 – Funcionamento do Smoke Detector [25]

Ele é usado para disfarçar servidores importantes, enviando alerta de tentativas de invasão ao administrador da rede, para permitir o bloqueio dos recursos reais em tempo hábil.

Classificação: baixa interação / produção

4.1.5. KFSensor [46]

KFSensor é um *honeypot* utilizado em plataforma Windows, projetado principalmente para proteção. Ele é preparado para bloquear ataques de recusa de serviço e estouro de buffer; registra os logs do atacante, podendo ser filtrado de várias maneiras para facilitar a análise em determinada porta ou protocolo. É um *honeypot* comercial, mas disponibiliza cópias para avaliação.

Classificação: baixa interação / produção

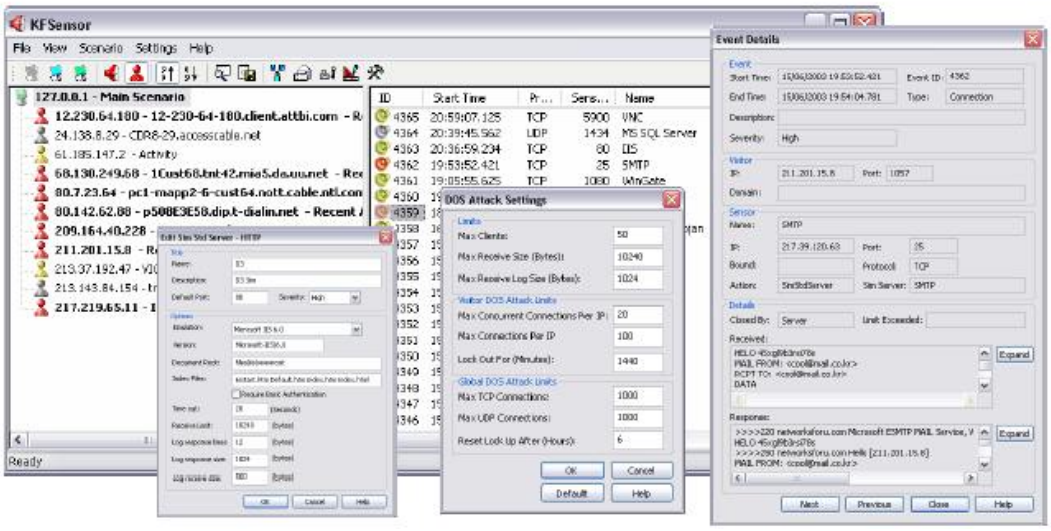

Figura 17 – Monitoramento do KFSensor [46]

4.2. Honeypots Free / OpenSource

4.2.1. BackOfficer Friendly [34]

É um programa para Windows que emula alguns serviços básicos de rede, como TELNET, FTP, SMTP, POP3. Quando o BackOfficer Friendly recebe conexão para um dos serviços citados, gera algumas respostas falsificadas, distraindo o invasor e proporcionado tempo para o bloqueio do ataque. Ele somente consegue monitorar sete portas por vez.

É indicado para iniciantes que desejam verificar o funcionamento de um *honeypot*.

Classificação: baixa interação / produção

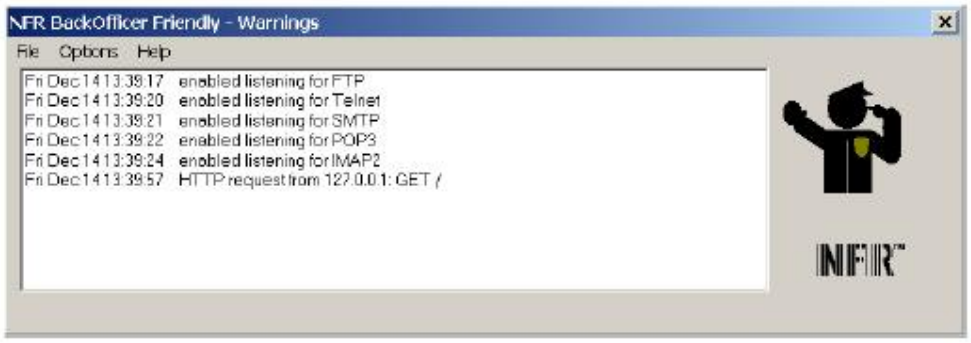

Figura 18 – Tela do BackOfficer Friendly [8]

