DETECÇÃO E BLOQUEIO DE ACESSOS INDEVIDOS EM SERVIDORES WEB LINUX

Willian Goedert, Francisco Adell Péricas
FURB – Universidade Regional de Blumenau
willian@furb.br; pericas@furb.br

Resumo
Este artigo descreve o funcionamento de sistemas de detecção e prevenção de invasão e a importância de implantar essas ferramentas em uma rede com acesso para a internet, destacando uma ferramenta adequada para o monitoramento e controle de acessos e apresentando o procedimento de instalação com uma configuração básica. Quanto ao investimento em sistemas de segurança, sabe-se o quanto é importante para se proteger de ataques mal intencionados que resultam em roubo de dados confidenciais, negação de serviços, espionagem e modificação de sites.

Palavras-chave: Web. IDS. IPS. Invasão. Segurança.

Abstract
This document describes the operation of detection systems and intrusion prevention and the importance of deploying these tools on a network with access to the internet, highlighting a suitable tool for monitoring and access control and presenting the installation procedure with a basic configuration. Regarding the investment in security systems, it is known how important it is to protect yourself from malicious attacks that result in the theft of confidential data, denial of service, eavesdropping and modification of sites.

Keywords: Web. IDS. IPS. Intrusion. Security.

1. Introdução

Com a evolução da informática, o mundo ficou cada vez mais dependente dessa tecnologia. Sendo assim, as empresas precisam de sistemas eficientes que na maioria das vezes precisam ser acessados de forma on-line. Com esta necessidade de acesso às informações a qualquer momento de qualquer parte do mundo, surgiram os usuários mal intencionados chamados de Crackers. Estes usuários tentam de diversas maneiras obterem acesso de forma ilegal, ou seja, invadir seu equipamento, e para se proteger destes invasores utilizam-se *sistemas de detecção de invasão* (IDS) e *sistemas de prevenção de invasão* (IPS) que, além de detectar uma invasão como o IDS, também bloqueia o acesso do invasor.

Este conceito vem sendo estudado desde os anos 80, mas é muito pouco explorado ainda e merece uma atenção especial, pois se destaca por ser uma ferramenta completa responsável em monitorar, identificar e notificar ocorrências de atividades anormais e sobre estes dados pode tomar decisões conforme o risco detectado (ANONIMO, 2000).

Utilizando esse conceito, este artigo apresenta uma ferramenta estável e adequada que pode ser implantada numa rede com acesso à internet prevenindo invasões em servidores web baseados no sistema operacional Linux. Assim como qualquer software, as ferramentas disponíveis analisadas neste artigo possuem vantagens e desvantagens, que serão apresentadas ao decorrer do texto. Por fim, a que apresentar as melhores características para o objetivo proposto por este trabalho será adotada para demonstração e análise.

2. Segurança em Redes

Segurança em uma rede significa proteger as informações contidas nela implantando políticas de segurança para se prevenir de

algum incidente que possa ocorrer. Para se ter uma ideia do quanto é necessário utilizar essas políticas, pode-se observar numa estatística lançada recentemente pelo *Centro de Estudos, Respostas e Treinamento de Incidentes de Segurança do Brasil* (www.cert.br), que mostra o aumento gradativo dos ataques efetuados nos últimos anos. A figura 1 mostra um gráfico da evolução de ataques efetuados no Brasil.

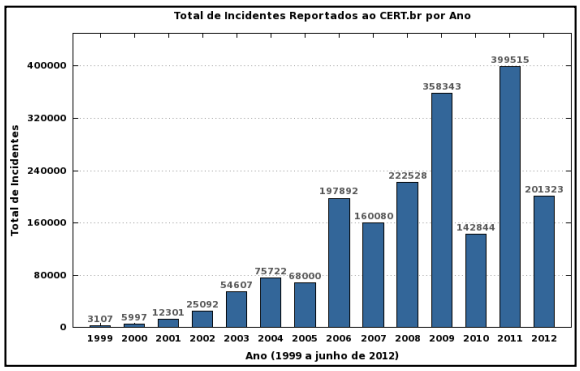

Figura 1 – Número de incidentes de segurança da internet no Brasil (CERT.BR, 2012)

