

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RIO
GRANDE DO NORTE
CURSO DE PÓS-GRADUAÇÃO EM REDES DE COMPUTADORES**

HONEYPOTS E HONEYNETS

Héber Paullus Gomes

Orientador:
Ricardo Kleber Martins Galvão, Msc.

LIGA DE HÉBER PAULLUS GOMES DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RIO
GRANDE DO NORTE
CURSO DE PÓS-GRADUAÇÃO EM REDES DE COMPUTADORES

Honeypots e Honeynets

HONEYPOTS E HONEYNETS

Héber Paullus Gomes

Monografia apresentada e aprovada em 11 de outubro de 2007 pela banca examinadora composta pelos seguintes membros:

Monografia apresentada ao Curso de Pós-Graduação em Redes de Computadores da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte como requisito parcial para obtenção do grau de Especialista em Redes de Computadores.

Orientador:

Ricardo Kléber Martins Galvão, Msc.

Orientador: Ricardo Kléber Martins Galvão (M. Sc.)
 Monografia (Especialização em Redes de Computadores) – Faculdade
 Natalense para o Desenvolvimento do Rio Grande do Norte.
 1. Redes de Computadores – Monografia. 2. Segurança da informação –
 Monografia. 3. Honeypots – Monografia. 4. Honeynets – Monografia. I. Título.
 CDU 004.73
 RN/FARN/BC

NATAL/RN

2007

Natal/RN, 23 de outubro de 2007.

HÉBER PAULLUS GOMES

Honeypots e Honeynets

RB 30277 M
FARN
BIBLIOTECA
Nº Reg
14.12.07

Gomes, Héber Paullus

Honeypots e honeynets / Héber Paullus Gomes. – Natal: FARN, 2007.
58 f.

Orientador: Ricardo Kleber Martins Galvão (M. Sc.)

Monografia (Especialização em Redes de Computadores) – Faculdade
Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Redes de Computadores – Monografia. 2. Segurança da Informação –
Monografia. 3. Honeypots – Monografia. 4. Honeynets – Monografia. I. Título.

RN/FARN/BC

CDU 004.72

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RIO
GRANDE DO NORTE
CURSO DE PÓS-GRADUAÇÃO EM REDES DE COMPUTADORES**

HONEYPOTS E HONEYNETS

Héber Paullus Gomes

Monografia apresentada e aprovada em 11 de outubro de 2007 pela banca examinadora composta pelos seguintes membros:

Ricardo Kléber Martins Galvão, Msc.
Orientador

Aluizio Ferreira da Rocha Neto, Msc.

Assim meus avós paternos Isabel Cristina da Costa (in memoriam) a qual não tive contato, ao meu avô paterno Francisco Luiz Filho (in memoriam) que queria ser um médico, ao meu avô materno Manuel Dêdo Gomes, e especialmente a minha avó materna Maria Abel da Silveira Gomes a qual amo e admiro o amor

Natal/RN, 23 de outubro de 2007. *e pelos netos.*

AGRADECIMENTOS

Agradeço primeiramente a DEUS omnipotente e onipresente, pelo Dom de vida que me deu, a minha família pebulho, morinha, Bel e Iyla, a minha noiva Jaziane por compreenderem que o estudo também é uma das fórmulas do sucesso pessoal.

A todos os mestres do curso de especialização em redes de computadores por compartilharem parte de seus conhecimentos conosco e estimularem novos desafios em nossas vidas pessoal e profissional; um agradecimento especial ao Prof. Ricardo Kléber que impôs o desafio de orientar pelo mundo dos honeypots.

A Antônio Marcelo (HoneypotBR) e Rosinei Mariz (Tuta) pelas inúmeras dúvidas tiradas via men e e-mail, a Cláudia pela paciente correção e adequação da monografia nas normas da ABNT, a Aluísio Rocha por lutar e conseguir esta especialização, a toda turma do curso de especialização (se for dizer um por um acho me esquecendo), a Da^ª Conceição (que sempre fazia altas guloseimas, e em silencioso esperada por todos).

Aos meus avós paternos Izabel Cristina da Costa (In memoriam) a qual não tive contato, ao meu avô paterno Francisco Luiz Filho (In memoriam) que queria ter um neto Dr., ao meu avô materno Manuel Dédeo Gomes, e especialmente a minha avó materna Maria Alvi da Silveira Gomes a qual amo e admiro o amor incondicional que sente pelos netos.

AGRADECIMENTOS

Agradeço primeiramente a DEUS onipotente e onipresente, pelo Dom da vida que me deu, a minha família painho, mainha, Bel e Ivla, a minha noiva Liziane por compreenderem que o estudo também é uma das fórmulas do sucesso pessoal.

A todos os mestres do curso de especialização em redes de computadores por compartilharem parte de seus conhecimentos conosco e estimularem novos desafios em nossas vidas pessoal e profissional, um agradecimento especial ao Prof. Ricardo Kléber que topou o desafio de orientar pelo mundo dos honeypots.

A Antônio Marcelo (HoneypotBR) e Rosinei Muniz (Tuta) pelas inúmeras dúvidas tiradas via msn e e-mail, a Cláudia pela paciente correção e adequação da monografia nas normas da ABNT, a Aluizio Rocha por lutar e conseguir esta especialização, a toda turma do curso de especialização (se for dizer um por um acabo me esquecendo), a Dn^a Conceição (que sempre fazia altas guloseimas, e era ansiosamente esperada por todos).

RESUMO

Esta pesquisa visa apresentar o mundo dos Honeypots aos administradores de sistemas, o que são e como funcionam, utilizando-se de uma linguagem clara e fácil, partindo da importância da segurança de informações para as instituições, abordando as principais ameaças, atacantes e sistemas de defesa, partindo posteriormente para apresentação dos honeypots, como eles funcionam, seus tipos e níveis de aplicações, vantagens e desvantagens de sua utilização até abordar as honeynets com seus componentes e riscos.

ABSTRACT

This research aims at to present the world of the Honeypots to the administrators of systems, what they are and as they function, using itself of a clear and easy language, breaking of the importance of the security of information for the institutions, approaching the main threats, aggressors and systems of defense, leaving later for presentation of honeypots, as they function, its types and levels of applications, advantages and disadvantages of its use until approaching honeynets with its components and risks.

2.3 ATAQUES	16
2.3.1 Motivações de um ataque	17
2.3.2 Ataques quanto ao seu objetivo	18
2.3.3 Ataques quanto à sua origem	19
2.4 FIREWALL	19
2.4.1 Tipos de firewall	21
2.4.1.1 Firewalls de filtragem de pacotes	21
2.4.1.2 Firewalls servidores de proxy	21
2.4.2 Funcionalidades de um firewall	22
2.4.3 Arquitetura de firewalls	23
2.5 IDS	24
2.5.1 Histórico IDS	24
2.5.2 O que é um IDS?	25
2.5.3 Objetivos de um IDS	25
2.5.4 Tipos de IDS	25
2.5.4.1 IDS baseado em host (Host-Based Intrusion Detection System)	26
2.5.4.2 IDS baseado em rede (Network-Based Intrusion Detection System)	26
2.5.4.3 IDS híbrido (Hybrid Intrusion Detection System)	26
2.5.5 Eficiência e eficácia de um IDS	27
2.5.6 Sistema de prevenção de intrusão (IPS)	27
3 HONEYPOT	29
3.1 HISTÓRICO HONEYPOT	29
3.1.1 Honeypot no Brasil	30
3.2 COMO FUNCIONA UM HONEYPOT	31
3.3 TIPOS DE HONEYPOT	31
3.4 NÍVEIS DE HONEYPOT	32
3.5 APLICAÇÕES DE UM HONEYPOT	33
3.6 POR QUE UTILIZAR UM HONEYPOT?	34
3.7 VANTAGENS DA UTILIZAÇÃO DOS HONEYPOTS	34

SUMÁRIO

1 INTRODUÇÃO	11
1.1 OBJETIVOS	12
1.1.1 Objetivo geral	12
1.1.2 Objetivos específicos	12
1.2 MOTIVAÇÃO DO TRABALHO	12
1.3 ORGANIZAÇÃO DO TRABALHO	13
2 SEGURANÇA DA INFORMAÇÃO	14
2.1 PRINCIPAIS AMEAÇAS	14
2.2 ATACANTES	15
2.3 ATAQUES	16
2.3.1 Motivações de um ataque	17
2.3.2 Ataques quanto ao seu objetivo	18
2.3.3 Ataques quanto a sua origem	19
2.4 FIREWALL	19
2.4.1 Tipos de firewall	21
2.4.1.1 Firewalls de filtragem de pacotes	21
2.4.1.2 Firewalls servidores de proxy	21
2.4.2 Funcionalidades de um firewall	22
2.4.3 Arquitetura de firewalls	23
2.5 IDS	24
2.5.1 Histórico IDS	24
2.5.2. O que é um IDS?	25
2.5.3 Objetivos de um IDS	25
2.5.4 Tipos de IDS	25
2.5.4.1 IDS baseado em host (Host-Based Intrusion Detection System)	26
2.5.4.2. IDS baseado em rede (Network-Based Intrusion Detection System)	26
2.5.4.3 IDS híbrido (Hybrid Intrusion Detection System)	26
2.5.5 Eficiência e eficácia de um IDS	27
2.5.6 Sistema de prevenção de intrusão (IPS)	27
3 HONEYPOT	29
3.1 HISTÓRICO HONEYPOT	29
3.1.1 Honeypot no Brasil	30
3.2 COMO FUNCIONA UM HONEYPOT	31
3.3 TIPOS DE HONEYPOT	31
3.4 NÍVEIS DE HONEYPOT	32
3.5 APLICAÇÕES DE UM HONEYPOT	33
3.6 POR QUE UTILIZAR UM HONEYPOT?	34
3.7 VANTAGENS DA UTILIZAÇÃO DOS HONEYPOTS	34

3.8 DESVANTAGENS DA UTILIZAÇÃO DOS HONEYPOTS	35
3.9 RISCOS DA UTILIZAÇÃO DOS HONEYPOTS	35
3.10 LOCALIZAÇÃO DE UM HONEYPOT	36
3.11 ASPECTOS LEGAIS DE UM HONEYPOT	37
4 HONEYNETS	39
4.1 HISTÓRICO HONEYNET	39
4.2 COMO FUNCIONA UMA HONEYNET	39
4.3 EVOLUÇÃO DAS HONEYNETS	40
4.3.1 Primeira geração	40
4.3.2 Segunda geração	43
4.4 TIPOS DE HONEYNET	44
4.5 OBJETIVOS DE UMA HONEYNET	45
4.6 COMPONENTES DE UMA HONEYNET	45
4.7 RISCO EM TORNO DAS HONEYNETS	48
5 OUTROS COMPONENTES RELACIONADOS	50
6 CONCLUSÃO	52
REFERÊNCIAS BIBLIOGRAFICAS	53

1 INTRODUÇÃO

Uma rede de computadores hoje é essencial não só para instituições corporativas como para tantas outras instituições que precisam trocar uma grande quantidade de informações ou dados de forma rápida, eficiente e segura.

