Marcelo Eller de Amorim
eller@cbpf.br
Marita Maestrelli
marita@cbpf.br

Sistemas de Detecção de Intrusos

Resumo

- Esta nota técnica aborda aspectos sobre sistemas de detecção de intrusos, dando algumas características e funcionalidades, e também fornece um passo a passo para a instalação de um desses sistemas de uso gratuito.

Sumário

1 Introdução

- Segurança = Visibilidade + Controle
- Produtos de segurança provêem dois benefícios primários: visibilidade e controle, e é a combinação desses dois fatores que torna possível a criação e reforço de uma *política de segurança** para tornar uma rede privada de computadores mais segura.
- Visibilidade - É a habilidade de ver e entender a natureza e o tráfego de uma rede.
- Controle - É a habilidade de afetar o tráfego da rede incluindo o acesso à rede ou a partes dela.
- Visibilidade é fator primordial na tomada de decisões. Ela torna possível a criação de uma política de segurança baseada em dados reais. Esta política irá aumentar apropriadamente os gastos com soluções de segurança e ajudará a evitar gastos desnecessários ou prematuros. Adicionalmente, visibilidade é o primeiro elemento de uma análise preventiva, permitindo investir em tecnologias preventivas antes que uma vulnerabilidade seja explorada. Sistemas que proporcionam visibilidade, também ajudam a configurar melhor os *dispositivos de controle**,* por proverem um meio de verificar a performance e a eficiência da política de segurança que controlam eles.
- Controle é fator primordial para aplicação da política de segurança. Sistemas que proporcionam controle permitem a profissionais de segurança dar forma ao *tráfego de rede**,* logo se pode assegurar, razoavelmente, que as informações pertencentes à rede não estão vulneráveis e/ou comprometidas.

1.1 Analogia com a segurança de um aeroporto.

- Para melhorar o entendimento destes dois conceitos, faço uso de uma analogia com a segurança de um aeroporto. Abaixo então defino o que vem a ser controle e visibilidade para este exemplo.
- Controle é equivalente aos guardas que regulam a entrada e a saída dos portões de um aeroporto. Como um elemento de controle, os guardas restringem a entrada, somente permitindo o

ingresso de pessoas que possuam um ticket, e permitem a saída de qualquer pessoa. Esse sistema permite que pessoas com um ticket entrem com algum tipo de objeto não permitido (faca, arma etc), e também, pelo fato de qualquer pessoa poder sair, alguém com um ticket falso pode entrar na área interna, roubar a bagagem de terceiros e sair sem maiores complicações.

- Visibilidade é equivalente aos detectores de metais, aparelhos de raio-x de bagagem, câmeras de vídeo, detectores de substâncias químicas, etc que aumentam a eficiência dos guardas (dispositivos de controle), por proverem visibilidade sobre o conteúdo das coisas que as pessoas estão carregando. Com esta informação adicional, o aeroporto torna-se muito mais seguro porque agora os guardas possuem mais elementos a se considerar antes de deixar alguém passar pelo portão. A decisão de deixar ou não alguém passar é auxiliada pelos dispositivos mencionados acima, sendo a detecção de algo errado (ticket falso, porte de arma etc) raramente é feita por intuição.
- Sem a combinação de controle e visibilidade, neste exemplo, o aeroporto é mais ou menos seguro dependendo de quão bons são os guardas em realizar seu trabalho. Se o guarda for insuficientemente treinado para identificar possíveis ameaças ou muito ocupados com outras tarefas para efetivamente reforçar o controle da entrada, resulta diretamente numa queda da segurança.
- Com as redes de computadores não é diferente, as redes possuem informações sobre negócios, pessoas, clientes, etc que devem ser restritas a apenas usuários autorizados, logo as redes necessitam também de dispositivos que proporcionem visibilidade do que está trafegando por elas, para melhorar a performance dos dispositivos de controle, e com isso aumentar a segurança.
- O principal dispositivo de controle em uma rede é o *firewall** e estende-se aos *roteadores*, listas de controle de acesso (ACLs)**, e permissões de usuários. Já o principal dispositivo que proporciona visibilidade em uma rede é o *sistema de detecção de*

*intrusos (IDS)** e estende-se aos *scanners de vulnerabilidades**.

2 O que são sistemas de detecção de intrusos?

- Sistemas de Detecção de Intrusos são programas (softwares independentes ou embutidos em hardware proprietário) que monitoram uma rede ou um host a procura de sinais padrões de comportamento que sejam considerados maliciosos, ou seja, que podem constituir um ataque ou uma outra atividade não permitida.

3 Principais tipos de IDS

- Existem vários tipos de IDSs disponíveis atualmente, caracterizados por diferentes métodos de monitoração e análise. Cada método possui vantagens e desvantagens distintas. Entretanto, todos os métodos podem ser descritos em termos de um modelo de processo genérico para IDSs.

Modelo de processo para IDSs.

- A maioria dos IDSs pode ser descrita em termos de 3 componentes fundamentais:
- Fonte de Informações: As diferentes fontes de informações sobre eventos usados para determinar quando uma intrusão ocorre. As fontes mais comuns são um *host** ou um *segmento de rede**.
- Análise: É a parte do sistema de detecção de intrusos que efetivamente organiza e dá sentido aos eventos derivados da fonte de informações, decidindo quando estes eventos indicam que uma intrusão está ocorrendo ou já foi realizada. Os métodos de análise mais comuns são detecção baseada em assinaturas e detecção baseada em anomalias.
- Resposta: É o conjunto de ações que o sistema faz quando detecta uma intrusão. Estas são tipicamente agrupadas em medidas ativas e passivas, com medidas ativas envolvendo intervenção automatizada em parte do sistema e medidas passivas envolvendo a geração de relatórios para posterior

interpretação e intervenção humana.

- De acordo com a fonte de informações podemos classificar os IDSs em: baseado em rede e baseado em host.

