Slackware, Snort, Acid, mySQL, Flexresp, Snortsam.

Introdução:

Este manual se destina a instalação de um servidor **IDS(Sistema de Detecção de Intrusão)**, utilizando o sistema operacional Linux distibuição **Slackware**, para isto iremos utilizar um produto gnu chamado **snort**, e fazer a sua integração com o banco de dados **mySQL**, utilizando um sistema de gerenciamento de ***logs*** chamado **ACID**, com o bloqueio de pacotes, para isto utilizaremos o **snortsam** que faz a integração com **Checkpoint Firewall-1** e a facilidade de ***reset*** na conexão dos pacotes, utilizando **flexresp**.

Escolha dos Produtos:

O sistema operacional foi escolhido com base em minha experiencia profissional em sistemas operacionais baseados em **Unix**, basicamente **AIX** e **Linux**.
A distribuição foi escolhida pois se trata de uma das melhores e mais confiáveis além de ser adotada pela nossa instituição com sendo a distribuição para os servidores.
O **Snort** foi escolhido pois foi testado outros sistemas e o mais completo, funcional, com facilidade de manipulação de pacotes e integração com sistema de firewall.
Os outros pacotes foram escolhidos pois se integram com o **Snort**.

Objetivos:

O objetivo deste manual, não é ensinar a instalação do sistema operacional nem dos produtos utilizados e sim as suas configurações para que o servidor tenha o desempenho necessário para a função designada.

Produtos:

Os produtos necessários para a instalação estão no quadro abaixo, não colocarei a versão, pois sempre será utilizado a ultima versão de cada produto.

Slackware	http://www.slackware.org
Snort.	http://www.snort.org
Acid.	http://acidlab.sourceforge.net
Adodb.	http://php.weblogs.com/adodb
phplot.	http://www.phplot.com
jpgraph	http://www.aditus.nu/jpgraph
gd.	http://www.boutell.com/gd
MySQL.	http://www.mysql.com
Snortsam.	http://www.snortsam.net
Apache.	http://www.apache.org
Php	http://www.php.net

Definição do Projeto:

A definição nesta parte é um passo importante, pois toda a sua configuração deve ser feita e seguida conforme a definição do seu projeto de **IDS**, no caso eu utilizei tres servidores, sendo um para o **Snort**, outro para o repositorio de dados onde ficarão os alertas, e outro onde será a console de gerenciamento. Sendo assim um servidor **IDS** (**snort**), um servidor de Banco de Dados (**mySQL**) e outro servidor **Web** (**Apache**).

Instalações:

Neste apendice iremos verificar apenas as instalações dos produtos ficando assim a configuração para o apendice seguinte.

1. Instalação do Slackware:

A instalação do sistema operacional é padrão, como não é o nosso objetivo ensinar a sua instalação e partindo do princípio que os leitores utilizam o slackware, não detalharei a sua instalação.

2. Instalação do mySQL.

Se a instalação do **slackware** foi padrão, então o **mysql** já esta instalado, o que falta ser feito é a sua configuração, que iremos tratar mais adiante, no item Configuração.

3. Instalação do Snort.

Utilizando o usuario *root* e após baixarmos **snort** do link especificado anteriormente, move-lo para a pasta */usr/src*, descompacta-lo utilizando o comando "*tar -zxvf*". Será criado um diretório com o nome snort-x.y.z, onde x.y.z é a versão do produto.
Feito isto, entramos no diretório criado e faremos a compilação do **snort**, seguindo os passos:
#./configure –prefix=/usr –enable-flexresp –with-mysql
#make
#make install
o comando acima irá preparar o **snort** para aceitar comandos de **reset** de conexão e irá fazer a conexão com o banco de dados **mysql**, além de ser instalado a partir do */usr* do seu servidor.
Note que se tivermos que fazer a integração com o **firewall-1** da **Checkpoint**, primeiro faremos o passo 4 (Instalação do snortsam), depois antes de compilar o **snort**, utilizaremos os comando aclocal, autoheader, automake, autoconf, ficando assim:
#./configure –prefix=/usr –enable-flexresp –with-mysql
#aclocal
#autoheader
#automake
#autoconf
#make
#make install

4. Instalação do snortsam.

Este é feito em dois passos, o primeiro é feito do servidor **snort** e o segundo feito na console de gerenciamento do servidor **firewall-1**, iremos mostrar as duas instalações.

