Ministério da
Ciência, Tecnologia e Inovação

sid.inpe.br/mtc-m21b/2014/04.22.19.29-MAN

PROCEDIMENTOS PARA IMPLANTAÇÃO DE AMBIENTE DE MONITORAÇÃO DE REDE USANDO SNORT.

Anacleto José Mendes Júnior

URL do documento original:
<http://urlib.net/8JMKD3MGP5W34M/3G6URBP>

INPE
São José dos Campos
2014

PUBLICADO POR:

Instituto Nacional de Pesquisas Espaciais - INPE
Gabinete do Diretor (GB)
Serviço de Informação e Documentação (SID)
Caixa Postal 515 - CEP 12.245-970
São José dos Campos - SP - Brasil
Tel.:(012) 3208-6923/6921
Fax: (012) 3208-6919
E-mail: pubtc@sid.inpe.br

Ministério da
Ciência, Tecnologia e Inovação

sid.inpe.br/mtc-m21b/2014/04.22.19.29-MAN

PROCEDIMENTOS PARA IMPLANTAÇÃO DE AMBIENTE DE MONITORAÇÃO DE REDE USANDO SNORT.

Anacleto José Mendes Júnior

URL do documento original:
<http://urlib.net/8JMKD3MGP5W34M/3G6URBP>

INPE
São José dos Campos
2014

AGRADECIMENTOS

Agradeço primeiramente a Deus, por me conceder o privilégio da vida, por me dar uma família e um lar. Agradeço à minha orientadora Dra. Lília de Sá Silva, pela paciência e orientação em prol do desenvolvimento desta publicação.

RESUMO

Esta publicação visa orientar quanto à instalação e configuração do software para detecção de intrusos em redes de computadores, Snort. O software Snort é capaz de analisar tráfego de dados de rede em busca de assinaturas anômalas e realizar captura de tráfego para posterior análise. Este documento trata da instalação do software Snort em um sistema operacional Debian Linux para fins de análise efetiva do tráfego anômalo e visualização de alertas gerados pela aplicação.

Palavras-chave: Redes de Computadores, Segurança, Linux

ABSTRACT

This publication aims to guide the deployment and configuration of software for intrusion detection in computer networks, Snort. Snort software is able to analyze network data traffic for anomalous signatures and perform traffic capture for later analysis. This document deals with the Snort software installation on a Debian Linux operating system for the purpose of effective analysis of anomalous traffic and viewing alerts generated by the application.

Keywords: Computer Networks, Security, Linux

LISTA DE FIGURAS

Pág.

LISTA DE SIGLAS E ABREVIATURAS

INPE	Instituto Nacional de Pesquisas Espaciais
NIDS	Network Intrusion Detection System
ICMP	Internet Control Message Protocol
HTTP	Hyper Text Transfer Protocol
SMTP	Simple Mail Transfer Protocol
POP	Point of Presence
IMAP	Internet Message Access Protocol
DNS	Domain Name Service
FTP	File Transfer Protocol
DDOS	Distributed Denial of Service
HTTPS	Hyper Text Transfer Protocol Secure
SSH	Secure Shell
DAQ	Data Acquisition
VRT	Vulnerability Research Team

SUMÁRIO

1 INTRODUÇÃO

A crescente evolução das redes de computadores e dos sistemas computacionais proporciona para a sociedade vários benefícios, incluindo armazenamento de dados, troca de informações e gestão do conhecimento.

No entanto, os sistemas computacionais estão continuamente sujeitos a diferentes tipos de ameaças digitais que podem comprometer a sua segurança, em termos de disponibilidade, confiabilidade e integridade. Logo, a segurança de sistemas computacionais e redes de comunicação de dados é uma questão vital em qualquer organização, seja ela pública ou privada.

Além da implantação de tecnologias de segurança no ambiente computacional, é necessária a realização de uma análise periódica de eventos de rede e de sistemas em busca de anomalias, a fim de que possam ser desenvolvidas medidas preventivas e corretivas.

A análise de grandes volumes de dados provenientes do ambiente de redes e sistemas através da intervenção humana é praticamente inviável. Deste modo, torna-se fundamental a automatização de tarefas repetitivas e/ou complexas referentes à análise de dados, visando prover agilidade na detecção de eventos anômalos e melhor desempenho dos procedimentos operacionais de gerenciamento de redes e sistemas.

Desenvolver métodos e aplicações para automatizar as tarefas relacionadas ao gerenciamento e segurança de sistemas é um processo contínuo, que demanda pesquisa de técnicas e constante esforço de desenvolvimento na busca de soluções e tecnologias adequadas.

2 MOTIVAÇÃO

Analisando a rede de computadores do prédio Beta do INPE, observou-se que esta rede necessitava ser constantemente monitorada para fins de detecção de ocorrências de tráfego de dados anômalos.

Dentre as técnicas conhecidas para monitorar um ambiente de redes em busca de anomalias, destaca-se os sistemas de detecção de intrusos em redes (NIDS – Network Intrusion Detection System). Um NIDS é capaz de analisar o tráfego de rede em busca de padrões e assinaturas de ataques digitais conhecidos, tornando-se uma ferramenta indispensável em um ambiente corporativo e com dados sensíveis.

3 SOLUÇÃO PROPOSTA

Através de estudos sobre o comportamento da rede a ser monitorada, das técnicas e ferramentas que poderiam ser utilizadas e dos equipamentos disponíveis para monitoração de tráfego, optou-se por utilizar uma solução de NIDS gratuita e em constante desenvolvimento e atualização pela comunidade de software livre. Além disso, por ser uma ferramenta de segurança ativa e preventiva, escolheu-se o Snort para analisar o tráfego da rede monitorada.

4 OBJETIVO

O uso do Snort na rede tem como objetivo analisar o tráfego em busca de anomalias, prevenir a rede de incidentes de segurança e obter parâmetros e valores reais do que é transmitido pela rede.

5 DESENVOLVIMENTO DO AMBIENTE

A preparação do ambiente é um dos pontos mais importantes na monitoração de uma rede de dados. É preciso levar em consideração certos fatores que podem determinar a legitimidade e integridade dos dados. Dentre os fatores considerados neste trabalho, destacam-se: origem do tráfego de rede, meios físicos por onde a informação trafega até chegar na estação de monitoração (cabos e elementos ativos de rede), ambiente local ou distribuído para a coleta de dados, local de armazenamento dos dados históricos, serviços de rede

envolvidos nos processos de captura de dados, tratamento, análise e apresentação dos dados.

