Utilização de Sistema de Detecção e Prevenção de Intrusos modo NIDS

Denis Pohlmann Gonçalves[1]

[1]Coordenação de Tecnologia da Informação – Instituto Federal Farroupilha campus São Vicente do Sul (IFFARROUPILHA-SVS) - São Vicente do Sul – RS – Brazil

denis.goncalves@iffarroupilha.edu.br

Abstract. *This meta-paper presents the results obtained from the use of an intrusion detection system using the tool called Snort, running on free software adapted for firewall, pfSense. This technology has been used at the edge of the network infrastructure of computers of Instituto Federal Farroupilha campus São Vicente do Sul. Its use provided great security to the academic environment against attacks and intrusion, showing good results.*

Resumo. *Este artigo apresenta os resultados obtidos com a utilização de um sistema de detecção de intrusos utilizando a ferramenta chamada Snort, sendo executada sobre o software livre adaptado para firewall, pfSense. Esta tecnologia foi utilizada na borda da infraestrutura da rede de computadores do Instituto Federal Farroupilha campus São Vicente do Sul. Sua utilização proporcionou grande segurança para o ambiente acadêmico contra ataques e intrusões, mostrando resultados consideravelmente satisfatórios.*

1. Introdução

Segundo [Tanenbaum 2003] desde o início da década de 1990, onde a internet se tornou comercial, houve um crescimento exponencial de dispositivos na rede de dados, através dos grandes avanços das tecnologias em *hardware* e *software*, possibilitando cada vez mais a troca de informações entre seus usuários. Além das demandas atuais, novos serviços sempre estão surgindo, com aplicações de inúmeras funcionalidades, como transferências de informações sigilosas e operações financeiras, necessitando uma infraestrutura que garanta a proteção e transmissão segura das informações.

Qualquer serviço, computador ou rede que esteja acessível via Internet pode ser alvo de um ataque, assim como qualquer computador com acesso à Internet pode participar de um ataque [Cert 2015]. Os incidentes normalmente ocorrem explorando a vulnerabilidade, visando diferentes alvos, tais como, empresas diversas, instituições bancárias, instituições governamentais e usuários domésticos. Para isso, utilizam variadas técnicas, como, negação de serviço, *phishing*, *worms*, *trojans*, *spywares* e *keyloggers*. Sendo assim, o uso de um sistema de detecção e prevenção de intrusos torna-se indispensável em qualquer infraestrutura que se deseja ter uma camada extra de segurança contra ameaças.

Este artigo apresenta resultados da utilização de um sistema de detecção e prevenção de intrusos (IDS/IPS) em modo NIDS, chamado *Snort*, executando sobre um sistema operacional baseado em *FreeBSD* e implementado no *firewall* de borda da infraestrutura de redes do Instituto Federal Farroupilha campus São Vicente do Sul (IFFarroupilha-SVS). Contudo, não serão abordados tópicos de instalação do sistema operacional e da ferramenta *Snort*. Esta pesquisa contribui com os resultados obtidos que poderão auxiliar os administradores de rede no tratamento de incidentes em dois aspectos principais, sendo, a coleta de informações referentes aos tipos mais frequentes

de ataques sofridos e os bloqueios que poderão ser efetuados de forma autônoma com o mecanismo IPS, prevenindo ataques futuros e recorrentes.

A estrutura deste artigo apresenta na Seção 2 conceitos fundamentais dos sistemas de detecção e prevenção de intrusos. A Seção 3 apresenta a implementação do sistema IDS/IPS. Na Seção 4 são apresentados os resultados obtidos com a implementação do sistema. A Seção 5 apresenta alguns trabalhos relacionados e na Seção 6 as considerações finais do artigo e trabalhos futuros.

2. Conceitos fundamentais

Para entendimento do artigo esta seção descreve alguns conceitos fundamentais sobre os sistemas IDS, como funções, tipos de sistemas de detecção de intrusão, localização do sensor e mecanismo de bloqueio.

2.1. IDS

Um sistema de detecção de intrusão (*Intrusion Detections System* - IDS) é um mecanismo que tem como principal função detectar diversos ataques e intrusões em redes de computadores, proporcionando uma camada muito grande de segurança, tornando-se um mecanismo essencial em um ambiente corporativo. O IDS trabalha como uma câmera ou alarme contra as intrusões, podendo realizar a detecção com base em algum tipo de conhecimento, como assinaturas ou em desvios de comportamento [Nakamura 2007].

