

Honeypot na Detecção de Intrusão em Redes de Computadores

Felipe Salimen da Silva

Acadêmico do Curso de Sistemas de Informação da ULBRA Guaíba
fsalimen@gmail.com

Professor Orientador do Curso de Sistemas de Informação da ULBRA Guaíba
andre.peres@ulbra.tche.br

Resumo

A palavra *honeypot* vem do inglês pote de mel. O mel foi na antigüidade um elemento cobiçado por ser de doçura extrema e ser o alimento de nobres reis. Muitas pessoas consideram o mel como uma iguaria desejada e de grande sabor. O conceito de *honeypot* em uma rede é ser um elemento atraente para o invasor, ou melhor, uma iguaria para um hacker.

O propósito de um *honeypot* é ser uma ferramenta de análise de invasões, onde a função do sistema é ser comprometido (invadido). Através de falhas de seguranças reais ou simuladas colocadas de maneira proposital, a ferramenta cumpre o seu papel de coletar dados de ataques, worms, capturas de ferramentas com a finalidade de um estudo, e a reversão para o comunidade de segurança em ferramentas de defesa. (Antônio, Marcelo e Pitanga, Marcos - 2003)

Este projeto tem por finalidade a implementação de ferramentas *honeypots* na rede Labin Ulbra Guaiba buscando simular um ambiente virtual para estudo e análise do comportamento destes softwares nas plataformas proprietárias e de código livre. A classificação dos sistemas será feita conforme os níveis de interatividade e a plataforma operacional onde serão instalados.

1 - INTRODUÇÃO

Atualmente é extensa a lista de novas tecnologias que nascem e crescem a cada dia pela utilização de empresas em busca da competitividade no mercado. A informação passou de um bem abstrato para um bem de valor concreto utilizada por estas empresas que buscam lugar de destaque frente à concorrência. A globalização e o rompimento de fronteiras através da internet e o aumento da disponibilidade de links de banda larga vêm contribuindo significativamente para a disseminação da informação e conhecimento na internet. Diante deste fato, a informação precisa ser protegida e ocultada da ação de indivíduos que cada vez mais se especializam em explorar novas falhas de segurança que são publicadas na Web.

A utilização de firewalls, antivírus, programas IDS, sistemas de auditoria e demais ferramentas de segurança surgiram diante da febre por segurança gerada com o crescimento do comércio eletrônico e da própria internet. Estas ferramentas apenas resumem uma forma de prevenção contra possíveis invasões, mas em diversos casos não apresentam a técnica, ferramentas ou a falha que foi explorada pelo invasor. A necessidade de um maior estudo e atualização constante das ferramentas de segurança abriu um espaço para a compreensão das técnicas e da filosofia criadas pelos atacantes de sistemas.

Uma nova classe de softwares de análise e estudos foi gerada diante desta necessidade, e hoje é utilizada por algumas empresas, mesmo que seja de uma forma modesta, os *honeypots* conquistaram seu espaço através do mercado de software ou no mundo *opensource*.

A função de um *honeypot* está em simular um sistema com possíveis falhas de segurança e desta forma compreender e demonstrar os métodos utilizados por um invasor ao tentar comprometer um sistema operacional de produção. Um *honeypot* é um atrativo colocado de forma proposital dentro de uma rede visando desviar a atenção de um atacante para outros sistemas e desta forma cumprir a sua função de ser invadido e comprometido. Obviamente existem pontos negativos na utilização desta técnica por pessoas despreparadas, o que pode resultar na abertura de uma brecha de segurança real e o comprometimento de toda uma rede.

2 - OBJETIVO

O objetivo deste trabalho é apresentar e divulgar uma análise dos conceitos e da utilização de sistemas *honeypots* em redes de computadores, através de dados e demonstração prática do conteúdo estudado. Após a análise julgar se é produtiva (retorno de investimento) e segura a implementação desta técnica em uma rede corporativa.

