

**Relatório de Segurança e Confiabilidade**

Trabalho 3

Engenharia Informática

Grupo 51

João David n49448

João Marques n49038

Luís Moreira n49531

Índice

[Parte I – iptables 3](#_Toc8732406)

[Regras utilizadas 3](#_Toc8732407)

[Observações realizadas 3](#_Toc8732408)

[Parte II – snort 4](#_Toc8732409)

[Configuração 4](#_Toc8732410)

[Observações realizadas 5](#_Toc8732411)

# Parte I – iptables

## Regras utilizadas

## Observações realizadas

# Parte II – snort

## Configuração

A forma utilizada para invocar o comando snort foi:

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

O ficheiro snort.config contêm as seguintes configurações:

preprocessor frag3\_globalpreprocessor frag3\_engine

#A

alert tcp any any -> any 1:1023 (msg:"server session"; sid:20180405;rev:0;)

event\_filter \

gen\_id 1, sig\_id 20180405, \

type both, \

track by\_dst, \

count 3, seconds 30

#--------------------------

#B

alert tcp any any -> any 23456 (msg:"server session"; sid:20181305;rev:0;)

event\_filter \

gen\_id 2, sig\_id 20181305, \

type threshold, \

track by\_src, \

count 5, seconds 15

No primeiro caso (#A), pretende-se receber alertas de ligações TCP para portos inferiores a 1024 (usa-se 1:1023), ligações essas que não têm ter origem na mesma máquina, posto isto, na definição do filtro, faz-se track by\_dst, e type both, de forma a que seja gerado apenas um alarme nesse meio minuto.

No segundo caso (#B), pretende-se sempre que forem recebidas 5 ligações da mesma máquina emissora (track by\_src) para o porto do servidor (que no caso do trabalho realizado é o 23456), durante um intervalo de 15 segundos ,deve haver um alerta por cada conjunto de 5 ligações observadas, portanto é necessário usar o type threshold.

Em ambos os casos, não há especificação de ip’s, nem de portos de origem, logo esses campos ficam any.

## Observações realizadas