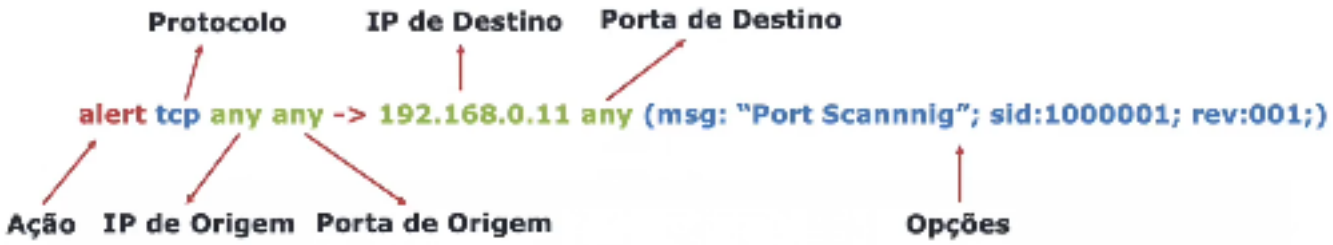
Entendendo e Criando Regras de IDS

+ Mostraremos o exemplo de montagem de regras do snort

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

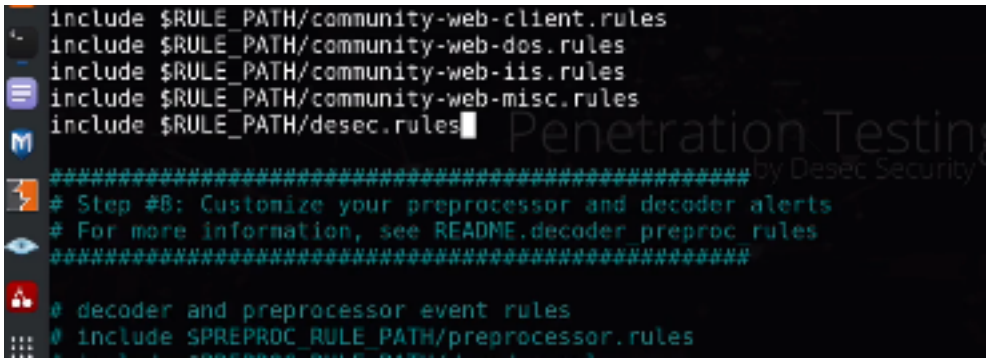
```
snort -A console -q -n 192.168.0.0/24 -c snort.conf
```

+ Segue abaixo o modelo padrão de uma regra simples

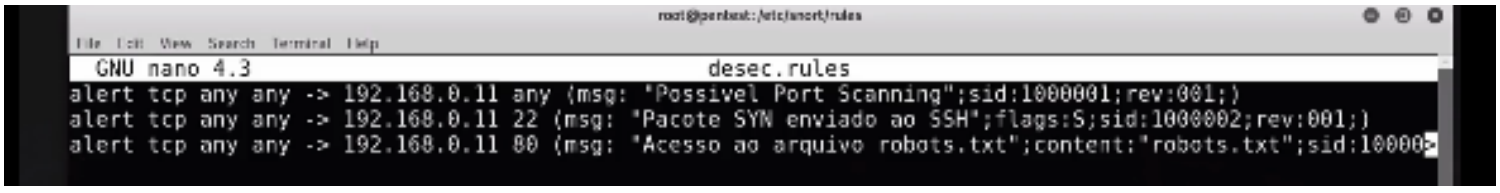


→ sendo a mensagem uma declaração qualquer, que podemos escolher à vontade
→ sid é um identificador (é necessário que sempre haja pelo menos 5 zeros no meio)
→ rev é o marcador da revisão (quantas vezes modificamos a regra)

+ Na prática, fez-se com o nano o arquivo desec.rules
+ Abriu-se o arquivo padrão de configurações do snort com o nano no diretório /etc/snort e habilitou-se o desec.rules da seguinte maneira:



+ Exemplo de regras incluídas



→ 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