3.1 IDS baseado em rede

- A maioria dos IDSs comerciais é baseada em rede. Estes IDSs detectam ataques pela análise dos *pacotes da rede** atraves de uma escuta em um segmento de rede. Com isso um IDS tem a capacidade de monitorar o tráfego de todos os hosts que estão conectados neste segmento, protegendo-os.
- IDSs baseados em rede geralmente consistem de um conjunto de sensores colocados em vários pontos da rede, estas unidades monitoram o tráfego, realizando uma análise local do mesmo e relatando ataques a um console central de gerenciamento. Como os sensores são limitados a executarem somente o IDS, eles podem ser mais facilmente protegidos contra ataques. Muitas das vezes, estes sensores ficam rodando em uma *bridge**, para tornar mais difícil a localização de um sensor por um atacante.

Vantagens dos IDSs baseados em rede

- Poucos IDSs instalados, mas bem posicionados podem monitorar uma grande rede.
- A instalação provoca um pequeno impacto na rede, pois eles são dispositivos passivos que escutam a rede sem interferirem no seu funcionamento. Logo, é geralmente simples adicionar esse tipo de IDS a uma rede.
- Podem ser bem seguros contra ataques e ainda podem ser invisíveis a muitos atacantes.

Desvantagens dos IDSs baseados em rede.

- Podem ter dificuldades em processar todos os pacotes em uma rede grande e sobrecarregada, logo, eles podem falhar no reconhecimento de um ataque lançado durante períodos de tráfego intenso.
- Muitas das vantagens dos IDSs baseados em rede não se

aplicam as redes mais modernas baseadas em *switches**, pois estes subdividem a rede em muitos segmentos e proporcionam links dedicados entre hosts servidos pelo mesmo switch.

- IDSs baseados em rede não podem analisar informações *criptografadas**. Este problema é crescente visto que mais organizações (e atacantes) usam *VPNs (Virtual Private Networks)** e outros meios de conexão.
- A maioria não pode informar quando um ataque foi bem sucedido. Eles só podem alertar que um ataque foi iniciado, e cabe ao administrador investigar cada host atacado para determinar de fato quais destes foram violados.

3.2 IDS baseado em host

- IDSs baseados em host operam sobre informações coletadas de um único host. Eles podem analisar atividades com grande precisão, determinando exatamente que processos e usuários estão envolvidos em um ataque, pois eles podem diretamente acessar e monitorar os dados e processos do sistema que são geralmente alvo de ataques.

Vantagens dos IDSs baseados em host.

- Com sua habilidade de monitorar eventos localmente num host, podem detectar ataques que não são detectados por um IDS baseado em rede.
- Podem operar em ambientes onde o tráfego seja criptografado, quando os dados são encriptados no host antes do envio e decriptados no host após a recepção.
- IDSs baseados em host não são afetados por switches.

Desvantagens dos IDSs baseados em host.

- São difíceis de gerenciar, pois para cada host monitorado deve ser instalado e configurado um IDS.
- Desde que ao menos as fontes de informações (e algumas vezes parte do mecanismo de análise) residam no host monitorado, o IDS pode ser atacado e desativado mascarando assim um ataque.

- Não são apropriados para detectar scans de rede.
- Podem ser desativados por certos tipos de *ataques de negação de serviço**.
- Consomem recursos computacionais dos hosts que estão monitorando, diminuindo a performance dos mesmos.
- De acordo com o método de análise os IDSs podem usar detecção baseada em assinaturas, detecção baseada em anomalias ou uma mistura dos dois.

3.3 Detecção baseada em assinaturas

- Detectores deste tipo analisam as atividades do sistema procurando por eventos ou conjuntos de eventos que correspondam a padrões pré-definidos de ataques e outras atividades maliciosas. Estes padrões são conhecidos como assinaturas. Geralmente cada assinatura corresponde a um ataque ou outra atividade específica.

Vantagens da detecção baseada em assinaturas.

- São muito eficientes na detecção (comparando-se com a detecção baseada em anomalias) sem gerar grande número de alarmes falsos.
- Podem diagnosticar o uso de uma ferramenta ou técnica específica de ataque.

Desvantagens da detecção baseada em assinaturas.

- Estes detectores somente podem detectar ataques conhecidos, ou seja, que estão incluídos no conjunto de assinaturas que o IDS possui, necessitando-se assim de constante atualização deste conjunto.
- A maioria destes detectores possui as assinaturas muito específicas, não detectando assim as variantes de um mesmo ataque.

3.4 Detecção baseada em anomalias

- Detectores baseados em anomalias identificam comportamentos não usuais (anomalias) num host ou rede. Eles funcionam a partir

do pressuposto que ataques são diferentes da atividade normal e assim podem ser detectados por sistemas que identificam essas diferenças. Detectores baseados em anomalias constroem um perfil que representa o comportamento normal de usuários, hosts e conexões de rede. Este perfil é construído a partir de dados coletados em um período de operação normal. Estes detectores monitoram a rede e usam uma variedade de medidas para determinar quando os dados monitorados estão fora do normal, ou seja, desviando do perfil.

- Infelizmente, este tipo de detecção geralmente produz um grande número de alarmes falsos, pois o comportamento de usuários e sistemas pode variar amplamente. Apesar desta desvantagem, pesquisadores afirmam que a detecção baseada em anomalias pode identificar novas formas de ataques, coisa que a detecção baseada em assinaturas não pode fazer.
- Além disso, algumas formas de detecção baseada em anomalias produzem uma saída que pode ser usada como fonte de informações para detectores baseados em assinaturas. Por exemplo, um detector baseado em anomalias pode gerar um número que representa a quantidade "normal" de arquivos acessados por um usuário em particular, com isso um detector baseado em assinaturas pode possuir uma assinatura que gera um alarme quando esse número excede 10%.
- Ainda que alguns IDSs comerciais incluam formas limitadas de detecção por anomalias, poucos, se não nenhum confiam somente nessa tecnologia. A detecção por anomalias, que existe em sistemas comerciais, geralmente gira em torno da detecção de scans de rede ou de portas. Entretanto, a detecção por anomalias continua na área da pesquisa e pode se tornar muito importante nos IDSs futuros.