As redes normalmente não são montadas com o foco na segurança e sim para terem o máximo de eficiência e disponibilidade. Isso em princípio é muito bom para os empresários, pois qualquer pessoa pode montar uma rede em curto espaço de tempo e com baixo custo. Entretanto não se poderia prever que tantos criminosos e vândalos virtuais fossem explorar de forma tão deplorável a estrutura dessas redes. A segurança de redes se tornou um assunto crítico e dispendioso para as empresas, tendo que contar muitas vezes com programas computacionais, equipamentos e profissionais especialistas e experientes na área para se proteger.

A maioria das redes baseia-se na arquitetura cliente-servidor, na qual os usuários utilizam estações de trabalho para se conectarem aos servidores que compartilham informações é aí que residem os grandes problemas, pois a maioria dos incidentes em segurança são provenientes de dentro das redes corporativas.

Essas tentativas advém, geralmente, de usuários mal intencionados querendo obter acessos a serviços e informações negados a ele. Entretanto, o mesmo passa parte do seu tempo de produção buscando na internet, ferramentas para burlar sistemas de defesa, e com isso abrem “brechas” em seu computador para instalação de vírus, spywares, Cavalos-de-tróia, worms, keyloggers, back doors, dentre outros softwares maliciosos, que podem infectar toda a rede, abrindo outros canais de comunicação, danificando programas instalados, ou simplesmente tornando os computadores infectados zumbis, para posteriores ataques de negação de serviço (Denial of Service – DoS).

Os honeypots surgiram para ajudar em trabalhos e experiências na área de segurança, sendo isca para atacantes, capturando informações e informando em tempo real o que se passa

em nossa rede. Com isso, aprende-se muito mais sobre falhas de segurança, ferramentas de ataque, técnicas de ataques e conseqüentemente sobre os atacantes.

1.1 OBJETIVOS

1.1.1 Objetivo geral

Apresentar o que são e como funcionam os Honeypots e Honeynets.

1.1.2 Objetivos específicos

- Apresentar conceitos sobre segurança da informação, englobando principais ameaças, atacantes, ataques, firewall e sistemas de detecção de intrusão;
- Apresentar os honeypots a partir de seu histórico, como funciona, tipos, níveis, aplicações, porque utiliza-los, vantagens e desvantagens, riscos e arquitetura.
- Apresentar as honeynets a partir de seu histórico, como funcionam, evolução, tipos, objetivos, componentes e riscos.

1.2 MOTIVAÇÃO DO TRABALHO

A motivação do trabalho está diretamente ligada ao estudo de uma nova ferramenta para o auxílio na área da segurança da informação, donde poderemos obter mais dados para aplicações em firewall, sistemas de detecção de intrusão, bem como saber quem anda tentando burlar os sistemas de segurança.

1.3 ORGANIZAÇÃO DO TRABALHO

- 1 Capítulo: Introdução, objetivos (geral e específicos), motivação e organização do trabalho;
- 2 Capítulo: Conceitos de segurança da informação, principais ameaças, atacantes, ataques, motivações de um ataque, ataques quanto ao seu objetivo, ataques quanto a sua origem, firewall, tipos de firewall, firewalls de filtragem de pacotes, firewalls servidores de proxy, funcionalidades de um firewall, arquitetura de firewalls, IDS, histórico, O que é um IDS, Objetivos de um IDS, Tipos de IDS, IDS baseado em host, IDS baseado em rede, IDS híbrido, eficiência e eficácia de um IDS, sistema de prevenção de intrusão (IPS);
- 3 Capítulo: Honeypot, histórico, honeypot no Brasil, como funciona um honeypot, tipos de honeypot, níveis de honeypot, aplicações de um honeypot, por qu utilizar um honeypot?, vantagens, desvantagens e riscos da utilização dos honeypots, localização de um honeypot, aspectos legais de um honeypot.
- 4 Capítulo: Honeynets, histórico, como funciona uma honeynet, evolução das honeynets, primeira geração, segunda geração, tipos de honeynet, objetivos de uma honeynet, risco em torno das honeynets;
- 5 Capítulo: Outros componentes relacionados, honeytoken, honeyfarm e honeydummie;
- 6 Capítulo: Conclusão.

2.1 PRINCIPAIS AMEAÇAS

Pode-se classificar as ameaças em três categorias: ameaças físicas, internas e externas.

2 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é o sistema que possui aspectos básicos como confidencialidade, integridade e disponibilidade, e pode ser aplicada as mais diversas áreas do conhecimento técnico científico.

A segurança da informação vem se tornando uma real necessidade no dia-a-dia das organizações para proteger seus segredos de negócio ou suas estratégias comerciais, sendo considerada hoje fator de sobrevivência e competitividade para as corporações modernas. (1)

Atualmente, todas as empresa responsáveis armazenam suas informações em ambientes computacionais, para facilitar a realização de trabalhos dos seus colaboradores e serviços oferecidos pelas mesmas. Segundo (2), uma organização que deseja ser bem sucedida deve possuir um conjunto de regras e padrões sobre o deve ser feito para assegurar que as informações e serviços importantes para a empresa recebam a proteção conveniente. “A medida que as empresas tornam-se mais dependentes da informática, mais vulneráveis elas ficam à ação dos piratas informatizados.” (3)

Segundo (4) “segurança é, portanto, a proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulação não autorizada, de forma e reduzir a probabilidade e o impacto de incidentes de segurança”.

2.1 PRINCIPAIS AMEAÇAS

Pode-se classificar as ameaças em três categorias: ameaças físicas, internas e externas.

Ameaças Físicas: Podem ser causadas por alterações ambientais, ex: incêndios e inundações, falhas em outros sistemas, falhas elétricas, e até mesmo pela falta de manutenção dos equipamentos.

Ameaças Internas: Problemas relacionados com usuários (geralmente internos), que inevitavelmente podem colocar em risco a segurança do sistema (consciente ou inconscientemente). Os usuários podem ser uma ameaça utilizando inapropriadamente o sistema, divulgando ou vendendo intencionalmente informações sem autorização. As ameaças internas ainda englobam problemas com engenharia de software, ex: falha na produção e evolução do software e erros de configuração e dimensionamento de hardware e software.

Ameaças externas: Pessoas utilizando-se geralmente de softwares para exploração de sistemas computacionais, confeccionados ou não por elas, que acessam indevidamente informações do sistema, o que chamamos de atacantes.

2.2 ATACANTES

Indivíduos que beneficiando-se com a descoberta de falhas em sistemas operacionais, redes e serviços computacionais, para obter informações de forma ilegal, podendo a vir causar danos irreparáveis, geralmente para provar que pode fazê-lo (prazer pessoal), desafio (penetrar em sistemas altamente protegidos) ou para ser reconhecido pela comunidade cibernética, ganhando assim, status na mesma.

Carders: Roubam informações e fazem compras com cartão de crédito alheio ou gerado por softwares desenvolvidos para esta finalidade;

2.3.1 Motivação Hackers: Pessoas com facilidade de análise, assimilação, compreensão, e habilidades técnicas surpreendentes na área de computação, utilizando-se das mais diversas técnicas para obtenção de acesso a sistemas computacionais restritos, tendo por ideologia a observação e comportamento do sistema invadido; Com isso pode-se identificar inúmeros motivos para efetivação de um ataque a uma rede, dentre eles pode-se citar:

Crackers: Sua principal diferença para os hackers é a ideologia, geralmente quando obtém acesso um sistema computacional restrito, roubam e prejudicam os serviços e sistemas ativos, deixando por fim mensagens anárquicas;

Phreaking: Profundo conhecedor dos sistemas de telefonia fixa e móvel, utilizam-se de técnicas pouco conhecidas para beneficiar-se dos mesmos armazenados no computador (phishing scam);

Script Kiddies: Geralmente jovens frequentadores de salas de bate-papo entusiasmados com o poder da internet denominando-se hackers ou querendo ser reconhecidos na comunidade cibernética como um, utilizam-se de softwares desenvolvidos para explorar vulnerabilidades já existentes em determinado serviço (exploit).

2.3 ATAQUES

Segundo (5), Um ataque corresponde a um comprometimento em nível de sistema de segurança através de um ato inteligente ou deliberado, afetando serviços e violando a política de segurança de um sistema.

2.3.1 Motivações de um ataque

A vulnerabilidade pode ser causada por uma falha no sistema operacional, protocolo, serviços ou quaisquer outros componentes no sistema que permitem acesso ou intervenção de pessoas não autorizadas. Com isso pode-se identificar inúmeros motivos para efetivação de um ataque a uma rede, dentre eles pode-se citar:

Ganhos financeiros: O atacante invade o sistema para obter informações sigilosas vendendo-as posteriormente a quem interessar, podendo utilizá-la também para chantagear a vítima. Outro exemplo é a obtenção indevida de dados bancários, geralmente obtidos através de cavalos de tróia, dando assim acesso não só informações bancárias, como a muitas outras que venham a ser armazenadas no computador (phishing scam);

Vingança: Geralmente efetuada por funcionários da empresa insatisfeitos ou ex-funcionários aproveitando-se de senhas antigas e brechas de segurança conhecidas pelos próprios;

Aceitação na comunidade cibernética: Não importa muito se o atacante é novo ou velho na comunidade, os atacantes efetuam ou pelo menos tentam atacar, procurando obter sucesso para que seu nickname e ataque sejam assunto da mídia convencional, levando a comunidade hacker ao delírio e ganhando um status quo dentro dela;

Curiosidade: Muitos atacantes, “motivados” por sua ignorância (por não saberem o que estão fazendo e o que pode acontecer) ou meramente por um sentimento anárquico, geralmente utilizando-se de scripts, lançam ataques indiscriminados

2.3.1 Ataques na internet pela simples curiosidade do que poderá acontecer com seu alvo ou com ele mesmo;

Ataque Integral: Caracteriza-se por atividades que visam burlar, abusar ou

Idealismo: Com a ideologia que nada na grande rede pode ser restrito;

no ambiente computacional.

Aprendizado: Neste ponto pouco se enquadram, são geralmente gestores ou estudantes em busca de conhecimento, aplicáveis a pesquisa e soluções de segurança em instituições

Pode-se classificar o ataque, inicialmente quanto ao seu objetivo em ativo e passivo e também quanto à sua origem em interna e externa.

