Snort – Fundamentos, Funções e Aplicações

Mateus Victorio Zagonel[1] e Cassiano Mônego[1]

[1]Pós Graduado em Resiliência de Redes e Sistemas Distribuídos – Universidade Regional Integrada (URI)
Caixa Postal 709 – 98.400-000 – Frederico Westphalen – RS – Brasil

mateuszagonel@hotmail.com, cassianomonego@gmail.com

Abstract. *With the expansion of communication networks and the consequent increase in the use of these networks, a demand for availability and quality of service was created. Within this context there was a need to improve the management and monitoring of networks in order to avoid failures. A lightweight, secure and open source monitoring tool is Snort, with which it can monitor network traffic and set rules to inform the network administrator of improper access. This article will describe management and monitoring fundamentals using Snort as a tool. Additionally, a test scenario will be presented with the aforementioned tool, as well as a description of its functions. The results demonstrate the possibility of creating monitoring rules and a tool for easy installation, updating and learning for a network administrator.*

Resumo*. Com a expansão das redes de comunicação e o consequente aumento do uso destas, criou-se uma demanda por disponibilidade e qualidade de serviço. Dentro deste contexto houve uma necessidade de aprimorar o gerenciamento e o monitoramento das redes a fim de evitar falhas. Uma ferramenta de monitoramento leve, segura e de código aberto é o Snort, com ela é possível monitorar o trafego da rede e definir regras para informar ao administrador da rede acessos indevidos. Neste artigo serão descritos fundamentos de gerenciamento e monitoramento utilizando como ferramenta o Snort. Adicionalmente, será apresentado um cenário de testes com a ferramenta supra citada, bem como uma descrição das funções desta. Os resultados demonstram possibilidade de criação de regras de monitoramento e uma ferramenta de fácil instalação, atualização e aprendizado para um administrador de rede.*

1. Introdução

Com a crescente utilização de redes de computadores para provimento de serviços surgiu à necessidade de utilizar ferramentas para monitorar recursos e comportamentos das redes de computadores. A utilização de ferramentas de gerenciamento e monitoramento tem o objetivo de aprimorar questões tais como: segurança, desempenho e falhas. E, desta forma prevenir, por exemplo, acessos indevidos, queda de rendimento da rede e falhas na rede.

Nesse contexto, uma ferramenta que se destaca é o Snort. O Snort se trata de um IDS (*Intrusion Detection System*) ou sistema de detecção de intrusos, e é responsável por monitorar o tráfego da rede. Com a utilização do Snort é possível definir regras com alertas, gerar dados estatísticos de quais acessos são suspeitos na rede, ativar regras ao identificar determinado acesso, identificar maiores tráfegos (*host* origem/*host* destino), personalizar mensagens, entre tantas outras tarefas.

O presente artigo tem por objetivo apresentar cenários de testes utilizando máquinas virtuais a fim de apresentar o tráfego de dados na rede, demonstrando quais

dados podem ser verificados utilizando Snort de forma a mostrar como tal ferramenta pode ser útil para monitoramento e gerenciamento do tráfego da rede. Adicionalmente foi realizada a integração com o Snorby a fim de demonstrar em modo gráfico resultados obtidos com o monitoramento do Snort.

O artigo segue a seguinte organização. Na seção 2 é apresentado um texto introdutório de monitoramento e gerenciamento, em seguida a ferramenta Snort e por fim o Snorby. Na seção 3 é apresentado um comparativo entre os IDSs existentes e as vantagens do Snort. Na seção 4 são apresentados os cenários de testes com a criação de regras e os testes realizados com estas. Ainda são apresentados resultados do monitoramento do Snort em modo gráfico com integração deste com Snorby. Na seção 5, são feitas as considerações finais dos autores e as sugestões de trabalhos futuros.

2. Fundamentação Teórica

Nesta seção serão abordados fundamentos de Monitoramento e gerenciamento com relação à necessidade que existe atualmente nas redes de comunicação. Em seguida serão apresentadas características do Snort bem como seu funcionamento. Por fim, será feita uma breve descrição do Snorby que possibilita visualizar em modo gráfico a atuação do Snort na rede.

2.1 Monitoramento e Gerenciamento

O monitoramento e o Gerenciamento são duas características buscadas nas redes de Computadores. Com a proliferação da Internet e o aumento de dispositivos conectados as redes criou-se uma exigência para que além de haver disponibilidade de dados e serviços houvesse sistemas íntegros e cada vez mais seguros.