Vantagens da detecção por anomalias.

- Detecta comportamentos não usuais, logo possui a capacidade de detectar sintomas de ataques sem um conhecimento prévio deles.

- Produz informações que podem ser usadas na definição de assinaturas para detectores baseados em assinaturas.

Desvantagens da detecção por anomalias.

- Geralmente produz um grande número de alarmes falsos devido ao comportamento imprevisível de usuários e sistemas.
- Requer muitas sessões para coleta de amostra de dados do sistema, de modo a caracterizar os padrões de comportamento normais.

4 Opções de respostas para IDSs.

- Uma vez que o IDS obteve informações de eventos e as analisou a procura de ataques, ele gera respostas. Algumas destas respostas envolve o relato de achados em um local pré-especificado. Outros envolvem respostas automáticas mais ativas. Os IDSs suportam uma grande variedade de opções de respostas, geralmente caracterizadas como respostas ativas e passivas.

4.1 Respostas ativas

- As respostas ativas dos IDS são ações automatizadas realizadas quando determinadas técnicas de intrusão são detectadas. Há três categorias de respostas ativas.

1- Coletar informações adicionais: Geralmente é realizada por meio do aumento da sensibilidade do IDS, por exemplo, aumentar o número de eventos a serem monitorados. Estas informações adicionais ajudam na determinação do que o intruso fez e na determinação da origem do ataque.

2- Mudar o ambiente: É a tentativa de bloquear o ataque e subseqüentes tentativas de acesso do atacante. Tipicamente, IDSs não possuem a habilidade de bloquear o acesso específico de uma pessoa, mas ele bloqueia o endereço *IP** de onde o ataque aparenta estar vindo. Ele faz isso por meio das seguintes ações:

- Injetar pacotes com o flag reset ativado na conexão do atacante, tentando assim finalizar a conexão do mesmo.
- Reconfigurar roteadores e firewalls para bloquear pacotes vindos da aparente localização do atacante (endereço IP).
- Reconfigurar roteadores e firewalls para bloquear portas, protocolos ou serviços que estão sendo usados pelo atacante.
- Em casos extremos, reconfigurar roteadores e firewalls para separar todas as conexões que usam certas *interfaces de rede**.

3- Atacar o invasor: É o lançamento de ataques contra a rede do invasor. Essa prática não é aconselhável, pelo fato do ataque ser baseado no IP que pode ser adulterado facilmente e também porque muita das vezes essa atitude é ilegal.

4.2 Respostas passivas

- Resposta passiva consiste em prover informações sobre os ataques para o administrador, de modo que ele providencie o bloqueio dos ataques. A maioria dos IDSs possui esse método de resposta. Existem duas categorias de respostas passivas:

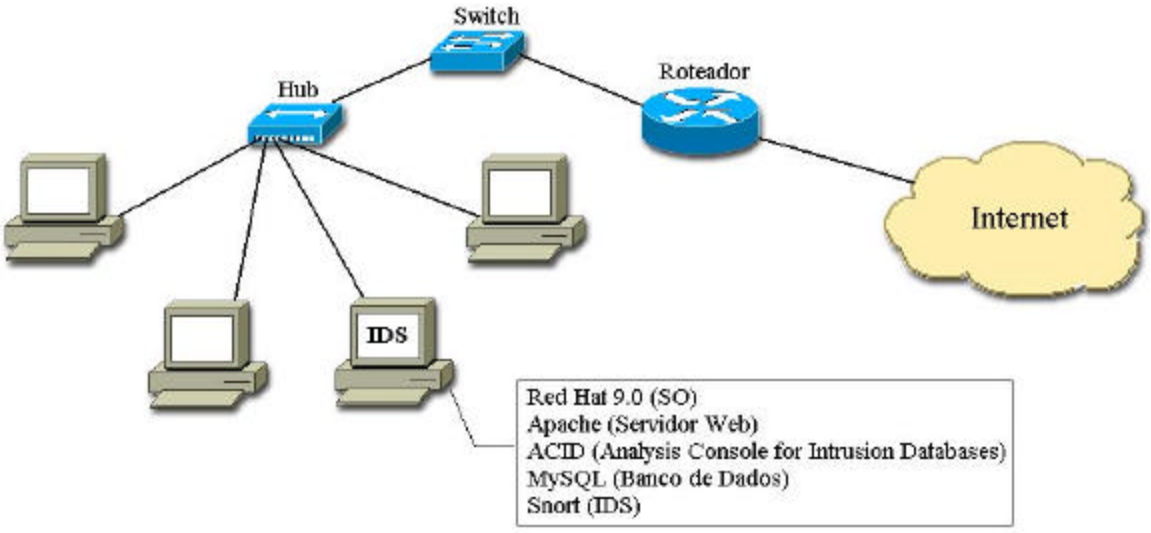
1- Alarmes e notificações: São gerados pelo IDS e enviados a um banco de dados ou via e-mail ao administrador, para posterior análise.

2- Armadilhas *SNMP**: Alguns IDSs foram desenvolvidos para gerar alertas e relatá-los a sistemas de gerenciamento. Estes usam armadilhas SNMP e mensagens para enviar alertas para consoles centrais de gerenciamento de rede, onde eles podem prestar serviço ao administrador. Muitos benefícios estão associados com este sistema, incluindo a habilidade de adaptar a infraestrutura da rede para responder a um ataque, e a habilidade de mover a carga de processamento com uma resposta ativa para outro sistema que não esteja sendo atacado.

Após essa noção sobre a arquitetura de um IDS, a seguir é apresentado um IDS em particular, o SNORT.