O ambiente de monitoração proposto foi planejado a partir dos seguintes pontos: definição do tráfego a ser monitorado; análise dos principais processos envolvidos e seleção das ferramentas necessárias em cada processo. A preparação do ambiente durou cerca de 6 meses. Dentre os fatores que influenciaram na preparação do ambiente destacam-se: falhas de hardware com computadores, tempo de liberação de espelhamento de portas, execução de testes do ambiente, liberação de portas nos switches para a estação de monitoração, instalação e configuração das ferramentas em ambiente de teste e migração da ferramenta Snort para ambiente de produção.

5.1. Definição do Tráfego

Conforme a meta estabelecida no projeto, a solução proposta envolveu a análise de todo o tráfego da rede monitorada, incluindo dados provenientes da rede externa e das redes internas que compõem a rede monitorada. Os sensores do Snort foram posicionados entre o firewall e estas redes.

O tipo de tráfego monitorado compreende, principalmente: HTTP, HTTPS, conexões peer-to-peer, SMTP, POP, IMAP, DNS, ICMP, FTP, NetBIOS, NTP. Também envolve a análise de dados de tráfego não autorizados, indevidos ou ilegítimos. Vulnerabilidades tais como backdoors, spywares, phishing, DDOS e botnet participaram do critério de ilegitimidade do tráfego.

5.2. Processos envolvidos

Os processos desenvolvidos para monitoração da rede monitorada compreendem:

a) captura do tráfego e detecção de tráfego malicioso pelo Snort, a partir de biblioteca de captura de pacotes (libpcap) e de regras de filtragem definidas;

b) processamento dos dados de tráfego capturado pelo Barnyard2, que converte o dado do formato unified para formato binário e o armazena na base MySQL;

c) apresentação dos dados convertidos no Snorby, um front-end web que permite visualização mais legível dos dados, através de gráficos e relatórios, proporcionando a aplicação de contramedidas imediatas a partir dos alertas informados.

As ferramentas acima descritas foram instaladas e configuradas na estação de monitoração da rede.

A Figura 5.1 mostra o diagrama de processos que compõem o ambiente de monitoração.

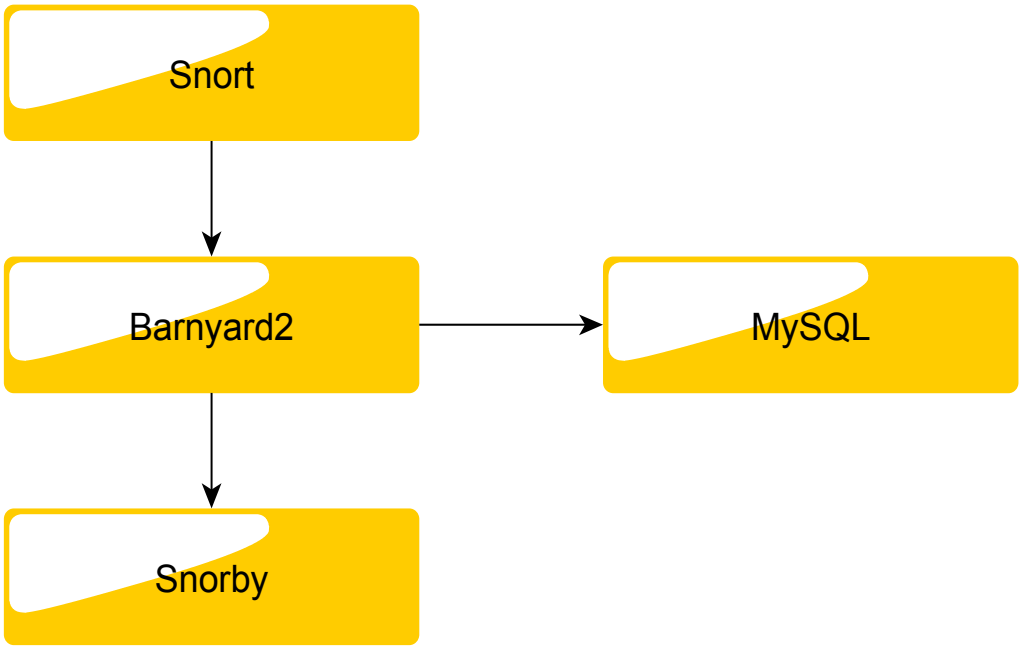

Figura 5.1 - Diagrama de Processos

5.3. Recursos de desenvolvimento

Para desenvolvimento deste projeto, foram necessários recursos de hardware e software e artefatos para prover conectividade das estações de trabalho em rede.

5.3.1. Hardware

Para ser a máquina de captura e análise de tráfego (estação de monitoração), foi utilizado um computador desktop Intel Core 2 Duo 1.86GHz, com 3GB RAM e 2 discos rígidos de 500 GB cada, 3 interfaces de rede de 10/100 Mbps, para realizar a captura de três redes distintas.

5.3.2. Rede

Nos switches que interligam as redes que possuem conexão com a rede monitorada, incluindo rede interna, rede interna de acesso restrito e a rede externa, foi configurado o mecanismo de espelhamento de porta para capturar o tráfego das redes de interesse que é direcionado para as interfaces de rede do gateway.

Foram providenciados cabos de rede e uso de portas disponíveis nos switches para conexão da estação de monitoração no ambiente de rede.

5.3.3. Software

Na estação de monitoração foi instalado o sistema operacional Debian Linux, versão 6, 64 bits.

As ferramentas para compor o ambiente de monitoração do tráfego foram escolhidas com base em estudos de software utilizado no mercado para captura e análise de tráfego em busca de eventos anômalos ou detecção de tráfego malicioso. Também foi levado em consideração ampla documentação do software, comunidade ativa com o desenvolvimento de ferramentas, confiabilidade do produto reconhecida pelo mercado, facilidade de uso,

tratamento adequado dos dados, formas de apresentação refinada e adequada dos dados para facilitar a interpretação humana.

A principal ferramenta de software instalada foi o Snort, utilizado para captura, processamento e geração de alertas sobre os dados do tráfego de rede de interesse.