2.3.2 Ataques quanto ao seu objetivo

Ataque ativo: O objetivo é a desativação dos serviços críticos da rede, comprometendo e destruindo informações nos servidores, desperdiçando recursos, podendo até atingir fisicamente os recursos da rede. "Ataques ativos prejudicam diretamente o conteúdo do recurso atacado, modificando e eliminando informações ou gerando informações falsas".(4)

Ataque passivo: Conhecido como phishing scam ou simplesmente como scam, este ataque objetiva pela busca de informações, furtos de senhas, endereços de e-mail, espionagem digital, fraudes bancárias e lavagem de dinheiro. "Ataques passivos são aqueles que não interferem no conteúdo do recurso que foi atacado". (4)

2.3.3 Ataques quanto a sua origem

Ataque interno: Caracteriza-se por atividades que visam burlar, abusar ou destruir recursos computacionais aos quais se tem direito de acesso regularmente no ambiente computacional.

Ataque externo: Caracteriza-se por atividades nocivas ao funcionamento do domínio, partindo de usuários não autorizados ou ilegítimos do sistema.

Os ataques passivos, ativos, internos ou externos podem ser feitos por diversos e inúmeros tipos de pessoas, o que vem primeiramente em mente, devido inclusive a mídia televisiva são os hackers, mas dependendo de sua atuação e das conseqüências dos seus atos podem receber outras nomenclaturas como já apresentado, mas também não pode-se descartar os próprios funcionários, ex-funcionários e estagiários que atualmente são a maior fonte de ataques dentro das empresas. Uma outra possível fonte de ataque podem ser os consultores externos (por terem participado da implantação, desenvolvimento ou manutenção dos sistemas da organização), e dependendo do dado manipulado não pode-se descartar os concorrentes do setor e até o crime organizado (esses por interesse meramente financeiro).

2.4 FIREWALL

Segundo (6), "Firewall é um ponto entre duas ou mais redes, que podem ser um componente ou um conjunto de componentes, por onde passa todo o tráfego, permitindo que o controle, a autenticação e os registros de todo o tráfego sejam realizados.", (7) define como: "controles de acesso baseados no cabeçalho e/ou nos conteúdos dos pacotes e podem combinar quatro técnicas para garantir a segurança".

2.4.1 Tipos de Firewall

Controle dos serviços: Determina os tipos de serviços da rede que podem ser acessados. O fluxo de serviços potencialmente vulneráveis, por exemplo, pode ser barrado pelo firewall.

Classificação dos firewalls de acordo com o que desempenham e as duas abordagens principais: os firewalls de filtragem de pacotes e servidores de proxy.

Controle de direção: Determina a direção pela qual uma determinada solicitação de serviço pode ser iniciada.

Controle dos usuários: Controla o acesso a determinados serviços de acordo com o usuário que está tentando acessá-lo.

Controle de comportamento: Controla o modo como determinados serviços podem ser utilizados.

O firewall pode e deve ser utilizado para evitar tráfego de dados não autorizado entre domínios, por não possuir capacidade de analisar toda a extensão do protocolo, geralmente fica restrito ao nível 4 da camada OSI, passando a ser um ponto de controle para a administração de segurança, auditoria e monitoração. Logo, torna-se elemento estratégico tanto na proteção da rede quanto na análise do tráfego.

Podem ser implementados para oferecer proteção contra ataques a protocolos ou aplicações individuais e detecção de malwares, mas sua utilização não é a garantia de segurança ou proteção contra ataques desconhecidos, sua instalação e configuração dependem do tamanho da rede, complexidade das regras e do grau de segurança almejado.

Sendo o firewall a linha de frente no quesito segurança, torna-se fundamental para tentar bloquear os acessos indevidos ao sistema, lembrando que os firewalls não constituem uma solução única para garantir a segurança, é apenas um dos diversos dispositivos necessários para a proteção da rede.

2.4.1 Tipos de firewall

Classificamos os firewalls de acordo com o que desempenham e em duas abordagens principais: os firewalls de filtragem de pacotes e servidores de proxy.

2.4.1.1 Firewalls de filtragem de pacotes

Os firewalls de filtragem de pacotes ainda podem ser divididos em:

Filtro de pacotes estáticos: realizam o roteamento seletivo de pacotes por meio da análise de seu cabeçalho e de acordo com regras de filtragem pré-definidas, pode filtrar os pacotes com base em seus endereços de origem e destino, portas TCP ou UDP de origem e destino, número total de bits do cabeçalho, tipo de protocolo e determinados flags;

Filtro de pacotes dinâmicos: verifica somente o primeiro pacote de uma conexão de acordo com as regras de filtragem e a partir daí passa a utilizar-se das informações da tabela de estados para permitir ou não a passagem dos demais pacotes.

O grande problema desse tipo de firewall, é que as regras aplicadas podem ser muito complexas e causar perda de desempenho da rede ou não serem eficazes o suficiente.

2.4.1.2 Firewalls servidores de proxy

Possuem capacidade de executar amplas varreduras de segurança e validação nos pacotes processados, registrando todo o tráfego que circula entre redes, impedindo que o tráfego transite livremente entre redes.

Segundo (6), os firewalls híbridos misturam elementos dessas duas tecnologias, de modo a garantir alto grau de segurança dos proxies e o bom desempenho do filtro de pacotes.

2.4.2 Funcionalidades de um firewall

Segundo (6), o firewall possui 7 funcionalidade 4 delas primarias (filtros, proxies, bastions hosts e zonas desmilitarizadas) e as 3 restantes (NAT – Network Address Translation, VPN – Rede Privada Virtual e Autenticação/certificação) foram inseridas no contexto devido a evolução natural e a necessidade de segurança.

Filtros: analisa individualmente os pacotes à medida que estes são transmitidos da camada de enlace “2” para a camada de rede “3” do modelo OSI, levando em consideração as regras de filtragem e estados de conexões.

Proxies: sistemas que atuam como um gateway entre duas redes, permitindo as requisições dos usuários internos e as respostas dessas requisições de acordo com a política de segurança.

Bastions hosts: são equipamentos configurados para realizarem papel crítico na segurança da rede interna, deve possuir uma estrutura simples, de forma que seja fácil de garantir a segurança. Segundo (8), define que "bastions hosts são áreas críticas de defesa, geralmente apresentando paredes fortes para desencorajar os atacantes"

Zona desmilitarizada: DMZ (DeMilitarized Zone), ou perimeter network, é o nome dado a uma topologia de rede situada entre uma rede protegida (interna) e

uma externa, considerada por muitos especialistas um ótimo esquema de segurança.

NAT - Network address translations: criado com o objetivo de suportar o crescimento das redes de computadores na Internet e a escassez de endereços IP válidos. O NAT oferece um método de criação de redes privadas, com endereços não roteáveis de acordo com a [RFC1918], que poderiam passar por um sistema que faria a tradução para um endereço válido (real) e roteável, capaz de ser reconhecido em toda a Internet.

VPN – Virtual Private Network: é uma conexão onde o acesso e a troca de dados somente é permitido a usuários e/ou redes que façam parte de uma mesma comunidade de interesse.

Autenticação/Certificação: Podem ser baseadas em endereços IP, senhas, certificados digitais, tokens, smartcards ou biometria.

2.4.3 Arquitetura de firewalls

Apresento aqui as arquiteturas de firewalls mais comuns, entretanto há muitas outras variações que podem ser usadas.

Dual Home-Host: Pode como um roteador entre a rede externa e a interna. Uma observação importante é que sistemas dentro do firewall podem se comunicar com o host dual-homed assim como sistemas fora do firewall, mas estes sistemas não podem se comunicar entre si. Um host dual-homed pode fornecer apenas serviços através de servidores proxy, ou ainda permitir que usuários conectem-se diretamente a si. (9)

Screened Host: Fornece serviços a partir de um bastion host que é conectado apenas a rede interna, usando um roteador para separá-la da Internet, chamado screening router. Nesta arquitetura, a segurança principal é feita por packet filtering. (9)

Screened Subnet: Considerada uma das mais seguras arquiteturas de firewalls, essa arquitetura adiciona uma camada extra de segurança através da perimeter network, que isola a rede interna da Internet. Nela a dois screening router. Um entre a rede DMZ e a rede interna, e outro entre a rede DMZ e a rede externa, e o bastion host fica localizado dentro da DMZ e não mais na rede interna.

2.5 IDS

Segundo (10), IDS são: “Softwares ou hardwares que automatizam o processo de monitorar os eventos que ocorrem em um sistema computadorizado ou em uma rede, analisando os para sinais de problemas de segurança”.

2.5.1 Histórico IDS

Segundo (11), tudo começou na década de 80, James Anderson introduziu o conceito de detecção de intrusão, onde ele definia uma tentativa de intrusão ao ameaça como sendo uma possibilidade em potencial de um acesso deliberadamente não autorizado a informações, manipulação de informações deixando-as inacessíveis.

Depois de um alavancamento nas pesquisas realizado pelo governo americano a Dr^a Dorothy Denning propôs o primeiro modelo de IDS, com o objetivo de permitir respostas em

tempo real a invasões, certo tempo depois propôs também um IDS que possuísse a capacidade de detectar intrusão com um padrão prévio definido, propondo duas técnicas de detecção as baseadas em regras previamente definidas e a baseada em métodos estatísticos.

Mas em 1990 Davis's Todd introduz o conceito de IDS baseado em rede o NIDS (Network Intrusion Detect System).

2.5.2.O que é um IDS?

Segundo (10), a detecção de intrusão é o processo de monitorar os eventos que ocorrem em um sistema computadorizado ou em uma rede e que analisam os sinais destas intrusões com a finalidade de comprometer o confidencialidade, integridade, disponibilidade, ou para burlar os mecanismos da segurança. As intrusões ou tentativas, são causados pelos atacantes que alcançam os sistemas via internet, usuários autorizados dos sistemas que tentam ganhar os privilégios adicionais, e os usuários autorizados que empregam mal os privilégios dados a eles. Os sistemas da detecção do Intrusion (IDSs) são os produtos do software ou da ferragem que automatizam estes monitoração e processo da análise.

2.5.3 Objetivos de um IDS

Segundo (6), “Um sistema de detecção de intrusão (Intrusion Detection Sistem – IDS), que tem como objetivo detectar atividades suspeitas, impróprias, incorretas ou anômalas”, ou mesmo (12), “O objetivo final de qualquer IDS é capturar os infratores na ação antes de realmente danificarem seus recursos.”

2.5.4 Tipos de IDS

Segundo (6) existem dois tipos primários de IDS, o baseado em host (Host_based Intrusión Detection System – HIDS) e o baseado em rede (Network-Based Intrusión Detection

System – NIDS), O IDS Híbrido (Hybrid IDS) surgiu com a evolução da tecnologia e das necessidades, aproveita as melhores características do HIDS e do NIDS.

