Ciências ULisboa

Faculdade de Ciências da Universidade de Lisboa

Segurança e Confiabilidade

2016/2017

snort

Grupo 005

Autores

Francisco João Guimarães Coimbra de Almeida Araújo, n.º 45701

João Marques de Barros Mendes Leal, n.º 46394

Joana Correia Magalhães Sousa, n.º 47084

Regras snort:

event_filter gen_id 1, sig_id 20160405, type limit, track by_src, count 1, seconds 60

alert tcp any any -> any :4096 (msg:"varrimentos de portos"; sid:20160405; rev:0; flags:S; detection_filter: track by_src, count 5, seconds 60;)

event_filter gen_id 1, sig_id 20160406, type threshold, track by_src, count 5, seconds 45

alert icmp any any -> any any (msg:"tentar descobrir uma password de acesso ao servico"; sid:20160406; rev:0; detection_filter:track by_src, count 1, seconds 45;)

Forma de invocação

Para invocar as regras snort é necessário abrir um terminal na pasta onde o ficheiro com estas regras está gurdado e executar o comando no terminal:

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

Método de teste e observações

Para a regra que gera avisos na máquina servidora ao fim de 5 pedidos TCP num porto inferior a 4096 após 1 minuto foram feitos pedidos telnet para um porto inferior a 4096 a partir de uma máquina no laboratório 1.3.12 e verificámos que as mensagens surgiam como previsto. Em seguida parámos os pedidos telnet por 1 minuto e ao fim desse intervalo voltámos a fazê-los e observámos que as mensagens apenas voltavam quando ao fim de 5 pedidos, tal como devia ser. Também aplicámos este processo utilizando um porto superior a 4096, o 5000, e observámos que não surgiam quaisquer avisos, extamente como devia ser.

Para a testar a regra que gera um alerta para a consola sempre que forem recebidas 5 ligações da mesma máquina emissora para o porto do servidor, durante um intervalo de 45 segundos, fizemos ping para máquina servidora a partir do mesmo computador usado anteriormente e observámos que ao fim de 5 ligações começavam a surgir as mensagens, exatamente como devia. Em seguida esperámos 45 segundos para voltar a fazer ping e as mensagens só começaram a aparecer ao fim de 5 ligações, tal como previsto.