O Snort é um sistema de detecção de intrusão de código fonte livre capaz de realizar análise de tráfego em tempo real e registrar logs de pacotes em redes IP. Este IDS pode executar análise de protocolos, busca e associação de conteúdos e pode ser utilizado para detectar uma grande variedade de ataques, tais como buffer overflows e scan de portas, e vários outros tipos de ataques.

O Snort pode trabalhar de quatro modos distintos, listados a seguir:

- Sniffer: realiza leitura dos pacotes que trafegam na rede e os mostra na tela de console para o usuário.
- Packet Logger: armazena os registros de logs dos pacotes capturados.
- Network Detection Intrusion System (NIDS): considerado o modo mais complexo, permite que o Snort analise o tráfego de rede para serem processados em uma base de regras previamente definidas em seu arquivo de configuração, podendo gerar alertas para o usuário caso seja considerado um tráfego malicioso.
- Inline: a partir de pacotes obtidos com iptables em fez de utilizar o libpcap, faz com que o iptables bloqueie ou libere os pacotes baseados nas regras que foram definidas especificamente para o iptables.

Este IDS, se configurado da maneira adequada, ajustando seus parâmetros de acordo com a rede existente, é capaz de detectar anomalias e a partir de seus logs de alertas, fornecer dados importantes para o profissional de rede realizar ações necessárias para diminuir estes riscos.

A figura abaixo ilustra o diagrama e estrutura do Snort:

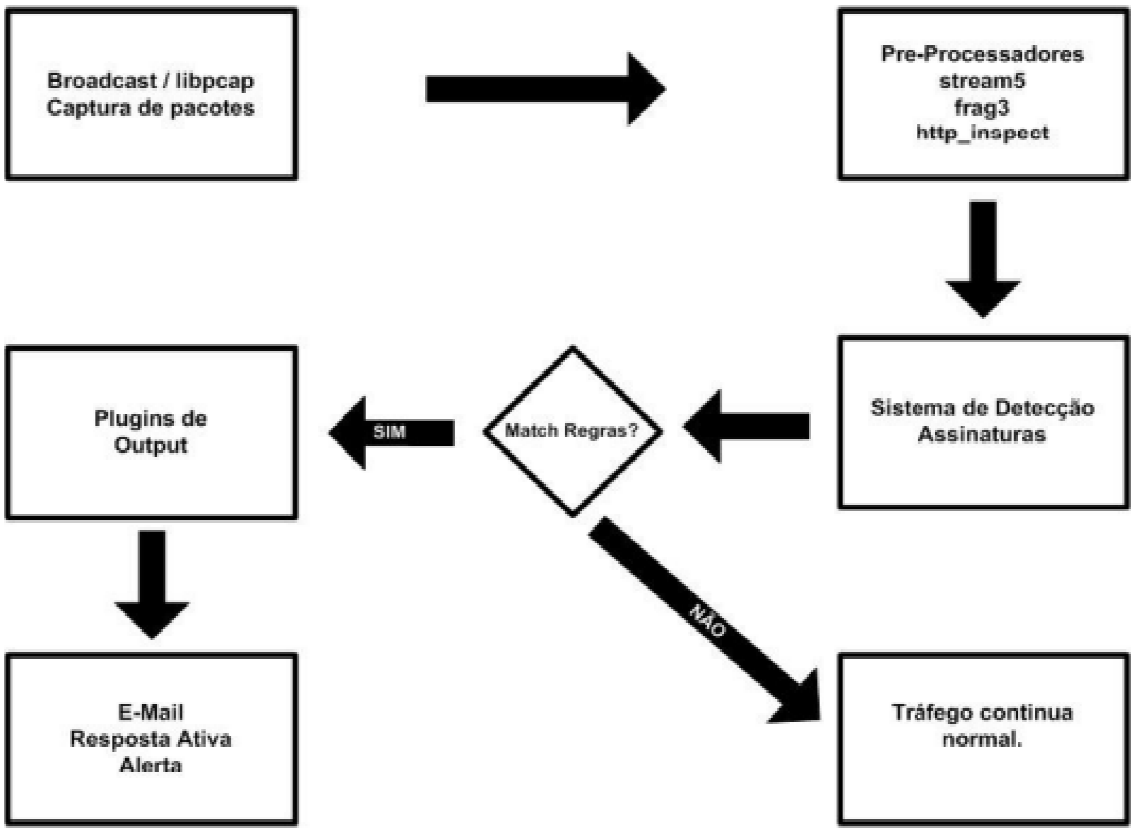

Figura 5.2 - Diagrama do Snort

Além do Snort, foram empregadas as seguintes ferramentas para desenvolvimento do ambiente de monitoração: SSH, para administração remota da estação de monitoração, Barnyard2, banco de dados em MySQL, para armazenamento dos eventos e históricos de alertas, bibliotecas de Ruby e Python, necessárias para visualização dos dados através de um navegador web e da ferramenta Snorby, capaz de organizar os dados gerados pelo Snort para fácil leitura em um ambiente web .

6 IMPLANTAÇÃO DO AMBIENTE DE MONITORAÇÃO

A seguir, são descritos os procedimentos operacionais utilizados na instalação dos itens de software necessários ao ambiente de monitoração de dados.

6.1. Instalação e Configuração do Sistema Operacional

Por ser um software de código aberto, o Snort possui versões para diversos sistemas operacionais GNU/Linux e também para Microsoft Windows. Foi utilizado o sistema Debian GNU/Linux 6.0, devido a sua grande estabilidade e ampla documentação disponível.

Durante a instalação do sistema Debian na estação de monitoração, deve-se desmarcar todas as opções, mantendo apenas “Minimum Install”. Dessa forma, apenas o sistema básico será instalado, evitando, assim, a instalação de programas e serviços desnecessários que podem criar vulnerabilidades no ambiente computacional.

Após a instalação do sistema operacional, este deve ser devidamente ajustado, com a instalação de pacotes essenciais, e configurado.

A instalação de pacotes requer o uso do seguinte comando com privilégio de usuário root:

apt-get update && apt-get install apache2 libapache2-mod-php5 libwww-perl mysql-server mysql-common mysql-client php5-mysql libnet1 libpcre3 libpcre3-dev autoconf libcrypt-ssleay-perl libmysqlclient-dev php5-gd php-pear libphp-adodb php5-cli libtool libssl-dev gcc-4.4 -g++ automake gcc make flex bison apache2-doc ca-certificates vim mc

Durante a instalação do pacote mysql-server, será questionada uma senha de root para administração do banco de dados. Deve-se, portanto, criar uma senha forte para proteger o banco de dados.

