# IDS - Sistemas de Detecção de Intrusão

Luiz Arthur

Atualmente nossa sociedade esta a cada dia mais dependente dos computadores e das redes de dados que os ligam. Isto se dá devido ao fato de que são nesses equipamentos que está contido o maior bem da sociedade atual que é a informação.

Então é muito importante manter um sistema computacional, principalmente que esteja conectado a uma rede (Internet) seguro, de forma que as informações contidos nesses sempre se mantenham integras, com um alto nível de confidencialidade e disponibilidade.

Assim, a segurança da informação em sistemas computacionais atuais não podem mais depender apenas de sistemas anti-vírus, ou apenas alguns Firewalls. São necessários sistemas mais complexos que analisem a rede e interajam com está e seus elementos (hosts) de forma interativa, visando uma maior segurança da informação.

Neste cenário surgem os Sistemas de Detecção de Intrusão. Pois, fazer a monitoração contra tentativas de ataques e intrusão está se tornando fundamental para a segurança por exemplo, de uma empresa ou organização.

Assim, um IDS ou em português SDI é basicamente um sistema capaz de analisar o trafego da rede ou o conteúdo de um computador e procurar possíveis tentativas de ataques.

Não é uma tarefa muito fácil descobrir se um computador ou uma rede foi invadido. Para saber se um computador ou uma rede foi invadido há necessidade de analisar a rede verificando uma série de informações, como:

- Registros de *log* (registro de armazenamento de eventos);
- Processos não autorizados;
- Contas de usuários;
- Sistema de Arquivos alterados;
- e outros.

Descobrir se um computador ou uma rede foi invadido é uma tarefa muito difícil e demorada para se fazer, e os responsáveis pela segurança da rede podem não dar conta de fazer tudo, havendo então a necessidade de se utilizar os Sistemas de Detecção de Intrusão (SDI) para fazer essas funções.

O modo mais simples de definir um IDS seria descrevê-lo como uma ferramenta especializada, capaz de ler e interpretar o conteúdo de arquivos de $log$ de roteadores, Firewalls, servidores e outros dispositivos de rede e gerar um alerta sobre um possível ataque, identificando se existe alguém tentanto ou não invádir o sistema computacional.

Um SDI normalmente é formado por um banco de dados no qual são armazenados às assinaturas (códigos) de ataques, isto é bem semelhante ao funcionamento de um antivírus que contém as assinaturas ou códigos dos vírus, ou seja, existem estruturas de dados que, por exemplo, se forem encontradas em um fluxo de rede irão identificar que esta acontecendo um determinado ataque.

Tais assinaturas devem ser constantemente atualizadas assim como em um antivírus para que não passe nenhum código novo despercebido, ou o sistema não irá identividar um ataque recem criado (um novo ataque).

Se for detectada qualquer tentativa de ataque suspeita, o IDS deve gerar um alerta para o administrador do sistema computacional, esta resposta pode ser um e-mail, um aruqivo de log, emitir um alerta sonoro, alguma tipos de ações automáticas para tentar avisar sobre o ataque ou mesmo tomar uma atitude para tentar bloquear o ataque, variando desde a desativação de links da Internet até a ativação de rastreadores e fazer outras tentativas de identificar atacantes. É claro que essas respostas são geradas de acordo com as regras configuradas no Sistema de Detecção de Intrusão.

Bem antes de continuar falando sobre IDSs devemos ter em mente um problema causado por sistemas de detecção, que é o de gerar alertas falsos ou de simplesmente não gerar uma alerta em um momento de invasão.

**Falso Positivo e Falso Negativo**

Falso positivo é quando o sensor do IDS gera um alerta que não devia, ou seja, classifica uma atividade normal na rede como sendo um ataque. Quanto menos falsos positivos um IDS gerar melhor, pois quando um administrador examina um IDS e vê um monte de alertas este pode pensar que o sistema está sendo atacado, e na verdade esses alertas são falsos, isto se dá devido a má configuração do IDS, por exemplo. Outro problema gerado por este tipo de problema é que como o IDS gera alertas falsos sobre ataques que não estão ocorrendo o administrador pode futuramente ignorar um ataque real pensando que este também é um Falso Positivo.

Falso negativo é quando ocorre um ataque e o sensor do SDI não gera nenhum alerta. Existem algumas causas que podem gerar falsos negativos são elas: um ataque desconhecido, uma sobrecarga ou configuração errada no sensor. Falsos negativos não devem ocorrer, pois um falso negativo pode ser um ataque que passa despercebido pelo IDS e pode comprometer a segurança da rede ou das informações contidas nos sistemas computacionais. Para evitar este tipo de problema é recomendável sempre mantar as assinaturas atualizadas, assim como se fosse um anti-vírus.