4.2.2. Honeyd [53]

Honeyd é um dos principais aplicativos utilizados na construção de *honeypots*, sendo projetado para sistemas Unix. Ele emula centenas de sistemas operacionais, podendo simular aplicações no espaço de endereços IP não utilizados, utilizando vários simultaneamente.

Pode assumir a identidade de um IP que não esteja sendo utilizado e interagir com um atacante, respondendo suas requisições e registrando seu ataque; pode monitorar todas as portas baseadas em UDP e TCP. Grande facilidade de configuração.

Honeyd é OpenSource, ou seja, permite alteração no código fonte, podendo surgir novos scripts que emulam novos serviços.

Classificação: baixa interação / produção

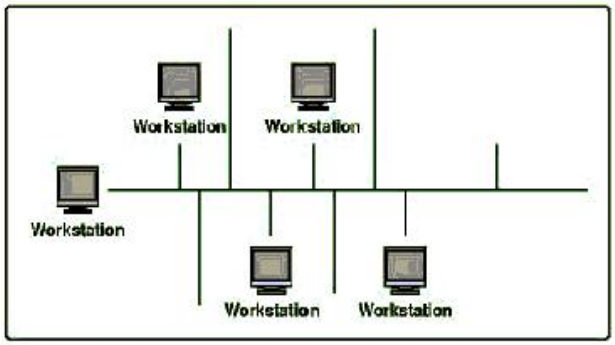

Figura 19 – Rede com endereços IP não utilizados [54]

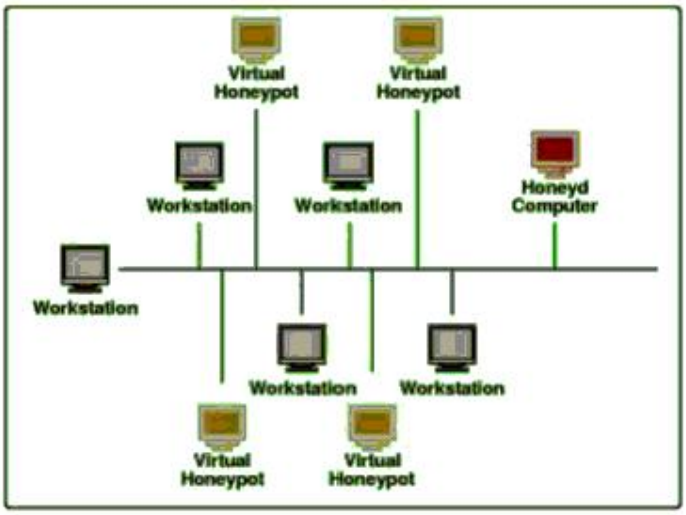

Figura 20 – Honeyd monitorando endereços IP não utilizados [54]

4.2.3. LaBrea Tarpit [43]

LaBrea Tarpit é um *honeypot* OpenSource desenvolvido para sistemas Windows ou Unix, projetado para diminuir a velocidade ou parar um ataque. LaBrea é um programa que cria um tarpit (poço de piche), assumindo o comando de endereços de IP novos em uma rede e criando máquinas virtuais que respondem a tentativas de conexão. As respostas forjadas enviadas pelo *honeypot* são utilizadas para manter uma conexão aberta com o atacante, diminuindo a velocidade ou até parando o ataque automatizado.

Classificação: baixa interação / produção

4.2.4. Deception ToolKit [45]

Deception Toolkit é utilizado para simular que um sistema possui um grande número de vulnerabilidades, atendendo as entradas do atacante e fornecendo respostas personalizadas falsas. São utilizadas rotinas para registrar todos os passos do atacante.

