Segurança e Confiabilidade

# Relatório Projeto 3

## Snort

---

Engenharia Informática
2018/2019


**Grupo 17**

**Diogo Nogueira, Nº 49435**

**Filipe Capela, Nº 50296**

**Filipe Silveira, Nº 49506**

# Índice

# Regras definidas para o comando Snort

Para poder alertar o sistema de que estão a ser feitos pedidos indevidos, foi pedido ao grupo para definir alertas que pudessem notificar para os seguintes casos:

***"Deve ser gerado um alerta para a consola quando forem recebidas na máquina servidora 3 ou mais ligações TCP para portos inferiores a 1024 durante um intervalo de meio minuto."***

Para este caso foi produzido o seguinte alerta:

```
alert tcp any any -> 10.101.149.0/23 1:1023 (flags: S; msg:"Mais de 3 ligações efetuadas para os portos 1 a 1024"; sid:12344; rev:0;)
event_filter \
        gen_id 1, sig_id 12344, \
        type both, \
        track by_dst, \
        count 3, seconds 30
```

Neste alerta tem-se que, para todas as tentativas de conexão feitas para o servidor, para os portos 1 até 1024, estas serão contabilizadas até um total de 3 por cada 30 segundos. Se for atingido o máximo de 3 pedidos, o alerta será lançado. O mesmo processo é repetido após terminados os 30 segundos e após serem detectados outros 3 pedidos de conexão (mesmo sendo de IP's diferentes, pois temos o uso do ***"by_dst"***). Denote-se que o facto de estar a ***"flag S"*** ativada, indica que só deve ser considerado o SYN da conexão para fazer a contagem de ligações feitas.

***"Deve ser gerado um alerta para a consola sempre que forem recebidas 5 ligações da mesma máquina emissora para o porto do servidor, durante um intervalo de 15 segundos."***

Para este caso foi produzido o seguinte alerta:

```
alert tcp any any -> 10.101.149.0/23 23232 (flags:S; msg:"Tentativa de descodificacao de password"; sid:12345; rev:0;)
event_filter \
        gen_id 1, sig_id 12345, \
        type threshold, \
        track by_src, \
        count 5, seconds 15
```

Neste alerta, se forem feitas cinco ou mais ligações para o servidor, o snort deve alertar para este facto, uma vez que se assemelha a um ataque de descodificação de passwords. Neste caso, é lançado o alerta por cada conjunto de 5 ligações observadas (uso do ***"threshold"***) e que venham da mesma máquina (uso do ***"by*_src"**). Denote-se que o facto de estar a ***"flag S"*** ativada, indica de que só deve ser considerado o SYN da conexão para fazer a contagem de ligações feitas.

# Forma de invocação do comando Snort

Primeiramente, inicializou-se o terminal numa das máquinas pedidas (na sala 1.3.12 ou 1.2.15) e, dentro da pasta onde se encontra o ficheiro "*snort.config"* executou-se o seguinte comando:

*sudo /usr/sbin/snort -c snort.config -A console*

Após esse momento verificou-se então que o *snort* fica à espera de que sejam feitas ligações TCP ou que sejam recebidos *pings* de outras máquinas (dependendo dos alertas definidos), e, quando se verificar alguma das condições tratadas pelos alertas, o *snort* lançará a devida mensagem.

# Método de teste e observações

## Computadores utilizados

Para testar dispôs-se de dois computadores, localizados na sala de aula 1.3.12, ou seja, estes fazem parte da sub-rede pedida, 10.101.149.0/23.

Visando simplificar a compreensão, estes denominam-se Computador A (10.101.149.63) e Computador B (10.101.149.64).

No computador A foi inicializado o servidor *MsgFileServer* no porto 23232 e, noutro terminal, inicializou-se o utilitário snort.

## Testes realizados

A partir do computador B foram feitos vários pedidos de ligação para o computador A, sendo estes separados em duas partes.

Foram feitas 5 ligações TCP, feitas do seguinte modo:

*telnet 10.101.149.63 23232*

As 5 ligações foram feitas aproximadamente ao mesmo tempo, e, o esperado verificou-se, pois, no terminal onde estava a correr o utilitário snort foi lançado o alerta referente a serem feitas 5 ou mais ligações TCP num curto espaço de tempo.

Numa segunda parte foram feitas 3 ligações TCP também, mas para o porto 10 (pois está entre 1 e 1024). Este tinha a seguinte constituição:

*telnet 10.101.149.63 10*

As ligações foram feitas aproximadamente ao mesmo tempo e o alerta que deveria ser lançado apareceu no terminal tal como era de esperar.

