Manual de Instalação do Snort

Snort, MySQL e ACID no Redhat 7.3

Agosto, 2002

Versão 1.5

Preparado por Steven J. Scott
sjscott007@yahoo.com
http://home.earthlink.net/~sjscott007

Tabela de Conteúdo

Reconhecimento

Eu gostaria de agradecer as seguintes pessoas por sua ajuda em criar esta guia, e em suportar o projeto que ajudou a criar.

Fred Beste

Sua aptidão para empossar e complementar suas habilidades com outras pessoas contribuirá somente para o seu contínuo sucesso. Eu não posso começar a explicar as grandes coisas que podem ser realizadas quando você tem o controle sobre seu próprio destino. Isso apenas mostra como os grandes líderes deixam suas pessoas comandar, e compartilhar da riqueza com aquelas que as executam.

Bob Kaelin

Por cuidadosamente ajudar a endireitar os vários sensores enquanto garantia que a documentação fluísse durante todo o processo. Magnífico!!

Comentários e Correções

Se encontrar algum erro ou gostaria de fazer comentários favor envie-os para sjscott007@yahoo.com

Aonde adquirir a última versão deste Guia

A última versão deste guia pode ser encontrada em http://home.earthlink.net/~sjscott007/. você pode também encontrá-lo em http://www.snort.org.

Introdução

A finalidade desta guia é documentar a instalação e a configuração de uma implementação completa do Snort. Este guia contém toda a informação necessária para instalação e compreensão do plano de arquitetura da implementação.A informação neste guia foi escrita para implementação do Snort 1.8 usando o Redhat 7.3.Você pode encontrar algumas discrepâncias se você estiver instalando versões diferentes de Snort ou estiver usando versões diferentes de Redhat.
Este guia foi escrito com a suposição que vocês compreendam como funciona o Snort e ter uma compreensão básica de Linux. Isto inclui a edição de arquivos, fazer diretórios, software compilado e comandos gerais de compreensão Unix. Este guia não explica como usar ou configurar o Snort, mas informações de onde obter esta informação pode ser encontrado na seção “Informação Adicional”.

Softwares Requeridos

A seguir esta uma lista dos softwares requeridos e as versões que foram utilizadas

Redhat 7.3 ftp://ftp.redhat.com
Snort v1.8.7 http://www.snort.org/dl/
MySQL v3.23.52 http://www.mysql.com/downloads/mysql-3.23.html
Webmin v.99 http://www.webmin.com/
NetSSLeay v1.20 http://symlabs.com/Net_SSLeay/
ACID 0.9.6B21 http://acidlab.sourceforge.net/
    PHP v4.1.* ftp://updates.redhat.com/7.3/en/os/i386/
    ADODB v2.31 http://php.weblogs.com/adodb
    PHPLOT v4.4.6 http://www.phplot.com/
GD v1.8.4 http://www.boutell.com/gd/
Snortd file http://home.earthlink.net/~sjscott007/snortd
Mozilla http://www.mozilla.org/
Snort Webmin Module v1.1 http://msbnetworks.net/snort/

Topologia Conceitual

Há cinco pacotes de software preliminares que produzem esta topologia. O servidor web Apache, o servidor de banco de dados MySQL, Webmin, ACID e Snort. Esta topologia supõe que seus sensores estarão funcionando em um hardware dedicado separado da base de dados e do console ACID. Abaixo está uma descrição breve de cada uma dos pacotes e de sua finalidade na topologia.

Apache Web Server

Este é o web server de escolha para a maioria dos websites que são acessados na Internet. A única finalidade da Apache é de hospedar o console ACID Baseado na Web.

MySQL Server

MySQL é um servidor de base de dados baseado em SQL para uma variedade de plataformas e é a plataforma mais suportada para armazenar alertas do Snort. Todos os alertas do IDS que são provocados por nossos sensores são armazenados na base de dados do MySQL.

Webmin

Webmin é uma interface baseada na web para administrar usuários baseados em Unix. Fornece uma interface gráfica para a maioria dos serviços e opções de configuração que estão disponíveis no nível shell. Webmin é escrito em Perl e os novos módulos (plugins para administrar serviços. Por exemplo o DNS, os usuários & os grupos) estão sendo criados toda hora. Há também um módulo do Snort que é instalado e que permite que você administre graficamente o Snort.

Analysis Console for Intrusion Databases (ACID) (Console de análise para base de dados do intruso)

O ACID é uma aplicação baseada na web para que os logs (registros) do Firewall possam ser vistos.Este é o lugar onde toda a informação do sensor é consolidada para a visão.

Snort

Snort é um sistema de detecção de intruso em pequenas redes (lightweight) , capaz de executar análises de tráfego e registros de pacotes no IP da rede em tempo real .Este é o pacote de software que é usado para recolher informações da rede.

