# *Honeypots e Honeynets: as vantagens de conhecer o inimigo*

**Alexandre Lopes**

**Faculdade de Tecnologia de Ourinhos – FATEC**

**Orientador: Profº. Esp. Thiago José Lucas**

## Introdução

Segundo Ulbrich e Della Valle (2009 p.36) hoje há computadores por toda nossa volta e presente em diversas tarefas do nosso cotidiano. Com o aumento da globalização, e conseqüentemente os aumento das conexões de computadores espalhadas pelo mundo, novos conceitos em relação à tecnologia vão surgindo. Mas nem toda nova tecnologia que surge é para o bem da humanidade, no mesmo ritmo que surgem tecnologias novas com intuito de melhorar a vida da população, também surgem tecnologias inovadoras para tirar lucros e vantagens, explorando as vulnerabilidades e falhas no mundo da tecnologia da informação.

A informação é um dos tesouros mais cobiçados atualmente, mais ainda no mundo digital. Como todo bem valioso a informação necessita de uma segurança dedicada, eficiente e sofisticada, para que o acesso a este bem seja restrito e controlável.

Para Campos (2007 p.21) "a informação é elemento essencial para todos os processos de negócio da organização sendo, portanto, um bem ou ativo de grande valor."

A informação é o ativo mais valioso que uma organização pode ter e esta pode ser alvo de ataques a qualquer instante. Visto que a informação é um bem muito importante em todos os segmentos, em especial nas empresas, os profissionais de segurança da informação vivem em constante "queda-de-braço" com essa comunidade secreta comumente chamada de clãs ou como todos os conhecem os famosos e tão enfatizados "hackers".

De acordo com Ulbrich e Della Valle (2009) antigamente as invasões eram cometidas apenas por pessoas especialistas e com grandes conhecimentos técnicos. Hoje em dia com o fácil acesso a Internet, qualquer pessoa com pouco conhecimento em informática, e com o auxilio de tutoriais e ferramentas disponibilizadas na mesma,

conseguem fazer ataques a redes e sistemas desprotegidos, obtendo êxito na maioria das vezes.

Contra a isso as empresas estão se conscientizando que não basta apenas ter uma política de segurança minimizando alguns incidentes indesejáveis, pois a mesma não previne totalmente os ataques.

De acordo com Barbato e Montes (2003) quando descobrimos o perfil do inimigo como, suas táticas e técnicas, ferramentas e principalmente seus objetivos, torna-se mais fácil a criação de métodos de defesa capazes de combater e impedir diretamente esses ataques.

Baseado na idéia de que apenas a detecção dos ataques não era o suficiente para garantir a segurança dos ativos, as comunidades de segurança da informação perceberam que era necessário adotar uma nova técnica onde era preciso conhecer o inimigo, saber quais são suas motivações, métodos, ferramentas e táticas utilizadas para o ataque. Foi a partir desse conceito que surgiu o *Honeypot*.

## Honeypot

Segundo Rocha (2003), Jessen e Chaves (2008), Montes (2004), Marcelo e Pitanga (2003) os primeiros indícios de um método utilizando os princípios dos *honeypots* foram relatados no artigo "The Cuckoo's" do astrônomo Clifford Stoll, onde relatou um ataque sofrido nos sistemas da LBL (LawrenceBerkeley Laboratory) em 1988, no qual colheu informações como a origem do ataque, motivos e redes-alvos.

Em 1992 o artigo "An Evening with Berferd" do professor Bill Cheswick e o "There Be Dragons" do pesquisador e professor Steven M. Bellovin mostraram o estudo e criação de um sistema preparado para ser invadido, visando o aprendizado. Estes artigos foram muito importantes para o desenvolvimento futuro do *honeypot*, pois muitos especialistas de segurança se basearam nesta metodologia para atrair e capturar invasores.