É um produto para plataformas Linux; exige um compilador de C e um interpretador de PERL.

Foi um dos primeiros *honeypots* desenvolvidos de forma completa, sendo bastante interessante para estudo.

Classificação: baixa interação / produção

4.2.5. Tiny Honeypot [48]

Tiny Honeypot é um software OpenSource, desenvolvido para plataforma Linux. Simula serviços de TELNET e FTP.

O *honeypot* monitora todas as portas e provê uma série de respostas falsas aos pedidos do atacante. A meta não é enganar atacantes qualificados, e sim deixar o processo mais difícil com uso de serviços falsos.

Classificação: baixa interação / produção

5. Outros Níveis de Honeypots

5.1. Honeytoken

Tradicionalmente os *honeypots* e *honeynets* são associados a computadores, recursos físicos utilizados para monitorar e/ou bloquear ataques; a real definição de um *honeypot*, apresentada no início desse trabalho, é a de ser um recurso de segurança criado para ser sondado, atacado ou comprometido, não o restringindo a um item físico. Qualquer informação que possa ser "plantada" nos processos de informação, que colabore com o objetivo inicial de um *honeypot*, pode ser chamada como tal. Esse tipo de *honeypot* não físico foi convencionado por honeytoken.

Um honeytoken pode ser uma conta de usuário com falsos privilégios, uma planilha ou uma abertura em um banco de dados.

Qualquer uso de informação disponibilizada através de um honeytoken é uma atividade não autorizada. É uma técnica antiga e extremamente simples, sendo indicada principalmente para detecção de ameaças internas.

Uma conta aparentemente privilegiada, contendo senha fraca, pode ser disponibilizada na rede; se os sistemas de monitoramento e detecção de intrusos estiverem preparados, o uso de tal conta pode ser imediatamente detectado, ajudando a identificar alguém tentando usar uma conta / acesso não permitido. [24]

Honeytokens, no entanto, possuem muitos empecilhos, pois a caracterização do uso indevido é feita através de sistemas de detecção de

conteúdo, e uso de criptografia ou compactação de dados atrapalham essa análise.

5.2. Honeyfarm

Em ambientes corporativos grandes, com milhares de redes distribuídas pelo mundo, o uso de *honeypots* é inviável pelo custo exigido nos recursos e profissionais. O desafio aumenta ainda mais se for utilizado *honeynets*.

Os *honeypots* de baixa interação capturam poucos dados, de grande valor sem dúvida, mas nada comparado as *honeynets*, que são mais flexíveis, poderosas e também mais complexas, consumindo muitas horas de trabalho, principalmente na análise de argumentação. O acompanhamento de milhares de pontos de *honeynet* de uma rede consumiria tempo excessivo.

Uma solução viável é a utilização do conceito de honeyfarm, que em vez de espalhar inúmeros *honeypots* pela rede, simplificaria o processo concentrando-os em uma única posição.

Toda atividade sem autorização é redirecionada, assim os atacantes são encaminhados para um *honeypot* contido na honeyfarm, achando que estão interagindo com um ponto de uma rede local.

A distribuição proposta facilita a manutenção, pois se torna mais simplificada; os riscos diminuem, já que o controle de dados é efetuado em uma única posição.

Honeypots, já citados nesse trabalho, como Honeyd e NetBait, são capazes de implementar esse recurso.