2.5.4.1 IDS baseado em host (Host-Based Intrusion Detection System)

Segundo (13), O IDS host-based monitora as conexões de entrada no host e tenta determinar se alguma destas conexões pode ser uma ameaça. Monitora também arquivos, file systems, logs, ou outras partes do host em particular, que podem ter atividades suspeitas representando uma tentativa de intrusão ou até mesmo uma invasão bem sucedida. Instalado em um host que será alertado sobre ataques ocorridos contra ele mesmo. Avaliando a segurança deste host como base em arquivos de logs de Sistema Operacional, logs de acesso e logs de aplicação, tendo grande importância, pois fornece segurança a tipos de ataques que o firewall e um IDS network-based não detectam.

2.5.4.2. IDS baseado em rede (Network-Based Intrusion Detection System)

Geralmente com a interface de rede em modo promiscuo monitora o tráfego de rede, realizando a captura e análise dos conteúdos e cabeçalhos dos pacotes, comparando-os com assinaturas ou padrões conhecidos. Uma característica importante do NIDS é sua capacidade de detecção de ataques em tempo real.

2.5.4.3 IDS híbrido (Hybrid Intrusion Detection System)

A junção do que é de melhor no HIDS e NIDS, resolvendo a problemática de trabalhar só com um ou com outro, oferecendo uma capacidade de detecção superior se só estivesse utilizando-se de um tipo. Trabalhando como o NIDS, coletando o tráfego da rede, processando os pacotes e detectando e respondendo a ataques, processando somente os pacotes endereçados

ao próprio sistema, surgindo o problema de escalabilidade já que deve ser instalado em cada equipamento da rede.

2.5.5 Eficiência e eficácia de um IDS

Para medir a eficácia e eficiência de um IDS, podem ser utilizados os seguintes critérios (14):

Falso Positivo: quando uma ocorrência é classificada como intrusão, mas caracteriza apenas uma situação diferente do padrão, sem constituir violação de segurança. Representa um custo desnecessário pela ineficiência da solução, e tende a comprometer a confiança da ferramenta.

Falso Negativo: quando uma atividade maliciosa não é percebida pelo IDS, sendo classificada como ocorrência normal. Configura ineficácia da solução, pois um ataque deixa de ser identificado.

Subversão: quando o IDS é enganado pelo invasor, sendo forçosamente levado a não reconhecer uma violação de segurança, como acontece na inserção e na evasão. Difere do falso negativo porque, quando este ocorre, não houve tentativa de burlar o sistema – o IDS simplesmente não conseguiu perceber o ataque –, enquanto que na subversão o atacante nota a presença do IDS e faz com que ele não registre a ocorrência.

2.5.6 Sistema de prevenção de intrusão (IPS)

Os sistemas de prevenção de intrusão estão despontando na área de segurança os IPS (Intrusion Prevention System) surgiu como muitas outras tecnologias adaptando-se as

necessidades de utilização dos analistas de segurança, combinando a capacidade de inspeção de pacotes com as características de filtragens dos firewalls.

Segundo (15), a principal diferença entre IDS e IPS é que enquanto o IDS só age após a ocorrência de intrusão, o IPS foi desenvolvido como medida de prevenção, eles agem antes que os possíveis ataques tenham sucesso, ou pelo menos limitam consequências caso a intrusão realmente aconteça.

HoneyPot pode ser definido como sendo: "recursos de rede cuja função é de ser atacado e comprometido (invadido). Significa dizer que um HoneyPot poderá ser testado, atacado e invadido. Os honeypots não fazem nenhum tipo de prevenção, os mesmos fornecem informações adicionais de valor inestimável".

Pode-se definir também como: "sistema que possui falhas de segurança, mas os ataques, colocados de maneira proposital, a fim de que seja invadido e o fruto dessa invasão possa ser estudado".

Apesar de que muitos especialistas em segurança e administradores de redes pensam, HoneyPot não é uma ferramenta de segurança nem muito menos um IDS (intrusion detection system) é sim, uma ferramenta de estudos em segurança, onde a partir de uma análise profunda de ataques e das ferramentas utilizadas pelo mesmo, poderemos utilizar-nos de artifícios para construção de ferramentas de defesa para um determinado sistema na rede.

2.1 HISTÓRICO HONEYPOT

Tudo começou quando o astrônomo e especialista em informática Clifford Stoll em 1983 decidiu publicar suas experiências com monitoramento de ataques na Internet relatando ataques sofridos pelo Lawrence Berkeley Laboratory (LBL). Stoll relata que nesta ocasião ao invés de bloquearem os recursos, ele e os especialistas do laboratório resolveram permitir acesso ao servidor enquanto monitoravam suas atividades, a fim de descobrir sua origem. Todo esse trabalho levou cerca de dez meses e ao final revelou não só a origem do ataque, mas também objetivos e motivos do atacante bem como as redes que estava interessado. Esta experiência

3 HONEYPOT

Do Inglês Honey (mel), pot (pote), juntando Honeypot ou no português pote de mel.

Procurando a fundo encontraremos definições clássicas como a de Lans Spitzner (16) que define honeypots como sendo: “recursos de rede cuja função é de ser atacado e comprometido (invadido). Significa dizer que um Honeypot poderá ser testado, atacado e invadido. Os honeypots não fazem nenhum tipo de prevenção, os mesmos fornecem informações adicionais de valor inestimável”.

Pode-se definir também como: “sistema que possui falhas de segurança, reais ou virtuais, colocadas de maneira proposital, a fim de que seja invadido e o fruto dessa invasão possa ser estudado”.

Ao contrário que muitos especialistas em segurança e administradores de redes pensam, honeypot não é uma ferramenta de segurança nem muito menos um IDS (intrusion detection system) é sim, uma ferramenta de estudos em segurança, onde a partir de uma análise profunda do atacante e das ferramentas utilizadas pelo mesmo, poderemos utilizar-se de artifícios para construção de ferramentas de defesa para um determinado sistema ou rede.

3.1 HISTÓRICO HONEYPOT

Tudo começou quando o astrônomo e especialista em informática Clifford Stoll em 1988 decidiu publicar suas experiências com monitoramento de ataques na internet relatando ataques sofridos pelo Lawrence Berkeley Laboratory (LBL). Stoll relata que nesta invasão ao invés de bloquearem os recursos, ele e os especialistas do laboratório resolveram permitir acesso ao invasor enquanto monitoravam suas atividades, a fim de descobrir sua origem. Todo este trabalho levou cerca de dez meses e ao final revelou não só a origem do ataque, mas também objetivos e motivos do atacante bem como as redes que estava interessado. Esta experiência

cuminou em 1989 em seu segundo livro: "The Cuckoo's Egg: Tracing a Spy through the Maze of Computer Espionage".

Em 1992, o especialista Bill Cheswick publicou o artigo "An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied", explicando e descrevendo os resultados do acompanhamento de uma invasão ocorrida em 7 de janeiro de 1991 no Laboratório Bell AT&T, projetado especialmente para ser invadido e comprometido. Este monitoramento durou meses e contou com inúmeras participações inclusive de Steven M. Bellovin quem teve uma enorme contribuição com o projeto desenvolvendo várias ferramentas para capturar as ações do invasor.

"Em 1997, Fred Cohen desenvolveu o Deception ToolKit (DTK), composto por um conjunto de scripts em Perl e C" (11) "é primeira ferramenta open source com o objetivo principal de enganar Hackers, isto se consegue com emulação de diversos serviços, vulnerabilidades e coleta de informações sobre os ataques sofridos" (17). Nesta mesma época surgiu o termo Honeypot como definição para um recurso de segurança criado especificamente para ser sondado, atacado e comprometido e para registrar essas atividades (16).

Em 1998, a Cybercop começa a comercializar o Sting, primeiro honeypot comercial que curiosamente não foi escrito para ambiente Unix e sim Windows NT, com uma série de recursos ele simulava uma rede completa, emitia respostas falsas e simulava diversos sistemas operacionais.

3.1.1 Honeypot no Brasil

No Brasil existe o projeto HoneynetBR (www.honeynet.org.br), criado e mantido em parceria por especialistas do Instituto Nacional de Pesquisas Espaciais (INPE) e do grupo brasileiro de resposta a incidentes de segurança (NBSO). O projeto utiliza honeypots de alta interação com sistemas reais, porém com algumas modificações que permitem a captura de todos os dados, inclusive os criptografados. De certo modo, como descrito na literatura, a própria honeynet pode ser considerada como um único honeypot composto por diversos

sistemas, porém o projeto brasileiro refere-se a cada sistema individual dentro da HoneyNet como um honeypot individual (17).

O projeto brasileiro iniciou-se com um Hub e cinco máquinas, sendo uma delas para o gerenciamento e as demais para compor a rede da HoneyNet. Os sistemas operacionais utilizados foram o Linux e o OpenBSD, e todos os softwares open source.

Alguns meses após seu lançamento, o projeto tornou-se membro da HoneyNet Research Alliance (<http://www.honeynet.org>), que reúne diversos grupos do mundo, com o objetivo de desenvolver a tecnologia de honeynets.

3.2 COMO FUNCIONA UM HONEYPOT

Funciona basicamente quando um atacante faz uma requisição de serviço seja ele web, ftp, telnet ou mesmo ssh a uma determinada máquina, esta máquina que emula o serviço lhe retorna com mensagens “falsas” a requisição e com isso captura os dados do atacante.

3.3 TIPOS DE HONEYPOT

Martin Roesch, criador do Snort e autoridade na área de “forensics”, classifica em dois tipos: honeypots de pesquisa, utilizado em universidades e órgãos governamentais inclusive militares, e os honeypots de produção geralmente utilizado por organizações comerciais.

Honeypots de pesquisa: ferramentas de pesquisa em segurança utilizadas na captura de ações dos atacantes, conseqüentemente das ferramentas utilizadas e vulnerabilidades exploradas no sistema. Eles têm um grau alto de comprometimento e trabalham em redes externas ou sem ligação com a rede principal.

Esses resultados são de valor inestimável ao profissional de segurança pois eles podem traçar um perfil do atacante e responder à algumas perguntas como: O que foi explorado? Por que? Como? Quais ferramentas foram utilizadas? Quais as conversas mantidas com outros invasores?.

HONEYPOT – SEGUNDO NÍVEL DE INTERAÇÃO

HoneyPot – Nível de interação	Baixo	Médio	Alto
Sistema Operacional	Baixo	Baixo	Alto
Risco	Baixo	Baixo	Alto
Infraestrutura	Baixo	Baixo	Alto
Tecnologias de rede	Baixo	Baixo	Alto
Conhecimento para administração/gestão	Baixo	Baixo	Elevado
Conhecimento para desenvolvimento	Baixo	Elevado	Elevado
	Baixo	Baixo	Muito elevado

3.4 NÍVEIS DE HONEYPOT

Quanto aos níveis de Honeypots encontraremos três, os de baixa, média e alta interação.