O termo *honeypot* surgiu no ano de 1997, quando Fred Cohen desenvolveu a ferramenta Detection Toolkit (DTK), a primeira utilizada para emulação de diversas vulnerabilidades e armazenamento das informações coletadas sobre os ataques sofridos. A ferramenta é um conjunto de scripts desenvolvidos na linguagem Perl e C, tendo seu código aberto e gratuito para uso.

No ano de 1998, foi desenvolvida pela empresa Cybercop o primeiro *honeypot* comercial, o Sting. Ele rodava em sistemas operacionais Windows NT e simulava uma rede inteira, emitindo falsas respostas aos atacantes. Essa ferramenta facilitou o processo de instalação, configuração e manutenção, tornando o programa mais acessível. Ainda no mesmo ano, foi criado um *honeypot* para o governo dos Estados Unidos, onde era emulada uma rede classe C inteira, com sete sistemas operacionais diferentes simulados. O criador desse *honeypot* é o mesmo criador do Snort (IDS), o especialista em segurança de rede Martin Roesch.

Ainda em 1998 houve o lançamento do BackOfficer Friendly, um *honeypot* baseado em Windows e Unix desenvolvido por Marcus Ranum e lançado pela Network Flight Recorder. Ele era livre e extremamente fácil de usar, podendo rodar em qualquer sistema de desktop Windows.

Em 1999, foi criado o *Honeynet Project*, um grupo de 30 especialistas em segurança da informação liderado por Lance Spitzner. Eles conseguiram desenvolver várias metodologias para implementação de *honeypots*, uma delas foi o Honeyd, um *honeypot* de código aberto criado em 2002 por Niels Povos e muito utilizado até hoje. A partir do *Honeynet Project*, os *honeypots* ganharam repercussão mundial e demonstraram a importância do estudo do comportamento dos invasores de uma rede para o desenvolvimento de novas ferramentas e sistemas de defesa.

Foi criado em 2002, o Honeynet Research Alliance, fórum de organizações que compartilham suas informações sobre tecnologias de *Honeypots* e *Honeynets* por todo o mundo.

No Brasil a história do Projeto Honeynet.BR teve início com uma palestra do especialista Lance Spitzner, um dos criadores do *Honeynet Project* em junho de 2000.

Apesar das dificuldades, a idéia ganhou força a partir de 2001. Nessa época, o INPE (Instituto Nacional de Pesquisas Espaciais) e o NBSO (Grupo de respostas a Incidentes de Segurança mantido pela CERT/CC) iniciaram uma cooperação maior e, no final daquele ano surgiu a idéia de implementar um protótipo do projeto em um laboratório do Curso de Pós-Graduação em Segurança de Sistemas de Informação do INPE. Deste protótipo, partiu-se para um projeto maior, desenvolvendo pesquisa na área e envolvendo diversos alunos de doutorado e mestrado.

Assim, em março de 2002 começaram as operações do Honeynet.BR. Três meses após o seu lançamento, em junho de 2002 o Projeto Honeynet.BR tornou-se

membro da Honeynet Research Alliance. O objetivo do projeto era aumentar a capacidade de detecção de ataques e incidentes, porém desde 2008 o projeto não é mais mantido.

Segundo Marcelo e Pitanga (2003) o termo *Honeypot* vem do inglês e significa pote de mel. O mel na antiguidade era um alimento muito cobiçado, por ser muito consumido por nobres e reis, e também devido a sua doçura extrema. Um *honeypot* em uma rede de computador dever seguir este princípio, ser muito atraente para atacantes.

Afirma Assunção (2008) que um *honeypot* é uma ferramenta ou sistema criado com objetivo de enganar um atacante e fazê-lo pensar que conseguiu invadir o sistema, quando na realidade, ele está em um ambiente simulado, tendo todos os seus passos vigiados.

"*Honeypots* são recursos computacionais dedicados a serem sondados, atacados ou comprometidos, num ambiente que permita o registro e controle dessas atividades." (Honeynet.Br, 2005)

Spitzer (2002) define um *honeypot* como sendo um recurso em uma rede, cuja função é de ser atacado e invadido, assim possibilitando um futuro estudo das ferramentas e métodos utilizados no ataque. Esta ferramenta possui falhas de segurança reais ou virtuais, expostas de maneira proposital, possibilitando a invasão da rede.

