

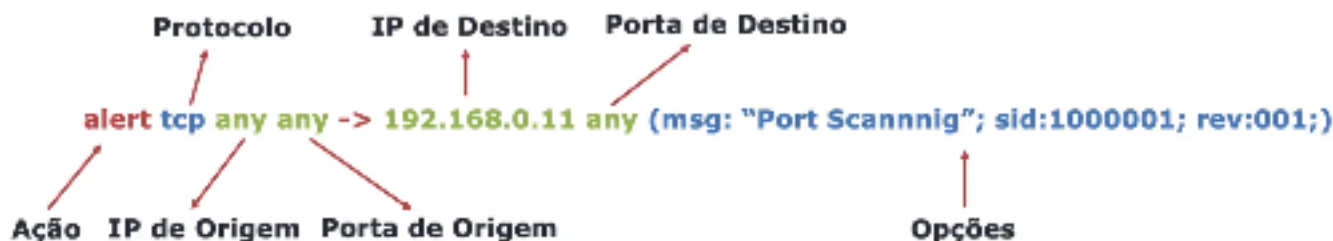
# Entendendo e Criando Regras de IDS

+ Mostraremos o exemplo de montagem de regras do snort

+ O comando para verificar os alertas do snort é o seguinte:

```
snort -A console -q -n 192.168.0.0/24 -c snort.conf
```

+ Segue abaixo o modelo padrão de uma regra simples



→ sendo a mensagem uma declaração qualquer, que podemos escolher à vontade

→ sid é um identificador (é necessário que sempre haja pelo menos 5 zeros no meio)

→ rev é o marcador da revisão (quantas vezes modificamos a regra)

+ Na prática, fez-se com o nano o arquivo `dsec.rules`

+ Abriu-se o arquivo padrão de configurações do snort com o nano no diretório `/etc/snort` e habilitou-se o `dsec.rules` da seguinte maneira:

```
include $RULE_PATH/community-web-client.rules
include $RULE_PATH/community-web-dos.rules
include $RULE_PATH/community-web-iis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/dsec.rules

#####
# Step #B: Customize your preprocessor and decoder alerts
# For more information, see README.decoder preproc rules
#####

# decoder and preprocessor event rules
# include $PREPROC_RULE_PATH/preprocessor.rules
```

+ Exemplo de regras incluídas

A captura de tela mostra o editor GNU nano 4.3 abrindo o arquivo `dsec.rules`. O conteúdo exibido é:

```
alert tcp any any -> 192.168.0.11 any (msg: "Possivel Port Scanning";sid:1000001;rev:001;)
alert tcp any any -> 192.168.0.11 22 (msg: "Pacote SYN enviado ao SSH";flags:S;s Sid:1000002;rev:001;)
alert tcp any any -> 192.168.0.11 80 (msg: "Acesso ao arquivo robots.txt";content:"robots.txt";sid:1000003;rev:001;)
```

→ Com essas regras, o IDS identificará

- qualquer pacote TCP que saia de qualquer endereço e qualquer porta e chegue no endereço 192.168.0.11 em qualquer porta como um possível port scanning.
- Qualquer pacote TCP que saia de qualquer endereço chegue ao endereço 192.168.0.11 na porta 22 como pacote SYN enviado ao ssh.
- Qualquer pacote TCP que saia de qualquer endereço e de qualquer porta e chegue ao 192.168.0.11 na porta 80 e acesse o robots.txt