Nesse contexto surgiram ferramentas de Monitoramento e Gerenciamento. Neste grupo podemos incluir os IDS (Intrusion Detection System) que constituem Sistemas de Detecção de Invasões e permitem monitorar e gerenciar dados obtidos por este monitoramento. Com o uso de um IDS um administrador da rede pode identificar vulnerabilidades em se tratando de ataques e ainda pode identificar gargalos na rede (serviços centralizados, sobrecarga de servidores, entre outros). Uma das ferramentas que atende a tais necessidades (monitoramento e gerenciamento) consiste no Snort que será explicado com mais detalhes no título 2.2 (Santos, 2005).

2.2 Snort

O Snort constitui o IDS, mais utilizado atualmente por ser leve, seguro e de código aberto e por ser portável, podendo ser utilizado em *Windows, Linux Solaris MacOS*, entre outros Sistemas Operacionais. Ele foi desenvolvido por Marty Roesch em 1999. O Snort é baseado em assinaturas de ataques de forma a comparar o tráfego da rede com as assinaturas de ataques existentes em seu banco de regras (Konrath et al, 2002; Santos, 2005).

A sua principal função é inspecionar os dados que estão contidos dentro dos pacotes da rede de forma a verificar se estes podem ser considerados ameaças ou não. Em caso de identificação de pacotes suspeitos são emitidos alertas para que o administrador da rede possa tomar providências no sentido de impedir tais ataques corrigindo as vulnerabilidades (Konrath et al, 2002; Santos, 2005; Garcia, 2013).

Em relação a outras ferramentas de monitoramento, o Snort permite que o administrador de rede desenvolva assinaturas de ataques permitindo a adição de novas regras para identificar ataques a rede. Nesse quesito é importante que o banco de assinaturas esteja em constante atualização e que o administrador da rede faça a gerencia

das regras no sentido de verificar alertas falsos positivos (Santos, 2005). A arquitetura de funcionamento do Snort é apresentada conforme a Figura 1.

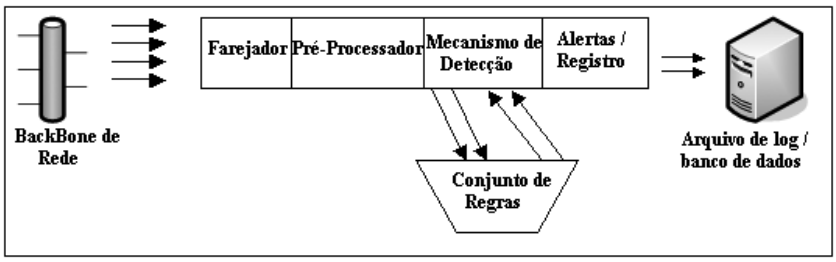

Figura 1. Arquitetura do Snort (Santos, 2005)

Conforme a Figura 1, todo o tráfego da rede é capturado no farejador, em seguida passa por um pré-processador, este identifica os tipos de pacotes e envia para os mecanismos de detecção. A partir do conjunto de regras criadas, é definido o que cada pacote representa na rede. Para tal definição é feita uma analise pelos mecanismos de detecção baseada nas regras, então é determinado se o pacote pode ser considerado uma ameaça ou não. Por fim são gerados os alertas, estes podem ser armazenados em banco de dados ou em logs. Ao visualizar os alertas emitidos pelo Snort o administrador pode tomar decisões para eliminar vulnerabilidades do sistema (Santos, 2005).

Por se tratar de um sistema de código aberto às regras dos principais ataques se encontram disponíveis na página do Snort (www.snort.org) basta que o administrador mantenha o sistema atualizado. Entretanto caso o administrador queira personalizar estas, o Snort permite a criação de regras.

As regras no Snort têm a seguinte estrutura, conforme apresentado na Figura 2. São divididas, basicamente, em "Cabeçalho da Regra" e "Miolo da Regra". No cabeçalho da regra estão contidas as ações tomadas pela regra, o Protocolo, o IP de Origem e o IP de Destino. Seguem as principais ações que uma regra pode tomar (Santos, 2005):

- ***Activate:*** Gera um alerta e possibilita ativar uma regra dinâmica;
- ***Dynamic:*** Deixa a regra inativa até que uma regra *Activate* a dispare;
- ***Alert:*** Registra o pacote e emite mensagem de alerta;
- ***Pass:*** Ignora pacote pré definido;
- ***Log:*** Pacote apenas é registrado sem alerta.

