Honeypots - A segurança através do disfarce

Tiago Souza Azevedo
(tiago@ravel.ufrj.br)
Ravel - COPPE/UFRJ
GRIS - DCC/UFRJ

9 de Agosto de 2005

Resumo

Este artigo foi desenvolvido como fruto do estudo de honeypots, baseado na tese de mestrado PROPOSTA E AVALIAÇÃO DE UM MODELO ALTERNATIVO BASEADO EM HONEYNET PARA IDENTIFICAÇÃO DE ATAQUES E CLASSIFICAÇÃO DE ATACANTES NA INTERNET[1], e no livro Honeypots: Tracking hackers[2]. Portanto o principal objetivo é o entendimento dos conceitos inerentes a honeypots, sua origem e desenvolvimento, como também, suas características e aplicações práticas.

Conteúdo

1 História

Podemos considerar o início do conceito de honeypot com a publicação do livro "The Cuckoo's Egg"[3], seguido da publicação do artigo "An Evening with Berferd in Wich a Cracker is Lured, Endured, and Studied"[4], uma vez que antes de 1990, não há informações sobre redes que possuiam o objetivo de atrair atacantes e estudá-los.

No livro "The Cuckoo's Egg"[3], Clifford Stoll relata os eventos ocorridos, de um período de 10 meses, compreendidos entre 1986 e 1987, no laboratório Lawrence Berkeley. Ele descobriu ocasionalmente que um atacante, "Hunter", havia invadido seu sistema e resolveu monitorá-lo.

O artigo de Bill Cheswick, "An Evening with Berferd in Wich a Cracker is Lured, Endured, and Studied"[4] é mais técnico que o livro de Clifford Stoll, por ele ser um profissional de segurança e relata as tentativas de ataques ocorridas em um sistema construido para ser comprometido.

Sete anos após a publicação destes trabalhos, começaram a surgir as primeiras ferramentas. A primeira, chamada Deception Toolkit(DTK)[5], foi desenvolvida por Fred Cohen e teve seu primeiro release, DTK version 0.1, em novembro de 1997. Era uma ferramenta free desenvolvida em C e Perl para sistemas Unix. Logo depois, em 1998, a primeira ferramenta comercial, CyberCop Sting, foi desenvolvida por Alfred Huger, para Windows NT.

Em 1999 foi formado o Honeynet Project[6], um grupo de pesquisa formado por 30 profissionais de segurança dedicado a pesquisar sobre a comunidade hacker e compartilhar suas experiências. Em 2001 eles lançaram a série de artigos "Know your enemy"[8] que compilava suas experiências e pesquisas.

Recentemente as pesquisas envolvendo honeypots e honeynets são baseadas em três áreas principais: Honeypots Dinâmicas, Honeytokens e Honeypot Farms.

Honeypots dinâmicas são honeypots que uma vez conectadas ao sistema, automaticamente determinam quantas honeypots montar, como montá-las e como elas deveriam ser para se misturarem ao sistema. Além disso estas honeypots se adaptam observando as mudanças do ambiente. Se o sistema receber uma nova configuração Linux por exemplo, serão criadas novas honeypots Linux.

Honeytokens são honeypots que não são computadores. São um tipo de entidade digital. Um honeytoken pode ser um número de cartão de crédito, uma planilha Excel, uma apresentação em PowerPoint, um banco de dados, ou um login falso. Honeytokens podem ser diferentes entidades, mas compartilham o conceito de uma honeypot: um recurso de sistema de informação que disfarça seus valores para uso não autorizado deste recurso. A principal aplicação dos honeytokens estão no estudo do comportamento de um atacante, quando este compromete o sistema, e no valor de atração adicionado ao ambiente, por exemplo, honeypots contendo números de cartão de crédito são muito mais atrativas.

O conceito de Honeypot Farms é simples, ao invés de manter um grande número de honeypots ou honeypots espalhadas por várias redes, mantemos uma única rede em um único lugar. Os atacantes são então redirecionados para esta rede de honeypots ao tentarem qualquer ação contra a rede real.

2 Conceitos e Classificações

2.1 Definição

Mesmo que as idéias de honeypots tenham surgido há 15 anos atrás, esta nunca teve uma definição precisa, o que, de certa forma, prejudicou o desenvolvimento do tema. Durante estes 15 anos, várias pessoas definiram as Honeypots como: sistemas para atrair hackers, sistema para detecção de intrusão, etc.

