Parte II:
Relatório snort

Segurança e Confiabilidade
2021/2022
Trabalho 2

Henrique Barata fc54387

Hugo Marques fc54400

João Vidal fc54467

Foram criadas 2 regras snort para detetarem alguns dos possiveis ataques contra o Servidor Trokos, inicializado na maquina MServer no por 45678.

A primeira regra deve ser gerar um alerta para a consola quando forem recebidas na máquina servidora 5 ou mais ligações TCP para portos inferiores a 1024 durante um intervalo de um minuto (pode indicar um varrimento de portos) (NOTA: nesse minuto deve ser gerado apenas um alarme, qualquer que seja a máquina que inicia as ligações, i.e., as ligações não têm todas de ter origem na mesma máquina).

alert tcp any any -> 10.101.204.4 :1023 (msg:" varrimento de portos"; sid:1; ver:0;)

**event_filter **

**gen_id 1, **

**sid_id 1, **

**type both, **

**track by_dst, **

**count 5, **

seconds 60

type both: queremos um alerta quando se observar 5 eventos num intervalo de tempo de 60 segundos

track by_dst: o filtro é aplicado ao IP destino, o IP do server

Na segunda regra deve ser gerado um alerta para a consola sempre que forem recebidas 4 ligações da mesma máquina emissora para o porto do servidor, durante um intervalo de 20 segundos (pode indicar que estão a tentar descobrir uma password de acesso ao serviço) (NOTA: deve haver um alerta por cada conjunto de 4 ligações observadas).

alert tcp any any -> 10.101.204.4 45678 (msg:"tentativa de adivinhar password"; sid:2; ver:0;)

**event_filter **

**gen_id 1, **

**sig_id 2, **

**type both, **

**track by_src, **

**count 8, **

seconds 20

type both: queremos um alerta quando se observar 4 eventos num intervalo de tempo de 20 segundos

count passa a 8 por cada ligação tcp conta com dois pacotes (4*2)

track by_dst: o filtro é aplicado ao IP destino, o IP do server

Foi corrido o mesmo cliente com a password errada para a testagem desta regra, mais de 4 vezes.