1. APLICAÇÕES DE UM HONEYPOT

Honeypots de baixa interação (Low-interaction Honeypots): Simples e de fácil gerenciamento, emula serviços, sistemas operacionais e respostas falsas aos atacantes, por serem relativamente seguros, pois não permitem que o atacante interaja com o sistema, são apropriados para redes de produção e recomendados para a complementação dos sistemas de detecção de intrusão (SDI).

Honeypots de média interação: “Indicados para honeynets de pesquisa é um pouco mais difícil, pois exige a utilização e configuração de scripts que emulem os serviços desejados” (18), simulando detalhadamente um ambiente falso, criando para o atacante a ilusão do domínio da máquina.

Honeypots de alta interação (High-interaction Honeypots): Perigoso, difíceis de administrar, manter e principalmente requer uma estrutura de rede segura, usa serviços legítimos (mas comprometidos) como isca, se o atacante for experiente

pode assumir o controle total da máquina, por isso requer cuidados especiais para que o mesmo não seja ponte para novos ataques.

HONEYPOT – SEGUNDO NÍVEL DE INTERAÇÃO

Honeypot – Nível de interação	Baixo	Médio	Alto
Sistema Operacional “Real”	Não	Não	Sim
Risco	Baixo	Médio	Elevado
Informações	Ligações	Pedidos	Completa
Tentativas de Invasão	Não	Não	Sim
Conhecimento para administração/gestão	Baixo	Baixo	Elevado
Conhecimento para desenvolvimento	Baixo	Elevado	Elevado
Tempo de manutenção	Baixo	Baixo	Muito elevado

3.5 APLICAÇÕES DE UM HONEYPOT

Tomando-se por base que um honeypot é uma ferramenta para estudos em segurança, a sua aplicação depende do tipo de resultado que se quer alcançar.

Os honeypots de baixa interação oferecem baixo risco de comprometimento e são indicados para redes de produção, quando não há pessoal e/ou hardware disponível para manter uma honeynet, ou quando o risco de um honeypot de alta interatividade não é aceitável. Dependendo de sua localização na rede podem detectar ataques internos; identificar intenções, varreduras e ataques automatizados; detectar máquinas mal configuradas ou comprometidas e coletar códigos maliciosos (malware) bem como assinatura de ataques.

honeypots de alta interatividade são indicados para redes de pesquisa, introduzem um risco a mais para instituição, são justificáveis quando o objetivo é estudar o comportamento dos atacantes, motivações, além de analisar detalhadamente as ferramentas utilizadas e vulnerabilidades exploradas. O uso de honeypots de alta interatividade demanda tempo, pessoal mais qualificado e técnicas de contenção mais eficientes.

COMPARAÇÃO ENTRE HONEYPOTS

Características	Honeypot de baixa interatividade	Honeypot de alta interatividade/Honeynet
Instalação	Fácil	Mais difícil
Manutenção	Fácil	Trabalhosa
Risco de comprometimento	Baixo	Alto
Obtenção de informações	Limitada	extensiva
Necessidade de mecanismos de contenção	Não	Sim
Atacante tem acesso ao S.O. real	Não (em teoria)	Sim
Aplicações e serviços oferecidos	Emulados	reais
Atacante pode comprometer o honeypot	Não (em teoria)	sim

Tabela retirada de: <http://www.cert.br/docs/whitepapers/honeypots-honeynets/>

3.6 POR QUE UTILIZAR UM HONEYPOT?

Atualmente, a organização de grupos de hackers faz com que as ferramentas, principalmente as novas, não sejam encontradas. Ao mesmo tempo, novas classes de ataques encontram-se em constante evolução, o que faz com que o aprendizado dessas técnicas inovadoras seja cada vez mais importante para uma defesa adequada.(6)

Enquanto os hackers basta encontrar apenas um ponto de ataque, os profissionais de segurança devem defender todo o perímetro, contra estes ataques e contra riscos futuros.

3.7 VANTAGENS DA UTILIZAÇÃO DOS HONEYPOTS

- Exigência de recursos mínimos para instalação, implantação e manipulação;
- Diferente de outras tecnologias de segurança, o honeypot captura tráfego criptografado;

- Coletam dados só quando há interação, diferente do IDS que gera um volume enorme de alertas;
- Evitam o problema do falso positivo, pois todas as atividades, por default, serão não autorizadas, permitindo assim que o administrador elimine os alertas falsos;
- Diferente da tecnologia IDS (que não detectam atividades desconhecidas) o honeypot identifica novas ferramentas, ataques ou comportamentos estranhos na rede, não apresentando o problema de falsos negativos;
- Como ele não é um sistema que faz parte da produção, pode ser retirado da rede a qualquer momento para análise dos dados, ou por motivo de ter sido comprometido, e ser recolocado sem que haja prejuízo para os sistemas de produção.(19)

3.8 DESVANTAGENS DA UTILIZAÇÃO DOS HONEYPOTS

- Atrai atacante para a rede monitorada;
- Visão relativamente limitada, pois só capta o que cruza o seu caminho;
- Sem tráfego, informações, estudo, resulta trabalho em vão.

3.9 RISCOS DA UTILIZAÇÃO DOS HONEYPOTS

O resultado de uma implementação bem sucedida de um honeypot representa uma melhoria na identificação, qualidade nos alarmes de invasão, aprendizado de novas técnicas, e conhecimento de novas ferramentas utilizadas pelos atacantes, mas caso se perca o controle do honeypot e da situação, esta máquina antes utilizada para estudos e monitoração do tráfego de rede pode virar ponte para novos ataques a outros sistemas, bem como fonte para proliferação de vírus, bots, worms e malwares.

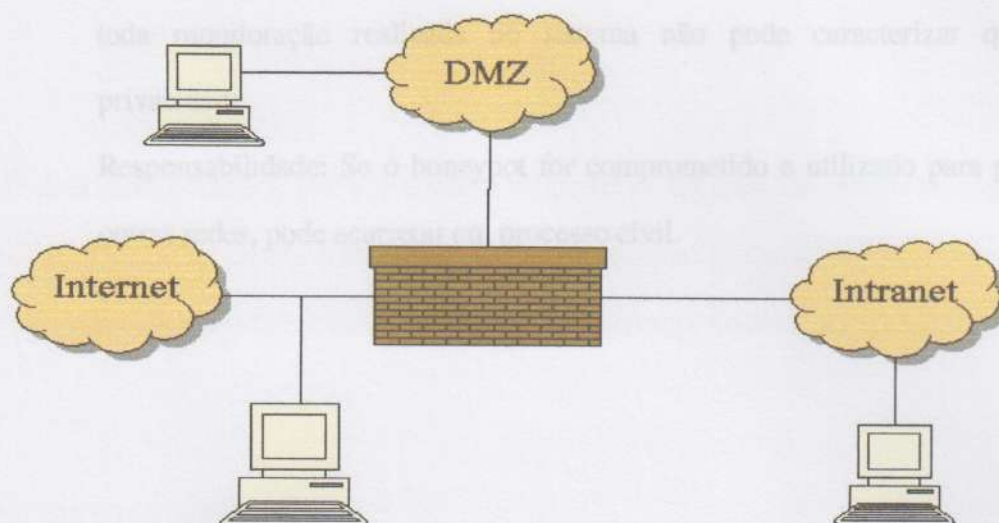
3.10 LOCALIZAÇÃO DE UM HONEYPOT

A localização de um honeypot deve levar em consideração a política de segurança e o que o administrador de rede quer analisar, por isso, deve-se pensar estrategicamente em sua localização.

DMZ (DeMilitarized Zone): Preferida pelos profissionais de segurança como o melhor local para se posicionar o honeypot, providenciando uma segurança adicional e utilizando o firewall para controlar o tráfego de entrada / saída e isolando o honeypot da rede de produção.

Em frente ao firewall (internet): O risco de ter um sistema comprometido atrás do firewall é eliminado, ele só irá atrair um tráfego enorme proveniente de portscans (sniffing de portas) ou padrões de ataques, sua principal vantagem é de não ter a necessidade de controlar regras do firewall e alertas provenientes do IDS e sua principal desvantagem é a dificuldade de localizar ataques de dentro da rede interna, especialmente se a firewall limitar o tráfego outbound, limitando, portanto o tráfego para o honeypot.

Atrás do firewall (intranet): Normalmente implementado para descoberta de atacantes internos ou detectar alguma configuração vulnerável do firewall, “aumenta consideravelmente a proteção do sistema, pois algumas regras específicas devem ser adicionadas ao firewall e modificações devem ser feitas nas assinaturas do sistema de detecção de intrusão, para que não ocorram alertas desnecessários toda vez que o mesmo for consultado por intermédio de varredores de portas e por meio de pacotes icmp.” (11) uma de suas desvantagens é que se for atacado e comprometido, o atacante terá acesso a toda rede, sem bloqueio do firewall (caso não tenha firewalls adicionais na rede).



3.11 ASPECTOS LEGAIS DE UM HONEYPOT

Quando tratamos dos aspectos legais de um honeypot, devemos 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”.(20)

Esta armadilha deve ser utilizada só para defesa, ela por si só não deve induzir a atacante a fazer o que ele não quer, tem que ser instintivo, o atacante tem que por si só explorar falhas e descobrir maneiras de comprometer o honeypot. Normalmente estas armadilhas não são utilizadas para incriminar o atacante, e sim, para aprender novas técnicas. E descobrir novas ferramentas.

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 em processo civil.

4.1 HISTÓRICO HONEYNET

Em 1999, um grupo de pesquisadores e especialistas em segurança liderados por Lance Spitznagel, lançam o HoneyNet Project, uma rede especificamente projetada para ser comprometida, tendo como objetivo revelar ferramentas, técnicas e motivações dos hackers, bem como desenvolver ferramentas contra esses ataques.

Em Janeiro de 2002 foi formada a HoneyNet Research Alliance que hoje inclui mais de dez organizações no Brasil, Grécia, Índia, México, Irlanda e Estados Unidos.

4.2 COMO FUNCIONA UMA HONEYNET

A honeynet é uma rede onde são colocados sistemas de produção, os chamados honeypots. Eles são os alvos para os invasores. Nesta rede são instalados sistemas de monitoração configurados de forma a evitar que os invasores sintam que estão sendo monitorados, porém invasores mais experientes poderão notar e tentar inutilizar os sensores ou mesmo, ainda não existe ainda um sistema que seja totalmente seguro e imune a detecção. Alguns pontos a observar (21):

4 HONEYNETS

É uma rede guardada por um sistema de proteção no qual são contidos, capturados e controlados os dados recebidos e enviados. Em seguida, essas informações são analisadas para adquirir o conhecimento sobre táticas, ferramentas e motivações dos atacantes.(21)

4.1 HISTÓRICO HONEYNET

Em 1999, um grupo de pesquisadores e especialistas em segurança liderados por Lance Spitzner, lançam o Honeynet Project, uma rede especificamente projetada para ser comprometida, tendo como objetivo revelar ferramentas, táticas e motivações dos hackers, bem como desenvolver ferramentas contra esses ataques.