Primeiro passo:

Este não é uma instalação e sim uma aplicação de *patch*, devemos baixar do site o produto snortsam-patch.tar.gz, após baixarmos do produto devemos coloca-lo no diretório */usr/src*. Após move-lo devemos descompacta-lo utilizando o comando "*tar -zxvf*", feito a descompactação devemos utilizar o comando patchsnort.sh, conforme o exemplo abaixo:
#./patchsnort.sh snort-xx.yy.zz
isto irá aplicar as bibliotecas necessárias para o funcionamento do **fwsam** no **snort** e assim poder fazer o bloqueio de pacotes utilizando os recursos do **firewall-1**.
Depois é o passar para a compilação do produto descrito no item 3 instalação do **snort**.

Segundo Passo:

Devemos baixar do site o programa para leitura dos alertas gerados e para fazer a interpretação do bloqueio para o **firewall-1**, este programa nada mais é que um agente que fica em background "escutando" os alertas do snort e passando as informações para o **firewall-1**.

O agente é o snortsam-opsec-xx.yy.zip, onde o xx.yy é a versão, após baixar este arquivo devemos criar um diretório no console do **firewall-1** e descompacta-lo neste diretório. Será necessário fazer um arquivo de configuração para este agente, que veremos mais adiante.

Tome cuidado e baixe somente o agente para o sistema operacional que esta sendo utilizado no console do **firewall-1**. No meu caso eu utilizo **windows NT.**

5. Instalação do PHP.

Se a instalação do **slackware** foi padrão, então o **PHP** já esta instalado, o que falta ser feito é a sua configuração, que iremos tratar mais adiante, no item Configuração.

6. Instalação do ACID.

O **ACID** é um gerenciador de alertas do snort, ele é muito flexivel, pois pode ser carregado de qualquer browser e em qualque máquina, não sendo necessário uma console específica para ele

Na verdade não é uma instalação e sim uma descompactação dos arquivos, no diretório de web do servidor, faltando apenas fazer as configurações para o seu funcionamento, no qual veremos a seguir.

Devemos baixar o arquivo *acid-0.9.6b23.tar.gz*, e descompacta-lo no diretório */var/www/htdoc*, ficando assim

#pwd

#/var/www/htdocs/acid

7. Instalação do adodb.

O **adodb** é uma biblioteca do php para acesso de dados nos gerenciadores de abnco de dados.

Na verdade não é uma instalação e sim uma descompactação dos arquivos, no diretório de web do servidor, faltando apenas fazer as configurações para o seu funcionamento, no qual veremos a seguir.

Devemos baixar o arquivo *adodb.xx.tgz*, e descompacta-lo no diretório */var/www/htdoc*, ficando assim

#pwd

#/var/www/htdocs/adodb

8. Instalação do phplot.

Este pacote serve para gerar gráficos no **php**, facilitando assim a visualização dos alerta e geração de relatórios nod **ACID**.

Na verdade não é uma instalação e sim uma descompactação dos arquivos, no diretório de web do servidor, faltando apenas fazer as configurações para o seu funcionamento, no qual veremos a seguir.

Devemos baixar o arquivo *phplot-x.y.z.tar.gz*, e descompacta-lo no diretório */var/www/htdoc*, ficando assim

#pwd

#/var/www/htdocs/phplot

9. Instalação do jpgraph.

Esta é uma classe biblioteca para o **php** e necessita do **gd** para gerar os gráficos dinamicamente.
Na verdade não é uma instalação e sim uma descompactação dos arquivos, no diretório de web do servidor, faltando apenas fazer as configurações para o seu funcionamento, no qual veremos a seguir.
Devemos baixar o arquivo *jpgraph.x.yy.z.tar.gz*, e descompacta-lo no diretório */var/www/htdoc*, ficando assim
#pwd
#/var/www/htdocs/jpgraph

10.Instalação do gd.

Este é uma biblioteca para criação de imagens dinâmica e assim facilita o trabalho do php no tratamento de gráficos.
Na verdade não é uma instalação e sim uma descompactação dos arquivos, no diretório de web do servidor, faltando apenas fazer as configurações para o seu funcionamento, no qual veremos a seguir.
Devemos baixar o arquivo *gd.x.y.zz.tar.gz*, e descompacta-lo no diretório */var/www/htdoc*, ficando assim
#pwd
#/var/www/htdocs/gd

Configuração:

Neste apendice iremos ver as configurações necessárias para o funcionamento do produto, lembre-se que estas configurações são customizavéis sendo possivel a sua alteração confirme o projeto do seu snort.