## Tipos de Sistemas de Detecção de Intrusão

Conforme a sua arquitetura, os SDI podem ser: baseados em redes, baseados em host e distribuídos.

## Sistemas de Detecção de Intrusão Baseado em Host

Os Sistemas de Detecção de Intrusão baseados em *Host* (SDIH ou em inglês HIDS) foram os primeiros IDS que surgiram, seu objetivo é monitorar todas as atividades existentes em um determinado *host*. Sendo que este captura somente o trafego destinado ou único host (e não a uma rede) não gerando muita carga para a CPU.

Os SDIHs podem atuar em diversas áreas dentro de um mesmo host, como por exemplo, analise de todo o sistema de arquivos, monitoramento da atividade da rede, monitoramento de atividades de *login* e do usuário. Essas ferramentas analisam os sistemas através de dados coletados na própria máquina.

## Sistemas de Detecção de Intrusão Baseado em Rede

Um sistema de detecção de invasão de rede é uma máquina ou um software que monitora conexões de rede à procura de sinais de invasão, negação de serviço, violações de diretivas ou outra atividade incomum especificada pelo administrador.

O Sistema de Detecção de Intrusão de Rede também chamado de SDIR ou em inglês NIDS, observará uma rede ou um grupo de máquinas.

Os NIDS trabalham com interfaces de rede em modo promiscuo, ou seja, todos os pacotes que circulam pela rede serão capturados pelo IDS, independente do destino. Esses pacotes que forem capturados serão analisados um-a-um, para que o IDS saiba se tais pacotes contém informações ditas normais ou se podem ser considerados uma tentativa de ataque.

Os NIDS são compostos geralmente por dois componentes, são eles: os sensores e as estações de gerenciamento.

Os sensores são dispositivos (de hardware ou software), colocados em segmentos distintos da rede, para farejar e analisar a rede procurando assinaturas que poderiam indicar um ataque.

As estações de gerenciamento podem possuir uma interface gráfica e são responsáveis por receber os alarmes dos sensores informando ao administrador da rede sobre ataques, por exemplo.

É claro que os dois podem ser instalados em uma mesma máquina, dependendo do tipo do IDS.

Vantagens dos NIDS são:

- Que um único sensor pode monitorar toda a rede ou um segmento da rede o que permite uma economia na sua implementação;
- Os NIDS não interfere no trafego da rede, somente analisa as informações que estão passando pela rede;
- É invisível para os invasores, pois não gera nenhuma resposta que possa indicar sua presença.

Desvantagens dos NIDS são:

- Se tiver muito trafego na rede o IDS pode não conseguir ser rápido o suficiente par monitorar todo o trafego que circula pelo segmento da rede e um ataque pode passar despercebido;
- Alguns NIDS têm problemas em redes com *switches,* pois o *switch* cria uma conexão direta entre a origem e o destino do pacote, deste modo o sensor não consegue capturar todos os pacotes;
- Não reconhece dados criptografados, pois não consegue comparar as regras com o conteúdo do pacote;
- Alguns NIDS não conseguem remontar os pacotes fragmentados (pacotes divididos em varias partes); Não consegue informar se o ataque foi ou não bem sucedido

Vantagens de HIDS são:

- Podem trabalhar em redes com criptografia, como analisa o *host,* verifica os dados antes de serem criptografados ou depois de serem descritografados;
- O HIDS consegue monitorar eventos locais, como alterações em arquivos do sistema;
- Não tem problemas em redes com *switches*, pois analisa o conteúdo que entra e sai do *host* no qual está instalado, não importa se o *switche* envia os pacotes para a rede inteira ou somente para a máquina destino;
- Detecta cavalos de tróia e outros ataques que envolvem brechas na integridade dos softwares.

Desvantagens dos HIDS são:

- Dificuldade de gerenciar vários HIDS;
- O atacante que conseguir invadir o *host* em que o SDI está instalado pode comprometer ou desabilitar o SDI;
- Não pode detectar *scan* de portas ou outra ferramenta de varredura que tenha como alvo toda a rede, porque só analisa os pacotes direcionados ao *host* em que está instalado;
- Se a quantidade de informação for muita, pode ser necessário adicionar mais área (espaço em disco), para o armazenamento dos *logs*;
- O SDIH influência no desempenho do *host* em que está instalado porque consome recursos para o processamento das informações e regras do IDS.

**SDI distribuído**

Os Sistemas de Detecção de Intrusão Distribuídos (SDID) funcionam em uma arquitetura gerenciador/investigação. Este tipo de sistema utiliza sensores, os quais ficam em locais distantes e se reportam a uma estação central de gerenciamento.