Para comprovar e relacionar a importância de uma rede segura com o mundo real são apresentados alguns casos mais comuns:

a) roubo de dados: este tipo de ataque acontece muito atualmente. Os maiores alvos são as instituições financeiras onde o criminoso tenta invadir o servidor com a intenção de obter algum lucro;
b) modificação de sites: geralmente sites do governo são os principais alvos. A intensão do invasor é modificar o conteúdo da página com um assunto bem diferente do que deveria apresentar, chamando assim a atenção de todos;
c) espionagem industrial: este tipo de ataque tem como principal objetivo roubar informações confidenciais da empresa alvo. Por exemplo, o invasor tenta roubar informação de uma determinada empresa e vende estas informações confidenciais para uma empresa concorrente, obtendo lucro com o crime;
d) ataque DoS (*Denial of Service*): este tipo de ataque tem a finalidade de tornar os recursos de um servidor web indisponíveis. Sites do governo são grandes alvos. Ao indisponibilizar determinados serviços o criminoso pode causar consequências graves como parar o trabalho ou o faturamento de uma empresa;
e) ataque DDoS (*Distributed Denial of Service*): este tipo de ataque tem a finalidade de tornar os recursos de um servidor web indisponível com a ajuda de vários computadores distribuídos ao redor do mundo e que estejam conectados à Internet. Estes computadores, chamados de *zumbis*, atacam simultaneamente o seu alvo (o servidor web) deixando este indisponível por não suportar essa sobrecarga;
f) ataque por *scan*: este tipo de ataque faz varredura de todas as informações que trafegam numa determinada rede com o intuito de identificar quais computadores e ou serviços estão ativos. Com esse procedimento, o invasor além de obter informações da rede e de seus usuários, pode destruir seus serviços ou atacar outros alvos a partir da sua máquina sem que ele seja descoberto.

Com esses exemplos, têm-se os motivos para que se procure ter uma rede o mais segura possível. E para isto, precisam-se adotar ferramentas automatizadas e inteligentes que detectam tentativas de invasão em tempo real, chamadas de *sistemas de detecção de invasão* (*Intrusion Detection System* – IDS). Quando se deseja além de detectar um alerta de invasão, também atuar sobre ele, bloqueando o acesso do intruso, utiliza-se outra ferramenta em conjunto chamada de *sistemas de prevenção de invasão* (*Intrusion Prevention System* – IPS).

Estudos para o desenvolvimento destes tipos de sistemas começaram por volta dos anos 80 e até hoje houve pouca evolução. O motivo é que a maioria das empresas não

investe muito em segurança, justamente pelo motivo delas verem isto como algo de custo elevado mas de retorno insignificante.

Para poder aplicar uma ferramenta de segurança em uma rede, primeiro é preciso estudá-la para saber como funciona. Após isto é preciso analisar e comparar ferramentas disponíveis (para este caso que rodem no sistema operacional Linux) e analisar qual mais atende às necessidades, observando um conjunto de critérios que será detalhado mais adiante.

3. Sistemas de Segurança

Um sistema de segurança de redes é responsável por proteger uma rede, impedindo que usuários mal intencionados executem alguma ação prejudicial a sua infraestrutura. Para isto existem ferramentas que aplicam regras de segurança capazes de monitorar todo o tráfico de informações da rede, e a partir dessas informações coletadas geram logs ou até mesmo aplicam políticas de controle de acesso. Estes sistemas são chamados de IDS e IPS.

3.1. Sistemas IDS

Sistemas de detecção de invasão (*Intrusion Detection System* – IDS) são responsáveis em detectar invasões registrando em log e enviando alertas aos administradores de rede quando é detectada alguma ameaça. Podem trabalhar de forma passiva, onde o IDS detecta uma potencial violação à segurança, registra a informação através de um registro de log e dispara um alerta ao administrador de rede. Outra forma é de trabalhar de forma reativa, onde o IDS responde a atividade suspeita finalizando a seção do usuário ou reprogramando um *firewall* para bloquear o tráfego de rede da fonte maliciosa suspeita (BACER, 2007). Contudo, existem também algumas desvantagens na utilização destas ferramentas que podem ser:

a) desempenho: tornará sua infraestrutura mais lenta por ter que monitorar todo o tráfego de rede e gerar logs;
b) falso positivo: o IDS detecta uma determina situação como invasão, mas na verdade ela não existe, pois se trata de uma coincidência ocasionando um alarme falso e eventualmente um bloqueio não desejado;
c) falso negativo: o IDS não detecta uma intrusão, onde o sistema determina que este pacote é um fluxo normal;
d) atualizações: é necessário fazer atualizações frequentes nas regras do sistema, pois a qualquer momento pode aparecer um novo tipo de ataque ou um novo tipo de vulnerabilidade no sistema.