1. Configurando o slackware.

Compreende-se configuração do **slackware**, toda a customização feita para deixar o servidor seguro, tirando os acesso e serivços desnecessários para a tarefa do **snort**.
Também podemos colocar aqui, a configuração de rede sendo assim necessário 2 placas de redes, sendo uma para a gerencia do snort e outra ficará em modo *stealth* ou seja, sem configuração de endereço *I.P.*
Para se fazer as configurações, será necessário pelo menos um conhecimento básico na distribuição slackware, pois, os serviços são dispostos de maneira diferente das outras distribuições.
Para colocarmos uma placa em *stealth mode*, podemos utilizar o comando *ifconfig*.
Como por exemplo:
#ifconfig eth1 up

Podemos colocar esta linha no arquivo */etc/rc.d/rc.inet1* para já iniciar a placa *eth1* como *up* no *boot* do sistema.
Verificar também se o *switch* no qual está ligao o cabo da placa *stealth* se esta com as configurações certas, por exemplo se esta em *full-duplex* e em *100mb*.
Se o *link bit* não subir utilize o comando *mii-tool* para ajustar a configuração da placa *ethernet* com o *switch.*

2. Configurando o apache.

Seja qual for a construção que deseja se fazer, é necessário se configurar um serviço *web* no servidor, no meu caso, utilizei um servidor *web* a parte para fazer a gerencia do **snort**.
Eu utilizei uma configuração do **apache** com **ssl**, ou seja, só configurei o serviço 443 no **apache**, para isto devemos ir no arquivo de configuração do **apache**

/etc/apache/httpd.conf, comentar as linhas onde tem o serviço 80 e deixar descomentada a linha do serviço 443, descomentar a linha onde tem o **mod_ssl** e o **mod_php**.
Editar o arquivo *mod_ssl.conf* e configurar o *virtual host* para que ele veja o diretório */var/www/htdocs/acid.* Não se esquecer de gerar as chaves em **openssl** para fazer a conexão segura. Não mostrarei este passo aqui, pois este é um outro documento já escrito por mim.
Alterar o *script* de inicialização automática do **apache**, */etc/rc.d/rc.httpd*, colocar o *apachectl startssl* neste *script*.

3. Configurando o mySQL.

Aqui mostrarei como ativar o banco automaticamente e como criar a base de dados para autilização do **snort**, neste caso eu também utilizei um servidor a parte.
Como eu já tinha um servidor de banco de dados **mySQL**, eu somente criei a base de dados, mas como o objetivo e configur-lo então vamos lá.
Se o servidor é o mesmo do snort ou um servidor a parte e é a primeira vez que se vai ativar o **mySQL** no servidor, devemos execurtar o comando *mysql_db_install*, isto fará com que se crie as base inicias para o **mySQL**.
Após isto devemos definir uma senha para o acesso ao **mySQL**, e a criação do banco do **snort**, basta seguir os passos:
#mysql
mysql> SET PASSWORD FOR usuario@localhost=PASSWORD('senha');
mysql> CREATE DATABASE snort;
mysql> GRANT INSERT, SELECT on usuario. to snort@localhost;*
mysql>exit
mysql>bye

Note que os passos acima ajustaram a senha para o usuário de administração do banco definido anteriormente, que no meu caso é snort, criado uma base de dados chamada snort e por último dados permissão de acesso de *insert* e *select* ao usuário criado.

Para criarmos as tabelas que serão utilizadas pelo **ACID,** devemos proceder da seguinte forma:
entrar no diretorio do snort contrib,
#cd /usr/src/snort-xx-yy-zz/contrib
#mysql -p < create_mysql snort

Agora devemos fazer com que o **mySQL** inicie automaticamente no *boot* do sevidor, ara isto devemos criar um *rc.mysql* no */etc/rc.d*, com a linha *safe_mysqld &,* e mudar o tributo do arquivo para 755. Assim ele será lido no boot do sistem e será inicialido.

4. Configuração do snort.

A configuração do snort é bastante simples, após a compilação e a instalação, devemos criar um diretório onde que irá conter o arquivo de configuração e os arquivos que contém as regras com as assinaturas de ataques.
Basta criar um diretório no */etc* com o nome *snort*.
#cd /etc
#mkdir snort
#cd snort
Dentro do diretório de instalação do **snort** tem um arquivo de exemplo de configuração com o nome *snort.conf* ,copie ele para dentro do */etc/snort*.
Feito isto, devemos edita-lo, descomentando as opções com os parametros necessários para o seu funcionamento de acordo com o que foi definido.