O campo Protocolo, Figura 2, pode ser ICMP, IP, UDP e TCP. Os campos de origem e destino são preenchidos com endereços IP. Pode-se utilizar *any* quando se quer selecionar qualquer endereço. Outra possibilidade é a utilização do sinal de exclamação (!) em frente a um endereço, isso caracteriza que tal endereço não pertence a aquela regra.

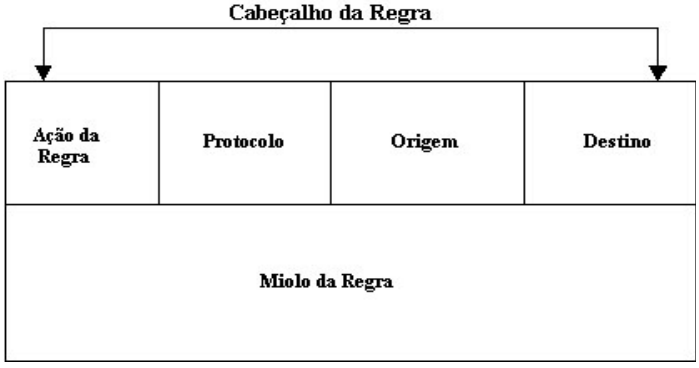

Figura 2. Cabeçalho de Regras no Snort (Santos, 2005).

O campo de Miolo da regra, conforme Figura 2, é responsável por definir: mensagens de alerta (msg), busca por conteúdo dentro de pacote (content), identificar se o IP de origem é igual ao de destino (sameip), capturar dados em texto puro da sessão de protocolo (session), entre inúmeras outras ações (Santos, 2005).

2.2 Snorby

O Snorby corresponde a uma ferramenta de apoio ao Snort com a possibilidade de visualizar em modo gráfico resultados obtidos do monitoramento da rede. O Snorby é responsável por organizar os dados e mostrar em gráficos e em níveis (alto, médio e baixo) o que cada pacote representa em se tratando de ameaças a rede (Maes, 2012; Ehrhorn, 2017). As funções do Snort, com a utilização de regras personalizáveis, e a sua integração com o Snorby apresenta uma possibilidade de monitoramento e gerenciamento do tráfego da rede de forma gráfica. Tal apresentação facilita o trabalho do administrador da rede no sentido de corrigir vulnerabilidades do sistema e prevenir ataques. As funções do Snorby serão apresentadas com mais detalhes no capítulo 4 Cenários de Teste.

3. Comparativo Snort x Outros IDSs

A utilização da rede deve ser controlada, para que sejam evitados transtornos, e consequentemente prejuízos, tanto de tempo, quanto financeiros. Para que este controle seja feito com efetividade tem-se várias ferramentas que fazem um trabalho de detecção de falhas, seja ela de uso ou de invasão de uma rede. Em Santos (2010) são apresentados quatro IDS. Na Tabela 1 é feito um comparativo entre estes e percebe-se que o Snort apresenta algumas vantagens por ser livre, multiportável e por ter características de ser um IDS de rede (NIDS) ou de host (HIDS). O IDS Real Secure apresenta a vantagem de poder operar em modo de rede como em modo host ao mesmo tempo, entretanto se trata de um IDS pago.

Tabela 1. Comparativo entre IDS.

Característica	**Snort**	**Real Secure**	**Bro**	**Open Source Tripwire**
Livre	X		X	X
NIDS/HIDS	X	X	NIDS	HIDS
Unix	X	X	X	X
Windows	X	X		

Conforme a Tabela 1, os IDS Bro e Open Source Tripwire não operam em ambiente Windows o que pode ser uma desvantagem e possuem limitações no seu modo de operar (Santos, 2010).

4. Cenários de Teste

Para que o Snort consiga monitorar todo o tráfego da rede ele opera com a placa de rede em modo promiscuo. Na realização dos testes foi utilizada uma Máquina Virtual Debian para instalação do Snort e ferramentas de apoio. As ferramentas de apoio, além do Snorby, instaladas foram:

- **Barnyard2**: Sistema responsável por transformar os logs binários do Snort em dados, para posteriormente gravar em banco de dados;
- **PulledPork**: Sistema responsável por buscar regras atualizadas na página do Snort;
- **Apache:** Servidor de Arquivos.