Em Janeiro de 2002 foi formada a Honeynet Research Alliance que hoje inclui mais de dez organizações no Brasil, Grécia, Índia, México, Irlanda e Estados Unidos.

4.2 COMO FUNCIONA UMA HONEYNET

A honeynet é uma rede onde são colocados sistemas de produção, os chamados honeypots. Eles serão os alvos para os invasores. Nesta rede serão instalados sistemas de monitoração configurados de forma a evitar que os invasores sintam que estão sendo monitorados, porém invasores mais experientes poderão notar e tentar inibir os sensores ou irem embora, afinal não existe ainda um sistema que seja totalmente seguro e imune a detecção. Alguns pontos a observar (21):

- Normalmente não há nenhum tráfego dentro honeynet, deste modo qualquer tráfego será considerado suspeito e deve ser registrado;
- Quando um honeypot dentro da honeynet estiver comprometido, este deve ser imediatamente bloqueado para que ataques a outras redes não se originem dali;
- O controle de dados se dá neste ponto através da restrição do fluxo de dados recebidos e enviados da honeynet.
- A automação deste processo deve ser feita sem que os intrusos suspeitem disto.
- Ao realizar a captura dos dados relevantes aos eventos de segurança, estes devem ser armazenados de forma segura.

4.3 EVOLUÇÃO DAS HONEYNETS

Existem dois tipos de honeynets que podem ser desenvolvidos em uma rede: Primeira ou Segunda Geração. O tipo a ser usado depende de vários fatores, tais como disponibilidades dos recursos, tipos de ataque e invasores que se deseja detectar e efetivamente da experiência metodológica que se possui sobre o assunto.(22)

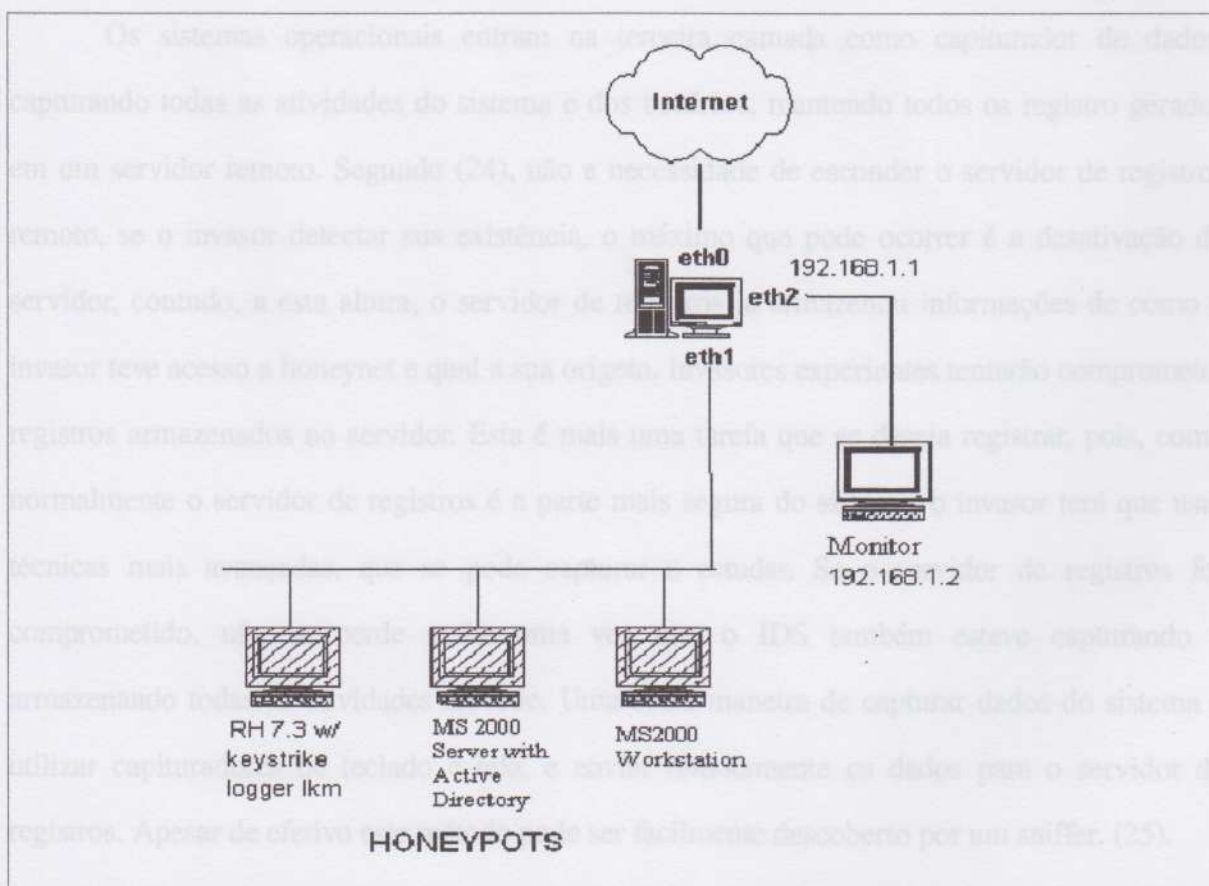
4.3.1 Primeira geração

A Primeira Geração implementa o Controle e Captura de Dados de maneira simples, e efetiva, mas não será tão efetiva como a segunda, devido a sua simplicidade e à quantidade de testes efetuada durante os últimos anos. Recomenda-se aos iniciantes nesta tecnologia a iniciarem sua implementação por esta geração.

Temos um firewall, de camada três, separando a rede em três subredes distintas: uma atendendo a rede administrativa, uma atendendo a própria honeynet e na outra ponta a Internet. Qualquer pacote que entrar ou sair da honeynet terá que passar tanto pelo firewall quanto pelo roteador. Nesta geração de honeynet ele se torna à ferramenta primária de controle das conexões

de entrada e saída. Deve-se configurar o firewall para que ele permita todas as conexões de entrada na honeynet e as de saída da honeynet até um limite estipulado, dando ao invasor a flexibilidade necessária para fazer o que quer que ele queira sem permitir o abuso. Não existe um número exato de conexões externas estipuladas. O Honeynet Project recomenda que de 5 a 10 conexões por hora são suficientes para um bom trabalho, porém tudo vai depender das funcionalidades que se deseja explorar. É instalado um roteador entre o firewall e a honeynet. Há dois motivos para isto. A primeira é que o roteador esconde o firewall, criando uma situação mais realista quando um honeypot for comprometido e seus invasores encontrarem um roteador entre eles e a rede externa. A segunda razão é pelo posicionamento do roteador funcionando como um segundo ponto de controle de acesso, ajudando o firewall a evitar ataques oriundos da honeynet, evitando spoofs, DOS ou ataques baseados em ICMP, permitindo que somente os pacotes com endereçamento IP de origem igual ao da honeynet saiam. Nenhuma honeynet deve depender de uma única camada para garantir o controle de dados. (23).

(23)



Implementado o controle de dados acima, agora é a vez da captura. O mesmo firewall usado anteriormente pode ser usado agora para capturar dados. Ele deve manter um registro sobre todas as conexões iniciadas e terminadas na honeynet, uma vez que, todas estas conexões são suspeitas. Estes registros serão usados posteriormente para descobrir novos padrões de ataque (assinaturas). Neste modelo ainda se instalariam dois IDS, um em eth2 e outro em eth1, que teriam dois propósitos: o primeiro é capturar toda a atividade da rede, o segundo é emitir alerta quando seus sensores detectarem qualquer atividade suspeita. É importante salientar que os sistemas IDS baseiam-se em assinaturas armazenadas em bases de dados, ou seja, quando um pacote da rede coincide com uma das assinaturas ele é considerado suspeito e é gerado um log sobre este pacote, podendo ou não o IDS tomar uma atitude adicional como enviar informações para que um firewall bloqueie o pacote que tenha a mesma origem daquele suspeito. Os sensores do IDS disponibilizaram informação detalhada sobre uma conexão específica. Uma das ferramentas mais usadas de IDS em honeynets é o SNORT, disponível em <http://www.snort.org>.

(23)

Os sistemas operacionais entram na terceira camada como capturador de dados, capturando todas as atividades do sistema e dos usuários, mantendo todos os registro gerados em um servidor remoto. Segundo (24), não a necessidade de esconder o servidor de registros remoto, se o invasor detectar sua existência, o máximo que pode ocorrer é a desativação do servidor, contudo, a esta altura, o servidor de registros já armazenou informações de como o invasor teve acesso a honeynet e qual a sua origem. Invasores experientes tentarão comprometer registros armazenados no servidor. Esta é mais uma tarefa que se deseja registrar, pois, como normalmente o servidor de registros é a parte mais segura do sistema, o invasor terá que usar técnicas mais avançadas, que se pode capturar e estudar. Se o servidor de registros for comprometido, não se perde nada, uma vez que o IDS também esteve capturando e armazenando todas as atividades na rede. Uma outra maneira de capturar dados do sistema é utilizar capturadores de teclado e tela, e enviar remotamente os dados para o servidor de registros. Apesar de efetivo este método pode ser facilmente descoberto por um sniffer. (25).

4.3.2 Segunda geração

A segunda geração de honeynets surgiu a partir da experiência adquirida pela primeira, que era despreocupada com a segurança das máquinas ao redor da honeynet. Na segunda geração houve uma preocupação maior com o isolamento do ambiente de sistemas de produção, separação do tráfego, controle do ambiente e uma maior transparência em relação aos atacantes com o principal objetivo de criar uma solução mais difícil de se detectar e mais fácil de se implementar, utilizando-se da criação de respostas mais inteligentes e flexíveis às ações dos invasores. Esse conjunto de “técnicas” recebeu o nome de GenII, possuindo as seguintes características principais:

Limite de conexões: o firewall pertencente à rede controla todo o tráfego de saída, diferenciado inclusive pelo tipo de protocolo utilizado. Para isso, são definidos limites máximos de conexões geradas por meio de um honeypot, e quando tal limite é atingido, o tipo de tráfego em questão deve ser bloqueado até que o tempo definido se esgote; (26)

Bridge: o sistema de bridge permite a existência de uma máquina de gerência entre os honeypots e a Internet. A máquina de gerência tem a responsabilidade de controlar e capturar todo o tráfego de forma transparente, sem que o atacante tenha conhecimento de sua existência; (26)

Utilização de IPS: o sistema de IPS permite uma filtragem de conteúdo dos pacotes gerados por meio da honeynet para a Internet. Quando descoberta a existência de pacotes com assinaturas de ataque, o IPS, em conjunto com o firewall, realiza alguns procedimentos para que esse ataque seja mal sucedido; (26)

Controle de log: o controle centralizado dos logs, assim como alguns sistemas de alerta, permitem ao administrador tomar conhecimento sobre ataques e reconhecimentos em tempo real, por meio do envio de mensagens pelo correio eletrônico, celular etc., além de proteger e facilitar o acesso dos mesmos. (26)

4.4 TIPOS DE HONEYNET

Existem dois principais tipos de honeynets, as clássicas e as virtuais.