Segundo [Nobre 2007], os IDS são sistemas autônomos que funcionam em tempo real no modo de escuta, considerados *sniffers*, analisando todo o tráfego de rede e detectando tentativas não autorizadas de acesso a infraestrutura lógica, sendo considerados como uma das principais ferramentas de defesa contra invasores.

Com base em dados dos incidentes relacionados a tentativas de ataque e invasões que aconteceram no Brasil, recebidos pelo [Cert 2015], são mantidas as estatísticas sobre as notificações a ele reportadas, sendo estas voluntárias. Na Figura 1, são mostrados por categoria, os incidentes reportados ao Cert.br de janeiro a dezembro de 2014.

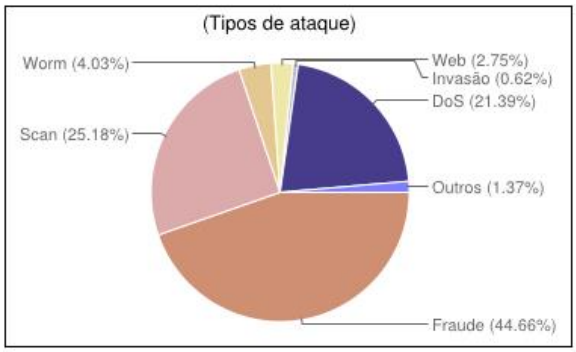

Figura 1. Incidentes reportados ao Cert.br em 2014

Considerando estas notificações é constatado uma incidência grande de fraudes realizadas, possivelmente ocorrências em que as instituições ou usuários tenham sofrido com perdas financeiras. Podemos perceber que as tentativas de ataques acontecem em variadas categorias, sendo que firewalls convencionais não são capazes de detectá-las**.** Estes firewalls utilizam somente controle de camada de rede e transporte, não possuindo a habilidade de verificar o conteúdo dos pacotes, em contrapartida, os IDS são capazes de analisar os pacotes a nível de aplicação e reconhecer padrões de tráfego malicioso se identificado. Empresas que detenham informações sigilosas correm grande risco de

roubo, fraude, dentre outros, se não possuírem algum sistema de segurança eficaz contra esses tipos de ataques, como por exemplo, um sistema IDS.

Existem dois tipos primários de IDS, sendo o baseado em *host* e o baseado em rede. Com o aprimoramento das tecnologias levou ao desenvolvimento do IDS híbrido (*Hybrid IDS*), que utiliza as características do HIDS e NIDS.

2.1.1. HIDS

O sistema de detecção de intrusos baseado em *host* (*Host-Based Intrusion Detection System* - HIDS) faz o monitoramento do sistema, com base em informações de arquivos de *logs* ou de agentes de auditoria. O HIDS pode ser capaz de monitorar acessos e alterações em importantes arquivos do sistema, modificações nos privilégios dos usuários, processos do sistema, programas que estão sendo executados, uso da CPU, entre outros aspectos, como a detecção de *port scanning* [Ranum 2001].

2.1.2. NIDS

O sistema de detecção de intrusos baseado em rede (*Network-Based Intrusion Detection System* - NIDS) monitora a atividade do tráfego em um determinado segmento de rede, utilizando normalmente suas interfaces de rede em modo promíscuo. A detecção é feita com a captura dos pacotes e análise comparativa com padrões ou assinaturas conhecidas pelo NIDS.

Uma característica relevante do NIDS é a sua possibilidade em detectar os ataques de rede em tempo real. Como o sensor atua em modo promíscuo no mesmo segmento de rede de um host atacado, por exemplo, ele pode capturar os pacotes referentes ao ataque, analisar e responder aproximadamente ao mesmo tempo em que o ataque é executado [Shah 2001].

2.1.3. IPS

Os sistemas IDS que capturam o tráfego para somente análise tem sua operação em modo passivo, não sendo possível gerenciar o tráfego de pacotes na rede. Segundo [Nakamura 2007] já os IPS com operação em modo *inline* diferem da operação passiva na forma de captura de tráfego, sendo capazes de detectar e prevenir os ataques. Esses sistemas que operam no modo *inline* são chamados de sistemas de prevenção de intrusão (*Intrusion Prevention System* - IPS).