Para realizar a configuração do Snort os seguintes diretórios das regras devem ser considerados, conforme Tabela 2.

Tabela 2. Diretórios do Snort

Diretórios	/etc/snort/rules	/etc/snort/rules/iplists	/etc/snort/preproc_rules	/usr/local/lib/snort_dynamicrules
Conteúdo	Regras	Listas de Ips	Processadores	Regras Dinâmicas

Na Tabela 2, seguem diretórios das regras do Snort. No diretório "iplists" se encontram a whitelist e a Blacklist. A Whitelist corresponde a endereços que não são considerados ameaças. Por outro lado a Blacklist apresenta endereços que são utilizados para ataques. A Blacklist pode ser atualizada juntamente com as regras na página do Snort.

Na realização dos testes foram utilizadas as seguintes máquinas, seguem características e seus endereços IP:

- 192.168.0.4: Win7. Máquina Física. Cliente. Hospedada.
- 192.168.0.7: Debian. Máquina Virtual. Snort. Hospedeira
- 192.168.0.8: WinXp. Máquina Virtual. Hospedeira
- 192.168.0.10: Win8. Máquina Física. Cliente.

Para simular testes foram definidas regras simples no Snort a fim de identificar o tráfego da Rede. A primeira regra definida teve a sintaxe:

Alert icmp any any -> $HOME_NET any (msg: "ICMP Test Detected"; GID:1 sid: 1000; rev: 001; classtype: icmp-event;)

A sintaxe da regra acima consiste em: um alerta de ICMP, independente da origem (any) e da porta (any), tendo como destino a HOME_NET e qualquer porta desta (any). A mensagem de alerta a ser emitida consiste em msg:"ICMP Test Detected"; o Id de geração da regra (GID: 1), o número da assinatura no arquivo de regras (Sid: 1000), a versão da regra (rev: 001) e a classificação (Classtype: icmp-event),

Para verificação do funcionamento da regra foi efetuado *ping* da Máquina 192.168.0.4 (hospedada) para a Máquina 192.168.0.7 (hospedeira). Segue *print* do Snort na Figura 3, emitindo alerta "ICMP test Detected". É possível também identificar os hosts de origem e destino.

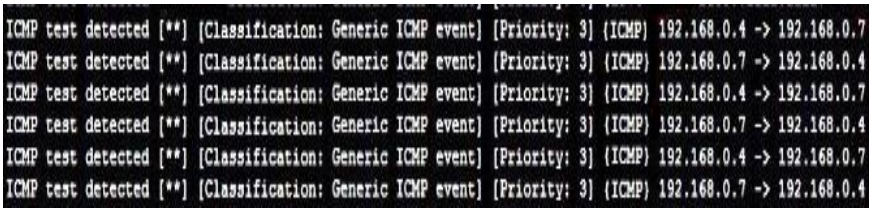

Figura 3. Preview do Snort com a regra de Teste ICMP.

Para realização de mais testes foi criada mais uma regra. Segue sintaxe:

Alert tcp 192.168.0.8 any -> 192.168.0.7 80 (msg: "Tentativa ou acesso, porta 80 – JZ"; GID:3 sid: 1002; rev: 001; classtype: tcp-connection;)

A regra acima gera alertas de tcp-connection quando o host de origem 192.168.0.8 por qualquer porta se comunicar com o host de destino 192.168.0.7 pela porta 80. A mensagem informa "Tentativa ou acesso, porta 80 – JZ". Na Figura 4 pode-se visualizar o Snort ao realizar o acesso via *browser* do Snorby.

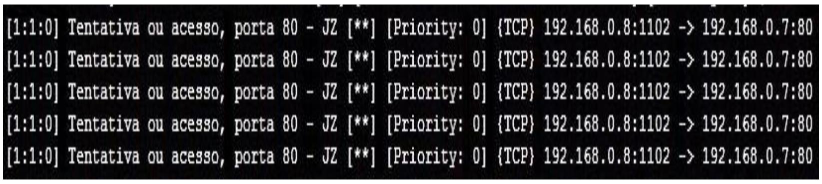

Figura 4. Preview do Snort com regra de TCP-connection de 192.168.0.8 para 192.168.0.7 via porta 80.

