IDS - Sistema de Detecção de Intrusos

+ O conceito de IDS, que pode estar funcionando em um host ou até mesmo em uma rede, é que ele acusa estar acontecendo um scanneamento de portas, exploração ou sequer interação com um determinado serviço.
Ele é basicamente um dedo-duro, pois alerta o admin.

+ Mas ele realiza esse aviso baseado nas regras que estão pré configuradas

+ Existe também o IPS, que é um sistema de prevenção
A diferença é que o IPS realiza alguma ação preventiva, ele não apenas avisa.

+ O sistema usado para o estudo no caso foi o snort

+ O diretório fica armazenado na máquina em /etc/snort

+ Suas regras ficam guardadas em /snort/rules

+ As configurções estão armazenadas no arquivo snort.conf

+ A maneira de iniciar as regras no terminal é:

```
snort -A fast -q -h 192.168.0.0/24 -c snort.conf
```

-A pelo tivo de arquivo
-h para setar a rede
-q de quiet para não mostrar tanta informação na nossa tela

+ Para verificar o que está ocorrendo, podemos ver no arquivo alert que fica em /var/log/snort

+ Ao executarmos o tail -f alert, poderemos ver em tempo real qualquer ação do atacante