Snort

Grupo 51
Henrique Catarino – 56278; Miguel Nunes – 56338; Vasco Maria – 56374

Regras:

alert tcp any any -> any :1024 (msg:"5 TCP in a minute in ports <1024"; sid:1; rev:0; threshold: type both, track by_dst, count 5, seconds 60;)
alert tcp any any -> 10.101.204.4 any (msg:"Possible NoTintol attack"; sid:2; rev:0; threshold: type both, track by_src, count 3, seconds 15;)

Invocação do Snort:

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

Análise:

O NoTintol inicializa 2000 threads, cada uma a fazer um pedido de conexão com o TintolmarketServer a cada 100 milissegundos, potencialmente até 20000 pedidos por segundo.

De acordo com os nossos testes o TintolmarketServer gastou até 10 vezes mais recursos que o NoTintol, enquanto que o NoTintol nunca usou mais de 5% do poder do processador, o TintolmarketServer estava constantemente a usar à ronda de 50% do processador.

Testes e Observações:

Para a primeira regra invocámos o Snort no MServer e abrimos os terminais de cinco outras máquinas, de cada uma destas invocámos o Tintolmarket para um port menor que 1024 do Mserver, o que ativou o alert do Snort.

Para a segunda regra invocámos o Snort e o TintolmarketServer no MServer e o NoTintol noutra máquina, o que causa um alert do Snort a cada 15 segundos como esperado.

Para mais facilmente descobrirmos a proporção de consumo de recursos do TintolmarketServer e do NoTintol testámos os dois fora da máquina virtual, porque não descobrimos como aceder o monitor de recursos dentro da VM.