3.1.1. Sistemas HIDS

São sistemas IDS baseados em equipamento. Estes sistemas monitoram e analisam informações coletadas em um único equipamento. Não observa o tráfico que passa pela rede, apenas verifica as informações relativas aos eventos, registros de log e sistemas de arquivos, como permissão, alteração, etc.

3.1.2. Sistemas NIDS

São sistemas IDS baseados em redes. Estes sistemas monitoram e analisam todo o tráfego no segmento da rede. Consistem em um conjunto de sensores que trabalham detectando atividades maliciosas na rede, como ataques baseados em serviços, *portscans*, etc. Seu principal objetivo é identificar se alguém esta tentando entrar no sistema ou se algum usuário legítimo está fazendo uso do mesmo com má fé.

3.1.3. Sistemas WIDS

São sistemas IDS baseados em redes *wireless*. Estes sistemas monitoram e analisam todo o tráfego de redes sem fio, onde identificam ataques e comportamentos anormais nessas redes. Funcionam da mesma forma que os demais, monitorando e gerando log de situações anormais.

3.2. Sistemas IPS

Sistemas de prevenção de invasão (*Intrusion Prevention System* – IPS) são responsáveis

em prevenir invasões aplicando políticas que bloqueiam o invasor quando detectada alguma ameaça. Sistemas IPS trabalham em conjunto com sistemas IDS, pois através dos sistemas IDS são detectadas possíveis ameaças e com o sistema IPS é tomada a decisão do que fazer com a situação ocorrida.

Existem dois métodos no qual estes sistemas detectam um ataque:

a) detecção por assinatura: este método analisa as atividades do sistema procurando por eventos que correspondem a padrões pré-definidos de ataque e outras ações maliciosas. Geralmente cada assinatura corresponde a um ataque. A desvantagem deste método é que ele pode somente identificar ataques conhecidos, ou seja, ataques que estão definidos na relação de assinaturas que o sistema possui, ficando dependente de atualizações constantes diante de novos ataques que surgem constantemente;
b) detecção por anomalias: este método considera que os ataques são ações diferentes das atividades normais do sistema. Este sistema monta um perfil que representa o comportamento rotineiro de um usuário, equipamento ou conexão de rede. Ele monitora a rede e usa várias métricas para determinar quando os dados monitorados estão fora do normal, ou seja, estão fora do perfil padrão. A desvantagem deste método é a geração de um grande número de alarmes falsos devido ao comportamento imprevisível de usuários e do próprio sistema.

Um sistema IPS tem utilidade importante como ferramenta de segurança em sistemas de diversos tipos de empresas do mundo, como por exemplo, em sistemas financeiros, sistemas industriais e sistemas governamentais.

4. Implantação de Sistemas de Segurança

Implantar um sistema de segurança não é tão simples, pois para isto é preciso um profissional com conhecimento em redes e em tecnologias atualizadas para que possa preparar toda a infraestrutura da melhor forma que atenda a empresa onde atua. Conforme proposto neste artigo, serão apresentadas formas de implantação de sistemas de segurança que possam ser monitorados a partir de um computador remoto (*management workstation*), conforme ilustrado na figura 2.

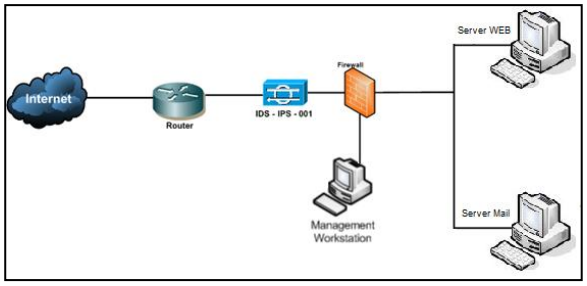

Figura 2 – Sistema simples de segurança de rede

4.1. Ferramentas

Existem várias ferramentas IDS e IPS disponíveis, algumas com pouca documentação. Para adotar uma ferramenta que atenda a proposta deste artigo, pesquisaram-se algumas ferramentas que acabaram mostrando-se bem interessantes.