5 SNORT

- O Snort (www.snort.org) é um IDS baseado em rede de código fonte aberto, ele usa como principal método de análise a detecção baseada em assinaturas, sendo estas assinaturas, no caso do snort, conhecidas como regras, essas regras podem ser modificadas e novas podem ser escritas, tudo isso usando uma sintaxe própria do programa, muitas delas vem por padrão escritas usando medidas passivas, mas na sintaxe existem comandos que fazem com que o snort tome medidas ativas também. Ele possui versões para os sistemas LINUX e Windows. Abaixo irei exibir um passo a passo de como instalar o Snort num sistema LINUX (Red Hat 9.0) junto com uma ferramenta de gerenciamento via web (ACID), e também a instalação do *MySQL**, e do *Apache** que são intermediários para o funcionamento deste sistema.
- A figura a seguir exibe a configuração testada.



- Neste caso, a própria máquina que está monitorando o tráfego da rede (sensor) está guardando os logs, isso não precisa ser necessariamente assim, pode-se instalar o snort em várias máquinas e todas elas mandarem seus logs para uma máquina central, mas como aqui se trata de um único sensor não há motivo para centralizar os logs em uma outra máquina.

5.1 Guia de Instalação

- De posse de uma máquina com o Red Hat instalado, pode-se começar o processo de instalação.
- Crie uma pasta e baixe todos os arquivos necessários à instalação, as URLs dos arquivos estão listadas abaixo:
- Download Snort 2.2.0

http://www.snort.org/dl/snort-2.2.0.tar.gz
http://www.snort.org/dl/snort-2.0.2.tar.gz

- Download MySQL 4.0.20 Source

http://mysql.secsup.org/Downloads/MySQL-4.0/mysql-4.0.18.tar.gz
http://dev.mysql.com/get/Downloads/MySQL-4.0/mysql-4.0.20.tar.gz/from/http://www.linorg.usp.br/mysql/

- Download apache 2.0.50

http://www.apache.org/dist/httpd/httpd-2.0.50.tar.gz
http://www.apache.org/dist/httpd/httpd-2.0.49.tar.gz

- Download PHP 4.3.3

http://www.php.net/distributions/php-4.3.3.tar.gz

- Download ADODB 3.90

http://phplens.com/lens/dl/adodb390.tgz

- Download Acid 0.9.6b23

http://acidlab.sourceforge.net/acid-0.9.6b23.tar.gz

- Download Zlib 1.2.1

http://www.zlib.net/zlib-1.2.1.tar.gz

- Download JPGraph 1.13

http://www.aditus.nu/jpgraph/downloads/jpgraph-1.13.tar.gz

- Download LibPcap 0.7.2

http://www.tcpdump.org/release/libpcap-0.7.2.tar.gz

- Agora, se você não está logado como root, você deve fazê-lo, pois para instalar os programas você precisa da permissão de superusuário, para isso use o comando **su**. Após, realize os passos listados abaixo:

Instale o zlib:

```
gunzip zlib-1.2.1.tar.gz
tar -xvf zlib-1.2.1.tar.gz
cd zlib-1.2.1
./configure
```

```
make test
make install
cd ..
```

Instale o LibPcap:

```
gunzip libpcap-0.7.2.tar.gz
tar –xvf libpcap-0.7.2.tar.gz
cd libpcap-0.7.2
./configure
make
make install
cd ..
```

Instale o MySQL:

- Crie um usuário e um grupo para o MySQL com os seguintes comandos:

```
groupadd mysql
useradd -g mysql mysql
```

- Entre na pasta **/root** no arquivo **.bash_profile** e edite a linha que inicia com a palavra PATH como se segue:

```
PATH=$PATH:$HOME/bin:/usr/local/mysql/bin
```

- Entre no diretório onde você baixou todos os arquivos, e use os comandos que se seguem para instalar o MySQL.

```
gunzip mysql-4.0.20.tar.gz
tar –xvf mysql-4.0.20.tar.gz
cd mysql-4.0.20
./configure --prefix=/usr/local/mysql
make
make install
cd scripts
mysql_install_db
cd ..
chown -R root /usr/local/mysql
chown -R mysql /usr/local/mysql/var
chgrp -R mysql /usr/local/mysql
cp support-files/my-medium.cnf /etc/my.cnf
```

- Após, adicione as linhas “/usr/local/mysql/lib/mysql” e “/usr/local/lib” no arquivo /etc/ld.so.conf.
- Depois de ter adicionado as linhas, execute o comando “ldconfig

–v", como root.

Testando o funcionamento:

/usr/local/mysql/bin/mysqld_safe --user=mysql &

- (você deve precionar enter para retornar ao prompt)
- Se você não tiver erros, digite "ps –ef |grep mysql". Você deve ver algo como isto:

```
[root@cyclone /]# ps-ef |grep mysql
root 13297 2290 0 11:20 pts/0 00:00:00 /bin/sh /usr/local/mysql/bin/mysqld_safe --user=mysql
mysql 13319 13297 3 11:20 pts/0 00:00:00 /usr/local/mysql/libexec/mysqld -- basedir=/usr/local/mysql
--datadir=/usr/local/mysql/var --user=mysql --pid-file=/usr/local/mysql/var/patrick-redhat.pid --skip-locking
```

- Se tudo funcionou, vá para o próximo passo, que é colocar o MySQL para inicializar junto com o sistema operacional.
- Ajustando o MySQL para inicializar automaticamente.
- Copie o arquivo "mysql.server" da subpasta support-files (ela está contida dentro da pasta de instalação do MySQL. Se você baixou todos os arquivos para a pasta /snortinstall, então o caminho para esse arquivo será /snortinstall/ mysql-4.0.20/support-files) para a pasta /etc/init.d e renomeie com o nome mysql.
- Use os comandos que se seguem para criar links simbólicos nas pastas de inicialização para rodar nos níveis 3 e 5. Com isso o MySQL será carregado automaticamente quando o sistema operacional for inicializado.

```
cd /etc/rc3.d
ln -s ../init.d/mysql S85mysql
ln -s ../init.d/mysql K85mysql
cd /etc/rc5.d
ln -s ../init.d/mysql S85mysql
ln -s ../init.d/mysql K85mysql
cd ../init.d
chmod 755 mysql
```

