

Relatório de Segurança e Confiabilidade

Trabalho 3 - snort

Engenharia Informática

Grupo 51

João David n49448

João Marques n49038

Luís Moreira n49531

Índice

Parte II – snort.....	3
Configuração	3
Testes e Observações.....	4

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 contém as seguintes configurações:

```
preprocessor frag3_global
preprocessor frag3_engine

alert tcp any any -> any 1:1023 (msg:"VARRIMENTO PORTOS";
sid:20190405;rev:0;)

event_filter \
  gen_id 1, sig_id 20190405, \
  type both, \
  track by_dst, \
  count 3, seconds 30

#-----

alert tcp any any -> any 23456 (msg:"DESCOBRIR PASSWORD"; flags:S;
sid:20191305;rev:0;)

event_filter \
  gen_id 1, sig_id 20191305, \
  type threshold, \
  track by_src, \
  count 5, seconds 15
```

No primeiro caso (VARRIMENTO PORTOS), 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 (DESCOBRIR PASSWORD), 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. Como se pretende que seja lançado o alerta quando alguém tenta descobrir a password de alguém, é necessário ter a flag S, que corresponde ao SYN que é ativado no handshake do TCP quando se estabelece uma ligação.

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

Testes e Observações

De forma a testar o funcionamento das configurações, foi ligado o MsgFileServer num computador no porto 23456 e a partir de outros dois computadores foram ligados o MsgFile (client). Os computadores utilizados foram os da sala 1.2.15. Tanto o servidor como o cliente, estavam a usar as policies da VM.

Para testar o “VARRIMENTO PORTOS”, os clientes tentaram conectar-se mais que 3 vezes a portos no intervalo [1,1023] durante 30 segundos, e verificou-se que apenas foi lançado 1 alerta durante os 30 segundos.

Para testar o caso “DESCOBRIR PASSWORD”, em vez de a máquina cliente se conectar ao intervalo de portos anteriormente referido, foi conectada ao porto listen utilizado no servidor (23456), os clientes tentaram conectar-se mais que 5 vezes, durante 15 segundos, e verificou-se que a cada 5 tentativas de ligação do mesmo cliente, era lançado um alerta para esse mesmo cliente.

Logo, a partir dos resultados dos testes, é possível concluir que o snort está a lançar os devidos alertas, e a funcionar correctamente.