Para a seleção da ferramenta mais adequada para a implantação proposta neste artigo, pesquisaram-se as seguintes opções:

a) Snort: é uma ferramenta de detecção e prevenção de intrusos de código fonte aberto desenvolvida pela Sourcefire. Possui uma versão estável e a mais recente pode ser baixada gratuitamente no site www.snort.org (SNORT, 2010);
b) Suricata: é uma ferramenta de detecção e prevenção de intrusos assim como o Snort. Foi desenvolvida pela OISF (*Open Information Security Foundation*) e utiliza os mesmo arquivos de regras da ferramenta anterior. Sua principal diferença é por rodar em sistemas *multi-core*, mas ainda está em fase de

evolução. Sua versão mais atual pode ser baixada no site www.openinfosecfoundation.org (SURICATA, 2012);

c) Snare: é uma ferramenta de detecção e prevenção de intrusos, também de código fonte aberto, desenvolvida pela Solutionary. Esta ferramenta pode analisar, coletar e enviar alertas de segurança, mas não é tão eficiente e conhecida como o Snort. Sua última versão pode ser baixada no site www.intersectalliance.com (SNARE, 1999);

d) IBM IPS: é uma ferramenta de detecção de intrusos não-gratuita para Windows desenvolvida pela IBM. Segundo a empresa, é uma ferramenta eficaz para monitoração e proteção contra ameaças. A ferramenta pode ser adquirida pelo site www-01.ibm.com/software/tivoli/products/security-network-intrusion-prevention (IBM, 2011);

e) Bro: é um sistema de detecção de intrusos de código fonte aberto que roda nas plataformas Linux, POSIX e UNIX desenvolvido por uma equipe de professores da Universidade da Califórnia chamada Vern Paxson. Possui arquivos de regras baseados em assinaturas específicas para ele. Sua versão está disponível em www.bro-ids.org/download (BRO, 2011).

Na análise destas ferramentas consideraram-se neste artigo os aspectos mais relevantes de um sistema IDS/IPS, conforme descrito anteriormente, e enumerado na Tabela 1.

Característica	*Snort*	*Suricata*	*Snare*	*IBM IPS*	*Bro*
Para Linux	X	X	X		X
Gratuito	X	X	X		X
Eficiente	X			X	X
Estável	X		X	X	X
Desempenho	X	X			
Instalação	X		X	X	
Documentado	X		X	X	X
Interface	X	X		X	
Continuidade	X			X	X
Uso comum	X				

Tabela 1 – Comparativo entre ferramentas IDS/IPS.

Com o resultado da comparação entre todos estes critérios (tabela 1), optou-se em utilizar a ferramenta chamada Snort, pois apresenta as melhores características em comparação com as outras ferramentas.

Outra ferramenta que se destacou foi o Suricata, que possui a vantagem de ser uma ferramenta que roda em sistemas *multi-core* e com algumas tecnologias de programação mais atualizadas, mas sua desvantagem é ser muito recente e ainda contém alguns *bugs* de programação, e, dependendo da sua eficiência, ainda poderá cair em desuso e ser descontinuada. Mas se futuramente essa ferramenta se adaptar ao mercado, nada impede de utilizá-la, pois ela utiliza os mesmos arquivos de regras que o Snort usa. As demais ainda precisam evoluir para competirem (SURICATA, 2012).

Como toda ferramenta, o Snort também possui suas desvantagens. A principal delas é que ela identifica apenas ataques conhecidos, ou seja, identifica o ataque através de regras definidas em arquivos que devem ser atualizados a cada novo ataque ou vulnerabilidade encontrada. Quanto aos alertas falsos positivos e falsos negativos, depende muito das regras aplicadas à ferramenta, pois isso ocorre também em qualquer outra ferramenta dependendo da sua configuração.