- Instalando e configurando o Apache com PHP:
- Este procedimento irá instalar o servidor web Apache na pasta "/www".
- Volte a pasta onde estão os arquivos de instalação e faça o que se segue para instalar o Apache e o módulo PHP.

gunzip httpd-2.0.50.tar.gz
tar -xvf httpd-2.0.50.tar.gz
cd httpd_2.0.50
./configure --prefix=/www --enable-so
make
make install

Digite "/www/bin/apachectl start"

- Cheque o sistema para ter certeza que o servidor web está funcionando (entre com o IP da máquina num browser).

Digite "/www/bin/apachectl stop"
cd ..
gunzip php-4.3.3.tar.gz
tar -xvf php-4.3.3.tar.gz
cd php-4.3.3
./configure --prefix=/www/php --with-apxs2=/www/bin/apxs --with-config-file-path=
/www/php --enable-sockets --with-mysql=/usr/local/mysql --with-zlib-dir=
/usr/local --with-gd (tudo isso em uma linha)
make
make install
cp php.ini-dist /www/ php/php.ini

- Agore edite o arquivo httpd.conf (ele está em /www/conf) e adicione:

LoadModule php4_module modules/libphp4.so (A nova versão do PHP adiciona isto para você).
AddType application/x-httpd-php .php (pressione ctrl-w e procure por AddType)
DirectoryIndex index.php index.html index.html.var (Procure por DirectoryIndex)

- Irá ficar parecido com as linhas abaixo quando você tiver terminado

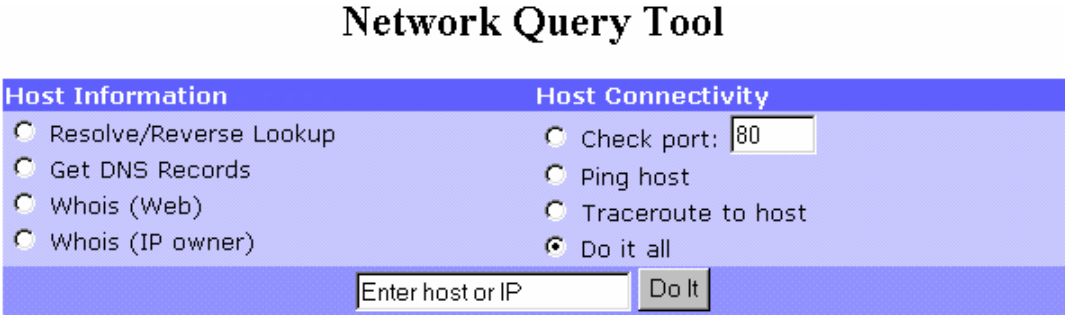
#
LoadModule foo_module modules/mod_foo.so
LoadModule php4_module modules/libphp4.so
AddType allows you to tweak mime.types without actually editing it, or $
make certain files to be certain types.
#
AddType application/x-tar .tgz
AddType image/x- icon .ico
AddType application/x-httpd-php .php
The index.html.var file (a type-map) is used to deliver content-

```
# negotiated documents. The MultiViews Option can be used for the
# same purpose, but it is much slower.
#
DirectoryIndex index.php index.html index.html.var
```

- Apache 2.0.50 está instalado na pasta /www. Entre na subpasta /www/bin e execute os seguintes com andos:

```
cp apachectl /etc/init.d/httpd
cd /etc/rc3.d
ln -s ../init.d/httpd S85httpd
ln -s ../init.d/httpd K85httpd
cd /etc/rc5.d
ln -s ../init.d/httpd S85httpd
ln -s ../init.d/httpd K85httpd
```

- (As linhas acima irão adicionar um script nos níveis 3 e 5 de inicialização)
- Para testar a instalação do Apache + PHP, crie um arquivo chamado test.php na pasta /www/htdocs. Adicione a seguinte linha de comando no arquivo “<?php phpinfo(); ?>” (sem as aspas).
- Inicie o apache usando “/etc/rc5.d/S85httpd start”. Agora use um navegador para ver o arquivo (http://Endereço_IP/test.php). Ele deve exibir informações do seu sistema Apache e PHP.
- Se você quiser fazer um outro teste tente usar http://shat.net/php/nqt/nqt.php.txt. Copie este arquivo para /www/htdocs e renomeie para index.php. Use um navegador para visualizar o arquivo (http://Endereço_IP/ index.php) e você verá isto:



- Instalando e ajustando o Snort e as regras do Snort:

groupadd snort
useradd -g snort snort
mkdir /etc/snort
mkdir /var/log/snort
gunzip snort-2.2.0.tar.gz
tar -xvf snort-2.2.0.tar.gz
cd snort-2.2.0
./configure --with-mysql=/usr/local/mysql
make
make install

- Instalando as regras e o arquivo .conf:
- A partir do diretório de instalação do Snort

cd rules
cp * /etc/snort
cd ../etc
cp snort.conf /etc/snort
cp *.config /etc/snort

- Modifique o arquivo snort.conf:
- No arquivo snort.conf que está localizado na pasta /etc/snort, faça as seguintes alterações.

var HOME_NET 10.2.2.0/24 (Esta variável define a sua rede interna)

- Altere a variável rule path

var RULE_PATH /etc/snort/

- Adicione a linha abaixo para o Snort usar o MySQL como seu banco de dados, a senha é a mesma que você usou na configuração do mysql.

output database: log, mysql, user=snort password=**senha** dbname=snort host=localhost

- Configure o snort para iniciar automaticamente:
- Use para isso o script localizado no diretório contrib contido na pasta de instalação do snort, S99snort. Copie ele para a pasta

/etc/init.d e renomeie com o nome snort (cp contrib/S99snort /etc/init.d/snort).