Estes sensores podem agir no modo promiscuo como os sensores de um HIDS, ou podem agir no modo não-promiscuo como os de um HIDS ou uma combinação entre os dois.

Os sensores destes tipos de sistemas devem mandar as informações a uma estação central de gerenciamento. Nesta estação central de gerenciamento é feito um *upload* dos *logs* de ataques e armazenados em um banco de dados.

Algumas vantagens do uso de SDID são: O Downloads de novas assinaturas de ataque pode ser feito nos sensores, de acordo com a necessidade; As regras de cada sensor podem ser personalizadas para atender as suas necessidades individuais.

Uma desvantagem do uso de SDID é que para fazer a comunicação entre os sensores e a estação central de gerenciamento deve se utilizar algum tipo de segurança extra, como criptografia, tecnologia VPN ou uma rede privada.

**Detecção de invasão baseado em assinaturas**

Este método trabalha coletando dados (de rede ou host) e compara com regras (que identificam os ataques), que são os códigos (assinaturas) do IDS ao qual se está utilizando. Essas assinaturas são fornecidas pelo desenvolvedor do IDS, mas se houver necessidade também pode se desenvolver assinaturas próprias ou adquiri-las de sites especializados em segurança e adaptar de acordo com o IDS.

A detecção de intrusão por assinatura normalmente gera um menor número de falsos positivos, ou seja, alertas falsos se comparados aos demais métodos de detecção. O método de detecção baseado em assinaturas é por sua vez mais rápido e especifico na procura por padrões de ataques já conhecidos, mas quando aparecem novos padrões de ataques, este método se torna ineficiente.

Uma assinatura é composta por uma seqüência de *bytes* que representam ou especificam um ataque. Quando é encontrado no trafego da rede algum código que seja idêntico às assinaturas, é uma provável indicação de ataque. Os SDI utilizam esta abordagem para a detecção de intrusão, através da utilização de expressões regulares, análise de contexto ou linguagens de assinatura, os pacotes de rede são analisados e comparados com uma base de dados de assinaturas.

**Detecção baseado em anomalias (comportamento)**

Este método de detecção tem um registro do histórico das atividades que são consideradas normais na rede, a partir desses registros do histórico é que o sistema descobre o que é permitido ou não na rede, se encontrar algo que não está dentro do padrão do sistema, é gerado um alerta.

Este método de detecção é mais complicado para se configurar, pois é muito difícil saber o que é ou não padrão em uma determinada rede.

A principal vantagem deste método de detecção é que ele é capaz de detectar qualquer tipo de ataques novos e desconhecidos.

Mas por outro lado a desvantagem é que ele gera um número muito grande de alertas. A maioria desses alertas podem ser falsos, ou seja, é apenas uma atividade que o usuário não costuma a fazer, e que o sistema não tinha registro desta atividade.

Por exemplo, o método de detecção baseado em anomalias tem um registro no qual um usuário só faz *login* em um determinado sistema durante o dia, se acaso for detectado que este usuário ta fazendo *login* no sistema de madrugada, deve emitir um alerta.

## OSSEC HIDS

O ossec hids é um sistema de detecção de intrusão baseado em Host de código fonte aberto que possui como desenvolvedor principal o brasileiro Daniel Cid.

O OSSEC HIDS realiza operações de analise de Logs, integridade de sistemas, monitoração de registros do Windows, detecção de rootkits, alertas e resposta ativa (regras no firewall). É possível instalar o OSSEC localmente, para monitorar uma única máquina, mas se for necessário monitorar várias máquinas é possível configurar uma como servidor e as demais como agentes, sendo que as agentes iram enviar informações para o gerente que fica responsável por analisar e apresentar as informações geradas pelos IDS, isto dá uma alta escalabilidade ao IDS.

Suporta os seguintes tipos de logs: Unix pam, sshd (OpenSSH) , Unix telnetd, Samba, Su, Sudo, Proftpd, Pure-ftpd, vsftpd, Solaris ftpd, Imapd and pop3d, Horde imp, Named (bind), Postfix, Sendmail, Iptables firewall, Solais ipfilter firewall, AIX ipsec/firewall, Netscreen firewall, Snort IDS, Apache web server (access log and error log), IIS web server, Squid proxy, Windows event logs, Generic unix authentiction (adduser, logins, etc).

O OSSEC pode ser instalado nos seguintes Sistemas Operacionais: OpenBSD, Linux, FreeBSD, Solaris, MacOSX, Windows XP/2000 ( no caso do windwos é somente o agente).

## OSSEC HIDS

O OSSEC-HIDS pode ser obtido na site: www.ossec.net

fim

fim