Modelo de alocação do sensor

Internet (Serviços Públicos/Saída de Tráfego)

A maneira mais praticada e padrão de alocar seus sensores são: antes e depois de um Firewall. Isto realiza três objetivos:

- Saber se alguma tentativa esta sendo feita antes de toda a filtragem do pacote estiver terminada (Pre-Firewall - Externo)
- Saber se uma tentativa foi bem sucedida ou bloqueada pelo Firewall (Pos-Firewall – Interno)
- Verificar as configurações dos Firewalls

É sempre bom saber se alguém está tentando invadir sua rede. Isto, é o porque que nós colocamos um Sistema da detecção de Intruso ***(IDS)*** antes do primeiro Firewall (lado externo). Você pode comparar isto como tendo uma câmera monitorando sua porta da frente, sem esta câmera você nunca saberia quem está tentado abrir a porta sem sucesso. Saber se uma tentativa foi bem sucedida na passagem através do seu Firewall pode deixá-lo focalizar as ameaças reais e ajudar-lhe reduzir em falsos positivos. O outro benefício está nos ambientes que usam a tradução de endereço da rede (NAT). Isto permitirá que você encontre o

endereço real da fonte correlacionando os eventos entre o sistema IDS antes e depois do Firewall.
Esta topologia permitirá que você verifique se suas linhas de referências do Firewall estão sendo seguidas, ou se alguém não fez nenhum erro ao mudar uma regra do Firewall. Se você sabe se suas linhas de referências do Firewall não declaram o uso de ftp e o seu sistema IDS pós Firewall estiver mostrando alertas de ftp, então sabemos que o Firewall não está bloqueando o tráfego de ftp. Isto é apenas um efeito lateral e não deve ser a única maneira que você verifica o concedimento com suas linhas de referências.

Extranet

As conexões da Extranet são monitoradas com um sistema IDS colocado do lado interno do Firewall ou do roteador. As razões de que nós não monitoramos o lado externo da Extranet são que as regras para esta conexão privada devem estar extremamente estreitas e o acesso deve ser limitado somente aos recursos (usuários) que são necessários para o relacionamento do negócio.

Como usar este guia

A maneira mais fácil de usar esta guia é construir primeiramente seu MySQL e o servidor ACID. Isto pode ser conseguido lendo as seguintes seções no guia: Instalação do Redhat 7.3, Pós-Instalação do Redhat , Console ACID & Base de dados centralizada do MySQL. Os sensores podem ser criados com as seguintes seções: Instalação do Redhat 7.3, Pós-Instalação do Redhat , Instalação do Snort, Instalação do Webmin.

Instalação do Redhat 7.3

1. Língua Inglesa (English language)
2. Configuração do teclado (Keyboard Configuration)

a. Próxima (Next)

3. Configuração do Mouse (Mouse Configuration)

a. Próxima (Next)

4. Tela de boas - vindas (Welcome Screen)

a.Próxima (Next)

5. Opções de Instalações (Install Options)

a. *usual próxima (Custom Next)*

6 – ***Separação de Estratégia***

Há duas estratégias separadas apontadas abaixo.Siga uma para o sensor do Snort ou outra para a base de dados/console ACID. Estas configurações são baseadas em uma configuração 18gig disco rígido (HD).

Sensor do Snort

a. Selecione, "***Manually partition with Disk Druid"***
b. Selecione *New*
i.(Ponto de montagem)Mount point: */boot*
ii. (Tamanho) Size (MB): 40
iii. Selecione "*OK*"
c. Selecione *New*
i. Filesystem: *swap*
ii. Tamanho (MB): 512
iii. Selecione "*OK*"
d. Selecione *New*
i. (Ponto de Montagem) Mount point: */var*
ii. (Tamanho)Size (MB): 4000
iii. Selecione "*OK*"
e. Selecione *New*
i. (Ponto de Montagem) Mount point: */*
ii. (Checar) Check, "*Fill to maximum allowable size*" (Preencha ao máximo valor aceitável)
iii. Selecione "*OK*"
f. Selecionet Next
MySQL Base de Dados/Console Acid
a. Selecione, "*Manually partition with Disk Druid*" *Next*
b. Selecione *New*
i. Mount point: */boot*
ii. Size (MB): 40
iii. Select "*OK*"
c. Select *New*
i. Filesystem: *swap*
ii.
ii. Size (MB): 512 (Tamanho)
iii. Select "*OK*"
d. Select *New*
i. Mount point: */*
ii. Size (MB): 4000
iii. Select "*OK*"
e. Select *New*
i. Mount point: */var*
ii. Check, "*Fill to maximum allowable size*"
iii. Select "*OK*"
f. Select Next
2. Boot Loader

a. Next
3. Grub Password
a. Next
4. Network Configuration (Config. Da rede)
a. Setup the IP address information for Eth0 (Setup do endereço IP)
i. Unselect, "*Configure Using DHCP option*" (Retire da seleção Configure using DHCP option)
b. Select *eth1* tab
i. Select, "*Activate at boot*"
c. Next
** Note que eth0 é sua interface interna e eth1 é sua interface sniffing. Você nunca deve atribuir um endereço IP a interface sniffing (eth1).