- Mude as seguintes linhas:

```
CONFIG=/etc/snort/snort.conf
SNORT_GID=snort
```

- Entre no diretório /etc/init.d e digite:

```
chmod 755 snort (Muda as permissões do arquivo que você copiou e editou)
cd /etc/rc3.d
ln -s ../init.d/snort S99snort
ln -s ../init.d/snort K99snort
cd /etc/rc5.d
ln -s ../init.d/snort S99snort
ln -s ../init.d/snort K99snort
```

- Ajustando o banco de dados no MySQL:
- Obs.: No MySQL o ponto e vírgula ";" é obrigatório ao final de cada linha e **senha** é a senha que você quer usar.

```
/usr/local/mysql/bin/mysql
mysql> SET PASSWORD FOR root@localhost=PASSWORD('senha');
>Query OK, 0 rows affected (0.25 sec)
mysql> create database snort;
>Query OK, 1 row affected (0.01 sec)
mysql> grant INSERT, SELECT on root.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> SET PASSWORD FOR snort@localhost=PASSWORD('new_password');
>Query OK, 0 rows affected (0.25 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort;
>Query OK, 0 rows affected (0.02 sec)
mysql> exit
>Bye
```

- A partir da pasta de instalação do Snort 2.2.0, execute os seguintes comandos:
- (Obs.: Quando você está trabalhando com o MySQL e ele pede uma senha, ele está se referindo a senha definida por você pela linha de comando: "SET PASSWORD FOR root@localhost=PASSWORD('**senha**');")

```
/usr/local/mysql/bin/mysql -u root -p < ./contrib/create_mysql snort
Enter password:
```

- Após, instale as tabelas extras do banco de dados usando o seguinte comando a partir da pasta contrib

```
zcat snortdb-extra.gz |/usr/local/mysql/bin/mysql -p snort
Enter password:
```

- Agora você precisa verificar se o banco de dados snort foi criado corretamente

```
/usr/local/mysql/bin/mysql –p
>Enter password:
mysql> SHOW DATABASES;
```

- (Você deve ver isto)

```
+------------+
| Database
+------------+
| mysql
| snort
| test
+------------+
3 rows in set (0.00 sec)
mysql> use snort
>Database changed
mysql> SHOW TABLES;
+------------------+
| Tables_in_snort
+------------------+
| data
| detail
| encoding
| event
| flags
| icmphdr
| iphdr
| opt
| protocols
| reference
| reference_system
| schema
| sensor
| services
| sig_class
| sig_reference
| signature
```

```
| tcphdr
| udphdr
+------------------+
19 rows in set (0.00 sec)>Bye
```

Instale o JPGraph:

- Volte ao diretório onde estão os arquivos de instalação

```
cp jpgraph-1.13.tar.gz /www/htdocs
cd /www/htdocs
gunzip jpgraph-1.13.tar.gz
tar –xvf jpgraph-1.13.tar.gz
rm –rf jpgraph-1.13.tar.gz
cd jpgraph-1.13
rm -rf README
rm -rf QPL.txt
```

Instale o ADODB:

- Volte ao diretório onde estão os arquivos de instalação

```
cp adodb390.tgz /www/htdocs/
cd /www/htdocs
gunzip adodb390.tgz
tar -xvf adodb390.tgz
rm –rf adodb390.tgz
```

Instalando e configurando o Acid:

- Volte ao diretório onde estão os arquivos de instalação

```
cp acid-0.9.6b23.tar.gz /www/htdocs
cd /www/htdocs
gunzip acid-0.9.6b23.tar.gz
tar –xvf acid-0.9.6b23.tar.gz
rm -rf acid-0.9.6b23.tar.gz
```

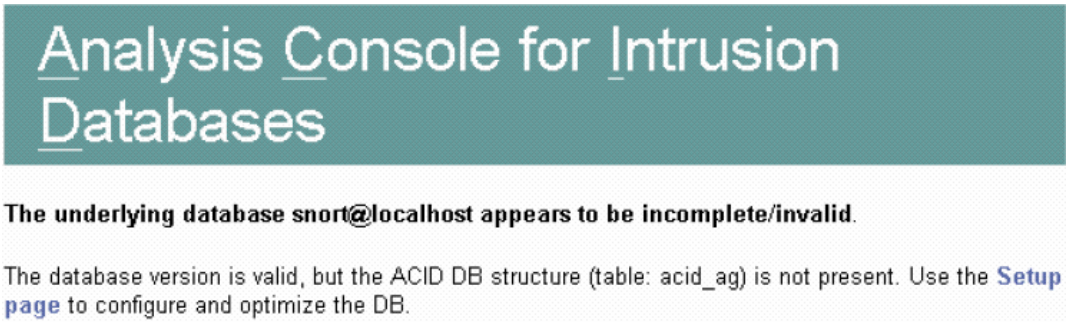
Configurando o Acid:

- Entre na pasta /www/htdocs/acid/ e edite o arquivo acid_conf.php. Você deve ver algo similar a isto:

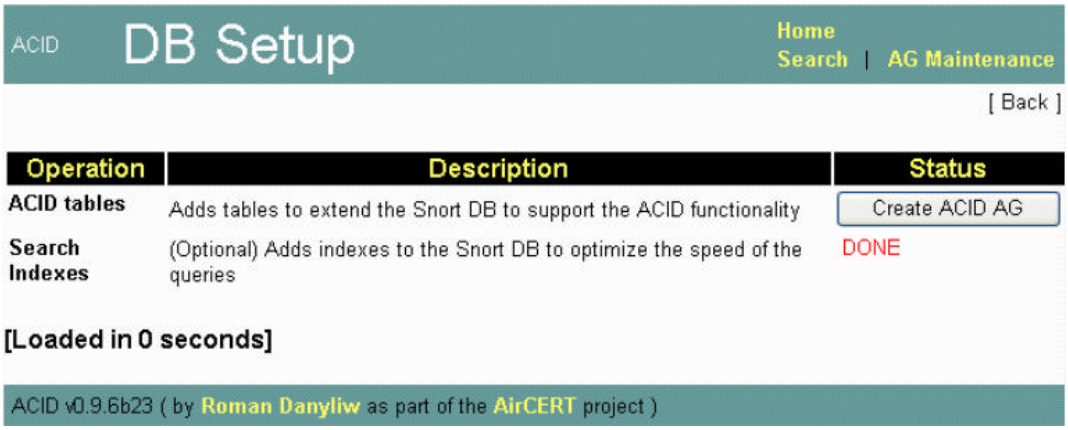
```
$DBlib_path = "/www/htdocs/adodb";
/* The type of underlying alert database
*
* MySQL : "mysql"
* PostgresSQL : "postgres"
* MS SQL Server : "mssql"
*/
$DBtype = "mysql";
/* Alert DB connection parameters
```

```
* - $alert_dbname : MySQL database name of Snort alert DB
* - $alert_host : host on which the DB is stored
* - $alert_port : port on which to access the DB
* - $alert_user : login to the database with this user
* - $alert_password : password of the DB user
*
* This information can be gleaned from the Snort database
* output plugin configuration.
*/
$alert_dbname = "snort";
$alert_host = "localhost";
$alert_port = "";
$alert_user = "snort";
$alert_password = "senha";
/* Archive DB connection parameters */
$archive_dbname = "snort";
$archive_host = "localhost";
$archive_port = "";
$archive_user = "snort";
$archive_password = "senha";
And a little further down
$ChartLib_path = "/www/htdocs/jpgraph-1.13/src";
/* File format of charts ('png', 'jpeg', 'gif') */
$chart_file_format = "png";
```

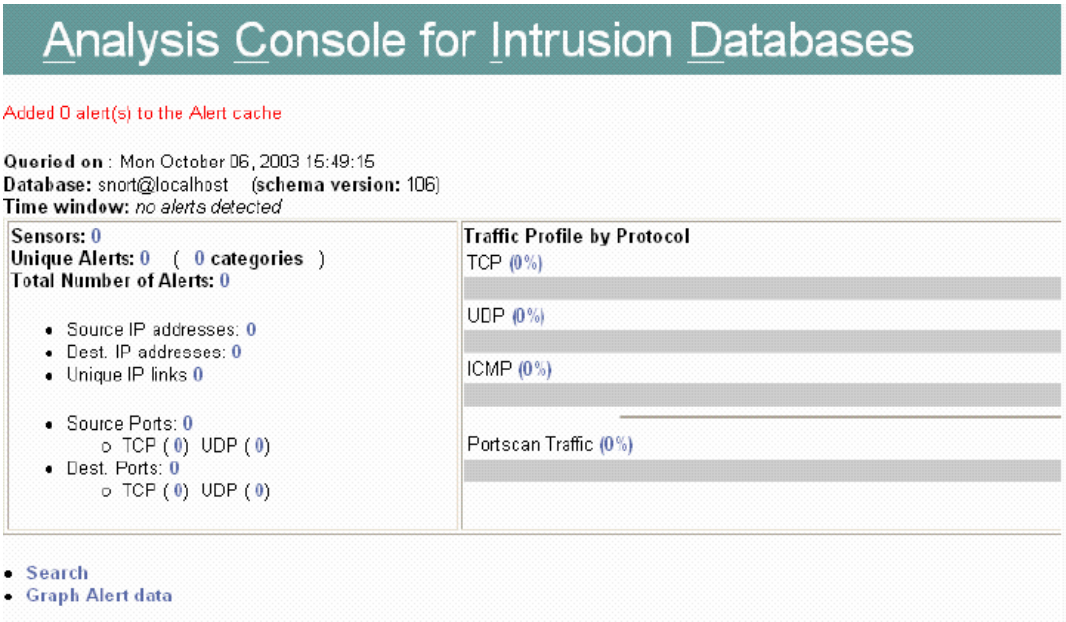
- Inicie o Apache e entre no endereço http://**seuhost**/acid/acid_main.php. Você irá ver uma mensagem como esta em seu navegador:



- Clique em “Setup Page” para criar as tabelas que o Acid usa, você irá ver o seguinte:



- Clique no botão “Create Acid AG”. Agora quando você entrar no endereço http://**seuhost**/acid/ você deve ver a página do ACID.



Restringindo o acesso a página do Acid:

- Como o Acid exibe informações de sua rede, é de se esperar que o acesso a essas informações seja restrito. Para prover um pouco de segurança, o Apache disponibiliza um meio de restringir o acesso, pedindo usuário e senha toda vez que você tenta acessar uma pasta com esse método de restrição habilitado.
- Abaixo está descrito como aplicar essa restrição na pasta do Acid.

mkdir /www/passwords
/www/bin/htpasswd -c /www/passwords/passwords **acid**

- **acid** será o nome do usuário, logo após será pedido uma senha para esse usuário, esse nome de usuário e senha serão os requisitados toda vez que você acessar a página do acid.
- Edite o arquivo httpd.conf (/www/conf) e inclua as seguintes linhas abaixo da seção que começa com </Directory>.

```
<Directory "/www/htdocs/acid">
AuthType Basic
AuthName "SnortIDS"
AuthUserFile /www/passwords/passwords
Require user acid
</Directory>
```

- Agora reinicie o serviço http (/etc/init.d/httpd restart) para tornar efetiva as alterações.