Um *honeypot* não contém dados ou aplicações importantes para a organização e seu único propósito é de passar-se por um legítimo equipamento da organização que é configurado para interagir com um hacker em potencial. Assim, os detalhes da técnica utilizada e do ataque em si podem ser capturados e estudados. (Nakamura, Geus, 2007 pag.276)

Para Marcelo e Pitanga (2003) além de capturar as informações sobre o ataque, um *honeypot* pode mostrar as intenções do ataque e também fazer com que, os hackers percam tempo com ataques não efetivos, enquanto os especialistas colhem o máximo de informações para poder melhorar a segurança das organizações.

## Tipos de Honeypots

Segundo Marcelo e Pitanga (2003), Assunção (2008), Montes (2004) e Hoepers, Jessen e Chaves (2007) os *Honeypots* se dividem em dois tipos, de pesquisa e de produção.

**Honeypots de Pesquisa:** Os *honeypots* de pesquisa são ferramentas de pesquisa programadas para observar as ações de atacantes ou invasores, permitindo análises detalhadas de suas motivações, das ferramentas utilizadas e vulnerabilidades exploradas. Eles são mais utilizados para estudos ou por empresas de proteção contra ataques. Esse tipo de *honeypot* trabalha fora da rede local da empresa, sendo que, uma configuração mal feita pode acarretar em novos ataques.

**Honeypots de Produção:** Os *honeypots* de produção são utilizados em redes de produção como complemento ou no lugar de sistemas de detecção de intrusão. Tem como objetivo analisar e detectar atacantes na rede, conseqüentemente tomando as devidas providencias o mais rápido possível. Os *honeypots* de produção são utilizados por empresas e instituições que visam proteger suas redes.

"A evolução dos ataques acontece em um fluxo normal, sendo que, conforme os mecanismos de defesa melhoram seu desempenho evitando os ataques, novas técnicas aparecem para testar e vencer a defesa." (Nakamura, Geus 2007 pag.276)

## Níveis de interação do Honeypots

Com afirma Montes (2004) os *honeypots* podem ser classificados em dois níveis de serviços: o de baixa interação e o de alta interação. Assunção (2008) completa dizendo que estes níveis de serviços são as formas de como os *honeypots* trabalham.

De acordo com Marcelo e Pitanga (2003), Assunção (2008) e Hoepers, Jessen e Chaves (2007) os níveis dos *honeypots* são:

- **Baixa Interação**: os *honeypots* de baixa interação são sistemas e serviços de rede que são emulados, onde o sistema real subjacente é inacessível, não permitindo que o atacante interaja com o sistema real. Sua instalação e configuração são muito fáceis, pois sua arquitetura é simples e seu funcionamento é básico.

- **Alta interação**: os *honeypots* de alta interação são máquinas que atuam como servidores de serviços de rede reais e totalmente acessíveis. O atacante pode ganhar total controle sobre esses sistemas, podendo oferecer um grande risco ao sistema. O *honeypot* deve ser implementado em um local onde se tenha um grande controle da rede através de métodos de proteção e detecção. Sua implantação é mais complexa, porém com ele podemos coletar uma vasta quantidade de informações dos atacantes.

Segundo Jessen e Chaves (2008) os *honeypots* de baixa e alta interatividade podem proporcionar um grande risco à rede da empresa quando forem mal configurados.

Marcelo e Pitanga (2009) dizem que, se os *honeypots* não forem configurados de maneira correta e utilizados por pessoas especialistas que tenham um grande conhecimento na área, provavelmente esses *honeypots* se tornarão uma grande oportunidade para o atacante invadir sistemas importantes de sua rede. Uma má configuração e utilização do *honeypot* podem proporcionar danos à empresa inimagináveis.

Jessen e Chaves (2008) diz que o principal objetivo quando se usa um *honeypot* de baixa interatividade é identificar scans e ataques automatizados, enganar script kiddies, atrair atacantes para longe dos sistemas operacionais e coletar o máximo de assinaturas de ataques.