Honeynets Clássicas: Composta por Honeypots reais, com instalações específicas, contendo vários sistemas operacionais independentes. Conhecida também como honeynets reais ou puras, têm como vantagens de dispor de dispositivos reais e prover mais segurança pela descentralização dos honeypots. Tem como desvantagens o custo elevado, dificuldades e complexidade na instalação, manutenção e administração, espaço ocupado grande.

Honeynets Virtuais: O ambiente é composto por apenas uma máquina, um honeypot virtual, que com um sistema operacional emula aplicativos de virtualização, estes softwares permitem executar diversos sistemas operacionais com aplicações e serviços instalados ao mesmo tempo.

As honeynets virtuais ainda são subdivididas em duas categorias: de auto-contenção e híbridas. Na primeira, todos os mecanismos, incluindo contenção, captura e coleta de dados, geração de alertas e os honeypots (implementados através de um software de virtualização) estão em um único computador. Na segunda, os mecanismos de contenção, captura e coleta de dados e geração de alertas são executados em dispositivos distintos e os honeypots em um único computador com um software de virtualização. (27)

Apresenta como vantagem o baixo custo e alocação de pouco espaço para funcionamento e manutenção simplificada. Como desvantagem tem-se a centralização dos honeypots no servidor (pouco tolerante a falhas), gerando instabilidade devido ao uso exaustivo de memória e processamento, o software de virtualização pode limitar o hardware e sistemas operacionais utilizados; o atacante pode obter acesso a outras partes do sistema, pois tudo compartilha os recursos de um mesmo dispositivo (no caso da categoria de auto-contenção), e possibilidade do atacante descobrir que está interagindo com um ambiente virtual (27) e alto custo de manutenção.

4.5 OBJETIVOS DE UMA HONEYNET

A Honeynet tem por objetivo aprender não na teoria, mas aprender na prática as táticas, as ferramentas, qual a motivação do indivíduo que o leva a ter atos maliciosos, ou seja, tem por finalidade coletar e analisar as informações do invasor. Com o Honeypot comprometido, são analisadas as informações e é onde se verifica os risco e vulnerabilidade do sistema. (28)

4.6 COMPONENTES DE UMA HONEYNET

Podemos dividir os componentes de uma honeynet em três grupos: Alvos, Dispositivos de contenção de fluxo e interconexão e Dispositivos de captura, armazenamento, e análise dos dados e logs.

Alvos: os honeypots.

Dispositivos de contenção de fluxo e interconexão: responsáveis pela interconexão dos honeypots e conexão com a internet, fazem a contenção do fluxo de dados maliciosos para a rede administrativa. São eles:

Roteador: equipamento usado para fazer a comunicação entre diferentes redes de computadores, provendo a comunicação entre computadores distantes entre si e até mesmo com protocolos de comunicação diferentes. Normalmente operam na camada 3 do modelo OSI, sua principal característica é selecionar a rota mais apropriada para repassar os pacotes recebidos, encaminhando os pacotes para o melhor caminho disponível para um determinado destino.

Os roteadores ou routers inicializam e fazem a manutenção de tabelas de rotas executando processos e protocolos de atualização de rotas, especificando os endereços e domínios de roteamento, atribuindo e controlando métricas de roteamento. O administrador pode fazer a configuração estática das rotas para a propagação dos pacotes ou através de processos dinâmicos executando nas redes. Os roteadores passam adiante os pacotes baseando-se nas informações contidas na tabela de roteamento. O problema da configuração das rotas estáticas é que, toda vez que houver alteração na rede que possa vir a afetar essa rota, o administrador deve refazer a configuração manualmente. Já o conhecimento de rotas dinâmicas são diferentes. Depois que o administrador fizer a configuração através de comandos para iniciar o roteamento dinâmico, o conhecimento das rotas será automaticamente atualizado sempre que novas informações forem recebidas através da rede. Essa atualização é feita através da troca de conhecimento entre os roteadores da rede. (29)

Firewall: Para uso na honeynet, tem que ser instalado um recurso adicional no firewall a fim de deixá-lo transparente, chamado de bridging (ponte). Um firewall usando esta tecnologia existe fisicamente, porém convém observar que não poderá ser utilizado como gateway de uma rede por causa da tecnologia empregada. Nesta tecnologia não há inserção de passo de rota (hop) e os pacotes que passam por ele não podem ser traçados, o que faz com que este equipamento seja praticamente não detectável por um atacante externo.(21)

IDS – Sistema de detecção de intrusão: IDS's são ferramentas de segurança automatizadas que visam proteger a rede através da monitoração do tráfego de dados, gerando alarmes e informando sobre ações que violem a política de segurança de uma organização. (30)

A tecnologia dos IDS e firewall diferem entre si, mas serve como complemento um do outro. Os firewalls situam-se nos nós transição entre uma rede e outra, buscando evitar ataques, os IDS precisam estar dentro da rede, com grande visibilidade para todos os pacotes que trafegam no meio, buscando detectar tentativas de intrusão e emitir alarmes.

Dispositivos de captura, armazenamento, e análise dos dados e logs: Tem a função de capturar, armazenar dados para posterior análise dos logs, provenientes da invasão e registros de auditoria dos honeypots.

Em uma honeynet requer a habilitação de geração de logs nos equipamentos, eles são de fundamental importância, pois fornecem uma visão das atividades que estão sendo executadas pelos sistemas, fornecendo assim, dados para análise de detecção de problemas ou falhas de segurança nos sistemas, podendo ser utilizado com evidências de um incidente de segurança, eles são uma das formas mais elementares de auditoria de sistemas. Os log

servers são utilizados em honeynets para armazenar cópia de todos os logs gerados nos equipamentos da honeynet.

A ativação da auditoria gera dados em demasia, porém sua análise pode conter dados preciosos que muitas vezes não são avaliados. A automação da sua captura torna mais simples o trabalho de análise de padrões dos eventos registrados. Estes logs usualmente são armazenados em arquivos ou diretórios específicos para cada caso, ou ainda em um sistema de armazenamento centralizado e remoto, chamado genericamente de LOGSERVER. Na honeynet, este é um componente de armazenamento dedicado e importante, pois armazena os logs que são para ele enviados pelos honeypots. (21).

4.7 RISCO EM TORNO DAS HONEYNETS

- Se o atacante estiver fazendo uso de criptografia, a análise do arquivo de log ASCII pode ser comprometida, não demonstrando com precisão os pressionamentos de tecla que originaram uma determinada situação. (31)
- Monitoramento da honeynet deve ser constante, pois um Honeypot comprometido pode ser utilizado para a invasão de outras redes, ou da própria rede de produção. (24);
- Quase todos atacantes irão apagar os logs gerados por eles durante o ataque, ou pelo menos irão tentar, deletando os arquivos de log, ou gerando uma quantidade exagerada de logs normais de sistema com a finalidade de encher e comprometer os arquivos de logs. Desta forma, deve-se garantir que a transferência destes para o servidor de log seja realizada constantemente e que este servidor tenha uma

5 OUTROS

boa capacidade de armazenamento, e em situações mais críticas, pudesse pensar até no bloqueio da honeynet. (21).

- Se o atacante perceber que está sendo monitorado, poderá desistir do ataque e não mais fazer acessos a esta rede; (24)

- Ausência de tráfego implica em gastos sem retorno, já que nada foi monitorado; (31)

- Visão limitada ao tráfego de dentro da honeynet; (31)

- A quantidade de atividade que se permite depende do risco aceitável. Quanto mais atividade se permitir, maior é o risco e maior é também o potencial de se aprender. (24).

5 OUTROS COMPONENTES RELACIONADOS

Dentre algumas derivações do honeypot podemos citar as honeynets, o honeytokens, honeyfarm e o honeydummie (Honeydumber) e podemos definir como:

Honeytokens: são pequenos conjuntos de informações que são inseridos em bancos de dados ou massas de informações, cujo sentido específico não é válido, mas o tráfego na rede representaria um acesso indevido. O conceito de honeytokens foi introduzido por André Paes de Barros, na lista de discussão do projeto honeynets, aprimorado e estudado por Lance Spitzner, trazendo mais um conceito interessante para a segurança de sistemas.(19)

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 às honeynets que são flexíveis, poderosas e também mais complexas, consumindo muitas horas de trabalho, principalmente na análise de argumentação, ou seja, da depuração das técnicas utilizadas pelo invasor. 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

6 CONCLUSÃO simplificada; os riscos diminuem, já que o controle de dados é efetuado em uma única posição.(31)

Honeydummie (Honneydumber): é o script kiddie que é vítima de um honeypot.

Este termo foi criado por Antonio Marcelo e Flávio Graf. (11)

Apresentamos um campo de visão limitado capturando somente as atividades direcionadas a ele, e nem deve ser usado como substituição as outras tecnologias já conhecidas e sim como complementação da política de segurança das empresas.

A utilização de qualquer um dispositivo de segurança construído por si só não trará um nível de segurança satisfatório a sua rede. Utilizado os honeypots corretamente tornam-se uma ferramenta útil na análise de segurança de perímetro e na estudo de novas técnicas e ferramentas de invasão utilizadas por atacantes. Aliada a firewalls, IDS e IPS evoluem a sua sistemas de segurança da informação completo, filtrando, prevenindo, analisando e reagindo a possíveis ataques a rede.

Nos dias atuais não basta só saber administrar um servidor com seus comandos, muitas vezes complicados ou apertar um botão, avançar aqui ou ali, saber as funções de seus roteiros ou switches, além de conhecer muito bem usuários, serviços e a rede em questão é imprescindível, mas hoje precisamos, além disso, manter-se sempre alerta e informado, a falhas nos softwares, estas, cada vez mais comuns e como um bom administrador de redes tem que estar atento a elas, pois uma atualização sem ser feita e seu sistema pode ser invadido.