# Imagens ilustrativas

Nesta página encontram-se expostas as imagens que demonstram aquilo que foi testado.

Na primeira imagem constam os pedidos de ligação, sendo possível observar tanto as cinco primeiras conexões ao servidor (alojado no porto 23232) como as três ligações ao porto 10.

Na segunda imagem verifica-se que foram lançados os devidos alertas no *snort*, o que demonstra que está bem configurado.

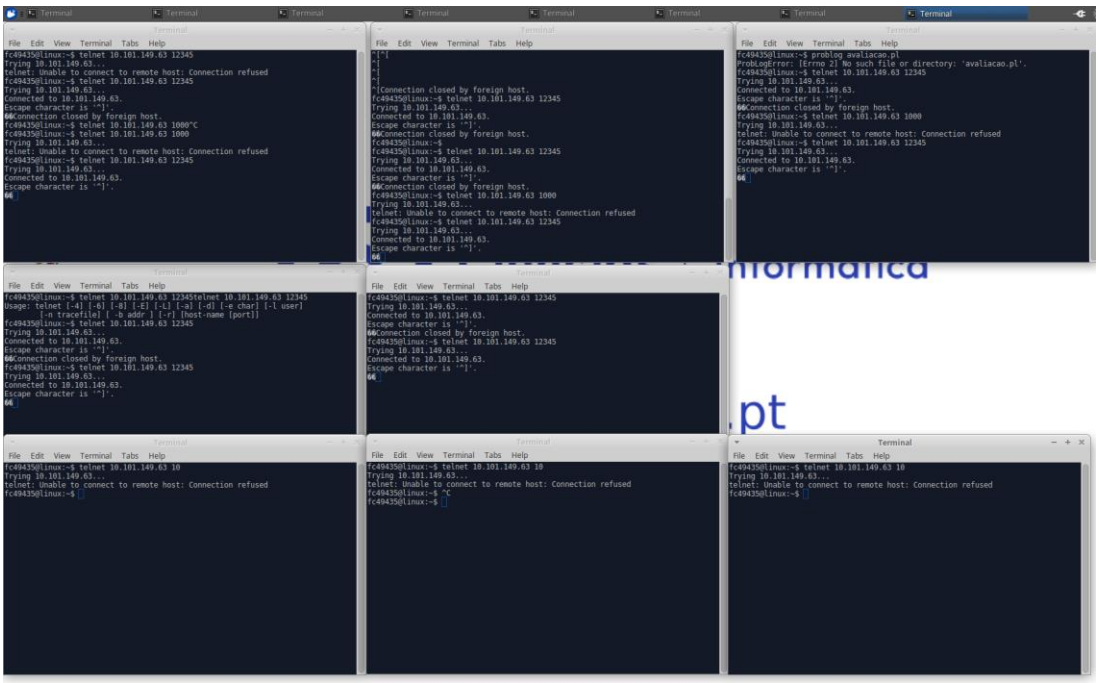

*Figura 1 - Terminais Computador B*

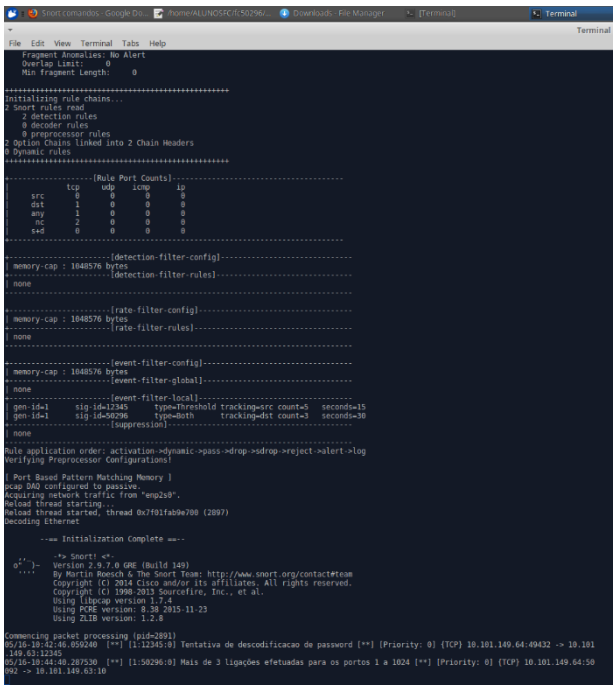

*Figura 2 - Lançamento de alertas (Snort)*