Atualizando as regras do snort automaticamente.

Autoria de Fernando Buzon Macedo
17/11/2008
Última Atualização 21/11/2008

Fernando B. Macedo nos traz mais uma boa contribuição, tratando de um dos softwares da área de segurança mais utilizados no mundo, o Snort. Saiba um pouco mais como gerenciar este poderoso software.

O script basicamente funciona assim:1. Baixa o arquivo a partir do site do snort utilizando o oinkcode, no meu caso aquele que se obtem gratuitamente fazendo o cadastro no site.2. Verifica se você está utilizando o snort em modo inline ou não e caso esteja ele apaga a regra de firewall que faz o divert pra posteriormente parar o snort sem atrapalhar nada.3. Renomeia a pasta 'rules' antiga pra 'rules.old' e atualiza uma nova pasta rules com o conteudo do arquivo baixado. Também substitui os arquivos antigos *.map, *.config, sid e generators, porém o snort.conf é mantido.

4. Muda a ação das regras, no meu caso ao invés de 'alert' uso 'drop'.

5. Comenta aquelas regras que vc decidir não utilizar, essa opção é bem útil, vou dar um exemplo:

Suponhamos que no meu 'snort.conf' eu também fiz um include para o conjunto de regras 'shellcode.rules', dentre essas regras temos uma chamada 'SHELLCODE x86 NOOP' que faz com que o acesso ao meu servidor pop3 não funcione portanto eu comentei apenas essa regra e quando atualizados os arquivos rules ela voltará descomentada causando problemas. Pra isso podemos utilizar um arquivo definido no macro 'ignore_rules', onde podemos colocar os nomes das regras que desejamos que sejam comentadas, uma por linha, nesse caso do exemplo colocaríamos nele apenas 'SHELLCODE x86 NOOP' e a linha dessa regra será comentada após a atualização.

6. Levanta novamente o snort e no caso de snort inline, verifica com sockstat se o serviço realmente está rodando pra poder re-aplicar o firewall e assim novamente aplicar a regra de divert, caso o snort não tenha rodado por algum motivo o firewall não é reaplicado e vc fica sem a regra de divert, ou seja, sem ids!

Segue o script:

Início==========#!/bin/sh

```
versao="2.8"
oink="e7a7c29497d45dbf0040b6b790cceab9c112xxxx"
log="/var/log/snort/atsnort.log"
tmp="/tmp/snort"
rules="/usr/local/snort/rules"
etc="/usr/local/snort/etc"
acao="drop"
stop="killall -9 snort"
start="/usr/local/bin/snort -J 5700 -D -c /usr/local/snort/etc/snort.conf"
ignore_rules="/root/ignore_rules.txt"
inline="enable"
divert_rule="1"
start_firewall="/etc/ipfw.sh"
inline_port="5700"

##########################################################################hoje=`date | awk '{print $3"-"$2}'`
hora=`date | awk '{print $4}'`

echo "Inicio $hoje ( $hora )" >> $log
echo "" >> $log

cd $tmp
echo "Baixando arquivo snortrules-snapshot-$versao.tar.gz em $tmp." >> $log
fetch http://www.snort.org/pub-bin/oinkmaster.cgi/$oink/snortrules-snapshot-$versao.tar.gz

if [ -e $tmp/snortrules-snapshot-$versao.tar.gz ]; then
```

```
echo "Arquivo snortrules-snapshot-$versao.tar.gz obito com sucesso." >> $log

if test "$inline" = "enable"; then
  echo "Snort modo inline! Afinal, pra que ser o passivo quando se pode ser o ativo? rs" >> $log
  echo "Apagando regra de divert antes de parar o snort." >> $log
  ipfw delete $divert_rule >> $log
fi

echo "Parando o snort, descompactando e copiando os novos arquivos." >> $log
$stop >> $log

tar zxvf snortrules-snapshot-$versao.tar.gz > /dev/null
mv -v $tmp/etc/*.config $etc >> $log
mv -v $tmp/etc/*.map $etc >> $log
mv -v $tmp/etc/sid $etc >> $log
mv -v $tmp/etc/generators $etc >> $log

rm -fr $rules.old
mv -v $rules "$rules.old" >> $log
mv -v $tmp/rules/ $rules >> $log

echo "Aplicando acao para $acao." >> $log
sed -i.bak "s/^alert /$acao /g" $rules/*
rm $rules/*.bak

if [ -e $ignore_rules ]; then

  echo "" >> $log
  echo "Comentando regras marcadas na ignore list." >> $log
  qtd_ignore=`wc -l $ignore_rules | awk '{print $1}'`
  a='1'
  while [ $a -le $qtd_ignore ]; do

    ignore=`sed "$a,$a!d" $ignore_rules`
    sed -i.bak "/$ignore/s/^/# /g" $rules/*
    echo "Comentado regra $ignore" >> $log

  a=`expr $a + 1`
  done
  echo "" >> $log
  rm $rules/*.bak

fi

if test "$tmp" != ""; then
  echo "Apagando arquivos desnecessarios." >> $log
  rm -fr $tmp/*
else
  echo 'Voce nao definiu o $tmp! Quer que eu te apague sua particao root inteira? rs' >> $log
fi

echo "Levantando novamente o snort." >> $log
$start >> $log
echo "" >> $log
if test "$inline" = "enable"; then
  sleep 20
  snort=`sockstat -4l | grep :$inline_port`
    if test "$snort" != ""; then
  echo "Snort inline rodando, reaplicando o firewall..." >> $log
      echo "" >> $log
      $start_firewall >> $log
      echo "" >> $log
    else
      echo "" >> $log
```

```
    echo "Snort nao levantou e o firewall nao sera reaplicado, estamos sem IDS!!" >> $log
      fi
  fi

else

  echo "Nao foi possivel obter o arquivo snortrules-snapshot-$versao.tar.gz." > $log

fi

hoje=`date | awk '{print $3"-"$2}'`
hora=`date | awk '{print $4}'`

echo "Fim $hoje ( $hora )" >> $log
echo "" >> $log
echo "================================================================================" >>
$log
```

Fim==========

Grande abraço a todos!

Autor: Fernando Buzon Macedo