Segurança Informática

2021/2022
Relatório da entrega 3

Aluno FC51601 - José Sousa

Relatório relativo à configuração do IDS Snort para deteção de intrusões:

Configurações:

Evento definido para que define a gestão de ligações provenientes de qualquer máquina com destino para portos entre 1 e 2048:

- event_filter gen_id 1, sig_id 516010001, type threshold, track by_dst, count 5, seconds 120

Regra que define alerta para ligações TCP provenientes de qualquer máquina com destino para portos entre 1 e 2048:

- alert tcp any any -> any 1:2048 (flags:S;msg:"Conexao a IP abaixo de 2048 detetada";sid:5160100001;rev:0;)

Regra que define alerta para ligações TCP provenientes de qualquer máquina com destino para porto 23456:

- alert tcp any any -> any 23456 (msg:"Multiplas conexoes ao porto servidor detetadas num curto espaco de tempo"; sid:516010002;rev:0; detection_filter: track by_src, count 4, seconds 40;)

Explicação:

O evento associado à regra 516010001 define que, num espaço de 2 minutos, o Snort deve contar o número de ligações que cumpram as condições definidas na regra 516010001. Caso este número de ligações exceda 5, um alerta deve ser lançado no terminal.

A regra 516010001 define que deve ser visto pelo Snort qualquer pacote proveniente de uma máquina exterior para qualquer porto entre 1 e 2048.

A regra 516010002 define que um alerta deve ser lançado no terminal apenas após 4 ou mais ligações à porta 23456 a partir uma máquina exterior se estas ocorrerem num espaço de 40 segundos.

Testes:

Estas regras foram testadas em máquinas virtuais Linux e em hosts Windows. Nos testes aconteceram uma variedade de acontecimentos inesperados, nomeadamente a repetição de múltiplos alertas por um fator que foi consistente observado durante todos os testes. Quando estas regras foram testado com ligações ICMP, os alertas foram disparados no número esperado de ligações definido nas mesmas.
Para testar estas regras foram estabelecidas ligações com clientes e servidores simples escritos em Python, Java e com a ferramenta telnet.
Após alguma investigação, o problema com estes alertas relaciona-se com a implementação de sockets ao nível do sistema operativo. Os testes foram realizados a portas que não estavam abertas, e dependendo do sistema operativo, o número de tentativas a ser realizadas para estabelecer uma ligação TCP deve ser 5, para Windows, ou 6, para o Linux, sendo este número o fator observado em múltiplos testes. Quando testadas contra um cliente simples escrito em Java que tentava estabelecer uma ligação com apenas 1 tentativa, os alertas definidos nas regras dispararam quando deviam e no número esperado de vezes para cada regra.