3 - REFERENCIAL TEÓRICO

O referencial teórico deste trabalho objetiva abordar as metodologias de ataques mais comuns, como as melhores práticas para implementação das tecnologias *honeypots* em um ambiente. Durante a coleta de informações, foi optado por não abordar as técnicas de prevenção como implementação de firewalls, Ids e demais sistemas de segurança, buscando não comprometer o foco do trabalho.

Um *honeypot* é um recurso 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. (Spitzner, Lance – 2003).

Desta forma, pode-se categorizar um *honeypot* como um sistema de detecção passivo, onde sua função é apenas gerar eventos de logs sobre toda a atividade e interação feita sobre ele. Diante destes fatos, surgiram variações de sistemas baseados em *honeypots* como as *honeynets*. As *honeynets* fazem parte da evolução de sistemas em *honeypots*, onde uma rede toda é simulada em diversas máquinas. A complexidade não está em desenvolver os *honeypots* em si, mas sim em projetar toda uma rede que ofereça capacidade de controle e de coleta de toda e qualquer atividade ou tráfego de/e para a *honeynet*. Este conceito existe há 10 anos e foi implementado por Spitzner em 2002 quando as *honeynets* ainda eram voltadas apenas para projetos de pesquisa e não para ambientes de produção. (Antônio, Marcelo e Pitanga, Marcos - 2003)

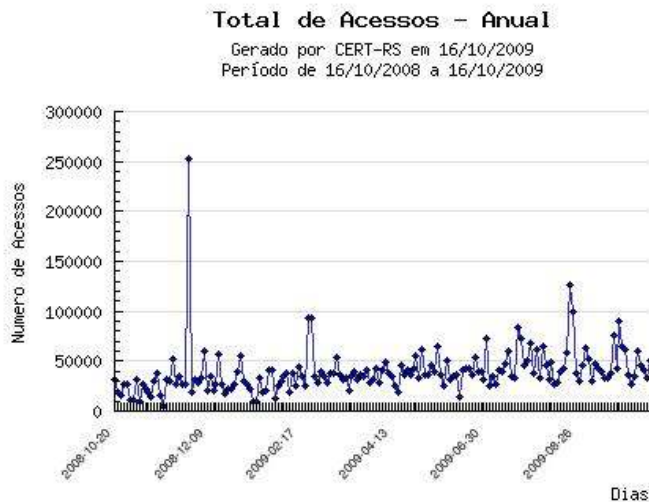
Hoje, existem diversas *honeynets* espalhadas pela internet com o intuito de catalogar assinaturas de ataques e prever com a maior precisão possível os tipos de ataques, vírus e worms existentes na rede mundial. Os esforços são muitos e dentre

eles podemos dar destaque ao honeynetproject onde são desenvolvidos softwares como o *honeywall*. O projeto honeynet começou a desenvolver, a partir de 2005, um software que representa um papel de gateway em modo bridge para interligação de uma *honeynet* com a internet. O *honeywall* não exerce um papel de roteamento, mas de um coletor de todo o tráfego de entrada e saída da rede virtual.

No Brasil, foi criado o honeynetprojectBR mais conhecido como o Consórcio Brasileiro de Honeypots, que nada mais é do que uma aliança entre órgãos públicos, bancos, empresas privadas e centros de pesquisa. Este projeto foi fundado pelo CERT após os primeiros testes com o software *Honeyd*, em 2003. Atualmente, o projeto conta com 40 integrantes espalhados por todo o território brasileiro e cada um com sua própria honeynet capturando tráfego e gerando logs para os relatórios de incidentes do CERT. Abaixo, temos os objetivos do projeto segundo o CERT:

- Implantar uma rede distribuída de honeypots de baixa interatividade (*Honeyd*), buscando cobrir a maior parte do espaço de endereços IP da Internet no Brasil;
- Montar um sistema de análise de dados que permita o estudo de correlações e tendências de ataques;
- Atuar conjuntamente com Grupos de Resposta a Incidentes de Segurança de Computadores (CSIRTs) na difusão destas informações.