6.2. Instalação de pacotes essenciais para o funcionamento do Snort

Deve-se instalar a biblioteca Libpcap para captura de pacotes, utilizando os seguintes comandos, respectivamente:

```
# cd /opt

# wget http://www.tcpdump.org/release/libpcap-1.3.0.tar.gz

# tar -zxvf libpcap-1.3.0.tar.gz && cd libpcap-1.3.0

# ./configure –-prefix=/usr –-enable-shared

# make && make install
```

Em seguida, deve-se instalar a biblioteca Libdnet, responsável pela manipulação de pacotes de rede em baixo nível, utilizando os seguintes comandos:

```
# cd /opt

# wget http://libdnet.googlecode.com/files/libdnet-1.12.tgz

# tar -zxf libdnet-1.12.tgz && cd libdnet-1.12

# ./configure –-prefix=/usr –-enable-shared

# make && make install
```

Para manipular os pacotes de rede, utiliza-se o pacote DAQ. Sua instalação deve ser feita utilizando os comandos abaixo:

```
# cd /opt
```

wget http://www.snort.org/dl/snort-current/daq-0.5.tar.gz

tar -zxf daq-0.5.tar.gz && cd daq-0.5

Depois de ser instalado, é preciso corrigir uma sintaxe na configuração da biblioteca DAQ em relação ao tamanho do buffer.

mcedit /opt/daq-0.5/os-daq-modules/daq_pcap.c

Na linha 219, corrije-se a entrada:

“context->buffer_size = strtol(entry->key, NULL, 10);” por “context->buffer_size = strtol(entry->value, NULL, 10);”

Somente depois de alterar este parâmetro, instale-o:

./configure

make && make install

Atualize as bibliotecas para que os recursos sejam compartilhados:

echo >> /etc/ld.so.conf /usr/lib && ldconfig

6.3. Instalação e configuração básica do Snort

O pacote pré-compilado do Snort que se encontra em repositórios Debian não acompanha o desenvolvimento do projeto Snort e, portanto trata-se de uma versão desatualizada.

Sendo assim, deve se utilizar a versão mais atual do Snort que se encontra no site oficial do projeto Snort (www.snort.org).

Em primeiro lugar, deve-se efetuar o download do código-fonte (da versão mais nova que estiver no site), seguindo os passos:

```
# cd /opt

# wget http://www.snort.org/dl/snort-current/snort-2.9.0.5.tar.gz -O snort-2.9.0.5.tar.gz

# tar -zxf snort-2.9.0.5.tar.gz && cd snort-2.9.0.5

# ./configure --enable-dynamicplugin --enable-perfprofiling -–enable-ipv6 --enable-zlib --enable-reload

# make && make install
```

Após a instalação bem sucedida do Snort, deve se criar os seguintes diretórios para uso no programa:

```
# mkdir /etc/snort /etc/snort/rules /var/log/snort /var/log/barnyard2 /usr/local/lib/snort_dynamicrules
```

É importante também utilizar um usuário específico para execução do Snort. Utilize acesso root somente quando necessário.

```
# groupadd snort && useradd -g snort snort
```

Deve-se definir as permissões das pastas de log apenas para este usuário:

```
# chown snort:snort /var/log/snort /var/log/barnyard2
```

Em seguida, deve-se copiar os arquivos da pasta /usr/src para /etc/snort para conveniência e organização, de modo a reunir todos os arquivos de configuração em uma pasta de fácil acesso:

cp /opt/snort-2.9.0.5/etc/*.conf* /etc/snort

cp /opt/src/snort-2.9.0.5/etc/*.map /etc/snort

Deve-se abrir o arquivo principal de configuração do Snort e mudar algumas opções:

mcedit /etc/snort/snort.conf

E alterar estas linhas:

ipvar HOME_NET 192.168.1.0/24 – coloque o endereço da sua rede interna

ipvar EXTERNAL_NET !$HOME_NET

var RULE_PATH ./rules – aqui informa-se onde ficarão guardadas as regras de análise do Snort. Neste exemplo, ele entende que é a pasta /etc/snort/rules

Deixar todas as linhas de preprocessador comentadas

Comentar todas as “include $RULE_PATH” exceto “local.rules”

Para testar se o Snort está funcionando deve-se criar a seguinte regra:

mcedit /etc/snort/rules/local.rules

E inserir neste arquivo o conteúdo abaixo:

alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001;)

Para testar o funcionamento usar o comando:

/usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0

É preciso especificar qual placa de rede efetuar o monitoramento, neste caso, foi usada a placa eth0.

Utilizando outro computador na mesma rede, efetuar um ping para a estação de monitoração:

ping <ip da estação de monitoração>

Na tela da estação de monitoração, deverão ser exibidos alertas sobre um Ping sendo realizado.

Aperte Ctrl +C para encerrar o Snort na estação de monitoração, concluindo assim o teste.

6.4. Instalando as regras do Snort

O Snort necessita de uma lista de regras para que os dados anômalos possam ser detectados efetivamente na sua rede. Essas regras devem ser atualizadas constantemente, mantendo a integridade e confiabilidade do serviço. No entanto, nem todas elas são disponibilizadas gratuitamente logo quando são lançadas.

As regras VRT Sourcefire, são as regras oficiais do projeto e tem como vantagem serem liberadas aos assinantes logo após terem sido desenvolvidas e testadas. Para obter estas regras atualizadas é preciso pagar uma assinatura mensal através do site do Snort.

Para usuários registrados no site mas que não podem pagar uma assinatura mensal, essas regras são disponíveis também mas após 30 dias da divulgação da mesma.

Os passos para se registrar no site serão descritos abaixo.

Ao acessar o site www.snort.org, deve-se clicar sobre o botão Sign In.