Posteriormente foram adicionadas as regras disponíveis na página do Snort e então foram verificados resultados do Snorby de forma a apresentar de forma mais clara os resultados. Conforme é apresentado na figura 5 o Snorby possui diversos menus para controle. Na referida figura o com o item *"Sources"* é possível se identificar quais são os hosts de origem e destino mais acessados. Conforme apresentado, nos testes realizados o IP de destino mais utilizado foi o da máquina hospedada (192.168.0.4). Percebe-se no gráfico outro IP de origem que teve muitos acessos foi o do roteador da rede (192.168.0.1).

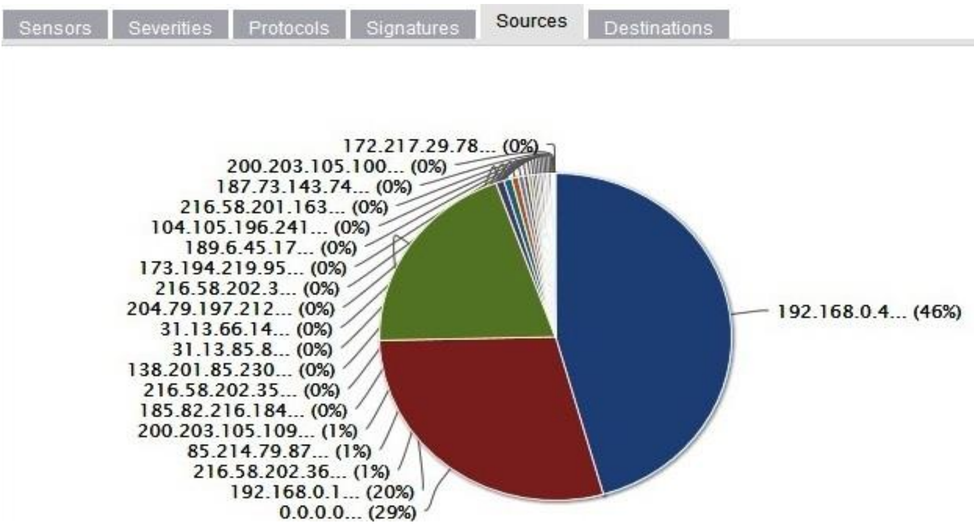

Figura 5. Tela do Snorby, Hosts de Origem mais utilizados.

Os demais itens de Menu que constam na Figura 5, apresentam as seguintes funções :

- ***Sensors**:* Apresenta em gráfico os sensores utilizados e a quantidade de ocorrências encontradas em cada um deles.
- ***Severities**:* É apresentado em gráfico às ocorrências de acordo com os níveis - alto médio e baixo de severidade da ocorrência.
- ***Protocols***: Apresenta os protocolos que estão sendo utilizados na rede.
- ***Signatures***: Responsável por mostrar a assinatura das regras com mais ocorrências na rede. No exemplo de testes, as regras com mais ocorrências foram a de "ICMP test Detected" que foi gerada pelo *ping* entre a máquina hospedada e a máquina hospedeira. E a mensagem de Utilização de SSH, visto que o *putty* estava sendo utilizado para enviar comandos a máquina virtual.
- ***Destination***: IPs de destino mais acessados.

Em outro teste foi alterado o IP da máquina Virtual Xp de 192.168.0.8 para 192.140.221.140. Esse IP estava inserido na "Lista Negra" do Snort. Na Figura 6 pode-

se visualizar que ele foi listado na lista de evento com um nível médio e a mensagem de alerta foi “reputation: Packet is blacklisted”.

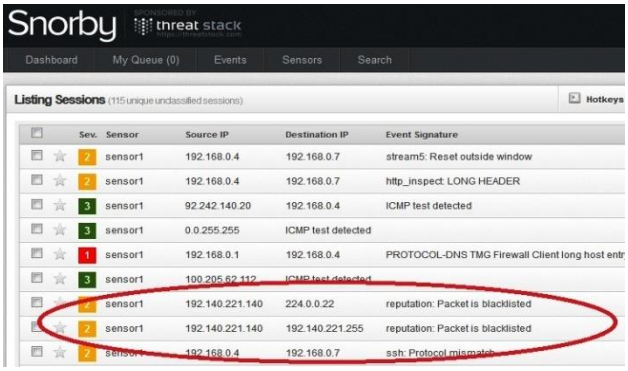

Figura 6. Evento de pacote da BlackListed.