4.2. Ferramenta Snort

Snort é um sistema de detecção e prevenção de intrusos de código fonte aberto, baseado em rede (NIDS). Foi desenvolvida na linguagem C baseada na biblioteca de

programação *libpcap* (biblioteca para captura de pacotes de rede). Seu criador foi Marty Roesch, que disponibilizou sua primeira versão de testes no ano de 1998. Hoje na sua versão mais evoluída é muito utilizada em todo mundo, possuindo mais de 400 mil usuários registrados no site (www.snort.org) (SNORT, 2010). Sua estrutura de funcionamento possui quatro etapas importantes conforme descrito nos próximos parágrafos.

A primeira etapa é o mecanismo de captura e decodificação dos pacotes, que em alguns documentos é citado como sensor ou até mesmo farejador. Nesta etapa o sistema captura todos os pacotes que passam pela rede, como TCP, UDP e ICMP. Depois de capturados, estes pacotes são decodificados de forma que fiquem legíveis à leitura das informações por um administrador de redes.

A segunda etapa se refere aos pré-processadores, que são *plug-ins* que efetuam ajustes e reagrupamento dos pacotes capturados. Com isto, quando os pacotes são enviados ao mecanismo de detecção, as regras são aplicadas de uma forma mais eficiente.

A terceira etapa consiste no mecanismo de detecção, que é o processo mais importante do Snort, pois nesta etapa são configuradas as regras para a análise dos dados provenientes dos pré-processadores. A partir destas regras, o sistema decide se os dados devem ser recebidos ou descartados, e se deverá ser gerado um alerta.

A quarta e última etapa se refere à saída das informações coletadas. Depois dos pacotes passarem pelas três etapas anteriores e forem classificados em uma das regras definidas, será preciso guardá-los para posterior análise humana. Para isto, existem vários *plug-ins* de saída que podem interagir com o Snort, e que tem a finalidade de executar as seguintes atividades:

a) gravar as informações coletadas num banco de dados (o MySQL é o mais usado);
b) interagir com um *firewall*, onde neste caso se tornaria um IPS, pois aplica uma ação em relação a uma ameaça detectada;
c) enviar e-mails de notificação de alertas gerados.

Depois de conhecer um pouco sobre a estrutura do Snort, precisa-se identificar os recursos de infraestrutura compatíveis com ele.

4.2.1. Pré-Requisitos de Instalação do Snort

Para fazer a instalação do Snort, devem ser especificados alguns requisitos para que a ferramenta seja eficiente durante a sua execução:

a) precisa-se de um servidor com o sistema operacional Linux. Para este trabalho utilizou-se a versão do Ubuntu mais recente;
b) precisa-se de um espaço razoável em disco, para que possa armazenar as informações coletadas. Neste caso será armazenado em um banco de dados MySQL;
c) precisa-se de uma interface de rede para conectividade típica (como Secure Shell (SSH) e serviços Web) e outra para o Snort que servirá como sensor propriamente dito com ótimo desempenho.

4.2.2. Instalando o Snort

Antes de instalar o Snort propriamente dito, é preciso instalar um conjunto de ferramentas e bibliotecas necessárias para o seu funcionamento como segue abaixo:

1. Instalação de pacotes básicos: execute o comando abaixo no console para que o sistema operacional instale as bibliotecas básicas necessárias para o Snort.

```
# sudo apt-get install apache2 mysql-server php5 php5-mysql libmysqlclient12-dev php5-gd php-pear php-image-canvas php-image-graph libpcap0.8 libpcap0.8-dev libpcre3 libpcre3-dev
```

Este comando também prepara o servidor web com o serviço Apache com PHP, que será útil mais adiante. Além disso, a biblioteca Libpcap é responsável por capturar pacotes de rede. Normalmente já

está incluída na instalação padrão e a sua documentação encontra-se em www.tcpdump.org. E a biblioteca Libndet disponibiliza acesso à rede com programação de baixo nível: ela pode ser baixada de libdnet.sourceforge.net, onde está toda a sua documentação.

2. É preciso instalar o PCRE, que é uma biblioteca que possui expressões regulares escritas em C e é necessária para a instalação do Snort.