A definição mais aceita é a de Lance Spitzner, autor do livro "Honeypot: Tracking Hackers"[2], segundo ele uma Honeypot é: "a security resource whose values lies in being probed, attacked, or compromised", ou seja, uma honeypot é um sistema de segurança que disfarça seus valores ao ser testado, atacado ou comprometido. Embora esta definição pareça um tanto vaga, ela permite que utilizemos uma honeypot para deter atacantes, detectar ataques, capturar e analisar ataques automatizados como worms além de fornecer informações importantes sobre a comunidade hacker.

2.2 Classificação

Podemos classificar as honeypots em duas categorias gerais: Honeypots de Produção e Honeypots de Pesquisa. Estas categorias foram primeiro propostas por Marty Roesch, desenvolvedor do Snort[7].

2.2.1 Honeypots de Produção

Honeypots de Produção, são sistemas que aumentam a segurança de um organização específica e ajudam a mitigar riscos. São mais fáceis de construir porque requerem menos funcionalidades. Usualmente possuem as mesmas configurações que a rede de produção da organização e transportam para ela todo o aprendizado obtido com os ataques sofridos. Analisaremos as Honeypots de Produção segundo as categorias de segurança definidas por Bruce Schneier em seu livro "Secrets and Lies"[**?**]. Schneier divide segurança em prevenção, detecção e resposta.

Nos termos definidos por Schneier, prevenção significa manter os invasores fora de sua rede. Fazendo uma analogia com a segurança de uma casa, prevenção significa instalar uma cerca no jardim, fechar as janelas e trancar as portas, ou seja, fazer todo o possível para manter do lado de fora qualquer ameaça. Sob este ponto de vista, honeypots tem pouco a acrescentar, uma vez que não conseguem barrar os possíveis atacantes, de fato possuem o objetivo

oposto.

Alguns pesquisadores alegam que Honeypots são importantes para a prevenção, por adicionarem alguns fatores como: o tempo e os recursos gastos na tentativa de ataque a uma honeypot, quando estes recursos poderiam estar sendo direcionados para uma rede de produção; e a preocupação infringida ao atacante por este saber que a rede de uma organização pode ser na verdade uma honeypot.

Estes argumentos são válidos para ataques contra alvos de escolha, onde os atacantes têm um grande nível de conhecimento e analisam a informação que recebem do alvo para efetuarem o ataque. Para alvos de oportunidade, nos quais o que mais importa para o atacante é a quantidade de alvos atingidos e na maioria das vezes, tais ataques são automatizados, uma Honeypot agrega pouco valor de prevenção.

A detecção se refere a alertar atividades não autorizadas. Seguindo a mesma analogia da segurança de uma casa, detecção significaria instalar alarmes pela casa, detectores de movimento, etc. Detecção é importante pois mais cedo ou mais tarde a prevenção falhará, seja por causa de uma má configuração do firewall ou uma nova vulnerabilidade de um serviço oferecido pelo sistema.

É na detecção que uma honeypot tem maior importância, uma vez que todo tráfego gerado para a Honeypot é suspeito e deve ser verificado. Apenas em alguns casos serão gerados falsos positivos, por exemplo no caso de alguém acidentalmente apontar seu browser para o endereço ip da honeypot. A detecção também se torna mais fácil pois os logs gerados pela honeypot estão livres do ruído existente em uma rede de produção real. Embora seja de grande valor, veremos nas próximas seções que uma honeypot possui a desvantagem de não poder detectar tráfego que não seja direcionado a ela.

Uma vez identificado um ataque, algumas ações são necessárias como coletar evidências de como o atacante conseguiu acesso ao sistema, o que ele fez ao sistema, de onde ele conseguiu acesso, e o encaminhamento destas informações às autoridades responsáveis. Tais ações se referem a resposta dada ao ataque.

Uma honeypot se mostra de grande valor para a reposta dada ao incidente, uma vez que a análise de um ataque é facilitada pois a coleta de evidências é simples e livre de ruídos. O sistema também pode ser imediatamente desconectado da rede, diferente de um sistema de produção real que fornece serviços que não podem ficar offline.

2.2.2 Honeypots de Pesquisa

As Honeypots de Pesquisa oferecem uma plataforma de estudo visando compreender a comunidade hacker, não apenas estudar as ferramentas utilizadas para a invasão, que normalmente são deixadas no sistema pelo atacante, mas obter informações preciosas como: qual ferramenta utilizada para testar o sis-

tema, qual exploit utilizado para comprometê-lo e cada tecla utilizada após a invasão do sistema.

Embora o ganho de conhecimento sobre as ações e motivações da comunidade hacker seja enorme, uma Honeypot de Pesquisa pouco acrescenta a uma organização, pois estão focadas nas ações do atacante e não apenas sua detecção.