Verifique se está tudo funcionando:

- Reinicie seu sistema, verifique se todos os programas iniciaram, você pode fazer isso digitando num shell “ps–ef |grep **serviço**” onde o campo **serviço** é qualquer processo em execução, como por exemplo, mysql, httpd, snort, etc.
- Agora você deve testar o snort, para isso use algum scanner de vulnerabilidades como o Nessus (http://www.nessus.org), rode o nessus contra a máquina que contém o snort, depois verifique o Acid, você deve encontrar uma dezena de alertas.
- Agora você deve ajustar o IDS para seu ambiente, eliminando regras desnecessárias, e até escrevendo novas, para manipular regras use o manual do usuário que se encontra no site www.snort.org.

6 Conclusão

- IDS's vieram para ficar, eles complementam a segurança de uma rede auxiliando no ajuste de outras ferramentas de segurança e fornecendo dados valiosos para a perícia de redes invadidas. Entretando os IDS's ainda são difíceis de configurar e operar e geralmente não podem ser eficientemente usados por pessoas

inexperientes. O processo de ajuste e possicionamento de um IDS's não é nada trivial, tendo que ser feita para isso uma análise do tráfego da rede, e a partir dessa análise ajustar que tipo de informações o IDS irá monitorar e em que pontos da rede deve ser feita essa monitoração.

- O assunto tratado neste texto representa um vasto campo para estudo e pesquisas. Visto a abrangência deste assunto esta nota técnica dá apenas uma noção básica sobre IDS's, reunindo conceitos fundamentais sobre essa tecnologia.

7 Glossário

ACID – Analysis Console for Intrusion Databases – Programa que proporciona uma interface via web para gerenciamento de alertas gerados por IDSs.

ACL Access Control List – Lista de controle de acesso é o meio usual pelo qual o acesso e a negação de serviços são controlados. É simplesmente uma lista que contém os host que podem acessar ou não determinados serviços.

Ataque de negação de serviço – Ocorre quando alguém maliciosamente direciona em um servidor intensas requisições de seu serviço ou gera condições de intenso tráfego fazendo com que o mesmo trave devido a sobrecarga.

Apache – Servidor web base linux gratuito.

Bridge – Dispositivo que repassa o tráfego entre segmentos de rede, baseado na camada de enlaçe do modelo OSI. Estes segmentos podem ser de uma mesma rede ou não.

Uma grande utilidade deste dispositivo, é usá-lo como filtro de pacotes, sem necessitar de alterações na configuração já estabelecida nos dispositivos de rede.

Criptografia – São os meios e métodos de se transformar informações legíveis em ilegíveis e a partir dessas mensagens ilegíveis poder retornar à informação original por meio de uma chave, como uma espécie de senha.

Dispositivo de controle – Software ou hardware que dita as regras com relação àpermissão de um dado tráfego de rede.

Firewall – Combinação de hardware e software cujo papel é filtrar o tráfego de informações entre redes privadas e a Internet. Uma de suas inúmeras aplicações é o bloqueio do acesso a serviços ou dados de uma rede

interna por meio de usuários externos não autorizados.

Host – Computador conectado a uma rede.

IDS Intrusion Detection Sistem – Sistemas de Detecção de Intrusos são programas que monitoram uma rede ou um host a procura de sinais padrões de comportamento que sejam considerados maliciosos, ou seja, podem constituir um ataque ou uma outra atividade não permitida.

Interfaces de rede - Dispositivo que permite a um computador conectar-se a uma rede (LAN, WAN, internet etc).

IP Internet Protocol – É um protocolo desenvolvido para uso em sistemas de comunicação por comutação de pacotes. Este protocolo especifica o formato dos pacotes (também chamados datagramas) e o esquema de endereçamento.

MySQL – Programa para criação e manipulação de banco de dados

Política de segurança – Conjunto de normas que ditam o que é e o que não é permitido em um rede, como por exemplo, que tipo de serviços podem estar ativos (ftp, http), que hosts podem ser acessados diretamente da internet, etc. Essas normas após definidas são implementadas no sistema por meio de firewalls, IDSs e outros dispositivos que se façam necessários.

Roteador – Dispositivo que usa uma ou mais medidas para determinar o melhor caminho por onde o tráfego de rede deve transitar. Roteadores repassam pacotes de uma rede para outra baseando-se na informação da camada de rede.

Scanner de vulnerabilidade – Programa que investiga um host, na maioria das vezes remotamente, para ver se este está vulnerável á um conjunto de tipos ataques. Muito útil para corrigir vulnerabilidades bem como para atacar um sistema.

Segmento de rede – Parte de uma rede, onde o trafego de mensagens é comum a todos os nós.

SNMP Simple Network Management Protocol – É um conjunto de protocolos para gerenciar redes complexas.

Switch – Dispositivo que filtra e repassa pacotes entre segmentos de uma LAN. Switches operam na camada de enlace do modelo de referência OSI.

Tráfego de rede – Conjunto de dados que transitam pelos dispositivos de uma rede de computadores.

VPN Virtual Private Networks – Rede privada virtual é uma rede privada construída sobre um meio público para conectar nós de uma rede. Tipicamente as redes envolvidas são redes IP, sendo a internet o exemplo mais comum. Para manter a privacidade da rede usa-se túneis encritados e outros mecanismos de segurança, de modo a garantir que somente usuários autorizados possam acessar a rede e que os dados não possam ser interceptados.

8 Referências Bibliográficas

Intrusion Detection Systems

Rebeca Bace and Peter Mell

- http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf

Deploying and Tunning Network Intrusion Detection Systems

Intrusion.com

- http://intrusion.com/products/download/Deploying_and_Tuning_NIDS.pdf

Snort, Apache, PHP, MySQL and Acid Install on RH9.0

By Patrick Harper, CISSP

- http://www.snort.org/docs/snort_acid_rh9.pdf

Snort User Manual

Martin Roesch, Chris Green

- http://www.snort.org/docs/snort_manual.pdf