5. Configuração do Firewall
a. *No Firewall Next*
6. Language Support (Linguagem Suportada)
a. Next
7. Time Zone Selection (Seleção de Fusorário)
a. Set UTC to the proper offset
b. Use daylight savings time option if appropriate (Horário de verão se apropriado)
c. Check the box "System clock uses UTC" (Checar o box citado)
d. Next
8. Account Configuration (Configuração da conta)
a. Set root password (senha da raiz "root")
b. Create individual accounts (Criar contas individuais)
c. Next
9. Authentication Configuration (Autenticação de configuração)
a. Next
10. Select Package Groups (Selecionar grupos de pacotes)
a. Select the following packages for installation: (Selecionar os seguintes pacotes)
Printing Support
Classic X Windows System
X Windows System
Gnome
Network Support
Messaging and Web Tools
Network Managed Workstation
Authoring and Publishing
Emacs
Utilities
Software Development
b. Next
a. Select your installed video card (Selecionar o seu video card já instalado)
11. Video Configuration

12. About to Install

a. Next
a. Choose the appropriate model *Next (Escolher Next)*
a. Choose color depth and resolution (Escolher profundidade de cor e resolução)
b. Choose, "*Text*" for your login type (Escolher texto para o login)
c. Next
d. Exit
13. When prompted insert Redhat CD 2
14. When prompted for Boot disk creation, choose *Skip* Next
15. Monitor Selection (seleção de monitor)
16. Custom X Configuration

Pós Instalação do Redhat

1. Instale todos os updates e patch relevantes do Redhat

   http://www.redhat.com/support/errata/rh72-errata.html

2. Desligue o serviço de PortMapper

a. chkconfig portmap off

Instalação do Snort

A primeira coisa que nós necessitamos fazer é instalar as dependências do MySQL para o snort. Para isso pode ser feito o download em http://www.mysql.com/

 # rpm –ivh MySQL-client-*.**.**-*.rpm

 # rpm –ivh MySQL-devel-*.**.**-*.rpm

A seguir faça o download do pacote snort tar na página http://www.snort.org/dl. Será chamado algo como snort-1.8.*.tar.gz. .Faça o download da última versão e compile-a.

 # cp snort-1.8.*.tar.gz /usr/src/redhat/SOURCES
 # cd /usr/src/redhat/SOURCES
 # tar –zxvf snort-1.8.*.tar.gz
 # cd /usr/src/redhat/SOURCES/snort-1.8.*
 # ./configure --with-mysql
 # make
 # make install

Download e instale as últimas regras.Faça o download das mesmas pela página http://www.snort.org/dl/signatures /, certifique-se que você esta fazendo o download do snortrules.tar.gz e NÃO do snortrules-current.tar.gz.

mkdir /etc/snort
cp snortrules.tar.gz /etc/snort
cd /etc/snort
tar –zxvf snortrule.tar.gz

Depois que você "***untared"*** o arquivo das regras será criado um diretório de regras em /etc/snort. Nós necessitamos mover todos os arquivos de regras para dentro do diretório /etc/snort. A razão que nós temos que fazer isto é por causa da Webmin e da variável $$RULE_PATH .Por alguma razão o módulo da Webmin não gosta da variável $$RULE_PATH e atrapalha você a editar suas regras.

 # cd /etc/snort/rules
 # mv * ../
 # cd ..
 # rmdir rules
 # vi snort.conf

Edite as seguintes linhas do arquivo snort.conf. Substitua o xxxx com a senha apropriada para a conta snort. A variável do host deve ser ajustada ao seu servidor IP do ACID/MySQL.

#output database: log, mysql, user=root password=test dbname=db host=localhost
to
output database: log, mysql, user=snort password=snort dbname=snort
host=000.000.000.000

Comment out the $RULE_PATH variable:

var RULE_PATH ../rules
para

#var RULE_PATH ../rules

Remova todas as variáveis $$RULE_PATH de cada uma das seguintes linhas. Por exemplo faça a primeira regra ser como esta: **include bad-traffic.rules**

#==
 # Inclua todas as regras(rulesets) aqui
#
 # shellcode, policy, info, backdoor, and virus rulesets are
 # disabled by default. These require tuning and maintance. (Isso requer ajuste e #manutenção.Por favor leia o arquivo especificado incluído para maiores informações)
 # Please read the included specific file for more information.
#==

include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/scan.rules

include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/telnet.rules
include $RULE_PATH/smtp.rules
include $RULE_PATH/rpc.rules
include $RULE_PATH/rservices.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/tftp.rules
include $RULE_PATH/web-cgi.rules
include $RULE_PATH/web-coldfusion.rules
include $RULE_PATH/web-iis.rules
include $RULE_PATH/web-frontpage.rules
include $RULE_PATH/web-misc.rules
include $RULE_PATH/web-attacks.rules
include $RULE_PATH/sql.rules
include $RULE_PATH/x11.rules
include $RULE_PATH/icmp.rules
include $RULE_PATH/netbios.rules
include $RULE_PATH/misc.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/shellcode.rules
include $RULE_PATH/policy.rules
include $RULE_PATH/porn.rules
include $RULE_PATH/info.rules
include $RULE_PATH/icmp-info.rules
include $RULE_PATH/virus.rules
include $RULE_PATH/chat.rules
include $RULE_PATH/p2p.rules
include $RULE_PATH/multimedia.rules
include $RULE_PATH/experimental.rules
include $RULE_PATH/local.rules

Crie um diretório de registro (log) para o snort. A informação de busca de Port é posta aqui. Também, se você estiver fazendo o registro (log) de pacotes ou não está povoando uma base de dados, essa informação é colocado então aqui :
 # mkdir /var/log/snort

Instale o script startup ***automatizado*** Snort. Você pode fazer o download do script em http://home.earthlink.net/~sjscott007/snortd. Se você tiver erros ao tentar executar o arquivo após feito o download certifique-se que a transferência é ASCII e não binária.A melhor maneira de garantir isto é cortar e copiar em um arquivo de texto.
 # cp snortd /etc/rc.d/init.d