Para começar devemos alterar a variável que contém o valor da rede que será analisada.
Exemplo: *var HOME_NET 10.1.13.0/24.*
Alterar o valor da variável que contém o path dos arquivos de configurações.
Exemplo: *var RULE_PATH /etc/snort*
Altarar a linha onde se encontra a maneira com a qual será guardado os logs e os alertas.
Exemplo: o*utput database: log, mysql, user=usuario password=senhadousuario dbname=snort host=nome do servidor*
Colocar a linha para que o snort faça o bloqueio de pacotes utilizando o firewall-.
Exemplo: *output alert_fwsam: endereço ip da console do fw-1/senha.*

Normalmente os preprocessor estão descomentados, eles é que fazer a verificação de assinaturas e consultam no arquivos de regras os sid relativos aos chamados ataque.
No meu caso eu deixo todos os preprocessors descomentados e também todos os arquivo de regras.
Exemplo: *include smtp.rules*
include imap.rules
include pop2.rules
include pop3.rules

Além dos arquivos de regras, existe tambem um outro arquivo não documentado que contém algumas assinaturas, voce deve conseguir no site: http://www.whitehats.com/ids, e baixar o arquivo *vision18.rules.gz*, depois, descompacta-lo no diretório /etc/snort, e incluir no final do arquivo snort.conf a linha:

include vision18.conf

Após feito a configuração do **snort**, devemos criar um arquivo para inicializa-lo autmaticamente no *boot* do sistemas, por exemplo: no */etc/rc.d*, o arquivo *rc.snort* com a linha de comando */usr/bin/snort -D -c /etc/snort.conf -i eth1*.
Isto fará com que o snort entre automaticamete após o sistema ser ativado.

5. Configuração do snortsam.

Anteriormente nós instalamos o snortsam na console do firewall-1que no meu caso é windows NT, criamos um diretorio chamado snortsam e dentro dele colocaremos os arquivos de configuração.
Os arquivos são:
snortsam.cfg e rootservers.cfg

o conteudo do arquivo *snortsam.cfg* é:
accept endereço ip do snort, senha
inlcude rootservers.cfg

o conteudo do arquivo *rootservers.cfg* é:
dontblock a.root-servers.net
dontblock b.root-servers.net
dontblock c.root-servers.net
dontblock d.root-servers.net
dontblock e.root-servers.net
dontblock f.root-servers.net
dontblock g.root-servers.net
dontblock h.root-servers.net
dontblock i.root-servers.net

dontblock j.root-servers.net
dontblock k.root-servers.net
dontblock l.root-servers.net
dontblock m.root-servers.net
dontblock a.gtld-servers.net
dontblock b.gtld-servers.net
dontblock c.gtld-servers.net
dontblock d.gtld-servers.net
dontblock e.gtld-servers.net
dontblock f.gtld-servers.net
dontblock g.gtld-servers.net
dontblock h.gtld-servers.net
dontblock i.gtld-servers.net
dontblock j.gtld-servers.net
dontblock k.gtld-servers.net
dontblock l.gtld-servers.net
dontblock m.gtld-servers.net

Feito estes passo, só será necessaio alterar as regras com os parametro necessarios para o bloqueio, isto veremos mais adiante.
Agora é só ativar o ssnortsam no gerenciador de console.
Exemplo:
C:snortsam>snortsam.exe <enter>
Note que ele ficará rodando em background, entãoterá uma janela window ssempre aberta para este aplicativo.

6. Configuração do PHP.

Como no já instalamos o slackware e ele já vem com o php instalado, não é necessário fazer qualquer tipo de configuração neste módulo.

7. Configuração do ACID.

O **acid** foi todo escrito em **php**, então todas os arquivos são textos e de configuração simples, devendo apenas alterar as variáveis que for indicada.
Esta é a mais simples das configurações, devemos ir para o diretório onde se encontra o **acid**, que na instalação foi o */var/www/htdocs/acid*, neste diretório tem um arquivo de configuração chamado *acid_config.php.*
Edite este arquivo e altere as variaveis:
DBlib_path = "../adodb";
$DBtype = "mysql";
$alert_dbname = "nome do banco";
$alert_host = "ip do servidor";
$alert_port = "";
$alert_user = "usuario adm do banco";
$alert_password = "senha do usuario";
$ChartLib_path = "../jpgraph/src";

8. Configuração do adodb.

Este pacote não necessita de nenhuma configuração, somente fazer a descompactação do pacote no diretório descrito no item de instalação.