Marcelo e Pitanga (2003) comentam que quando é usado o *honeypot* de alta interatividade o objetivo é observar o comportamento e as atividades dos atacantes, coletar o máximo de material para pesquisa e elaborar um treinamento com o objetivo de melhorar a segurança da informação.

**Baixa x Alta Interatividade**

| Caracteristicas | Baixa Interatividade | Alta Interatividade |
|---|---|---|
| **Instalação** | **Fácil** | **Fácil** |
| **Manutenção** | **Fácil** | **Trabalhosa** |
| **Obtenção de Informações** | **Limitada** | **Extensiva** |
| **Necessidade de mecanismo de contenção** | **Não** | **Sim** |
| **Atacante tem acesso ao s.o real** | **Não (em teoria)** | **Sim** |
| **Aplicações e servilos oferecidos** | **Emulados** | **Reais** |
| **Atacante pode comprometer o honeypot** | **Não (em teoria)** | **Sim** |
| **Risco da organização sofrer um comprometimento** | **Baixo** | **Alto** |

Quadro 1: Campus Party Brasil 2011, Sao Paulo – janeiro de 2011 – p. 25/41

## Ferramentas Honeypots

No mercado atual, existem várias ferramentas que são utilizadas para a implementação dos *honeypots*. Apresentarei algumas ferramentas honeypots a seguir, segundo Marcelo e Pitanga (2009), Assunção (2008), Jessen e Chaves (2008), Hoepers, Jessen e Montes (2003).

**Deception Toolkit (DTK)**

O Deception Toolkit ou DTK como é mais conhecido, foi o primeiro *honeypot* baseado em software. Criado por Fred Cohen este software é um conjunto de ferramentas escritas em Perl e C, que emula uma variedade de serviços básicos existente, assim usado para detectar e enganar os atacantes.

**CyberCop Sting**

O CyberCop Sting é um dos primeiros *honeypots* comerciais desenvolvidos para organizações. Criado pela empresa CyberCop, este software permite aos gestores monitorar silenciosamente atividades suspeitas em sua rede e identificar possíveis problemas e vulnerabilidades.

O Sting simula uma rede contendo vários tipos diferentes de dispositivos de rede, incluindo servidores Windows-NT, servidores Unix e roteadores. Cada dispositivo da rede virtual tem um endereço IP real e pode enviar e receber pacotes de verdadeira aparência, para emular ainda mais um verdadeiro sistema, para não levantar desconfiança do atacante.

**Honeyd**

O Honeyd é um software que emula vários sistemas operacionais e aplicações, permitindo a criação de hosts virtuais e também o anexo de scripts escritos em Perl para criações de interações em determinadas portas, assim levando os hackers a acreditar que aquela é uma rede real.

Criado pelo pesquisador e engenheiro de software Niels Provos em abril de 2002, o Honeyd é um software de código-aberto, feito para as versões Windows e Linux, onde possibilita a configuração para atender todas as necessidades dos usuários, tanto para pesquisa quanto para produção.

No ano de 2007 foi lançada a versão Honeyd 1.5 e sua próxima versão está sendo desenvolvida atualmente.

**KFsensor**

Desenvolvido pela empresa KeyFocus, o KFSensor é um *honeypot* comercial para Windows que trabalha com recursos de baixa interatividade, simulando serviços e respostas aos atacantes. Algumas das características inovadoras do KFSensor são os gerenciamentos remotos, os mecanismos de assinatura compatíveis ao Snort e as emulações de protocolos do Windows.

Ele permite a instalação de cenários em locais estratégicos na rede, possibilitando a monitoração do tráfego, assim enviando remotamente as respostas coletadas para o computador onde esta instalado o KFSensor.

**Nepenthes**

Aparentemente parecido com o Honeyd, o Nepenthes é um *honeypot* de baixa interação que emula vulnerabilidades para uma possível coleta de informações sobre ataques. Ele utiliza essas vulnerabilidades para coletar vírus e worms que tentam explorá-las. Além de ser um software gratuito, ele pode ser instalado em vários sistemas como Windows, Linux e MacOS.