 # cd /etc/rc.d/init.d
 # chmod 755 snortd
 # chkconfig --level 2345 snortd on

O parâmetro -u grava todas as vezes no UTC. O parâmetro -o muda a ordem da regra definida de Alert->Pass->Log to Pass->Alert->Log. Isto permite que Snort ignore os falsos positivos usando o arquivo das regras locais com a opção “pass” filtrar os ruídos das máquinas.
Vamos testar a nossa configuração do Snort
 # /etc/rc.d/init.d/snortd start
Certifique-se primeiramente de que o processo está funcionando emitindo um comando *ps –ef*. Procure o snort rodando. Gere algum tráfego ilegal no segmento monitorado (como uma varredura de NMAP). Seu console ACID deve agora indicar os resultados. Você deve também ver a contagem do sensor no incremento da pagina principal. Note que seu sensor não estará indicado no ACID até que um alerta seja gerado (mas a contagem do sensor no ACID começa a ficar incrimanado”***incriminated”***). Quando acabar o teste funcione o comando a seguir para que o Snort pare de funcionar
/etc/rc.d/init.d/snortd stop

Instalação do Webmin

Instale as dependências para usar as conexões SSL com o Webmin. Você pode fazer o download do Net_SSLeay em http://symlabs.com/Net_SSLeay/.
 # cp Net_SSLeayrpm-*-**.tar.gz /usr/src/redhat/SOURCES
 # cd /usr/src/redhat/SOURCES
 # tar –zxvf Net_SSLeay.rpm-*-**.tar.gz
 # cd Net_*
 # perl Makefile.PL
 # make install
Instale o Webmin RPM. Faça o download em http://www.webmin.com/
 # rpm –ivh webmin-0.99.-1.noarch.rpm
1. Configure SSL
a. Abra o browser Mozilla e vá ao endereço: http://127.0.0.1:10000
b. Faça o login como ROOT(Login as ROOT)
c. Selecione o ícone “*Webmin Configuration*”
d. Selecione o ícone, “*SSL Encryption*”
e. Selecione o botão, “*Enable SSL support if available*” e clique o botão “Save” (Salvar)
2. Configure o Proxy se voce estiver atrás do firewall
a. Selecione o ícone, “*Webmin Configuration*”
b. Selecione o ícone, “*Proxy Servers*”
c. Entre sua informação do proxy e clique no botão “SAVE” (Salvar)
3. Instale o Snort Webmin plugin
a. Selecione o ícone, “*Webmin Configuration*”
b. Selecione o ícone, “Webmin Modules”

c. Instale o modulo da pagina url:
http://www.snort.org/dl/contrib/front_ends/webmin_plugin/snort-1.0.wbm e clique "Install"
4. Configure Snort Plugin
a. Selecione o ícone, "Servers" que se encontra na parte superior da páginaWeb.
b. Selecione o ícone, "Snort IDS Admin" (Parece um porco!)
c. Selecione o "Module Config" que se encontra do lado esquerdo.

Você deve agora ver uma tela como esta:
Your configuration should match the following:
Full path to Snort executable (with options) = /usr/local/bin/snort -U -d -D -c /etc/snort/snort.conf
Full path to Snort configuration file = /etc/snort/snort.conf
Full path to Snort rule files directory = /etc/snort
Full path to Snort PID file = /var/run/snort_eth1.pid
Command to start Snort (optional) = /etc/rc.d/init.d/snortd start

(Sua configuração deve combinar com a seguinte)
(Caminho completo do executável do snort (com opções) = /usr/local/bin/snort - U - d - D –(c /etc/snort/snort.conf)
(Caminho completo para o arquivo de configuração do snort Snort = /etc/snort/snort.conf)
(Caminho completo para o diretório do arquivo de regras = /etc/snort)
(Caminho completo para o arquivo PID = /var/run/snort_eth1.pid)
(Comando para começar o snort (opcional) = /etc/rc.d/init.d/snortd start)
Quando terminado clique em no botão Save (Salvar).Está pronto !!!

Acid Console & Base de dados centralizado do MYSQL

A primeira coisa que devemos fazer é instalar o servidor web Apache para então o ACID ter uma "casa".

A última RPM para o Apache pode ser encontrado em
ftp://updates.redhat.com/7.3/en/os/i386/
 # rpm -ivh apache-1.3.X-X.i386.rpm
 # chkconfig --level 2345 httpd on
 # /etc/rc.d/init.d/httpd start
A seguir nós instalamos e configuramos a base de dados do MySQL.Faça o download na página http://www.mysql.com/.
 # rpm -ivh MySQL-3.23.X-X.i386.rpm
 # rpm -ivh MySQL-client-3.23.X-X.i386.rpm
 # rpm -ivh MySQL-shared--3.23.X-X.i386.rpm
 # mysql -u root

mysql> set password for 'root'@'localhost' = password('yourpassword');
mysql> create database snort;
mysql>exit
NOTA: Por alguma razão estranha o MySQL-3.23.56.i386.rpm não inicia o serviço do mysql no nível 3. Faça o seguinte para corrigir o problema.
 # chkconfig –level 3 mysql on
Note que depois que você ajusta a senha da raiz acima você precisa fazer o login usando uma senha para acessar a base de dados ***com raiz***. Por exemplo # mysql –u root -p

As tabelas da base de dados precisam ser ajustadas . Nós realizamos isso funcionando o script do create_mysql. Este pode ser encontrado na árvore de CVS em http://cvs.sourceforge.net/cgi-bin/viewcvs.cgi/snort/snort/contrib/.

