HONEYPOTS PARA DETECÇÃO E CONTENÇÃO DE BOTNETS

Milani, Thiago G.(IC); Kakuda, Claudio M. [1](O)
milinhamilani@yahoo.com.br
[1]*Departamento de Física, Universidade de São Paulo de São Carlos (USP)*

Com o amplo crescimento de equipamentos conectados a rede mundial de computadores, cresce também o número de tentativas de ataques, inclusive por *botnets.* Com isso os departamentos de segurança de redes das organizações tem se conscientizado da necessidade de adotar ferramentas além das tradicionais (*Firewall,* Anti-Vírus e *Proxies*) para entender e acompanhar esses ataques, o perfil dos atacantes e as ferramentas utilizadas. Um dos métodos empregados para esse tipo de compreensão e entendimento é o *honeypot.*

De acordo com Lance Spitzner, membro-fundador do Projeto *Honeynet*, 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, 2003).

Um *honeypot* tem a função de registrar e armazenar informações sobre ataques a sua rede, desviando toda a atenção do atacante para o *honeypot* ao invés das reais informações expostas na rede. Diante das diferentes formas de aplicação e implementação de *honeypots*, a escolha dependerá do que esperasse obter, utilizando-se o conceito de nível de interação, que determinará a forma com que o *honeypot* irá interagir com os atacantes. (SPITZNER, 2003). Esses dois tipos de *honeypots* são: os de alta-interatividade e os de baixa-interatividade.

Honeypot de alta-interatividade oferece aos atacantes, também conhecidos como *blackhats* um sistema operacional real, onde nada é emulado ou restrito, assim armazenando grande quantidade de informações sobre eles, sendo essa a principal diferença entre os *honeypots* de baixa-interatividade.
Nesse modelo de alta interação as oportunidades são maiores, onde podemos aprender novas técnicas, descobrir novas ferramentas, identificar vulnerabilidades no sistema operacional, e saber como funciona a comunicação entre os atacantes.

Ao criar um ambiente assim ele não se diferenciará muito de um sistema real, na realidade será igual, porém seu propósito é ser atacado e comprometido.

Nesse nível de interação existe um maior risco, pois, ao entregar uma máquina com serviços reais para um invasor, existe a chance de ele conseguir comprometer esse computador e obter acesso a outros computadores da rede. Afinal ele terá um sistema operacional real à disposição para fazer o que quiser. (ASSUNÇÃO, 2009).

Por sua maior vulnerabilidade da rede esse sistema de *honeypot* é muito mais difícil de mantes, englobando muitos outros mecanismos como o *firewall* e IDS que devem ser bem configurados, para assim minimizar os riscos oferecidos. Esse tipo de *honeypot* de alta-interatividade é recomendado apenas para pessoas ou organizações que tenham maior experiência na área de Segurança de Redes.

Um *honeypot* de baixa-interatividade fornece, como o próprio termo já apresenta, um nível de interação limitado entre os atacantes e o *honeypot.* (ANDRADE, 2009)

Honeypot de baixa-interatividade é um recurso de segurança que simula vários serviços, virtualizando vários tipos de servidores ao mesmo tempo, dando ao atacante um sistema mais restrito e com menos liberdade. Todos os serviços, seja um *shell* do sistema

ou um servidor de correio, são simulados. O invasor nunca terá acesso ao sistema real, apenas as versões simuladas dos mesmos (ASSUNÇÃO, 2009).

Neste tipo de interação não existe um sistema operacional real, o atacante interage com uma maquina virtual e com comandos restritos. Esse tipo de *honeypot* dá a possibilidade de se emular vários tipos de serviços como FTP, POP3, WEB entre outros. Por exemplo, um *honeypot* poderia emular um serviço FTP onde o atacante poderia obter *login* anônimo dentro do *honeypot,* e baixar uma cópia do arquivo do sistema de senha, uma tática usada por muitos atacantes. No entanto a conta anônima será a única com acesso, e o arquivo de senha não teria validade, pois seria um arquivo falso plantado no *honeypot* e usado para iludir o atacante. Nesse e em outros casos, o nível de interação é limitada a apenas tentativas de *login,* acesso anônimo e a capacidade de baixar o arquivo de senhas falsas. (JESUS, 2010).

Foram utilizados três grandes sistemas *honeypot* de baixa-interatividade para a elaboração deste trabalho. Essas ferramentas são: *Honeyd*, *KFSensor* e *Valhala Honeypot.*

- **Honeyd**: É o software pioneiro quando o assunto é *honeypots.* Ele permite a criação de *hosts* virtuais e o anexo de *scripts* personalizados em Perl para a criação de interações em determinadas portas. (ASSUNÇÃO, 2009), ele também necessita de IP's disponíveis na rede para criar seus *scripts* de *honeypot*. Possui também o código fone livre pela GPL. Existem disponíveis as versões para *Windows* e para *Linux.*

- **KFSensor**: É um *honeypot* comercial para *Windows.* Foi um dos primeiros a se destacar neste segmento e seu desenvolvimento foi implementado pela *Key Focus.* (ASSUNÇÃO, 2009). Assim como o *honeyd,* ele trabalha com baixa-interatividade simulando respostas ao invés de fornecer dados reais ao atacante. Uma dos recursos mais interessantes ele é a possibilidade de instalação de senários em locais estratégicos da rede, que permite monitorar o trafego e o tempo de respostas remotamente para o computador onde está rodando o servidor do *KFSensor.*

- **Valhala Honeypot:** É um *honeypot* desenvolvido totalmente em português. Ele foi desenvolvido para *Windows* e tem seu código aberto. Possui serviços de um *honeypot* de baixa-interatividade como de alta-interatividade. Outra questão é que ao contrário do gratuito *honeyd* e de outros *honeypots* comerciais, o *Valhala* ainda não suporta utilização de captura de IP's disponíveis na rede para a criação de *hosts* virtuais. (ASSUNÇÃO, 2009). É necessário utilizar o endereço IP atual da maquina na qual irá ser instalado o programa.

As ferramentas acima descritas foram instaladas e testadas para melhor entende-las e melhor explicar seus funcionamentos.