9. Configuranção do phplot.

Este pacote não necessita de nenhuma configuração, somente fazer a descompactação do pacote no diretório descrito no item de instalação.

10.Configuração do jpgraph.

Este pacote não necessita de nenhuma configuração, somente fazer a descompactação do pacote no diretório descrito no item de instalação.

11.Configuração do gd.

Este pacote não necessita de nenhuma configuração, somente fazer a descompactação do pacote no diretório descrito no item de instalação.

12.Configuração das regras do snort.

O meu intuito neste item não é ensinar como fazer ou criar uma nova regra do **snort**, e sim mostar como alterar as regras já existentes para o *reset* e o *bloqueio* dos pacotes.

Regras utilizando o flexresp:

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP ISS Pinger"; content:"\|495353504e475251\|";itype:8;depth:32;reference:arachnids,158;classtype:attempted-recon; sid:465; rev:1; ***resp:icmp_all****;)*

Note que colocamos uma opção resp que enviará um tcp reset para os pacotes que estão sendo enviados e para os que estão sendo recebidos, conforme tabela abaixo:

rst_snd	***TCP RST SND***
rst_rcv	**TCP RST RCV**
rst_all	**TCP RST ALL**
icmp_net	**ICMP NET UNREACH**
icmp_host	**ICMP HOST UNREACH**
icmp_port	**ICMP PORT UNREACH**
icmp_all	**ICMP UNREACH ALL**

Regras utilizando o snortsam:

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP ISS Pinger"; content:"\|495353504e475251\|";itype:8;depth:32;reference:arachnids,158;classtype:attempted-recon; sid:465; rev:1; ***fwsam:src, 1 day****;)*

Note que diferente do ***resp*** este bloqueio utiliza tempo, como o exemplo acima ele esta bloqueando a origem da conexão por 1 dia, podemos fazer o bloqueio por destino, colocando no lugar do ***src*** o ***dst***, e podemos colocar a duração de tempo de necessitarmos.

Dicas:

É bom criar um arquivo no */etc* com o nome *rc.local*, este arquivo é chamado na carga do sistema operacional, para que os produtao instalados no servidor entrem automaticamente, nos criamos alguns arquivos de carga, como por exemplo r*c.snort, rc.mysql*, este arquivos devem estar contidos no arquivo */etc/rc.d/rc.local*.

Exemplo do *rc.local*:

```
if [ -x /etc/rc.d/rc.snort ]; then
        /etc/rc.d/rc.snort
fi
```

Segurança:

É sempre recomendavel deixar ativo no sistema operacional somente os serviços necessários, como no nosso caso só iremos utilizar o snort, então devemos parar os

serviços desnecessários.
Também é recomendavel verificar sempre os patches do sistema operacional e fazer o upgrade sempre que existir algum patch novo.
Sempre mantenha o kernel do servidor atualizado.
Se possivél utilizar sempre um sistema de avalização de vulnerabilidade em seu servidor como por exemplo o **nessus**.

Atualizações:

O **snort** tem alguns utilitários para fazer o download das regras e deixa-las atualizadas, eu utilizo com sucesso o **oinkmaster**, um programa feito em **perl** facil de utilizar, mas a sua configuração ficará para um outro documento.

Testes:

Para podermos testar se as configurações do **snort** estão certas, é só digitar na linha de comando o comando do snort, sem a opção *-D* pois assim ele entra em f*oreground* e assim podemos visualizar se o arquivo de configuração esta correto, caso exista algum erro o **snort** não se inicializará e aparecerá na tela o erro e em que linha.
***#/usr/bin/snort -c /etc/snort.conf -i eth1*.**

Considerações Finais:

Este manual é apenas ilustrativo devendo ser utilizado como material de ajuda, dando apenas as informações necessárias de como proceder na instalação e configuração do produto em questão e as dificuldes encontradas por mim, não sendo material de curso ou treinamento

Contribuições e bibliografia:

www.slackware.org
www.php.net
www.snort.org
www.snortsam.net
www.checkpoint.com
www.kernel.org
www.linux.org