Ciências ULisboa

Faculdade de Ciências da Universidade de Lisboa

Segurança e Confiabilidade

2017/2018

Relatório do Snort da Fase 3

Grupo 09

Diogo Pereira, n.º 47888

José Águas, n.º 47804

Simão Ferreira, n.º 47827

Disclaimer: Para a máquina servidora nos nossos testes foi utilizada uma máquina do DI do laboratório 1.3.12 com o IP: 10.101.149.63.

Regras definidas para o comando Snort:

Criamos um ficheiro snort.config
Atraves do comando
"$ sudo /usr/sbin/snort -c /home/ALUNOSFC/fc47827/6Semestre/Segurança/Projeto3/snort.config -A console"
realizado na consola verificamos se existem tentativas de ligações superiores as que permitimos atraves de regras descritas a frente.

O "/home/ALUNOSFC/fc47827/6Semestre/Segurança/Projeto3/snort.config" é o path até ao ficheiro onde de configuração que criamos

A flag -A serve para definir o modo de alerta, neste caso utilizamos o parâmetro console para apresentar os alertas na consola.

Regra 1:

alert tcp any any -> 10.101.148.177 :1024 (msg:"Alerta! Houveram 5 ligacoes TCP para portos inferiores a 1024!"; gid:1; sid:1; rev:1;)
event_filter gen_id 1, sig_id 1, type both, track by_dst, count 5, seconds 60

Nesta regra fazemos enviamos alerta de uma ligação TCP vinda de um IP qualquer e de um porto qualquer para o IP da máquina servidora com portos inferiores ou iguais a 1024, isto é obtido através dos ':' antes do 1024 a dar essa indicação. É dada a mensagem de alerta que queremos através do parâmetro msg, com sid a 1 e rev a 1, de notar que são diferentes da regra 2 para não ocorrerem conflitos.

Posteriormente é feito um event_filter com o gen_id e o sid_id igual a 1 de modo a representarmos a regra específica que iremos filtrar, é dado o type both para que uma vez apenas se o alerta disparar 5 vezes dentro de 60 seg.
Aqui verificamos se o destination é sempre o mesmo pois não nos interessa ver 5 ligações de IP diferentes mas sim 5 ligações para a própria máquina.

Com isto obtemos uma mensagem caso haja 5 tentativas de ligações a um porto inferior a 1024 dentro de 60 segundos.

Regra 2:

alert tcp any any -> 10.101.149.63 23232 (msg:"A

event_filter gen_id 2, sig_id 2, type threshold, track by_src, count 4, seconds 20

Nesta regra fazemos um alerta de uma ligação TCP vinda de um IP qualquer e um porto qualquer para o IP da máquina servidora no porto do servidor que já tinha sido definido para 23232. Damos também a mensagem de alerta que queremos, dando um gid, um sid e o rev igual a 2.

Posteriormente fazemos um event filter dessa regra dando-lhe o gen_id e sig_id a 2 com o tipo threshold para que possa ser mostrado o alerta por cada ligação até ao número máximo (count) a 4 e num intervalo de 20 segundos conforme o pedido no enunciado.
Neste caso o event filter vai verificando a source para apenas disparar se houver 4 ligações do mesmo PC em menos de 20 segundos.

Com isto obtemos uma mensagem sempre que houver 4 ligações do mesmo IP para a máquina servidora em menos de 20 segundos.

Método de teste utilizado e observações realizadas

Foi utilizado um ficheiro chamado snort.config com o cabeçalho: preprocessor frag3_global e preprocessor frag3_engine e com as regras acima descritas nesse ficheiro.

Os testes realizados com o iptables e snort foram realizados no computador com IP: 10.101.148.177

Para a primeira regra utilizamos o comando “telnet” de outra maquina para ir fazendo os testes, e utilizamos a nossa aplicação para verificar a segunda regra.

Observações:
Lemos que o sid devia ser um valor acima de um milhão mas devido a problemas com encontramos na realização de testes no último dia, não o podemos testar.