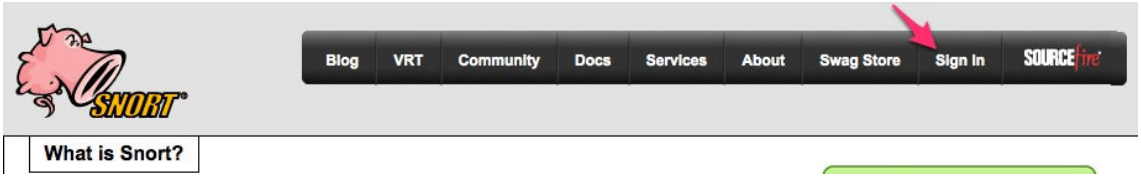

Figura 6.3 Acessando o site oficial do Snort

Na próxima tela, o link “Sign Up for an Account” é a opção para dar continuidade a criação da conta gratuita em Snort.org como mostra a figura a seguir:

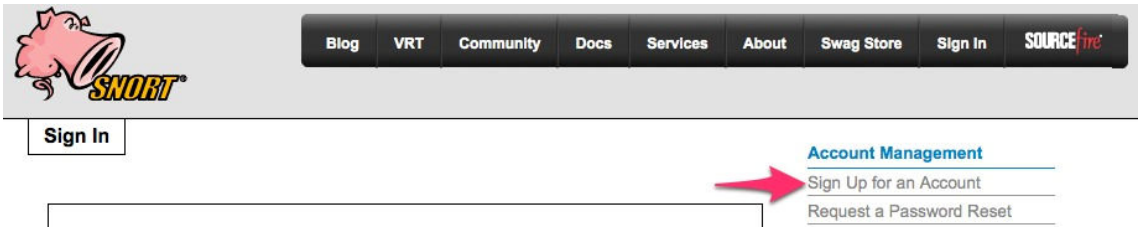

Figura 4 - Link para criação de conta no Site Snort.org

Preencher os campos abaixo é o último passo para conclusão na criação da conta, conforme exibido abaixo:

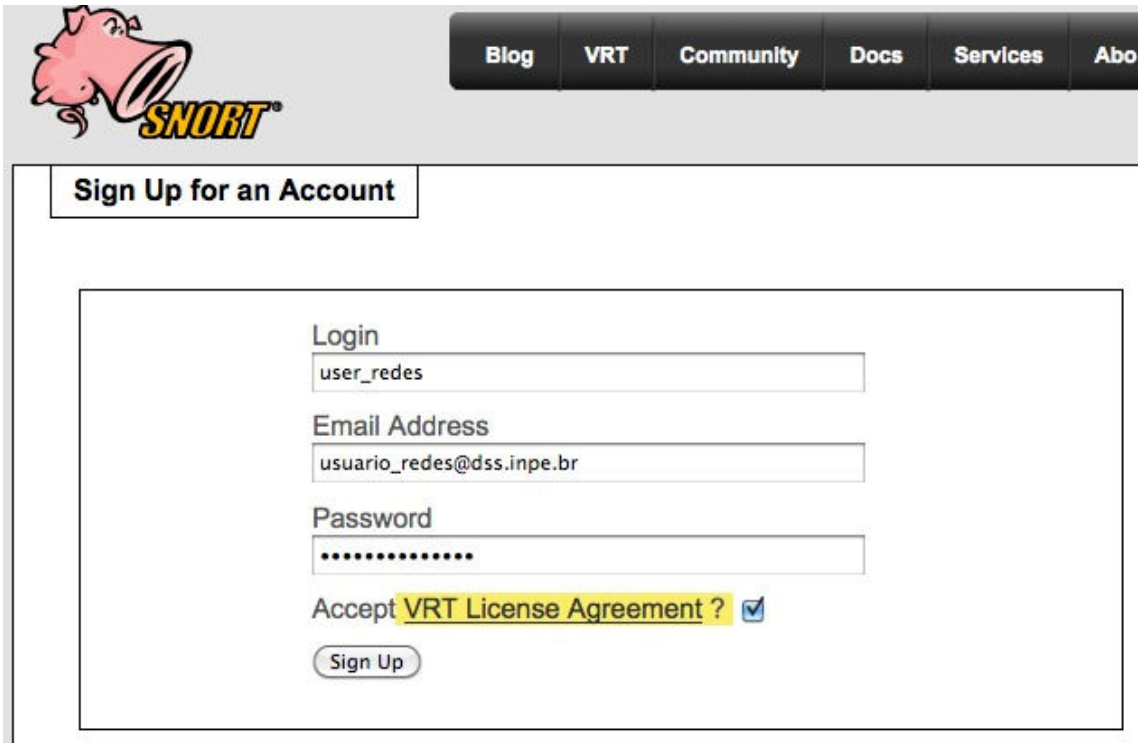

Figura 5 - Criação de Conta no site oficial do Snort

Logo após será enviado um e-mail ao endereço fornecido na etapa anterior confirmando a criação da conta e com o link fornecido no e-mail, já é possível entrar no site e fazer o download das regras.

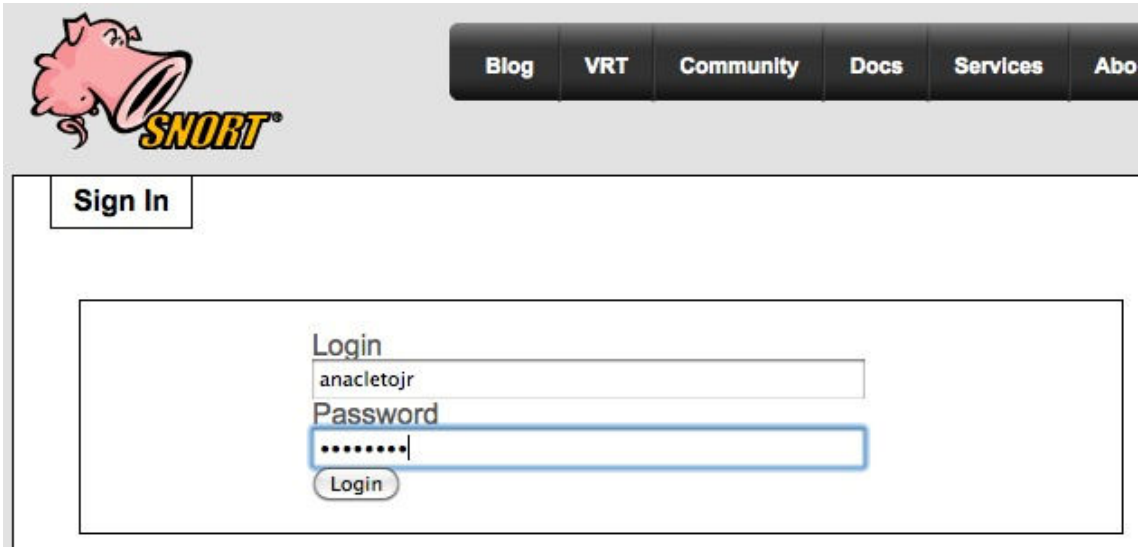

Figura 6 - Efetuando Login no site oficial do Snort

Atenção: deve-se usar o login informado na etapa de criação da conta e não a conta de email.