Se o arquivo não esta localizado no diretório de onde o programa Mysql esta rodando
adicione o trajeto à indicação da fonte. Por exemplo **mysql> source /home/john/create_mysql**
 # mysql –u root -p
mysql> connect snort
mysql>source create_mysql
mysql>grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort;
Para que você conecte localmente com essa conta
mysql>grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;
Crie um usuário que não possa deletar alertas da base de dados: pode somente necessitar da conta local
mysql> grant CREATE, INSERT, SELECT, UPDATE on snort.* to acidviewer;
Para que você conecte localmente com essa conta
mysql>grant CREATE, INSERT, SELECT, UPDATE on snort.* to acidviewer@localhost;
Ajuste as senhas para as contas do MySQL
mysql>connect mysql
mysql> set password for 'snort'@'localhost' = password('yourpassword');
mysql> set password for 'snort'@'%' = password('yourpassword');
mysql> set password for 'acidviewer'@'localhost' = password('yourpassword');
mysql> set password for 'acidviewer'@'%' = password('yourpassword');
mysql> flush privileges;
mysql> exit
O ACID requer a instalação de PHP e o módulo de suporte do Mysql. Faça o download em ftp://updates.redhat.com/7.3/en/os/i386/.
 # rpm -ivh php-4.1.*-*.i386.rpm
 # rpm -ivh php-mysql-4.1.*-*.i386.rpm

Agora é a hora de instalar o ACID.Você pode fazer o download de todos os arquivos em

ACID 0.9.6B21 http://acidlab.sourceforge.net/
ADODB v2.31 http://php.weblogs.com/adodb
PHPLOT v4.4.6 http://www.phplot.com/

GD v1.8.4 http://www.boutell.com/gd/

Uma vez que os arquivos untar downloaded seguinte das limas/var/www/html

 # tar -zxvf acid-0.9.*.tar.gz -C /var/www/html
 # tar -zxvf adodb231.tgz -C /var/www/html
 # tar -zxvf gd-1.8.4.tar.gz -C /var/www/html
 # tar -zxvf phplot-4.4.6.tar.gz -C /var/www/html

*** Importante: Remova o número de versão dos nomes do diretório (por exemplo **mv gd-1.8.4 to gd and mv phplot-4.4.6 phplot**)

Vamos configurar o arquivo de configuração do ACID:

 # cd /var/www/html/acid
 # vi acid_conf.php

Uma vez que você esta no arquivo *acid_conf.php* modifique as seguintes variáveis .Mude o xxxx para refletir a senha escolhida para a conta do snort.

$DBlib_path="../adodb";
$alert_dbname="snort";
$alert_user="snort";
$alert_password="xxxx";
$Chartlib_path="../phplot";

Em seguida vamos fazer a configuração apenas da visão do portal ACID(Sem deletar os eventos).Isso é válido para pessoas que apenas precisam da visão dos alertas.Copie : /var/www/html/acid para /var/www/html/acidviewer (veja apenas acid)

 # cp –R /var/www/html/acid /var/www/html/acidviewer
 # cd /var/www/html/acidviewer
 # vi acid_conf.php

Mude as seguintes variáveis em /var/html/www/acidviewer/acid_conf.php, novamente mude o xxx para refletir a senha que foi escolhida para a conta do *acidviewer*

$alert_user="acidviewer";
$alert_password="xxxx";

Agora asseguramos ambos websites ACID com o Apache.Configuramos as duas contas para o acesso ao Website da ACID. Quando requisitado entre com sua senha para essa conta da web.Muito cuidado para não incluir a opção –c na terceira linha !

 # mkdir /usr/lib/apache/passwords
 # htpasswd -c /usr/lib/apache/passwords/passwords admin
 # htpasswd /usr/lib/apache/passwords/passwords acidviewer

Adicione as seguintes linhas para a seção do DIRECTORY (Diretório) /etc/httpd/conf/httpd.conf. A seção significa a área geral quando vemos os outros formatos do diretório.

<Directory “/var/www/html/acid”>
AuthType Basic
AuthName “yourcompany”
AuthUserFile /usr/lib/apache/passwords/passwords
Require user admin
AllowOverride None
</Directory>
<Directory “/var/www/html/acidviewer”>
AuthType Basic
AuthName “yourcompany”
AuthUserFile /usr/lib/apache/passwords/passwords
Require user acidviewer
AllowOverride None
</Directory>
Reboot the server.
 # reboot

Acessando o Console ACID

Agora temos dois websites para o console ACID:
1) http://youracidhost/acid/index.html
Esse site é para o administrador e pode ser acessado usando a conta do ADMIN criado anteriormente. Podemos deletar os eventos usando esse site.
http://youracidhost/acidviewer/index.html
Esse site é para qualquer um que precisa acesso lido para os eventos e pode ser acessado usando a conta ACIDVIEWER que criamos anteriormente. Usuários desse site não pode deletar eventos.
A primeira vez que conectamos com a Website da ACID vamos ver um display como este: Click (Clique) <setup page>.
Uma vez que esta na página de setup (configuração) click “Create ACID AG”.
Uma vez completada click <Main Page> e estamos prontos!