**Dionaea**

Desenvolvido para ser o sucessor do Nepenthes, este *honeypot* de baixa interatividade foi criado em 2009 pelo Honeynet Project, tendo o Python como sua linguagem de scripts.

O Dionaea emula vulnerabilidades de sistemas operacionais, possibilitando que o ataque possa ser realizado através da rede. Ele é utilizado para capturar e armazenar os ataques, sendo os mesmos realizados com sucesso. Os ataques são armazenados em um banco de dados, que servirá como meio de pesquisa e estudos, possibilitando a criação de novos sistemas de defesas.

**BackOfficer Friendly (BOF)**

Escrito por Marcus Ranum o BackOfficer Friendly é um *honeypot* desenvolvido para ser usado na plataforma Windows, onde simula serviços básicos de redes. Quando ele recebe conexões como Telnet, FTP, SMTP e POP3, são geradas respostas falsas que distraem os atacantes enquanto medidas de bloqueio de ataques são elaboradas.

Uma desvantagem do BOF é que ele pode monitorar apenas 7 portas. Uma de suas grandes vantagens é o fácil manuseio, pois possui um ambiente de uso muito simples. Este software é uma excelente alternativa para iniciantes que desejam verificar e conhecer o funcionamento de um *honeypot*.

- **Specter**

O Specter é um *honeypot* de baixa interação projetado para ser executado no Windows. Criado pela NetSee, este software pode emular até 13 sistemas operacionais diferentes, serviços como Http, Telnet, Ftp e também possui uma variedade de recursos de configuração e notificação. Uma das maiores vantagens do Specter é sua facilidade na hora da instalação e uso.

Todas as tentativas de ataques são registradas com o IP do atacante, hora do ataque, tipo de serviço atacado e o estado atual do serviço que esta sendo emulado naquele momento. Todas essas informações são armazenadas em um banco de incidentes.

## Honeynets

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.

De acordo com Assunçao (2009) uma *honeynet* é formada por um conjunto de *honeypots* que simulam uma rede de produção, que é configurada para que as suas atividades possam ser monitoradas, gravadas e em certo grau, controladas. É uma rede configurada para ser invadida, no qual todo tráfego que entra ou sai do gateway/roteador é considerada uma invasão.

Segundo Azevedo (2010) *honeynet* é uma rede altamente controlada onde todo pacote que entra ou deixa a *honeynet* é monitorada, capturado e analisado.

Rocha (2003) afirma que a *honeynet* normalmente e composta por sistemas reais, e necessita de um mecanismo de contenção eficiente, por exemplo, um firewall, para que não seja usada como origem de ataques e também para que não alerte o invasor do fato de estar em uma *honeynet*.

Conforme Honeynet Project (2002), após ser comprometida, ela pode ser estudada para aprender sobre as características dos ataques como, as ferramentas utilizadas, as táticas e os motivos que levam os atacantes a cometerem tal imprudência.

## Tipos de Honeynets

Segundo Marcelo e Pitanga (2003), Assunção (2008), Horpers, Jessen e Chaves (2007), Jabuor e Duarte (2003) e Azevedo (2010) existem dois tipos de *honeynets*: *honeynets* reais e *honeynets* virtuais.

- **Honeynets Reais**: Em uma *honeynet* real todos os dispositivos que a compõem, incluindo o honeypot, mecanismos de contenção, mecanismo de alerta e mecanismo de coleta de informações são físicos. Exemplificando, uma *honeynet* real poderia ser composta por diversos computadores, sendo que cada um poderia conter um *honeypot*, firewall, IDS e IPS, entre outros.

As vantagens de utilizar *honeynet* real é o baixo custo por dispositivo e os atacantes interagem com ambientes reais. As desvantagens são as manutenções que são mais difíceis e trabalhosas, necessidade de mais espaço físico e o custo total tende a ser mais alto.