E por fim o download deve ser realizado.

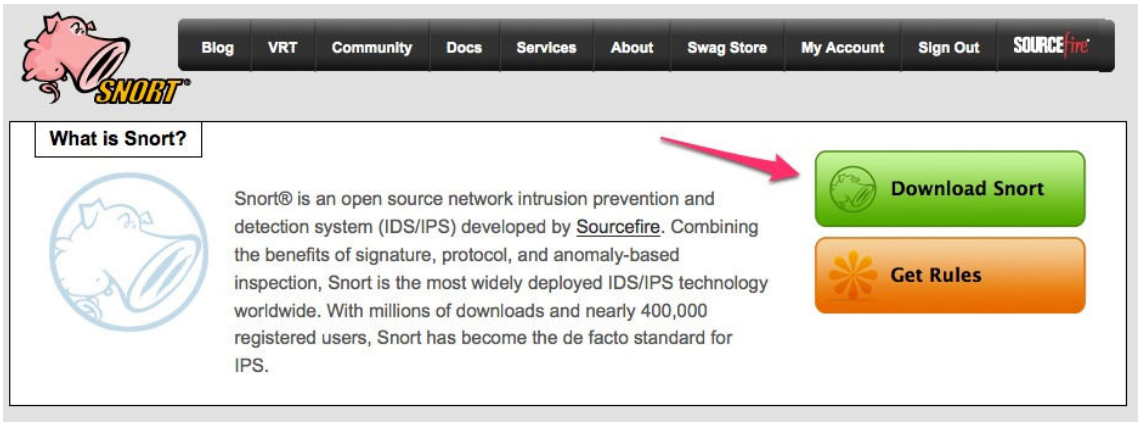

Figura 7 - Download das Regras do Snort

A lista da regras disponíveis para download é demonstrada na imagem abaixo. A versão da regra deve ser igual a versão do Snort que foi instalada.

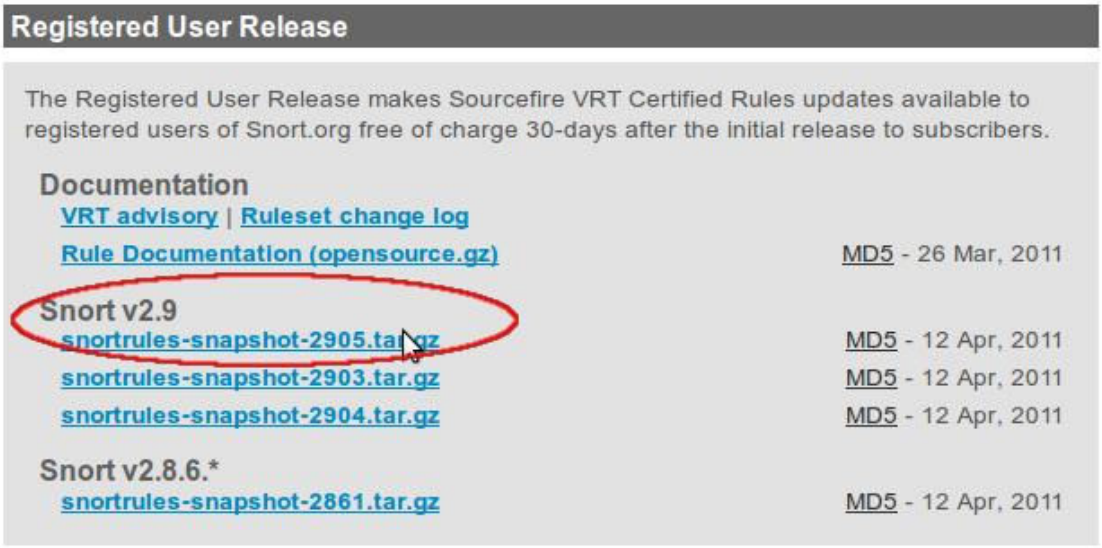

Figura 8 - Lista de Regras disponíveis

Após o download das regras (cerca de 30MB), deve-se descompactar o conteúdo do pacote para a pasta /etc/snort/:

tar -zxf snortrules-snapshot-2905.tar.gz (partindo da ideia de que as regras foram salvas na pasta /etc/snort)

Em seguida, verificar se a pasta /etc/snort/rules possui vários arquivos e também se foi criada a pasta /etc/snort/so.rules.

Para finalizar, deve- incluir as demais regras, descomentando-as no arquivo /etc/snort/snort.conf:

mcedit +395 /etc/snort/snort.conf

Tirar os comentários na frente das regras que serão utilizadas.

6.5. Instalação e configuração do Banco de Dados

Um banco de dados é extremamente necessário em uma aplicação deste nível. Será preciso armazenar os dados para futuras consultas e relatórios. Para isso, um banco de dados MySQL é suficiente.

Os seguintes comandos devem ser utilizados:

mysql -u root – p

Será solicitada a senha de root da base de dados que foi criada durante a instalação.

mysql> create database snort; # Cria a base Snort;

mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost; # Cria usuário snort para a base de dados e fornece privilégios a ele.

mysql> SET PASSWORD FOR snort@localhost=PASSWORD('mypassword'); # Define uma senha para o usuário snort do banco de dados

mysql> exit;

É preciso importar um modelo de base de dados já fornecido pelo Snort:

mysql -u root -p < /opt/snort-2.9.0.5/schemas/create_mysql snort; # digitar a senha novamente para importar

mysql -u root -p; # para acessar o MySQL

mysql> use snort; # para acessar o banco de dados Snort

mysql> show tables; # deve aparecer todas as tabelas criadas com a importação.

mysql> exit; # sair do MySQL

6.6. Instalação do barnyard2

O Barnyard2 é um complemento ao Snort, recebendo os pacotes do Snort em formato unified e convertendo-os para um formato de fácil compreensão para o gerenciador de banco de dados (que no nosso caso é o MySQL). Sem o uso do Barnyard2, os alertas do Snort seriam guardados na base de dados mas sem a possibilidade de saber realmente do que se trata.