Ajuste do Sensor

Usando o Webmin e o plugin do snort, podemos ajustar facilmente seus sensores. A seguir vamos demonstrar uma forma de lidar com as regras usando o Webmin. A primeira coisa que precisamos fazer é logar em um dos nossos sensores ,que pode ser acessado via https://yoursensor:10000. Faça o login usando a senha da raíz mostrada abaixo.
Você será apresentado a uma tela vista a seguir. Selecione o ìcone Sever na parte superior da tela
A seguir selecione o ícone Snort (P.S. o ícone parece um porco).
Você será apresentado a uma tela que permitirá que você controle a maioria dos aspectos do seu sensor. No centro da tela você verá todos os seus arquivos de regras. Note que os seus podem parecer diferente. Preste uma atenção especial nas regras locais. Esse é o local onde colocamos nossos filtros.
Vamos dar uma olhada nos arquivos de regras do DNS. Simplesmente clique em cima e verá uma tela como esta .
Como pode ser visto existem 4 colunas que constituem o arquivo de regra
Rule (Regra) : Apenas a ordem em que a regra aparece no arquivo de regra.
Signature (Assinatura): Essa é como uma assinatura atual do snort parece.
Status: A regra está habilitada ou desabilitada ?
Action: Essas são as ações que podem ser executadas para a regra dada.
Deve ser visível que você possa habilitar,desabilitar,mudar, e adicionar regras desta tela. Lembre-se que após feita alguma mudança você deve reiniciar o daemon do snort para que a mudanças tomam efeito. Você pode achar o botão para reiniciar o serviço na página principal do plugin do Snort ,no canto inferior da tela.

Filtrando as Regras

O filtro nos permite fazer exceções de regras sem desabilitá-las completamente .Ao progredir com seu sistema IDS você verá que algumas assinaturas são particularmente ruidosas e requer algum tipo de ajuste.O filtro é uma forma de sanar esse problema.
Para esse exemplo nós vamos usar a regra de número #4 do exemplo acima .Esta regra é usada para detectar transferências nas zonas DNS .Há muitos casos onde isso é legal e não queremos ser alertados disso quando for executado por hosts previstos.Aqui esta como a regra número # 4 se parece.
RULE #4: alert tcp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DNS zone transfer"; flags:A+; content: "|00 00 FC|"; offset:13; reference:cve,CAN-1999-0532; reference:arachnids,212; classtype:attempted-recon; sid:255; rev:5;)
Vamos dizer nesse sensor que é normal para o host 192.168.55.23. executar transferências nas zonas DNS com 192.168.12.5

Então selecione o botão volta e volte para a tela principal do plugin do snort.Clique no arquivo local de regras.O arquivo local de regra é usado para suas próprias regras.Você pode usar esse arquivo para suas próprias assinaturas e para filtragem.Uma vez dentro do arquivo de regras cole a regra que você copiou

dentro da caixa de adicionar regra (Add rule box) que se encontra na parte inferior da tela.
Então selecione adicionar e sua regra aparecerá .
Agora selecione editar a regra.Vamos agora adaptar a regra para filtrar transferências de zonas DNS esperadas.Neste caso vamos modificar as ações das regras,fonte,destino e campo de mensagem
1) A ação do campo será <pass>.
2) A fonte é 192.168.55.23
3) O destino é 192.168.12.5
4) O campo da mensagem descreve a assinatura.Eu mantenho a descrição da assinatura, mas adiciono um comentário porque estamos filtrando esse evento e adiciono minhas iniciais para dizer quem criou.
Agora clique em Save (Salvar).Como você pode ver sua nova regra aparece no arquivo Agora apenas reinicie o snort da página principal do plugin do snort e o seu filtro toma efeito.
A razão que isto funciona é devido à opção –o na inicialização do snort.

Zonas de Tempo (Fusorário)

Você pode estar alocando os seus sensores em fusorários diferentes.Portanto é muito importante que ajustamos a hora corretamente .Conseqüentemente nós podemos ajustar o fusorário apropriado e certificar que todos os tempos estão gravados no padrão UTC (Formalmente tempo médio de Greenwich).
A maneira mais fácil de realizar isto é ajustar o clock do harware (BIOS) para o UTC.Isto pode ser realizado durante a instalação do Redhat ou depois da instalação estar completada Um bom tutorial para o ajuste da hora pode ser encontrado em: http://www.linuxsa.org.au/tips/time.html. A seguir é como ajustar a hora depois que a instalação foi completada.
O arquivo atual do fusorário é armazenado no diretório */usr/share/zoneinfo.*Para selecionar um fusorário ,copie o arquivo apropriado para o diretório */etc* e nomei-o tempo local (localtime)*.* Eu não sei porque o Rehhat não usa um link simbólico aqui.
Para a hora central (central time):
 # cp /usr/share/zoneinfo/America/Chicago /etc/localtime
ou
 # ln -sf /usr/share/zoneinfo/America/Chicago /etc/localtime
Edite o arquivo */etc/sysconfig/clock* e mude a variável *UTC* igual a verdadeiro(equal to true).
UTC=true
Agora ajuste o relógio do sistema.O exemplo dado é para 25 de Março,2002 às 12:30pm (March 25, 2002 at 12:30pm CST).A hora é ajustada no modo 24 horas usando o seu tempo local (não o tempo do UTC) (your **local time** (not UTC time)).Veja a página principal para mais informações:data principal (man *date)*
 # date 032512302002
Ajuste o relógio do hardware para o relógio do sistema.
 # hwclock --systohc --utc

