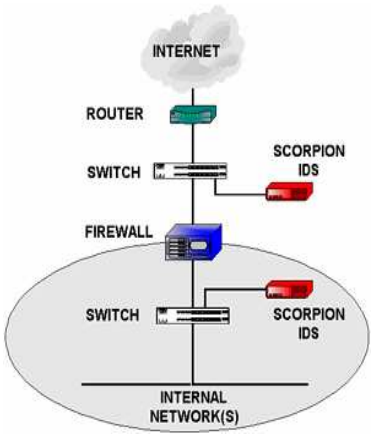
SEGURANÇA

IDS – Sistema de detecção de intrusos

Com a evolução da Internet houve a necessidade crescente por sistemas que garantissem a total segurança dos dados. Intruso é todo indivíduo que tenta acessar um recurso sem a devida permissão. Os sistemas de detecção de intrusos ou IDS (Intrusion Detection Systems), permitem a verificação da ocorrência de tentativas de invasão de redes privadas, de forma prevenir ataques que comprometam os sistemas ou recursos de rede.

A solução IDS traz um conjunto de ferramentas que, aplicado com o Firewall proporciona a monitoração de tráfego tanto de entrada quanto de saída das informações. Desta maneira é possível saber:

- Quais serviços estão sendo atacados ;
- Qual a origem dos ataques ;
- Portas e protocolos de acesso utilizados na tentativa de invasão;
- Software e Backdoors os quais o invasor tentou utilizar;
- Ocorrências hostis em geral;
- Tentativa de monitoração remota por ping ou softwares de rastreamento de portas;
- Acesso interno de sua rede a servidores IRC, ICQ, MSN, Yahoo Messenger, além outras informações.



Os acessos ou ações que configuram tentativas de invasão são armazenadas em banco de dados para permitir sua análise minuciosa. Os dados são agrupados em nível de protocolo para facilitar ao administrador da rede sua visualização por ocorrência, cada informação pode então ser avaliada individualmente, que pode enviada para o e-mail do administrador.

Essa ferramenta possibilita a visualização do histórico de ocorrências reportadas por uma interface web fácil e intuitiva.

Por que usar?

As razões por que você poderia usar os sistemas de detecção de intrusos são relativamente diretas, você deve se perguntar o seguinte:

- Quero proteger meus dados e a integridade dos seus sistemas ?
- Tenho certeza se algum dado nos servidores não foi violado ?
- Os servidores empresa na Internet estão sendo monitorados por alguém não autorizado ?
- Tenho certeza que não tive nenhum ataque vindo da Internet ?
- Quantas tentativas de ataques externos foram feitos no último mês ?
- Será que tem alguém dentro da empresa tentando acessar dados que não deveria ?

Nem sempre pode-se proteger a integridade dos dados em um ambiente com internet simplesmente usando-se apenas mecanismos como senhas e segurança de arquivos. Um sistema de segurança adequado é o primeiro passo para garantir a proteção dos dados.

Assim como um alarme avisa a possível tentativa de roubo, um sistema de detecção de intrusão na rede, avisa quando da presença de algum tráfego suspeito ou de uma provável vulnerabilidade nos sistemas operacionais ou aplicativos.