Sempre considerando fazer o download dos pacotes em sua última versão, os passos para instalação do barnyard2 são:

```
# cd /usr/src

# wget http://www.securixlive.com/download/barnyard2/barnyard2-1.9.tar.gz

# tar -zxf barnyard2-1.9.tar.gz && cd barnyard2-1.9

# ./configure --with-mysql

# make && make install

# mv /usr/local/etc/barnyard2.conf /etc/snort
```

Deve-se configurar o arquivo de configuração do barnyard2, utilizando os comandos a seguir:

```
# vi /etc/snort/barnyard2.conf
```

No final desse arquivo, adicione uma linha com o seguinte contéudo:

output database: log, mysql, user=snort password=<sua senha da base> dbname=snort host=localhost

É importante testar o Snort em conjunto com o Barnyard2 para verificar se está tudo ok:

```
# /usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i eth0 &
```

E em seguida, inicializamos o barnyard2 para que ele receba os dados do Snort:

```
# /usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.log -w /etc/snort/bylog.waldo -G /etc/snort/gen-msg.map -S /etc/snort/sid-msg.map -C /etc/snort/classification.config &
```

Na primeira vez em que o barnyard2 é executado, ele irá acusar que o arquivo bylog.waldo não existe. Não há problema, este arquivo será criado logo após o tráfego ser analisado pelo Snort.

Para conferir se o barnyard está alimentando a base no MySQL, use o seguinte comando:

```
# mysql –u root -p -D snort -e "select count(*) from event"
```

6.7. Instalação do Apache e recursos Web

Mundialmente conhecido pela sua estabilidade e confiança, o servidor HTTP Apache pode facilitar a análise de tráfego de dados. Através de um navegador web, será possível, em conjunto da aplicação Snorby, visualizar, gerenciar e exportar os resultados obtidos pelo Snort.

Mas antes torna-se necessário configurá-lo corretamente. Esta operação é descrita logo abaixo:

```
# cp /etc/apache2/sites-available/default-ssl /etc/apache2/sites-enabled
```

```
# mcedit /etc/php5/apache2/php.ini
```

Linha #317 -Mude essa linha para- error_reporting = E_ALL & ~E_NOTICE

Ativa-se o protocolo HTTPS, para um acesso seguro ao servidor Web

a2enmod ssl

O framework Pear proverá a capacidade do servidor HTTP Apache de renderizar imagens em HTML5, dados estes que serão gerados pelo Snorby:

pear upgrade PEAR

pear config-set preferred_state alpha

pear install –alll-deps Image_Color Image_Canvas Image_Graph Mail Mail_MIME

/etc/init.d/apache2 restart

6.8. Preparação do ambiente para instalação do Snorby

O Snorby é um frontend feito no framework Ruby on Rails para administração de alertas do Snort. Possuindo uma aparência muito organizada e prática, o Snorby pode exportar relatórios de incidentes, listar os eventos mais comuns na rede monitorada, adicionar novas classificações, categorias para os alertas registrados e diversas outras funções importantes.

Para a instalação do Snorby, faz-se necessária a instalação dos pacotes a seguir:

apt-get install ruby1.9.1 ruby1.9.1-dev libpng12-dev libjpeg62-dev libjasper-dev graphviz-dev libdjvulibre-dev libwmf-dev librsvg2-dev libfftw3-dev liblzma-dev

6.8.1. Instalação do Rubygems

Rubygems são essenciais para gerenciamento de pacotes Ruby de terceiros, que no nosso caso é a categoria em que o Snorby se encaixa.

cd /opt

wget http://production.cf.rubygems.org/rubygems/rubygems-1.8.10.tgz (ou superior)

tar zxvf rubygems-1.8.10.tgz

cd rubygems-1.8.10/

ruby1.9.1 setup.rb

cd ..

6.8.2. Instalação do Imagick

O ImageMagick é necessário para a manipulação correta das imagens e gráficos antes destes serem exibidos através do Snorby.

wget ftp://ftp.sunet.se/pub/multimedia/graphics/ImageMagick/ImageMagick-6.6.9-7.tar.gz

tar xfz ImageMagick-6.6.9-7.tar.gz

cd ImageMagick-6.6.9-7/

./configure

make && make install

cd ..

6.8.3. Instalação do wkhtmltopdf

Um dos pontos altos do Snorby é a possibilidade de exportar os alertas e eventos para o formato de arquivo PDF. O responsável por essa tarefa de conversão é um pacote chamado wkhtmltopdf:

wget http://wkhtmltopdf.googlecode.com/files/wkhtmltopdf-0.10.0_rc2-static-amd64.tar.bz2

tar xvjf wkhtmltopdf-0.11.0_rc1-static-i386.tar.bz2

mv wkhtmltopdf-i386 /usr/local/bin/wkhtmltopdf

chmod +x /usr/local/bin/wkhtmltopdf

cd ..

6.8.4. Instalação do Rails e demais pacotes

O pacote de instalação da linguagem Ruby não é o suficiente para execução do Snorby. Como parte fundamental na ferramenta, instala-se o pacote Rails da seguinte forma:

gem1.9.1 install rails

gem1.9.1 install bundler

gem1.9.1 install pdfkit

6.8.5. Instalação do Snorby

Na página oficial do projeto Snorby (www.snorby.org), deve-se fazer o download da versão mais recente:

Figura 9 - Download do Snorby

Após o download do pacote do Snorby, a instalação será descrita nos passos a seguir:

unzip Snorby-snorby-v2.3.10-0-ga1b1e28.zip

cd Snorby-snorby-a1b1e28/

Alguns parâmetros nos arquivos de configuração do Snorby são essenciais para o correto funcionamento da ferramenta, como descrito a seguir:

vi config/database.yml

No campo Username, é preciso informar o usuário usado para gravar os logs do Snort, este já definido anteriormente.

Em seguida no campo abaixo, Password, é exigido que a senha seja informada entre aspas. Ex: “labredes23”

Como se trata de uma aplicação web, é preciso também informar o endereço IP e a porta que será usada para acessar a interface do Snorby. Este processo está descrito logo abaixo:

vi config/snorby_config.yml

Linha domain: coloque localhost:3000 (pode ser usada outra porta para acessar, como porta 80)

Ainda no mesmo arquivo de configuração, informar o diretório que contém as regras do Snort é essencial. Sem essa informação, não será possível visualizar os eventos categorizados corretamente. Essa configuração é exibida abaixo:

Linha rules: informar o caminho absoluto das regras do Snort. Exemplo: “/etc/snort/rules”.