Esta biblioteca está disponível para baixar sua instalação em ufpr.dl.sourceforge.net/sourceforge/pcre/pcre-7.0.tar.gz. Após baixar deve-se instalá-la executando os comandos:

```
# sudo tar zxf pcre-7.0.tar.gz
# cd pcre-7.0
# sudo ./configure
# sudo make
# sudo make install
```

3. É preciso instalar o ADODB, que é uma ferramenta de administração de banco de dados para PHP. É um pré-requisito para a instalação do BASE que será descrito no item seguinte. Esta ferramenta pode ser baixada de prdownloads.sourceforge.net/adodb. Após baixar deve-se instalá-la executando os comandos:

```
# cd /var/www/
# sudo cp /diretAdodb/adodb493a.tgz .
# sudo tar zxf adodb493a.tgz
# sudo rm adodb493a.tgz
```

4. É preciso instalar o BASE (*Basic Analysis and Secure Engine*), que é uma ferramenta para buscar as informações salvas no banco de dados MySQL e que irá gerar estatísticas e gráficos. Existem outras ferramentas como por exemplo o Snorby, mas são ferramentas mais complexas tanto na instalação quando na dimensão de informações apresentadas na sua interface, por isso adotou-se uma ferramenta mais simples visando analisar o resultado de forma eficiente. Esta ferramenta pode ser baixada de base.secureideas.net, onde são apresentados os passos de instalação em sua documentação (BASE, 2000). Após instalado, é preciso configurar o arquivo do servidor /var/www/html/base/base_conf.php conforme abaixo:

```
$BASE_urlpath = '/html/base';
$DBlib_path = '/var/www/adodb/';
$DBtype = 'mysql';
$alert_dbname = 'snort';
$alert_host = 'localhost';
$alert_port = '';
$alert_user = 'snort';
$alert_password = 'senha_usuario_snort';
/* Archive DB connection parameters */
$archive_exists = 0; # Set this to 1 if
you have an archive DB
```

5. Instalação do Snort: é preciso baixar a ferramenta do site oficial do Snort: www.snort.org. Na sequência devem-se executar os seguintes comandos para compilar e instalar a ferramenta:

```
# sudo tar zxf snort-2.6.1.2.tar.gz
# cd snort-2.6.1.2
# sudo ./configure --with-mysql=/usr
# sudo make
# sudo make install
```

Depois de compilado e instalado, é preciso criar o diretório do Snort e então copiar seus arquivos de configuração. Mais adiante será mostrado como configurar estes arquivos. Para fazer a cópia execute no console os seguintes comandos:

```
# sudo mkdir /etc/snort
# cd /etc/snort
# sudo cp /diretSnort/etc/snort.conf .
```

4.2.3. Configurando e executando o Snort

Nesta etapa é preciso preparar o banco de dados para que o sistema possa salvar as informações coletadas. Para isso, deve-se criar um banco de dados para o Snort digitando os seguintes comandos no console:

```
# sudo mysql
# mysql> SET PASSWORD FOR
root@localhost=PASSWORD('password');
# mysql> create database snort;
# mysql> grant INSERT,SELECT on root.*
to snort@localhost;
# mysql> SET PASSWORD FOR
snort@localhost=PASSWORD('password_do_sn
ort.conf');
# mysql> grant CREATE, INSERT, SELECT,
DELETE, UPDATE on snort.* to
snort@localhost;
# mysql> grant CREATE, INSERT, SELECT,
DELETE, UPDATE on snort.* to snort;
# mysql> exit
```

Após ter criado o banco de dados, deve-se executar o script da pasta schemas da instalação do Snort para criar as tabelas necessárias para a sua execução:

```
# sudo mysql -u root -p <
~/diretSnort/schemas/create_mysql snort
```

Neste momento a ferramenta Snort está totalmente preparada. Agora se deve iniciar os serviços necessários como o servidor Web Apache, que será útil para análise e o banco de dados MySQL. Para isso, devem-se executar os seguintes comandos:

```
# sudo /etc/init.d/mysql start
//-- Inicia o mysql
# sudo /etc/init.d/apache2 start
//-- Inicial o Apache
# sudo snort -c /etc/snort/snort.conf
//-- Inicia o Snort
```

4.3. Executando Ataques e Analisando os Alertas

Para analisar resultados de ataques, executou-se o BASE que é a ferramenta de análise do sistema de segurança proposto por este artigo. Para isto, abriu-se o navegador e acessou-se a URL correspondente a sua instalação: localhost/base-1.4.5/base_main.php. Na primeira execução desta ferramenta é preciso configurar o banco de dados, onde a própria ferramenta já o faz clicando no link Setup Page, conforme a figura 3, e depois se deve clicar no botão Create BASE AG, conforme a figura 4.