2.3 Níveis de Envolvimento

Honeypots possuem diferentes funcionalidades, deste a simples simulação de um serviço até a construção de uma rede de honeypots oferecendo serviços reais, uma Honeynet. Para distinguir os tipos de honeypots, Lance Spitzner em seu livro[2] criou o conceito de "níveis de envolvimento", referente a maneira que a honeypot interage com o atacante.

2.3.1 Nível Baixo

O nível de envolvimento baixo, equivale a serviços emulados pela honeypot. Nesse tipo de envolvimento, o atacante possui uma mínima interação com a honeypot e por isso são poucos os dados gerados, em geral, informam apenas as tentativas de conexão.

2.3.2 Nível Médio

No nível de envolvimento médio, a interação entre a Honeypot e o atacante é maior, mas não equivale a um sistema real. Os serviços oferecidos ainda são emulados, mas estes respondem as requisições do atacante como serviços reais. Desta forma mais dados sobre o ataque são obtidos. Devido ao maior grau de interação com o sistema, os riscos também aumentam.

2.3.3 Nível Alto

No nível de envolvimento alto, os serviços são reais, não emulados. Por serem sistemas operacionais e máquinas reais, o nível de interação com o atacante é muito maior e desta forma a quantidade de dados obtidos sobre o ataque é enorme. Em contrapartida, este nível oferece o maior risco possível, uma vez que tendo invadido o sistema, o atacante tem um sistema operacional real para lançar ataques a outras máquinas.

3 Vantagens e Desvantagens

As Honeypots possuem vantagens e desvantagens em sua aplicação. Nesta seção examinaremos tais características.

3.1 Vantagens

Como consequência de seu conceito, todo tráfego de dados gerados tendo como origem ou destino, máquinas ou serviços que pertençam a uma honeypot ou honeynet deve ser tratado como uma ameaça. Por isso tal tráfego é bastante reduzido devido a ausência do nível de ruído que seria produzido por uma rede de produção verdadeira.

Outra vantagem é a simplicidade. Como Lance Spitzner cita em seu livro[2], não existem algoritmos a desenvolver, nenhuma base de assinaturas para manter. Apenas devemos montar uma honeypot em algum ponto da organização e esperar pelos resultados.

O retorno do investimento feito em uma honeypot é rápido. Assim que um ataque é realizado a uma honeypot, todos os dados gerados são significativos à organização.

3.2 Desvantagens

Provavelmente a maior desvantagem de uma honeypot é seu campo de visão direcionado. Uma honeypot só consegue visualizar a atividade de um ataque direcionada à ela, desta forma, se o atacante estiver ciente da honeypot e desta forma evitá-la, nenhuma informação será agregada.

Outra desvantagem que geralmente ocorre em versões comerciais é a possibilidade de identificação da Honeypot. Esta identificação é baseada em certas características ou erros de implementação. Por exemplo, uma honeypot que emula um servidor Web pode gerar uma reposta incorreta a uma requisição. Esta resposta incorreta se torna uma "impressão digital"da honeypot facilitando sua identificação.

Por fim temos o risco introduzido pela honeypot, pois se mal configurada, uma Honeypot atacada pode ser utilizada para alvejar outras máquinas. É importante lembrar que quanto mais complexa for a Honeypot maior o risco oferecido pela mesma.

4 Conclusão

HoneyPots e Honeynets são ferramentas recentes para a aquisição de conhecimento não apenas das ameaças provenientes do ambiente de rede, como também sobre as motivações e comportamento da comunidade Hacker. Embora não se apliquem como ferramentas de proteção direta às redes, são de grande importância para a prevenção de ameaças e mitigação de riscos. Mas para operarem corretamente, requerem cuidados minuciosos afim de evitar os riscos infringidos. Se tais cuidados forem tomados, Honeypots e Honeynets se tornam ferramentas fantásticas na segurança computacional.

Referências

[1] Proposta E Avaliação De Um Modelo Alternativo Baseado Em Honeynet Para Identificação De Ataques E Classificação De Atacantes Na Internet - Alexandre Pinaffi Andrucioli

[2] Honeypots: Tracking Hackers - Lance Spitzner

[3] The Cuckoo's Egg - Clifford Stoll

[4] An Evening with Berferd in Wich a Cracker is Lured, Endured, and Studied - Bill Cheswick

[5] Deception Toolkit - http://www.all.net/dtk

[6] The Honeynet Project - http://www.project.honeynet.org

[7] Snort, Open Source Intrusion detection System - http://www.snort.org

[8] The Honeynet Project, Know Your Enemy - http://www.project.honeynet.org/book/