- **Honeypot Virtual**: Uma *honeynet* virtual baseia-se na idéia de ter todos os componentes de um *honeypot* implementados em um número reduzido de dispositivos físicos. Para concretizar tal idéia, normalmente é utilizado um único computador com um sistema operacional instalado, que serve de base para a execução de um software de virtualização como o VMware, VirtualBox entre outros.

As vantagens de utilizar *honeynet* virtual é a manutenção que é bem mais simples, não há necessidade de um espaço físico maior para os equipamentos e o custo final tende a ser mais baixo. As desvantagens são o alto custo por dispositivo, pois são necessários equipamentos mais robusto para um bom desempenho da *honeynet.*, O atacante pode ter acesso a outras partes do sistema, pois tudo é compartilhado de um mesmo computador e o mesmo pode perceber que esta interagindo com um ambiente falso, uma rede virtual.

De acordo com Honeynet Projetc (2002) o conceito do funcionamento de uma *honeynet* é criar uma rede altamente controlada.

Spitzner (2002) diz que a idéia da *honeynet* é a de ter uma arquitetura que cria uma rede altamente controlada, onde colocamos dentro desta rede sistemas de produção e assim toda atividade realizada dentro dela será capturada, armazenada e analisada para criação de possíveis métodos de proteção contra ataques cibernéticos.

Honeynet Project (2002) ainda afirma que a captura de dados e o controle de dados são os grandes responsáveis para que uma *honeynet* seja bem elaborada.

## Controle de Dados

Após uma *honeynet* ser invadida temos que garantir que ela não seja usada para atacar outras redes e sistemas e essa garantia poder ser atingida através de um bom controle de dados.

Para tal controle podemos usar o firewall como ferramenta de segurança da informação. Segundo Assunção (2008) é essencial ter um firewall entre um roteador e um *honeypot/honeynet*, pois o mesmo será o responsável em armazenar em seus logs todo o tráfego de entrada e saída de uma *honeynet*. Deixar uma *honeynet* totalmente desprotegida não é aconselhável, sendo que possivelmente o atacante desconfiará que esta caindo em uma armadilha.

Segundo Honeynet Project (2002), em um período de 24 horas é aconselhável permitir de cinco a dez conexões externas realizadas pelos atacantes. Este período é suficiente para os invasores concluírem suas atividades e assim a captura de dados será bem sucedida. Meios automatizados devem ser usados para ter um controle de acesso ao *honeynet*, pois o ataque pode ocorrer a qualquer hora e nesses casos uma intervenção

manual pode ser um risco, podendo assim ser um grande potencial para falhas. Este meio automatizado pode ser um script específico do próprio firewall, assim quando o limite de conexões for atingido ele irá disparar alertas, controlar e bloquear o acesso a *honeynet*.

Como ainda explica Honeynet Project (2002) o objetivo das *honeynets* são capturar dados e aprender com eles, sendo assim a captura dos dados devem ser intensa, coletando todas as atividades que ocorrem dentro da *honeynet*. Esta captura de dados não pode ser armazenada localmente, mas sim em um local confiável e seguro, para que o atacante não possa ter acesso a essas informações.

## Captura de Dados

De acordo com Jabour e Duarte (2003) a captura de dados tem o propósito de registrar toda a atividade do invasor sem que ele perceba que está sendo monitorado, fazendo com que seja registrada todas as atividades feitas dentro da *honeynet*..

Segundo Honeynet Project (2002) existem várias camadas de captura de dados:

- **Camada de Controle de Acesso**: é a primeira camada da captura de dados, podendo ser um firewall ou roteador, assim toda informação passará por um dispositivo de controle de acesso. Todo tráfego que entra e sai da *honeynet* é considerado suspeito, e assim todas as ocorrências serão registradas no dispositivo de controle de acesso. Um problema desta camada é que não registra a atividade dentro da *honeynet*, apenas o tráfego que passa pelo dispositivo de controle de acesso.