6 CONCLUSÃO

Apresentou-se neste trabalho a tecnologia honeypot, que utilizado-se por si só pode ter um campo de visão limitado capturando somente as atividades direcionadas a ele, e nem deve ser usado como substituição as outras tecnologias já conhecidas e sim como complementação da política de segurança das empresas.

A utilização de qualquer um dispositivo de segurança conhecido por si só não trará um nível de segurança satisfatório a sua rede. Utilizado os honeypots corretamente tornam-se uma ferramenta útil na análise de segurança de perímetro e no estudo de novas técnicas e ferramentas de invasão utilizadas por atacantes. Aliada a firewalls, IDS e IPS evoluem a um sistema de segurança da informação completo, filtrando, prevenindo, analisando e reagindo a possíveis ataques a rede.

Nos dias atuais não basta só saber administrar um servidor com seus comandos muitas vezes complexos ou apertar um botão avançar aqui ou ali, saber as funções de seus routers ou switches, além de conhecer muito bem usuários, serviços e a rede em questão é imprescindível, mas hoje precisamos, além disso, manter-se sempre alerta e informado, as falhas nos softwares, estas, estão cada vez mais comuns e como um bom administrador de redes tem que estar atento a elas, pois uma atualização sem ser feita e seu sistema pode ser invadido.

NAKAMURA, Emilio Tassio, Gous, Paulo Lício. Segurança de redes em ambientes cooperativos. São Paulo: Pearson, 2003. V. 1.

STALLINGS, W. Cryptography and network security: principles and practices. 3. ed. Upper Saddle River, New Jersey: Prentice Hall, 2003. 681 p.

CHAPMAN, D. B.; ZWICKY, E. D. Building Internet Firewalls. O'Reilly Associates, Inc. June 2000, Second Edition.

REFERÊNCIAS BIBLIOGRÁFICAS

- (1) MOREIRA, N. S. Segurança Mínima: uma visão corporativa da segurança de informações. Rio de Janeiro: Axcel Books do Brasil, 2001.
- (2) FERREIRA, Fernando N. F; ARAUJO, Márcio T. Política de Segurança da Informação: guia Prático para Embalagem e Implementação. Rio de Janeiro: Ciência Moderna, 2006.
- (3) GABBAY, Max S. Fatores influenciadores da implementação de ações de gestão de segurança da informação: um estudo com Executivos e Gerentes de Tecnologia da Informação das Empresas do Rio grande do Norte. Tese (mestrado) – UFRN, Rio Grande do Norte, 2003.
- (4) DIAS, Cláudia. Segurança e Auditoria da Tecnologia da Informação. Rio de Janeiro: Axcel Books, 2000.
- (5) SHIREY, R. **Internet Security Glossary: RFC 2828**. Internet Engineering Task Force, Network Working Group, 2000.
- (6) NAKAMURA, Emilio Tissato, Geus, Paulo Lício. Segurança de redes em ambientes cooperativos. São Paulo: Futura, 2003. V. 1.
- (7) STALLINGS, W. Cryptography and network security: principles and practices. 3. ed. Upper Saddle River, New Jersey: Prentice Hall, 2003. 681 p.
- (8) CHAPMAN, D. B.; ZWICKY, E. D; Building Internet Firewalls. O'Reilly Associates, Inc. June 2000, Second Edition

- (9) RNP. Firewalls. Disponível em <http://www.rnp.br/newsgen/9708/n3-1.html#ng-servicos>. Acessado em: 15 de fevereiro de 2006. Ultimo acesso em 26 de agosto de 2006.
- (10) BACE, R; MELL, P.; Intrusion Detection System. National Institute of Standards and Technology. Scotts Valley, CA.
- (11) MARCELO, Antonio, Pitanga, Marcos. Honeypots a arte de iludir harckers. Rio de Janeiro: Brasport, 1993. V. 1.
- (12) Red Hat Enterprise Linux 4: Guia de Segurança. Disponível em: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-pt_br-4/ch-detection.html. Acessado em 25 de janeiro de 2006. Ultima visita em: 26 de agosto de 2006.
- (13) ANTUNES, Leonardo Chen. Artigo: Diferenças entre IDS e IPS <http://www.mettasecurity.com.br/artigoIDSIPS.html>. Acessado em 30 de maio de 2006. Ultimo acesso em 26 de agosto de 2006.
- (14) BRANDÃO, Antônio José dos Santos, Moreira, Edson dos Santos. Agentes Móveis e Sistemas de Gerenciamento SNMP. (Mathematics and Computing Institute). Universidade de São Paulo.
- (15) SCHULTZ, E.; ENDORF, C.; MELLANDER, J. The future of intrusion detection and prevention. In: _____. Intrusion detection and prevention. Emeryville, California: McGraw-Hill/Osborne, 2003. cap. 17. Disponível em: http://searchsecurity.techtarget.com/searchSecurity/downloads/IDP_Ch17.pdf Acessado em 30 de maio de 2006.

- (16) L. Spitzner and M. Ranum, "Honeypots: Tracking Hackers," in SANS 2002 Annual Conference, (Orlando, Florida, USA), April 2002.
- (17) CERT.BR – Honeynet: eficácia no mapeamento das ameaças virtuais - Parte 1. Disponível em <http://www.cert.br/docs/reportagens/2003/2003-06-24.html>. Acessado em: 10 de dezembro de 2005.
- (18) MARIZ, Léa Beatriz Ribas, Miranda, Fábio César, Wolski, Eduardo. Estrutura e benefícios da implementação de um ambiente controlado para estudo de ataques no ensino de segurança de redes. (Departamento de Engenharia Elétrica). Universidade de Brasília. Brasília.
- (19) RAVANELLO, Anderson Luiz, Hijazi, Houssan Ali, Mazzorana, Sidney Miguel. Honeypots e aspectos legais. 2004. 85f. Dissertação (Programa de Pós-Graduação em Informática Aplicada.), Pontifícia Universidade Católica do Paraná. Curitiba.
- (20) Honeypots: Are They Illegal. Disponível em <http://www.securityfocus.com/infocus/1703>. Acessado em 15 de fevereiro de 2006.
- (21) PEIXOTO, Jarbas de Freitas. Honeynet: Um ambiente para análise de intrusão. 2002. 42 f. Monografia (Bacharelado em Ciência da Computação), UNESP – Universidade do Estado de São Paulo. São Paulo.
- (22) Honeynet Project, **Know Your Enemy: Honeynets**. Disponível em: <http://www.honeynet.org/papers/virtual/>. Acessado em 24 de março de 2006.
- (23) BELCHIOR, Francisco de Oliveira, SOUSA, Iara Moura de, ARAÚJO, Leda Brito de. Projeto: Utilizando Honeynets como ferramenta auxiliar de verificação de vulnerabilidades em

sistemas operacionais. 2004. 125f. Monografia (Tecnólogo Tecnologia em Segurança da Informação), Faculdade AD1. Brasília. Distrito Federal. em 18 de março de 2006.

(24) The Honeynet Project. Know your Enemy: HONEYNETS. Disponível em: <http://project.honeynet.org/papers/honeynet/index.html>. Acessado em 18 de março de 2006.

(25) JABOUR, Eugênia C. M. G; DUARTE, Otto C. M. B. Monografia Honeynets: Invasores, Ferramentas, Técnicas e Táticas. Universidade Federal do Rio de Janeiro (UFRJ). <http://www.gta.ufrj.br/seminarios/CPE825/tutoriais/eugenia/honeynets.pdf>. (acessado em 24 de março de 2006).

(26) Andrucioli, Alexandre Pinaffi, Proposta e Avaliação de Um Modelo Alternativo Baseado em Honeynet Para Identificação de Ataques e Classificação de Atacantes na Internet. 2005. 146f. Monografia (PÓS-GRADUAÇÃO DE ENGENHARIA), Universidade Federal do Rio de Janeiro, Pesc/COPPE.

(27) CERT.BR – Honeypots e Honeynets: Definições e Aplicações. Disponível em <http://www.cert.br/docs/whitepapers/honeypots-honeynets/>. Acessado em: 05 de janeiro de 2006.

(28) HONEYNET PROJECT. Conheça o seu inimigo O projeto Honeynet. Tradução Kátia Aparecida Roque; revisão técnica da tradução: Álvaro 91Antunes. São Paulo: Pearson Education do Brasil Ltda, 2002, 324 p. Título original: The Honeynet Project: Know Your Enemy

(29) Roteador - Wikipédia. Disponível em <http://pt.wikipedia.org/wiki/Roteador>. Acessado em 23 de fevereiro de 2006.

(30) INNELLA, P. An Introduction to Intrusion Detection Systems. Disponível em <http://www.securityfocus.com/infocus/1520>. Acessado em 18 de março de 2006.

(31) ROJAS, Gislaine Aparecida. Análise de intrusões através de honeypots e honeynets. 2003. 67f. Dissertação (Tecnólogo em Processamento de Dados), Faculdade de Tecnologia de Americana. São Paulo.

(40) OLIVEIRA, L. B. de. Reconhecimento de padrões como auxílio à detecção de intrusão em

(32) Corporativas, Symantec Soluções. Honeypots de olho na empresa. Disponível em http://www.symantec.com/region/br/enterprisesecurity/content/framework/BR_2371.html.

Acessado em: 05 de janeiro de 2006.

(33) COSTA, André Moraes, Melo, Elisio, Alves, Sherman. Segurança de sistemas e redes. 2005. 32F. Relatório (Mestrado em Redes e Serviços de Comunicação) – Faculdade de Engenharia. Universidade do Porto.

(34) THOMAS, Leandro Anchieta. Estudo e implementação de uma ferramenta honeypot para análise de intrusão. 2005. 43f. Monografia (Bacharelado em Ciência da Computação), Universidade de Rio Verde. Goiás.

(35) Projeto Honeypot-BR. Disponível em <http://www.honeypot.com.br>. Acessado em: 15 de novembro de 2005.

(36) Consócio Brasileiro de Honeypots – Projeto Honeypots distribuídos. Disponível em <http://www.honeypots-alliance.org.br/index-po.html>. Acessado em 05 de janeiro de 2006.

(37) Intrusion Detection, Honeypots and Incident Handling Resources. Disponível em <http://www.honeypots.net/>. Acessado em 06 de janeiro de 2006.

(38) Honeypots: Tracking Hackers. Disponível em <http://www.tracking-hackers.com/>. Acessado em 07 de janeiro de 2006.

(39) Firewall - Wikipédia. Disponível em <http://pt.wikipedia.org/wiki/Firewall>. Acessado em 23 de fevereiro de 2006.

(40) OLIVEIRA, C. B. de. Reconhecimento de padrões como auxílio à detecção de intrusão em redes de computadores. 2001. 216 f. Dissertação (Programa de Pós-graduação stricto sensu em Informática) – Universidade Católica de Brasília, Brasília.