Figura 3 – Inicialização do BASE

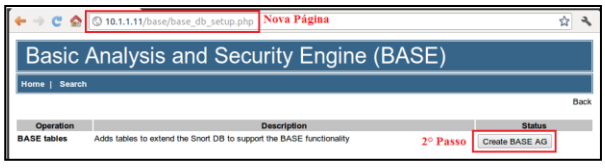

Figura 4 – Criação da base de dados do BASE

Precisa-se neste momento configurar as regras de controle do Snort, que são nada mais do que as políticas que serão aplicadas ao sistema de segurança. Pode-se aplicar regras para que a ferramenta opere em modo IPS ou IDS.

No exemplo deste artigo, implantou-se o Snort antes do *firewall*, fazendo com que ele funcione em modo IPS, pois todo o tráfico passa primeiramente por ele e dependendo das políticas definidas irá permitir ou bloquear o tráfico.

A primeira regra aplicada define ao Snort que bloqueie todo arquivo que contenha palavras específicas definidas na política de segurança, que neste caso será a palavra trojan. Para aplicar a regra, deve-se editar o arquivo *badwords.rules* e incluir essa palavra. O objetivo é aplicar uma política de controle para detectar o acesso a arquivos que contenha palavras maliciosas. A regra irá detectar mesmo que o arquivo esteja compactado. Abaixo é especificado como deve ser escrito a regra no arquivo:

```
alert tcp any any -> any any
(msg:"Palavra encontrada -> trojan <- |
Testes Regras | artigo IDS";
content:"trojan"; nocase; ver:1)
```

Agora se pode simular um ataque baixando um arquivo da web que contém a palavra trojan. O bloqueio efetuado pela regra é mostrado na figura 5.

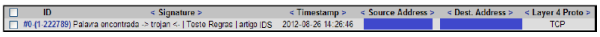

Figura 5 – Bloqueio de arquivo com a palavra trojan

A segunda regra consta em aplicar uma regra de segurança no servidor Web para que não seja incluído um comando *include* qualquer de um arquivo PHP no servidor Web. Para isto, deve-se habilitar a seguinte regra no arquivo *web-php.rules* (para habilitar uma regra basta retirar o caractere de comentário # do início da linha):

```
alert tcp $EXTERNAL_NET any ->
$HTTP_SERVERS $HTTP_PORTS (msg:"WEB-PHP
remote include path"; flow:established,
to server; content:".php"; nocase;
content:"path=", fast_pattern:only;
pcre:"/path=(https?|ftps?|php)/i";
classtype:web-application-attack;
sid:2002; ver:12;)
```

Após simular um ataque executando um script remotamente tentando efetuar um

include, o acesso será barrado. O bloqueio efetuado pela regra é mostrado na figura 6.

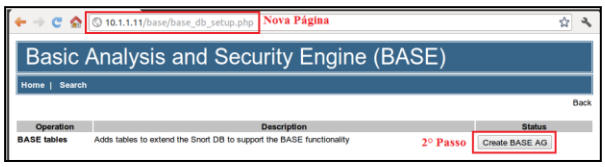

Figura 6 – Bloqueio de arquivo com um include PHP

Assim como estas regras apresentadas, podem-se implementar novas regras. Para isso, na pasta *rules* já existem várias regras pré-definidas e testadas pelos desenvolvedores da Snort, que podem ser habilitadas conforme a necessidade. Dentre elas, existe a *ftp.rules* para controle de acesso a FTP, *dos.rules* e *ddos.rules* para controle de ataques DOS/DDOS, *mysql.rules* para controle de acesso a banco de dados MySql, *smtp.rules* para controle de acesso a serviços de e-mail, *virus.rules* que poderá bloquear determinados tipos de arquivos como .exe, .bat, .dll, etc.