A efetividade deste consórcio pode ser vista nos gráficos gerados no dia 09/12/2008 quando a Microsoft lançou oito boletins de segurança para 28 falhas encontradas em toda a plataforma Windows.



O gráfico apresenta duzentos e cinquenta mil acessos somente na rede CERT-RS, demonstrando um alto nível de acessos às portas TCP/UDP monitoradas pela honeynet.

4 - SOLUÇÃO PROPOSTA

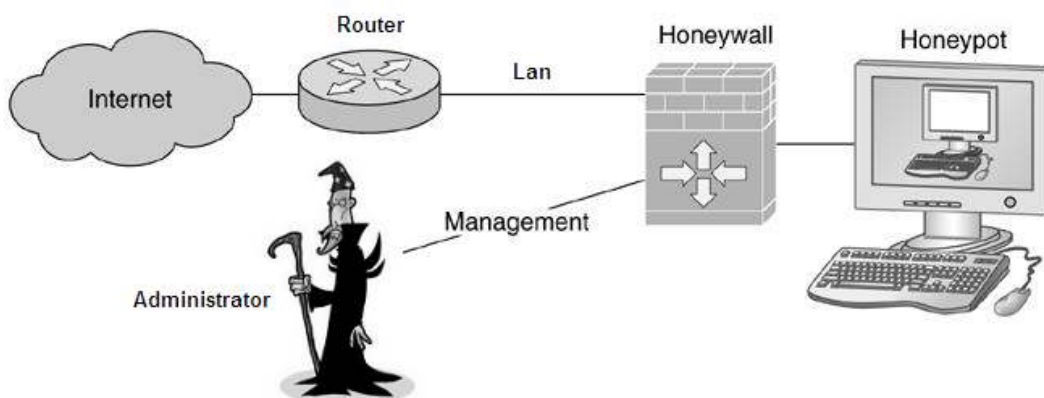
Atualmente, existem diversos tipos de *honeypots* desenvolvidos no mercado, que estão divididos por níveis de interatividade, e plataformas proprietária ou *opensource*. A metodologia empregada neste trabalho será comparar a qualidade dos relatórios e logs gerados pelas ferramentas, como a capacidade de *timeline*, técnica utilizada e a fidelidade nos ataques simulados. O processo de simulação de ataques será fundamental para comparar a fidelidade no comportamento de um *honeypot* com o comportamento de um sistema real, no momento em que a falha de segurança é explorada. Diante disto teremos três hipóteses de solução proposta:

- Hipótese 1: Comparar plataformas proprietárias com plataformas *opensource* de uma mesma escala de interatividade. Será utilizado software Trial para as plataformas proprietárias.
- Hipótese 2: Comparar *honeypots* virtuais (*software*) com *honeypots* reais (sistemas operacionais falhos) e encontrar qual o melhor método. Será utilizada a rede do Labin para análise e experimento.
- Hipótese 3: Após análise da hipótese 1 e 2, deverá ser definida a melhor forma de implementação. Esta hipótese irá julgar se é produtiva (retorno de investimento) e segura a implementação desta técnica em uma rede corporativa.

5 - CENÁRIO PROPOSTO

Para a segunda parte deste trabalho o cenário proposto é a construção de máquinas virtuais utilizando a plataforma de virtualização VMWare por possuir uma maior compatibilidade de sistemas operacionais existentes e *hardware* padrão *Intel*.

A rede será uma honeynet com classe de IP diferente da classe utilizada na rede do Labin Ulbra Guaíba, onde o elo de ligação será um *honeywall* que fará o papel de gateway em modo bridge para controle de todo o tráfego de passagem para dentro do ambiente virtual. O *honeywall* irá possuir três interfaces de rede, sendo a primeira para rede Labin, a segunda para rede *honeynet* e a terceira para console de administração. Os sistemas serão avaliados e comparados quanto ao nível de interação e o tipo de licença utilizada para implementação.