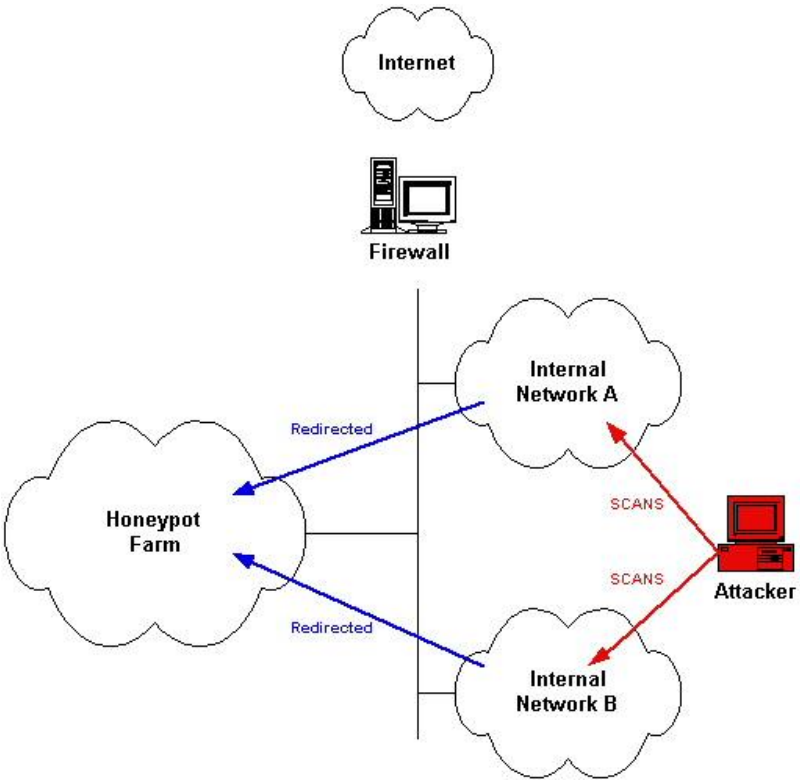

Figura 21 – Conceito de redirecionar atacantes para honeyfarm [22]

5.3. Dinamic honeypot

SPITZNER (2003) lançou idéias que tornariam o uso de *honeypots* muito mais facilitado, chamados de Honeypots Dinâmicos.

Hoje, o uso de *honeypots* é bastante trabalhoso, não importando qual tipo utilizado, de baixo ou alto nível, real ou virtual. A configuração exige bastante conhecimento e disponibilidade, pois tudo é manual; é necessário analisar quais sistemas operacionais serão anexados e se serão os mesmos da rede corporativa. A definição de quais os serviços que serão permitidos é de igual importância, já que erros podem tornar sua rede suspeita e sem efeito.

O acompanhamento dos *honeypots* é inevitável, pois exige atualizações constantes; novos sistemas são adicionados, antigos são modificados ou removidos e os *honeypots* devem acompanhar tais modificações para refletir corretamente a rede de produção.

SPITZNER sugeriu que fosse desenvolvido um *honeypot* plug-and-play, que automaticamente identifique uma rede de produção com seus sistemas operacionais e serviços. Por exemplo, quando Linux fosse adicionado à rede de produção, Linux automaticamente seria incorporado ao *honeypot*; quando ocorresse a remoção de Novell, este desapareceria do *honeypot*.

Essa implementação tem muitos pontos críticos:

- como o *honeypot* mapearia sua rede corporativa;
- ele poderia omitir um sistema e todas as tentativas enviadas ao sistema não teriam retorno;
- as atualizações não poderiam ser em tempo real, e sim em um intervalo de tempo pré-determinado.

No mapeamento poderá ser utilizada uma ferramenta de obtenção de impressões digitais passivo, que determinaria o número de sistemas, os tipos de sistemas operacionais, os serviços oferecidos, como estão se comunicando e com qual freqüência.

A ferramenta OpenSource p0f [55] tem muitas das capacidades relatadas, o problema é como fazer com que o *honeypot* utilize as informações fornecidas pelo software de forma adequada na criação de *honeypots* virtuais. O software Honeyd, já citado no trabalho, cria *honeypots* virtuais e também é OpenSource, assim a combinação deste com p0f seria um passo grande ao rumo do sonhado *honeypot* dinâmico. A concretização disso não está tão distante.

6. Conclusão

Honeypots são recursos de segurança planejados para serem comprometidos, com o propósito de colecionar informações sobre quem os ataca, suas técnicas, motivos e ferramentas utilizadas, levando ao desenvolvimento de tecnologias; podem ser utilizados também para desviar a atenção dos destinos reais.