5. Considerações Finais

O trabalho desenvolvido mostrou a viabilidade e um exemplo prático da utilização de sistemas de segurança de redes, onde se utilizaram as chamadas políticas de segurança que garantem a proteção das informações de uma empresa.

Com a evolução da internet, que acompanhou junto o aumento de crimes virtuais que vem prejudicando muito o trabalho das empresas, principalmente dos bancos, percebe-se a necessidade da implantação de sistemas cada vez mais robustos de segurança. Desta forma, protegendo-se desses usuários mal intencionados que são chamados de invasores.

Sobre as ferramentas de segurança disponíveis atualmente, foram analisados vários pontos importantes para que se tomasse a decisão em utilizar ao Snort. Dentre estes pontos, ele se destacou em ser uma ferramenta estável que tem um bom desempenho com eficiência por que irá passar por ela todos os dados da sua rede, mas dependendo do fluxo de dados poderá ficar completamente lenta. Além deste ponto, é uma ferramenta que está em uso por milhares de administradores de rede a bastante de tempo e não é paga o que diminui para o cliente o valor a ser investido na sua implantação, o que impacta muito nas empresas por alegarem que isso é um investimento sem pouco custo/benefício.

Contudo, se se for necessário, podemos ir um pouco mais além explorando a ferramenta e configurando ela para controlar acessos internos da sua empresa, assim saberemos de tudo o que o funcionário faz durante o seu trabalho, como por exemplo, analisar e bloquear o acesso a determinado site de internet, bloqueio de Skype, controle de acesso a e-mails e muito mais, precisa-se apenas estudar mais a fundo as regras do Snort, e melhor, muitas já estão testadas por profissionais e prontas onde apenas falta habilitar a regra para que funcione.

E por fim, pode-se concluir que a principal resposta que se tem das empresas de não investirem nesta área, é pelo custo um pouco alto que elas terão de assumir para manter estes sistemas atuantes e não têm ainda a real percepção de que o retorno indireto obtido pela confiabilidade da rede é um grande benefício. Mas com todas as questões levantadas neste artigo, acredito que fique um pouco mais claro o risco que as empresas correm, e que pode ser minimizado utilizando uma ferramenta de boa qualidade com baixo custo de implantação e de manutenção e que certamente trará benefícios através do aumento da segurança na sua rede de computadores.

Referências

ANONIMO. **Segurança máxima para linux**: o guia de um hacker para proteger seu servidor e sua estação de trabalho Linux. Rio de Janeiro: Campus, 2000.

BAKER, A. R.; ELTES, Joel. **Snort**: IDS and IPS toolkit. Estados Unidos: Syngress Publishing, 2007.

BASE. **Base analysis and security engine**. [S.l.], 2000. Disponível em: <base.secureideas.net/index.php>. Acesso em: 05 ago. 2012.

BRO. The **Bro network security monitor**. Berkeley, 2011. Disponível em: <http://www.bro-ids.org/index.htm>. Acesso em: 05 aog. 2012.

CERT.BR. **Centro de estudos, resposta e tratamento de incidentes de segurança no Brasil**: estatísticas do incidentes reportados ao CERT.br. Brasil, 2012. Disponível em: <www.cert.br/stats/incidentes>. Acesso em: 05 ago. 2012.

IBM. **IBM security network intrusion prevention system**. Estados Unidos, 2011. Disponível em: <http://www-01.ibm.com/software/tivoli/products/security-network-intrusion-prevention/>. Acesso em: 05 ago. 2012.

SNARE. **Specialists in event and intrusion analysis**. Austrália, 1999. Disponível em: <http://Contat.intersectalliance.com/>. Acesso em: 05 ago. 2012.

SNORT. **Snort official documentation**. Estados Unidos, 2010. Disponível em: <www.snort.org/docs>. Acesso em: 24 jul.2012.

STANGER, James; LANE, Patrick. **Rede segura Linux**. Rio de Janeiro: Alta Books, 2002.

SURICATA. **OISF open information Security Foundation**. Estados Unidos. Disponível em: <www.openinfosecfoundation.org/>. Acesso em: 05 ago. 2012.