Origem: Livro - *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*

As simulações de ataques serão executadas utilizando exploits compatíveis com a versão dos sistemas simulados dentro da honeynet. Também será utilizado ferramentas de scan de vulnerabilidades como o Scan Nessus para um ataque de pesquisa inicial. A listagem dos softwares que irão ser testados estão descritas na tabela abaixo:

Honeypot	OS Base	Licença	Interação
KFSensor	Windows 2003	Proprietário	Alta
Server Decoy	Solaris 8	Proprietário	Alta
Specter	Windows 2003	Proprietário	Alta
RedHat6.2	RedHat6.2	GPL	Alta
Honeywall	CentosOS	GPL	Alta
Honeyd	Fedora 9	GPL	Baixa

O processo prático será essencial, pois a honeynet não deverá afetar a estrutura atual do Labin e manter-se oculta na rede já existente. O processo será dividido em oito etapas que estão descritas a seguir:

1. Análise de requisitos necessários para implementação de uma honeynet no ambiente do Labin Ulbra Guaiba
2. Implementação experimental de um ambiente virtualizado com a plataforma VMWare para suportar os sistemas *honeypots*.
3. Implementação da honeynet de produção para coleta e análise dos dados.
4. Execução da simulação de ataques visando a geração dados
5. Elaboração de tabelas, gráficos e documentos com os resultados
6. Elaboração do artigo para Seminário de Andamento
7. Conclusões finais sobre o projeto
8. Entrega do TCC

Cronograma

Atividade	Março			Abril			Maio			Junho		
Análise de Requisitos	■	■										
Implementação experimental		■	■	■	■	■						
Implementação da honeynet – Labin Ulbra Guaiba		■	■	■	■	■	■	■	■			
Execução de ataques simulados			■	■	■	■	■	■	■			
Elaboração de tabelas, gráficos e documentos com os resultados			■	■	■	■	■	■	■	■		
Elaboração do artigo para Seminário de Andamento								■	■	■	■	
Conclusões finais sobre o projeto									■	■	■	■
Entrega do TCC												■

5 - CONCLUSÃO

Este trabalho tem como ponto diferencial comparar as tecnologias de *honeypots* existentes e identificar os níveis de interação possíveis para os softwares disponíveis com este propósito. A infraestrutura é baseada no modelo utilizado no livro *Virtual Honeypots: From Botnet Tracking to Intrusion Detection* como forma de isolar o ambiente dentro de uma rede local sem a utilização de uma *DMZ*. É evidente que a utilização desta tecnologia quando implementada de forma correta, gera benefícios para estudos e conhecimento de incidentes de segurança da informação e desta forma auxiliando na administração de um ambiente.

Até o momento, os livros e todo o material teórico têm servido de base para uma breve noção dos melhores métodos. No entanto, somente a implementação prática de uma honeynet irá apresentar os resultados reais para uma conclusão mais precisa.

Bibliografia

ADDISON, Wesley. **Conheça o seu inimigo: The Honeynet Project**. São Paulo: [Makron Books], 2002. 324p.

RUSSELL,Ryan; DUBRAWISKY,Ido; GRAND,Joe; MULLEN,Tim. **Roubando a Rede**
- Rio de Janeiro [Alta Books], 2003. 215p

MARCELO, Antonio; PITANGA, Marcos. **Honeypots – A arte de iludir Hackers**. Rio de Janeiro: [Brasport], 2003.97p

A. GRIMES, Roger. **Honeypots for Windows**. United States - NewYork [Apress], 2005. 424p

ADDISON, Wesley. **Honeypots: Tracking Hackers**. United States - Boston [Pearson Education, Inc], 2002. 480p

ADDISON, Wesley. **Virtual Honeypots: From Botnet Tracking to Intrusion Detection**. United States – Boston [Pearson Education, Inc], 2007. 480p

CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. *Disponível em:* <<http://www.cert.br>>. *Acesso em:* 22 de março 2009.

HoneynetProject - Honeynet Project . *Disponível em:* <<http://projects.honeynet.org/honeywall/>>. *Acesso em:* 10 de outubro 2009.