Sistemas de Detecção de Intrusões

Pedro Miguel Félix Alípio

Maio, 2002

Resumo

A distribuição cada vez mais alargada dos sistemas informáticos, tem permitido a construção de um mundo virtual com o objectivo de evitar as constrições habituais, no que diz respeito à disponibilidade da informação e do acesso a serviços. A evolução tecnológica e a adesão globalizada, permitiram que se criasse um novo espaço pleno de oportunidades de negócio, no qual muitas empresas investiram e onde algumas obtiveram sucesso imediato. No entanto, este mundo criado à imagem do mundo real, herdou também o lado negro humanidade - o crime. O crime, neste contexto, consiste em desrespeitar de alguma forma o uso para o qual estes sistemas informáticos foram concebidos. Este desrespeito pode ir desde o simples acesso ilícito à informação até "agressões violentas" tornando o sistema temporariamente ou permanentemente indisponível. Ao conjunto de acções que o individuo criminoso desencadeia para atingir um objectivo ilícito é dado o nome de ataque ou intrusão. As acções são designadas por eventos que podem por si só serem considerados maliciosos.

No sentido de evitar estes abusos, surgiu uma nova área de estudo designada por segurança de sistemas informáticos. Os peritos desta área estão preocupados em desenvolver políticas e sistemas de segurança que impeçam as incursões criminosas.

Hoje em dia é comum utilizarem-se *firewalls* em praticamente todos os sistemas ligados à *internet*. Este tipo de dispositivos permitem fazer alguma filtragem do tráfego que provém do exterior da rede, por exemplo, limitando a entrada na rede a tráfego dirigido a aplicações específicas, diminuindo desta forma o leque de opções de ataque do criminoso. Tem-se no entanto verificado que estes dispositivos não são suficientes para garantir a impenetrabilidade. Graças à qualidade duvidosa de grande parte do *software* existente nos sistemas informáticos, é possível utilizar essas falhas, que quando associadas a questões de segurança são designadas por vulnerabilidades, de forma a desencadear ataques. As

ferramentas que exploram essas vulnerabilidades são designadas por *exploits* e encontram-se disponíveis por toda a *internet*. A maior parte do ataques desencadeados por este tipo de ferramentas têm como objectivo provocar a indisponibilidade dos sistemas, mas podem também ser utilizadas para apenas desencadear um dos passos de um ataque mais devastador. Por vezes, a vulnerabilidade pode permitir a elevação de privilégios do intruso. Desta forma, o ataque poderá consistir na eliminação de informação vital, levando à destruição permanente de um sistema. Muitas destas vulnerabilidades estão associadas a servidores *http* e outros serviços disponíveis do exterior da rede, aos quais a *firewall* não nega o acesso. É fundamentalmente por este motivo que se torna tão importante a utilização de sistemas de detecção de intrusões.

Os sistemas de detecção de intrusões podem ser classificados segundo várias perspectivas: relativamente à arquitectura (*host* e alvo na mesma localização ou em localizações separadas), relativamente aos objectivos (responsabilização ou resposta), relativamente à estratégia de controlo (centralizada, parcialmente distribuída ou totalmente distribuída), relativamente ao tempo (tempo real ou intervalos), relativamente às fontes de informação (baseado no tráfego da rede ou em logs do sistema ou de aplicações), relativamente ao tipo de análise (detecção de abusos ou detecção de anomalias) e finalmente relativamente ao tipo de resposta (resposta activa ou passiva).

No caso particular dos sistemas baseados na análise do tráfego em tempo real, existem exigências de desempenho que constituem um problema complicado. Os componentes principais dum sistema deste tipo são: o *sniffer* - responsável pela extracção do tráfego que passa no *interface* de rede do *IDS* (*Intrusion detection System)* e o mecanismo de verificação de assinaturas - responsável pela verificação da existência de assinatura (regras) que correspondam ao padrão do tráfego capturado. Se o processo de análise implementado no sistema consistir apenas na análise dos cabeçalhos das unidades de tráfego, em princípio não serão necessárias grandes habilidades de implementação para construir um sistema deste tipo, sem que surja o problema da perda de unidades de tráfego por analisar. Este problema coloca-se em sistemas que introduzem funcionalidades mais avançadas, por exemplo, em sistemas que permitem a análise do *payload* das unidades de tráfego e/ou sistemas que permitem a manutenção de estado, isto é, que permitem manter informação acerca dos eventos com a finalidade de os poder relacionar temporalmente. Para tentar minimizar este problema existem algumas soluções já implementadas em alguns sistemas. Por exemplo, C. Jason Coit, Stuart Staniford e Joseph MacAlerny alteraram o famoso *snort*, desenvolvido por Marty Roesch, de forma a usar um algoritmo de *pattern-matching* extremamente eficiente que permite a verificação da ocorrência de múltiplos padrões numa

string que contem o *payload* da unidade de tráfego capturada. No entanto, o *snort* não mantém estado. Os sistemas que mantêm estado necessitam de um motor de inferência. O motor de inferência para além de permitir a verificação do conjunto de condições que constituem cada regra, permite também o raciocínio sobre o estado do sistema. Para garantir a rapidez do processo de inferência podem ser usadas as solucções aplicadas aos sistemas de produção, tais como algoritmos de indexação de regras. O algoritmo *RETE* desenvolvido por Charles Forgy em 1982 é um dos mais conhecidos. O motor de inferência poderá ainda ter que lidar com a incerteza provocada pela especificação de algumas regras pouco precisas ou incoerentes.

Uma outra funcionalidade fundamental que pode degradar o desempenho do sistema é a reordenação das unidades de tráfego fragmentadas. Por exemplo, o protocolo *IP* e o *TCP* permitem a fragmentação de unidades de tráfego. Desta forma, o sistema pode ser iludido se não usar um mecanismo que faça a reordenação das unidades de tráfego antes de serem analisadas. No *snort* é feita a reordenação utilizado *plugins* de préprocessamento.

Um sistema de detecção de intrusões baseado na análise do tráfego da rede em tempo real que mantenha estado, que permita a análise de *payloads*, que permita a reordenação de unidades de tráfego fragmentadas, que permita relacionar temporalmente eventos, que não tenha um desempenho exponencialmente degradado face ao aumento do número de regras e faça tudo isto com um mínimo de perda de unidades por analisar, é certamente um bom sistema de detecção de intrusões e uma grande contribuição para a segurança dos sistemas informáticos. É exactamente este o principal objectivo da minha dissertação de mestrado.