A integração do Snort com Snorby permite facilidade ao administrador da rede para verificação do tráfego da rede e auxílio na verificação de que as regras desenvolvidas se encontram em funcionamento. Com a possibilidade de monitoramento das regras mais utilizadas, *hosts* mais acessados, entre outras informações sendo visualizadas em tempo real, há possibilidade que sejam tomadas medidas para prevenção de ataques e aprimoramento da segurança da rede.

5. Conclusão

O Snort pode ser considerado o IDS mais utilizado para detecção de invasões nas redes atualmente. Um dos motivos do sucesso desta ferramenta se dá por ela ser livre e estar em constante atualização. Quando um ataque é identificado por algum membro da comunidade do Snort, em seguida já é desenvolvida uma regra com alerta de tal vulnerabilidade.

O objetivo do trabalho era apresentar o Snort e suas principais funções. Conforme apresentado, o Snort pode realizar o monitoramento da rede em tempo real, enviando alertas, gravando pacotes em logs, definindo a ativação de regras com determinado tráfego, entre outras. Todas estas funções têm o objetivo de auxiliar o administrador da rede de forma que em caso de tráfego suspeito, este possa corrigir vulnerabilidades identificadas.

Com o Snort foi possível definir regras simples, no sentido de apresentar exemplos de como se definir os controles desta ferramenta. Os testes apresentaram as mensagens criadas. O que fica claro é que com um estudo mais aprofundado da ferramenta pode-se criar regras mais robustas de alertas e refinar cada vez mais o monitoramento de todos os pacotes que trafegam na rede. Ao integrar o Snort com Snorby teve-se um resultado interessante, pois se pode identificar em forma gráfica ocorrências na rede. O Snorby, baseado nos dados obtidos dos sensores do Snort, apresentou em forma de gráficos quais os tipos de protocolo que mais trafegam na rede, qual o IP de origem mais acessado, qual o IP de destino mais acessado. Também foi possível listar regras e suas respectivas mensagens de alerta. Por ser uma ferramenta livre e portável o Snort constitui um IDS de fácil implementação e de resultados plenamente satisfatórios para monitoramento de redes.

5.1. Trabalhos Futuros

Como trabalhos futuros poderiam ser ampliados o número de regras criadas de forma a contemplar mais recursos do Snort e apresentar mais exemplos de cenários de teste. Outra

sugestão seria aprofundar o comparativo na fundamentação teórica e incluir tal comparativo nos cenários de testes. Por fim, também poderia ser desenvolvida uma aplicação em modo gráfico para atualizar, excluir e incluir regras no sentido de tornar a interação facilitada entre a ferramenta e o administrador da rede.

6. Referências

Araújo, A. S., Leite, L. S. e Costa, L. M. M. (2012). "Sistemas de Detecção de Intrusão", http://www.gta.ufrj.br/grad/12_1/ids/OpenSourceTripwire.html, Junho.

Ehrhorn, G. (2017). "Home Snorby", https://github.com/Snorby/snorby/wiki, Junho.

Garcia, R. B. (2013). "Sistema de Detecção de Intrusão e Bloqueio de Ataques Utilizando IDS-Snort". Trabalho de Conclusão de Curso de Técnologo em Redes de Computadores, pela Faculdade de Tecnologia de Lins.

Konrath, M. A et al. (2002). "E-Sentry+: Um IDS Baseado em Rede com Suporte à Especificação em Alto Nível de Assinaturas de Ataque". Em Workshop em Segurança de Sistemas Computacionais

Maes, E. M. (2012). "Desenvolvimento de um Software Web para configurar o Sistema de Detecção de Intrusão Snort". Trabalho de Conclusão de Curso do Curso de Sistema da Informação, pela FURB - Universidade Regional de Blumenau.

Santos, B. R. (2005). "Detecção de intrusos utilizando o Snort." Monografia de Conclusão do Curso de Pós Graduação em Administração de Rede Linux, pela UFLA - Universidade Federal de Lavras.

Santos, V. (2010). "Sistemas de Detecção de Intrusão Usando unicamente softwares Open Source", https://seginfo.com.br/2010/06/21/sistemas-de-deteccao-de-intrusoes-ids-intrusion-detection-systems-usando-unicamente-softwares-open-source/#snort, Junho.