Para finalizar a configuração do Snort, é preciso cumprir as dependências de pacotes e verificar os erros. Os comandos abaixos executam esta importante tarefa:

bundle install

bundle exec rake snorby:setup

O comando abaixo deve ser usado para testar a aplicação:

rails server -e test

Em um navegador web (dentro da mesma rede) é possível abrir o endereço informado no arquivo snorby_config.yml para ter acesso ao Snorby. Exemplo: http://localhost:3000.

A tela de login do Snorby é similar a exibida abaixo:

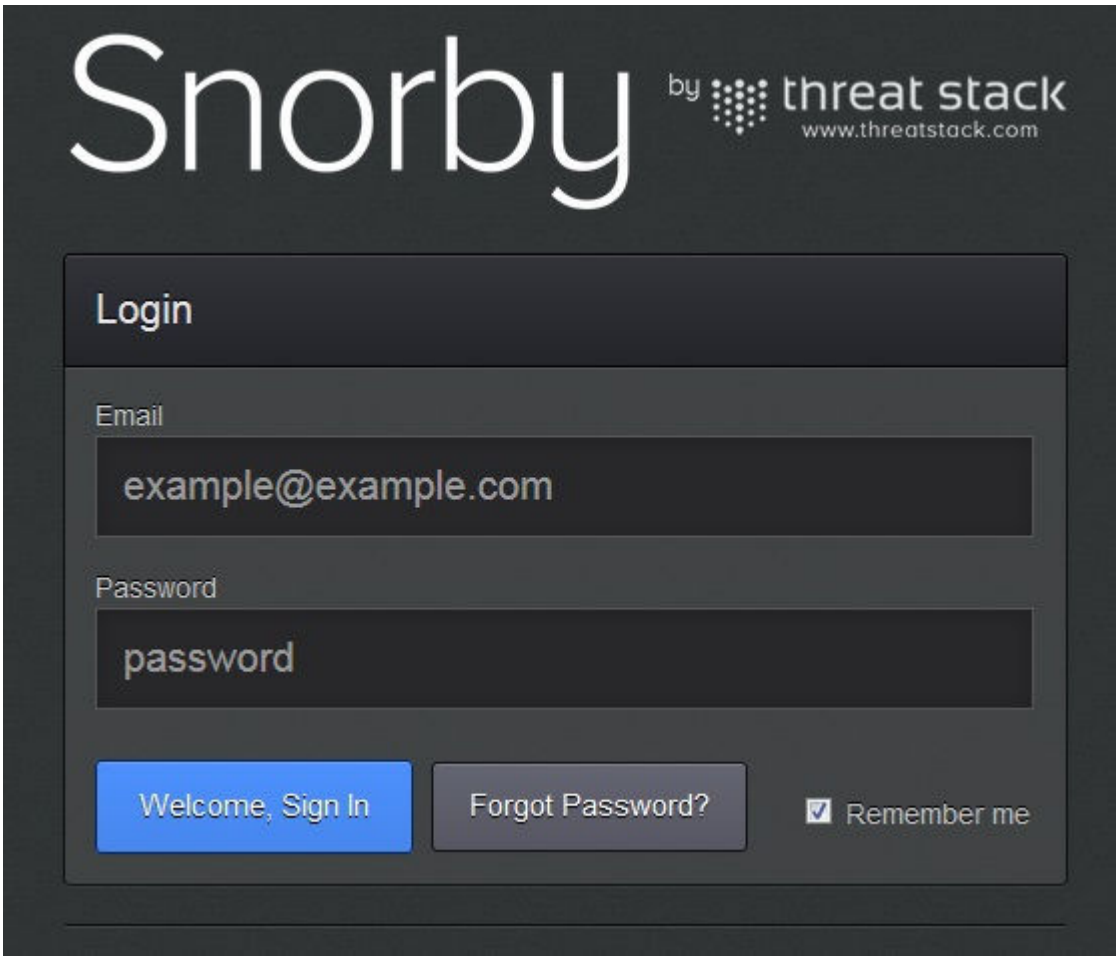

Figura 10 - Tela de Login do Snorby

Para o primeiro acesso, as credenciais são:

Campo Email: admin

Campo Password: deixar em branco

Instaladas todas as ferramentas acima, o Snort está devidamente configurado e pronto para uso e visualização dos alertas. O ambiente de monitoração de rede está devidamente configurado.

7 CONCLUSÃO

O ambiente de monitoração de redes utilizando-se do Snort como ferramenta principal de análise e detecção de anomalias mostrou ser uma alternativa poderosa para solucionar o problema no que tange as redes seguras de computadores. Esta implementação não é uma solução definitiva para todos os problemas de seguranças em uma rede de computadores mas deve ser encarada como uma camada extra de segurança aplicada ao ambiente.

Os resultados obtidos foram satisfatórios e possibilitou uma aproximação aos recursos utilizados em rede. Através do Snort foi possível detectar softwares desatualizados, violações em políticas de seguranças e estações de rede mal configuradas.

Uma possível atualização deste ambiente incluiria o uso de um HIDS trabalhando em conjunto com o IDS e integração com o firewall, permitindo bloquear origens de tráfego malicioso e atividades suspeitas.

REFERÊNCIAS BIBLIOGRÁFICAS

WEIR, Jason. Building a Debian\Snort based IDS. Disponível em <HTTP:// http://www.snort.org/assets/167/IDS_deb_snort_howto.pdf/>. Acesso em 6 de novembro de 2013.

CEZAR, Luis. Instalando o SAMBS (Snort + Apache2 + MySQL + Barnyard2 + Snorby) no Debian. Disponível em <HTTP:// http://imasters.com.br/artigo/21847/linux/instalando-o-sambs-snort--apache2--mysql--barnyard2--snorby-no-debian/>. Acesso em 11 de novembro de 2013.

MONTORO, Rodrigo. Sp0oker Labs – Série Snortando. Disponível em <HTTP://spookerlabs.blogspot.com/>. Acesso em: 18 de novembro de 2013.