- **Controle de Rede**: serve para capturar e analisar os pacotes que trafegam na rede. Um IDS pode ser usado para capturar a carga útil do pacote e disparar alertas com base em assinaturas suspeitas do administrador do sistema. As informações devem ser armazenadas de forma que seja fácil fazer sua analise posteriormente.

- **Camada de sistema**: caso o atacante use comunicação criptografada torna-se difícil capturar dados de pressionamento de teclas. Para resolver este problema

precisaremos capturar os registros do próprio sistema, onde fica todas as informações de como o invasor teve acesso e o que ele comprometeu no sistema. Estes registros precisam ser armazenados remotamente em um servidor protegido, para que o atacante não apague essas informações.

- **Camada Off-Line**: esta camada trabalha fazendo uma imagem do *honeypot* antes de ser colocado em atividade. Com isto, basta fazer uma comparação da imagem anterior com a atual para identificar todas as alterações feitas pelo invasor. Uma ferramenta que pode ser utilizada é o TRIPWIRE, que faz uma imagem antes de ser comprometido e a compara com o estado após a invasão. Podemos encontrar muitas informações valiosas, como ferramentas utilizadas pelos atacantes, seus códigos-fonte e suas configurações.

As *honeynets* são ótimas para controlar e capturar os dados de um atacante, mas de nada servirá essas informações se não forem de fácil entendimento.

Para isso os dados são capturados de forma inteligente, automatizando os processos que os coletam, como um e-mail de alerta. Serão examinados os logs do firewall, alertas de IDS e o tráfego capturado, registros do sistema e os pressionamentos de teclas.

## Tipos de Análises

Os tipos de análise Segundo Honeynet Project (2002) podem ser:

• **Logs de Firewall** – a análise de registros de um firewall geralmente é um processo muito trabalhoso, pois há grande quantidade de informações. No caso da *honeynet* o tráfego não é muito grande, pois não é um sistema de produção. Nela todo tráfego é suspeito, logo todo dado capturado é útil. Caso o firewall seja configurado para enviar alertas para o email do administrador quando há tentativas de entrada e saída de conexões, o processo de análise torna-se menos trabalhoso:

• **Análise do IDS** - o IDS captura três fontes de informações, a primeira são os alertas gerados pelo próprio IDS, a segunda é a captura de tráfego da rede armazenando num arquivo binário e a terceira são registros de histórico da sessão ASCII detectados na carga útil do pacote, como o pressionamento das teclas. Os alertas podem informar que tipo de serviço o atacante esta executando, onde se torna muito importante analisá-los.

• **Log de Sistema** - Em um sistema comprometido, o atacante tentará apagar ou modificar os arquivos de registro do sistema, por isso eles devem ser armazenados em um servidor remoto. Quando são mandados do *honeypot* comprometido para o servidor de registro de histórico remoto, esses dados são capturados pelo IDS através da rede. Com isso, os logs de sistemas estão em 3 lugares: no próprio sistema, no servidor de arquivos de registro remoto e na captura feita pelo IDS. Caso o atacante modifique os registros de histórico do sistema, basta fazer uma comparação com os dados capturados pelo IDS ou armazenados no servidor de arquivos de registro remoto.

## Conclusão

Os *Honeypots* e *Honeynets* são recursos que garantem uma melhor segurança das organizações. Seu uso é de muita utilidade para a segurança da informação, visto que através do estudo detalhado com as informações captura dos atacantes novos meios e técnicas poderão ser criadas contra os ataques de hackers.

Com o estudo detalhado dessas informações, conseguiremos saber a verdadeira face do inimigo, suas táticas e ferramentas utilizadas, seus métodos e os motivos que o levaram ao ataque.

Mesmo sendo de grande valor o uso dos *Honeypots* e *Honeynets* nunca se deve confiar a segurança da organização apenas a essas ferramentas, lembrando que elas não são meios de proteção direta, mas sim meios de estudos. Elas devem trabalhar juntos com meios de prevenções convencionais, para evitar assim que um atacante possa atacar outros sistemas ou redes.

