Snort

Regras

Começamos por definir os *preprocessors*:

```
preprocessor frag3_global
preprocessor frag3_engine
```

E uma variável que contém o *ip* da máquina onde corre o $TintolmarketServer$:

```
var TINTOL_SERVER 10.101.204.4/8
```

A primeira regra a ser definida é a seguinte:

```
alert tcp any any -> $TINTOL_SERVER 1:1023 (msg:"Foram recebidas na
     maquina 5 ou mais ligacoes TCP para portos inferiores a 1024
    num intervalo de um minuto";threshold:type both, track by_dst,
    count 5, seconds 60;sid:10001)
```

Nesta regra definimos um alerta no server caso receba 5 ou mais ligacoes TCP para portos compreendidos entre 1 e 1023 num intervalo de um minuto. Para tal, usamos o *threshold* com tipo *both*, de forma a gerar apenas um alerta no intervalo definido. O *tracking* é feito *by_dst*, de forma a que gerado apenas um alarme, independentemente da máquina que inicia as ligações. O *count* foi definido a 5 e o intervalo a 60 segundos.

A segunda regra é:

```
alert tcp any any -> $TINTOL_SERVER 12345 (msg:"Possivel ataque da
    aplicacao NoTintol"; threshold: type both, track by_src, count
    4, seconds 15; sid:10002;)
```

Aqui o alerta é definido caso ocorram mais de 3 ligações/tentativas de ligação num intervalo de 15 segundos no porto default do $TintolmarketServer$, 12345. O principio utilizado é semelhante ao utilizador, no entanto utiliza-se *tracking by_src* para que possa ser gerado um alarme dentro do intervalo de tempo, por IP de origem, i.e., se existirem duas máquinas a correr o $NoTintol$, serão criados dois alertas dentro do mesmo intervalo de tempo. O count foi definido a 4 e o intervalo a 15 segundos.

Estes comandos foram incluídos num ficheiro *snort.conf*, com o seguinte conteúdo:

```
preprocessor frag3_global
preprocessor frag3_engine

var TINTOL_SERVER 10.101.204.4/8

alert tcp any any -> $TINTOL_SERVER 1:1023 (msg:"Foram recebidas na
     maquina 5 ou mais ligacoes TCP para portos inferiores a 1024
    num intervalo de um minuto";threshold:type both, track by_dst,
    count 5, seconds 60;sid:10001)

alert tcp any any -> $TINTOL_SERVER 12345 (msg:"Possivel ataque da
    aplicacao NoTintol"; threshold: type both, track by_src, count
    4, seconds 15; sid:10002;)
```

Execução

O ficheiro *snort.conf* foi executado através do seguinte comando:

```
sudo snort -c snort.conf -A console
```

Que permite visualizar os alertas diretamente na consola.

Teste

De forma a testar a primeira regra, foi executada a aplicação *NoTintol* em várias máquinas da rede, da seguinte forma:

```
java NoTintol 10.101.204.4 1023 2000
```

Isto é, são criadas 2000 *threads* por máquina atacante, que se tentam ligar simultaneamente ao porto 1023 do servidor *TintolmarketServer*. Verificamos que é gerado um alarme a cada intervalo de 60 segundos, independentemente do número de máquinas atacantes.

Relativamente á segunda regra, o método de teste foi semelhante, sendo que foi executada a aplicação *NoTintol* através do seguinte comando:

```
java NoTintol 10.101.204.4 12345 2000
```

Sendo feita a uma alteração para que tenha como alvo o porto default do *TintolmarketServer*. Verificamos que ao executar este comando em cada máquina atacante é gerado um alerta por cada 15 segundos do ataque, por cada máquina atacante. Testamos também a execução do *Tintolmarket* e verificamos que ao iniciar e terminar rapidamente o programa é gerado um alerta na quarta comunicação com o porto 12345.

Durante os testes efetuados verificou-se que a ação da aplicação *NoTintol* teve bastante impacto no servidor *TintolmarketServer*, visto que muito rapidamente se liga e desliga dos seus serviços. Isto resulta num consumo de recursos muito grande e consequente perda de performance do mesmo, podendo resultar numa *denial of service* para clientes reais