Protocolo do Tempo de Rede (NTP)

Há uma necessidade de manter a hora precisa nos sensores sem ter que ajustar manualmente o relógio. A maneira mais fácil de manter os sensores em sincronismo é usando o protocolo do tempo de rede (NTP).
Edite o arquivo */etc/ntp.conf* .Mude a entrada do usuário para te refletir o timeserver (servidor de tempo).

nunca é usado para a sincronização a não ser que outra
fonte de sincronização está disponível.No caso do host local ser controlado por
uma fonte externa, como um oscilador externo ou um outro protocolo, a palavra-
chave preferida causaria que o host local iria tornar indiferente todas as outras
fontes de sincronização, a não ser as modificações em Kernel que estão em
uso e declarassem uma condição de não sincronismo .
#
server yourtimeserver.com
#fudge 127.127.1.0 stratum 10
A seguir inicialize o *ntpd* daemon e faça-o executar na inicialização.
 # /etc/rc.d/init.d/ntpd start
 # chkconfig ntpd on

Manutenção

Usando a rede do Redhat

Se você esta ajustando seus servidores pela primeira vez você precisa inicialmente registra-los.Emita os seguintes comandos e siga os alertas.
rhn_register
Há dois cenários em que pacotes não serão automaticamente atualizados.O primeiro é atualização no Kernel e o segundo é RPM´s o qual modifica o arquivo de configurações Certifique-se que você saiba quais pacotes estão sendo atualizado antes de fazer a mudanças seguintes.
Uma vez registrado faça o login em https://rhn.redhat.com/ e estabeleça um ***direito(Entitlement***) para o seu novo servidor.Então execute uma atualização da rede Redhat

Atualizações do Kernel

Execute o seguinte comando :
export display=
up2date –nox –configure

Edite a linha 23 ou a 24 dependendo de que versão up2date você esta usando .A linha deve conter a variável <pkgSkipList>.Limpe essa variável teclando o número da linha e depois tecle um “C” maiúsculo para limpar a entrada
Tecle enter para sair do up2date.
Execute o seguinte comando para fazer o download das atualizações do kernel:
rhn_check
Depois de completo “reboot” a máquina. Quando a máquina voltar inicie os seguintes comandos para verificar o sucesso da atualização. Caso a máquina não volte do reboot ,você terá que manualmente selecionar o kernel antigo ***do grub boot screen***.
Após feito com sucesso as atualizações do kernel, podemos limpar o antigo kernel .Edite o arquivo *grub.conf* no diretório */etc*.
vi /etc/grub.conf
Remova as 4 últimas linhas do arquivo que se refere sobre a versão antiga do kernel.
A seguir temos que limpar todos os arquivos de referência do kernel antigo.Os mesmos são encontrados no diretório */boot*. Delete os arquivos seguintes que adaptam a numeração da versão antiga do kernel.Os arquivos que eu listei possui um “ * “ representando a numeração da versão antiga.
rm initrd-*.*.*-*.img
rm module-info-*.*.*-*
rm system.map-*.*.*-*
#rm vmlinux-*.*.*-*
Execute o seguinte commando:
up2date –nox –configure
Edite a linha 23 ou 24 dependendo de qual versão do up2date que você está usando. A linha deve conter a variável <pkgSkipList>. Mude the able out by teclando o número da linha e depois ‘kernel*’. Isso irá parar que o kernel seja atualizado automaticamente .
Pressione enter para sair . Está pronto!

RPM’s o qual modifica o arquivo das configurações

Execute o seguinte comando:
export DISPLAY=
up2date –nox --configure
Edite a linha 19.A linha deve conter a variável <noReplaceConfig***>. Mude viable de ‘Yes’ to ‘No’.***
Pressione enter para sair do up2date.
Prossiga com a atualização executando os seguintes comandos:
rhn_check
Uma vez completo volte para a tela de configuração do up2date:
up2date –nox –configure
Edite a linha 19 mais uma vez e mude o valor de volta para o ‘Yes’.
Pressione enter para sair.
Está pronto!

Sincronizando o seu perfil do Redhat

Se você manualmente atualizou o RPM's ou se de alguma forma ficou fora de sincronismo com a rede do Redhat você terá que fazer um upload do seu perfil novamente. Execute o seguinte comando pra voltar ao sincronismo:
export DISPLAY=
up2date -p

Manualmente atualize os seus pacote do Redhat(sem a rede do redhat)

A melhor maneira para atualizar o seu servidor Redhat que está em posições remotas ***is to SSH in*** e execute os seguintes comandos:

 # export DISPLAY=
 # up2date --nox -u

Agora você deve observar a versão do comando de linha do up2date rodando.Uma vez que você saia do up2date todos os seus rpm´s foram atualizados .