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

Com o desenvolvimento dessa pesquisa foi possível compreender que esses sistemas devem ser monitorados constantemente e que o administrador possua conhecimentos profundos sobre o *honeypot* ou *honeynet* utilizado, para que o objetivo inicial seja alcançado e que, em caso de desajustes, este não seja utilizado como meio de ataque para outras redes.

A comunidade de segurança sempre esteve a um passo do inimigo, e com a disseminação dessa técnica, a cada dia o distanciamento é menor. A exposição dos resultados obtidos, como é feita pelas organizações aqui mencionadas, é de grande utilidade pública, pois permite que as empresas preparem suas redes e diminuam os riscos, baseando-se nas tendências e técnicas divulgadas.

Hoje, o uso correto de *honeypots*, como já afirmado, requer conhecimentos aprofundados sobre a rede, mas indícios de que isso será bastante facilitado já foram lançados: criação do *honeypot* dinâmico, não requerendo excessivas configurações e acompanhamentos, agraciando os profissionais de segurança.

6.1. Propostas para Trabalhos Futuros

- A semente sobre os *honeypots* dinâmicos foi lançada por Spitzner, fica aqui a sugestão para tentativa de união do *honeypot* Honeyd e a ferramenta de obtenção de impressões digitais p0f, ambos OpenSource. Certamente será de grande valor para toda comunidade de segurança.

- O trabalho apresentou a técnica, os tipos e os *honeypots* disponíveis no mercado; a documentação de um processo de monitoração, com todos os dados coletados através do uso de um dos *honeypots* mencionados complementaria este trabalho de graduação.

- A pesquisa sobre invasões em redes wireless ainda é escassa; implementação de mais honeynets nesse tipo de transmissão permitirá conhecer as vulnerabilidades para desenvolvimento de tecnologias de segurança mais consistentes.

Referências Bibliográficas

[1] The Honeynet Project. “Conheça seu inimigo – O Projeto Honeynet”. Editora Makron Books, São Paulo, 2002.

[2] CRONKHITE & MCCULLOUGH. “Hackers, Acesso Negado”. Editora Campus, Rio de Janeiro, 2001.

[3] The Honeynet Project. Acesso em 02/06/2003.
http://www.honeynets.org

[4] Intrusion Detection, Honeypots and Incident Handling Resources. Acesso em 02/06/2003. http://www.honeypots.net/

[5] Honeypots: Tracking Hackers. Acesso em 22/06/2003.
http://www.tracking-hackers.com

[6] Honeynet.BR. “Honeynet.BR: Desenvolvimento e Implantação de um Sistema para Avaliação de Atividades Hostis na Internet Brasileira”. Acesso em 25/05/2003.
http://www.lac.inpe.br/security/honeynet/papers/hnbr_ssi2002.pdf

[7] IEEE Computer Society. “The Honeynet Project: Trapping the Hackers”. Acesso em 22/06/2003. http://computer.org/security/sp2003/j2015abs.htm

[8] Reto Baumann, Christian Plattner. “Honeypots”. Acesso em 24/06/2003. http://security.rbaumann.net/download/diplomathesis.pdf

[9] Lance Spitzner. “Honeypots, definitions and value of honeypots“. Acesso em 22/06/2003. http://www.tracking-hackers.com/papers/honeypots.html

[10] Reto Baumann, Christian Plattner. “White Paper: Honeypots”. Acesso em 22/07/2003. http://security.rbaumann.net/download/whitepaper.pdf

[11] Jarbas Peixoto. “Honeynet: Um ambiente para análise de intrusão”. Dissertação, Unesp, São José do Rio Preto, 2002.

[12] Alexandre Andrucioli. “Honeypots”.
Dissertação, UFRJ, Rio de Janeiro, 2003.