Para que os *honeypost* e *honeynets* não virem uma arma para os invasores, é de extrema importância que as pessoas que forem implementar essas ferramentas tenham grandes conhecimentos em relação ao assunto, é importante que elas já tenham um

amplo conhecimento na área para que não haja falhas de segurança, assim possibilitando a exploração de vulnerabilidades do sistema da organização.

Se todas as medidas de segurança forem tomadas, o uso de *honeypots* e *honeynets* será indispensável quando o assunto for segurança dos sistemas e redes de computadores de uma organização.

## Referências


ASSUNÇÃO, Marcos Flavio Araújo. Segredos do Hacker Ético. 2. Ed. Florianópolis: Visual Books, 2008.

ASSUNÇÃO, Marcos Flavio Araújo. Aprenda a detectar e enganar invasores. Honeypots e Honeynets - Aprenda a Detectar e Enganar Invasores Ed. Florianópolis: Visual Books, 2008.

AZEVEDO, Hugo. Honeypots & Honeynets. Disponível em: <http://www.hugoazevedo.eti.br/doc/honeypot_honeynet.pdf> Acesso em 01 de Abril de 2013.

BARBATO, Luiz Gustavo C.; MONTES, Antonio. Tecnicas de Monitoração de Atividades em Honeypots de Alta Interatividade. Disponível em: < http://www.honeynet.org.br/papers/tmh-ssi2003.pdf> Acesso 24 de Abril de 2013.

CAMPOS, André. Sistema de Segurança da Informação – Controlando Riscos. Florianópolis. Visual Books, 2007.

HOEPERS, Cristine; JESSEN, Klaus Steding; MONTES, Antônio. Projeto Honeypots Distribuidos. Disponível em: <http://www.honeynet.org.br/presentations/hnbr-gts2003-slides.pdf> Acesso em 10 de Março de 2013.

HOEPERS, Cristine; JESSEN, Klaus Steding; CHAVES, Marcelo H. P. C. Honeypots e Honeynetes: Definições e Aplicações. Disponível em: <http://www.cert.br/docs/whitepapers/honeypots-honeynets/> Acesso em 12 de Abril de 2013.

HONEYNET.BR. Consórcio amplia conhecimento sobre ataques na Internet Brasileira. Disponível em: < http://www.honeynet.org.br/press/2005/2005-01-28.html> Acesso em 12 de Março de 2013.

JABOUR, E. C. M. G.; DUARTE, Otto C. M. B.Honeypots: Invasores, Ferramentas, Técnicas e Táticas. Disponível em:

<http://www.gta.ufrj.br/seminarios/CPE825/tutoriais/eugenia/honeynets.PDF> Acesso em 11 de Abril de 2013.

JESSEN, Klaus Steding; CHAVES, Marcelo H. P. C. Implantação de Honeypots de Baixa Interatividade com Honeyd e Nepenthes. Disponível em: <http://www.cert.br/docs/palestras/certbr-campusparty2008-2.pdf> Acesso em 24 de Abril de 2013.

MARCELO, Antônio; PITANGA, Marcos. Honeypots; A arte de iludir hackers. Rio de Janeiro: Brasport, 2003.

MONTES, ANTONIO. Honeypots e Honeynets: Contra-Iteligência no Ciberespaço. Disponivel em: <http://www.honeynet.org.br/presentations/hnbr-ABIN-CPqD04.pdf> Acesso em 29 de Março de 2013.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. Segurança de Redes em Ambientes Cooperativos. São Paulo: Novatec, 2007.

ROCHA, Luis Fernando. Honeynet: eficácia no mapeamento das ameaças virtuais – Parte 2. Disponivel em: <http://www.honeynet.org.br/press/2003/2003-06-30.html> Acesso em 25 de Abril de 2013.

SPITZNER, Lance. Honeypots: Trancking Hackers. USA: Addison-Wesley, 2002.

ULBRICH, Henrique Cesar; DELLA VALLE, James. Universidade do Hacker. São Paulo. Digerati Books, 2009.