Como remover totalmente um sensor da base de dados do MySQL

Entre no ACID e delete todos os eventos associados com aquele sensor.Isso pode demorar um pouco vai depender do número de eventos que será deletado e o tipo de harware que você esta rodando a base de dados.Seja paciente seu browser pode até ***time out*** enquanto espera o término. ***Use o topo para observar o serviço do mysqld***. Quando eu estava testando em uma caixa lenta ,eu tinha que entrar diversas vezes e continuar a deletar os eventos . Eu tinha mais que 60000 eventos e sensores múltiplos .Eu também tive que ficar saindo da tela e entrando de novo pois estava aparecendo "unsuccessful delete".(Deleção mal sucedida)
A seguir remova o sensor completamente da base de dados.Isso irá corrigir a contagem do sensor na página principal do ACID.

 # mysql -u root -p
mysql> connect snort
mysql> select * from sensor;

Procure o número sid do sensor que você deseja deletar Por exemplo. mysql> delete from sensor where sid=2;

mysql> delete from sensor where sid=<number>;

Características dos sensores

A finalidade de ter características dos sensores é de documentar e compreender o tráfego que transversa o link (a ligação) onde o sensor é encontrado. Você pode usar esta informação para reduzir os seus falsos positivos, ajustar seus sensores, e eventualmente encontrar anomalias no tráfego. Abaixo está o formato que usa quando povoamos os campos.

Fields Description (Descrição dos campos)

Sensor DNS Name of your sensor (Sensor DNS Nome do seu sensor)
IP IP address of the management interface (Endereço IP da interface de gerenciamento)
Mask Subnet mask for the above IP (Máscara Subnet Máscara para IP acima)
GW Default Gateway for the above IP
Network Placement Internet / Pre-Firewall / (External)

Internet / Post-Firewall / (Internal)
Extranet / Post-Firewall / (Internal)
Source Address Category External Internet Address
Internal Address (Endereço Interno)
Extranet Address (Endereço Extranet)
Proxy
Firewall
Destination Address Category External Internet Address
Internal Address
Extranet Address
Proxy
Firewall
Relacionamento com outros sensores .Este campo é usado para mostrar as relações com outros sensores.

Por exemplo,um sensor antes e depois do proxy.Se você observar um alarme no sistema IDS depois do proxy e quiser o verdadeiro endereço da fonte, você ira precisar da referência do sensor antes do proxy*.*
Comentários a respeito de qualquer circunstancia em especial
Contact Information on who to contact
Permitir o fluxo do protocolo. Este deve conter todos os protocolos permitidos que cruza o link
Serviços Públicos .Qualquer servidor acessível ao público (servers that are accessible to the public)

Example Template

Sensor: Coco23	**IP:** 127.2.44.2	**Mask:** 255.255.255.0	**GW:** 127.2.44.1
Network Placement: Internet / Pre-Firewall / (External)		**Source Address Category:** External Internet Address	
Destination Address Category: Proxy (10.77.3.4)			
Relationship to other sensors: Momo44 – To find the real destination address correlate events with Momo44 sensor.			
Contact:			
Comments:			
Allowable Protocols			

Source Address	**Direction (or)**	**Destination**	**Protocol**
Any		10.77.3.4	FTP
Any		10.77.0.0/16	HTTP

Public Servers		
Source Address	**Running Services**	**Contact**
10.77.3.4	FTP	Jimmy John (444)-555-1111

Informação adicional

Snort Home Page http://www.snort.org/
Snort Home Page Brasil http://www.snort.com.br
Snort FAQ http://www.snort.org/docs/faq.html
Snort Users Manua(Manual do Usuário)l http://www.snort.org/docs/writing_rules/
Snort-Setup for Statistics(Ajuste das Estatísticas)
http://www.linuxdoc.org/HOWTO/Snort-Statistics-HOWTO/
Man Page http://www.dpo.uab.edu/~andrewb/snort/manpage.html
Usenet Groups
- Snort-announce http://lists.sourceforge.net/mailman/listinfo/snort-announce
- Snort-users http://lists.sourceforge.net/mailman/listinfo/snort-users
- Snort-sigs http://lists.sourceforge.net/mailman/listinfo/snort-sigs
- Snort-devel http://lists.sourceforge.net/mailman/listinfo/snort-devel
- Snort-cvsinfo http://lists.sourceforge.net/mailman/listinfo/snort-cvsinfo

Snort CVS tree http://cvs.sourceforge.net/cgi-bin/viewcvs.cgi/snort/snort/
ACID Home Page http://acidlab.sourceforge.net/
MySQL Home Page http://www.mysql.com/
Webmin Home Page http://www.webmin.com/
Redhat Home Page http://www.redhat.com/
Redhat 7.2 Reference Books
http://www.redhat.com/support/resources/howto/rhl73.html
Redhat 7.2 Updates / Patches http://www.redhat.com/support/errata/rh73-errata.html
Redhat Network Guide https://rhn.redhat.com/help/basic/
Compaq Linux http://www.compaq.com/products/software/linux/
Nessus Vulnerability Scanner http://www.nessus.org/
Linux, Clocks, and Time http://www.linuxsa.org.au/tips/time.html

Mudanças de Log

V1.0 Maio 2002
- Documento Inicial (Initial document)

V1.5 Agosto 2002
- Refeito para Redhat 7.3
- Correções de erros

Seção de ajuste do sensor foi incluída
Seção de mudanças de log foi incluída
Seção Acessando o Console ACID foi incluída