[13] Modulo Security. Acesso em 27/07/2003.
http://www.modulo.com.br

[14] Hisham Kotry. “Building a virtual honeynet”. Acesso em 22/06/2003. http://www.linuxsecurity.com/feature_stories/feature_story-100.html

[15] Ricky M. Magalhaes. “Understanding Virtual Honeynets”. Acesso em 01/08/2003.
http://www.windowsecurity.com/articles/Understanding_Virtual_Honeynets.html

[16] Lance Spitzner. “The Value of Honeypots, Part Two: Honeypot Solutions and Legal Issues”. Acesso em 22/06/2003.
http://www.securityfocus.com/infocus/1498

[17] Michael Clark. “Virtual Honeynets”. Acesso em 27/07/2003.
http://www.securityfocus.com/infocus/1506

[18] Lance Spitzner. “Open Source Honeypots: Learning with Honeyd”. Acesso em 21/09/2003. http://www.securityfocus.com/infocus/1659

[19] Lance Spitzner. “Specter: a Commercial Honeypot Solution for Windows”. Acesso em 26/08/2003.
http://www.securityfocus.com/infocus/1683

[20] Lance Spitzner. “Honeypots: Are They Illegal?”. Acesso em 22/06/2003. http://www.securityfocus.com/infocus/1703

[21] Lance Spitzner. “Honeytokens: The Other Honeypot”. Acesso em 25/08/2003. http://www.securityfocus.com/infocus/1713

[22] Lance Spitzner. “Honeypot Farms”. Acesso em 20/08/2003.
http://www.securityfocus.com/infocus/1720

[23] Lance Spitzner. “Dynamic Honeypots”. Acesso em 21/09/2003.
http://www.securityfocus.com/infocus/1731

[24] Augusto Barros. “Honeytokens – O Próximo Nível dos Honeypots” Acesso em 25/05/2003.
http://www.augustobarros1.hpg.ig.com.br/artigos.html

[25] Lance Spitzner. “Honeypots – The Future”. Acesso em 20/09/2003. http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-spitzner.pdf

[26] Cristiano Gerlach. “Técnicas adotadas pelos crackers para entrar em redes corporativas e redes privadas”. Acesso em 19/06/2003.
http://www.rnp.br/newsgen/9903/crackcorp.shtml

[27] RNP. “Entidades mais vulneráveis a um ataque”. Acesso em 19/06/2003. http://www.rnp.br/newsgen/9903/vitimas.shtml

[28] CESET Unicamp. “Ataques de Recusa de Serviço”. Acesso em 27/08/2003. http://www.ceset.unicamp.br/servicos/sdos.htm

[29] Carl Constantinev. “Tools of the Trade: Part 2”. Acesso em 28/08/2003. http://linux.oreillynet.com/pub/a/linux/2001/06/29/tools_two.html

[30] Michael Anuzis. “Basic Methods of Allowing Access to Your Honeynet”. Acesso em 23/07/2003.
http://www.anuzisnetworking.com/whitepapers/hpaccess/

[31] “Bridge”. Acesso em 18/08/2003.
http://student.dei.uc.pt/~jsilva/informaticabasica/comunicacoes/redes/

[32] André Guerra. “Usando o Nmap”. Acesso em 31/08/2003.
http://www.invasao.com.br/coluna-andre-05.htm

[33] Fyodor. “Remote OS detection via TCP/IP Stack FingerPrinting”. Acesso em 30/08/2003.
http://www.insecure.org/nmap/nmap-fingerprinting-article.html

[34] BackOfficer Friendly. Acesso em 22/09/2003.
http://www.nfr.com/resource/backOfficer.php

[35] Specter. Acesso em 22/09/2003.
http://www.specter.com

[36] Mantrap. Acesso em 20/08/2003.
http://www.orbit2000.com/mantrap.asp

[37] Mantrap. Acesso em 24/09/2003.
http://www.trtec.com.br/pages/mantrap.html

[38] Wireless Honeynet Project. Acesso em 18/09/2003.
http://www.dfwwireless.org/honeynet.htm

[39] Marcelo Martins. “Protegendo Redes Wireless 802.11b”. Acesso em 26/09/2003.
http://www.xsecurity.ws/documentacao/papers/geral/wireless_mmartins.pdf

[40] Galileu (2003). “A nova brecha da Internet”. Março. Editora Globo.

[41] Kecia Gubbels. “Hands in the Honeypot”. Acesso em 27/07/2003.
http://www.sans.org/rr/paper.php?id=365

[42] Talisker Security Wizardry. “Honeypots”. Acesso em 28/08/2003.
http://www.networkintrusion.co.uk/honeypots.htm

[43] LaBrea. Acesso em 23/09/2003.
http://scans.bizsystems.net/paged_report.plx

[44] NetBait. Acesso em 23/09/2003.
http://www.netbaitinc.com/

[45] Deception Toolkit. Acesso em 24/09/2003.
http://www.all.net/dtk/dtk.html

[46] KFSensor. Acesso em 14/09/2003.
http://www.keyfocus.net

[47] Smoke Detector. Acesso em 17/09/2003.
http://palisadesys.com/products/smokedetector

[48] “Tiny Honeypot - resource consumption for the good guys”. Acesso em 20/09/2003. http://www.alpinista.org/thp/

[49] Verdade Absoluta. Acesso em 20/09/2003.
http://www.absoluta.org/index.htm

[50] Symantec. “Honeypots de olho na empresa”. Acesso em 23/09/2003.
http://www.symantec.com/region/br/enterprisesecurity/content/

[51] OpenlySecure. “Memoirs of an Invisible Firewall”. Acesso em 06/09/2003.
http://www.openlysecure.org/openbsd/how-to/invisible_firewall.html

[52] Interagir. Acesso em 08/09/2003.
http://www.geocities.com/interagir1/redes/bridge-firewall.zip

[53] Honeyd. Acesso em 28/08/2003.
http://www.citi.umich.edu/u/provos/honeyd/

[54] The Honeynet Project. “Virtual Honeypots”. Acesso em 28/07/2003.
http://niels.xtdnet.nl/papers/honeynet/

[55] “What is p0f v2?”. Acesso em 23/09/2003.
http://lcamtuf.coredump.cx/p0f.shtml

Glossário

Bridge	dispositivo que interliga redes locais que usam o mesmo protocolo, identificando a origem e o destino dos pacotes (ponte).
Buffer	local de armazenamento temporário de informações.
Bug	erro em um programa (software) ou mesmo em um equipamento (hardware), que provoca uma ação inesperada.
Default	configuração padrão utilizada automaticamente pelo sistema.
Emular	capacidade de um programa ou dispositivo para imitar outro programa.
Firewall	dispositivo constituído pela combinação de software e hardware, utilizado para dividir e controlar o acesso entre redes de computadores.
Firewall Invisível	firewall configurado para atuar como uma bridge: não possui IP nas suas interfaces e não decrementa o TTL (Time to Live) dos pacotes IP que o atravessam, tornando as chances de ataques bem menores.
Flag	bits do registro de estado (status).
Gateway	dispositivo que conecta redes que normalmente não se comunicam, permitindo a transferência de informações.
Host	qualquer computador de uma rede.
Kernel	núcleo do sistema operacional.
Log	Registro das ocorrências.
OpenSource	aplicativo que permite alteração no código fonte.
Recusa de Serviço	“bombardeamento” de mensagens através do correio eletrônico, podendo incapacitar temporariamente uma rede.

Rootkit	Coleção de softwares projetados para não deixar pistas de um invasor e fornecer portas de fundo para futuras invasões no sistema.
Roteador	dispositivo de uma rede que recebe dados e os envia aos pontos de destino, sempre usando as rotas mais curtas e livres disponíveis.
Sniffer	ferramenta de software que registra o tráfego da rede e remete a quem instalou.
Spoofing	modificação de endereço IP de origem simulando proveniência de outros sistemas ou redes, dificultando a identificação dos atacantes; normalmente utilizado para ataques de recusa de serviço.
Tripwire	ferramenta que verifica alterações não autorizadas na assinatura de arquivos e diretórios de todo o sistema.