Os IDS *inline* são capazes de finalizar as conexões enviando mensagens do tipo "*drop*" antes que cheguem ao destino, como acontece nas atividades de um firewall, diferentemente do que acontece nos IPS com operação em modo passivo, onde possuem formas de atuação normalmente com o envio de mensagens "TCP *reset*", possibilitando ao atacante obter informações que podem ser relevantes aos ataques [NetScreen 2002].

3. Implementação

Para a implementação do sistema de detecção e prevenção de intrusos que foi utilizado no ambiente em questão deste artigo, foram utilizados alguns materiais descritos nas subseções a seguir, bem como os métodos. A instalação e configurações básicas dos componentes não são abordadas, visto que o foco deste artigo são os resultados da implementação.

3.1. Hardware

O *hardware* utilizado para hospedar o serviço é um servidor de *rack* de 1u, composto de placa-mãe *Serverboard* X8DTi-F, 2 processadores Intel(R) Xeon(R) CPU E5540 de 2.53GHz contendo 8 *cores* físicos + 8 *cores* virtuais totalizando 16 CPUs, 12 GB de memória RAM DDR3 1333 Mhz, 2 *Hard Disks* SAS 1000 rpm de 600GB cada utilizados em modo RAID0, 2 *interfaces ethernet* de 1000baseT *full-duplex on-board* e 2 fontes de alimentação de 750W.

3.2. Sistema Operacional

Para o sistema operacional foi implementado o *pfSense*. O projeto *pfSense* é um *firewall* de rede de código fonte aberto, com base no sistema operacional *FreeBSD* composto de um *kernel* personalizado e incluindo pacotes de *software* livre terceiros para funcionalidades adicionais, assim sendo capaz de fornecer a mesma funcionalidade, ou mais, dos *firewalls* comerciais comuns [Pfsense 2015].

Segundo [Laskoski 2014], o projeto *pfSense,* desde sua criação em 2004, sempre desejou agregar novos serviços, tais como, VPN, proxy, autenticação de usuários, IDS, possuindo atualmente dezenas de pacotes adicionais que lhe permitem requisitar o posto de firewall UTM, visto que pode realizar a maioria das atividades de sistemas desse porte.

3.3. *Snort*

Snort é uma ferramenta NIDS *open-source* desenvolvida por Martin Roesch sendo muito popular pela sua flexibilidade nas configurações de regras e constante atualização diante das ferramentas de invasão de licença livre. Seu código fonte otimizado, é desenvolvido em módulos utilizando a linguagem C possuindo documentação de domínio público [*Snort* 2015].

Optou-se pela escolha de implementação do *Snort* devido ao sistema estar consolidado há vários anos no mercado, além de constante desenvolvimento de atualizações do sistema e de suas regras de detecção, também chamadas de assinaturas. Seus módulos são capazes de analisar o conteúdo dos cabeçalhos quanto dos pacotes em redes IP, produzindo grande quantidade de informação sobre os ataques detectados.
Além de realizar análises em tempo real com suporte a diversos protocolos a nível de rede e aplicação, sobre o conteúdo *hexa* e ASCII, uma das principais características do seu funcionamento é a ampla possibilidade de tratamento dos alertas gerados, através de ações que vão desde mensagens ao administrador de rede a bloqueios de tráfego.

Outro ponto que apoiou a escolha do *Snort* foi a característica do sistema ser baseado em assinaturas, trabalhando somente em comparação com seu banco de regras, ao contrário dos sistemas de detecção por anomalias que parte do princípio da detecção com base em ações diferentes das atividades normais de sistemas. Segundo [Kizza 2005], os IDS baseados em anomalias possuem algumas desvantagens como, falsos positivos equivocadamente sinalizados como intrusão em relação a atividades anômalas, porém não intrusivas e falsos negativos, por não produzirem alguma anomalia perceptível, assim tendo intrusões não detectadas.

3.4. Metodologia

Utilizando o *hardware* descrito na seção 3.1, foi instalada a versão mais recente do sistema *pfSense*, atualmente v.2.2.2, sendo configuradas todas as questões inicias de endereçamento, roteamento, autenticação e os controles de camada de transporte, utilizando a política padrão de bloqueio total, liberando somente o necessário. Após, via gerenciador de pacotes do *pfSense*, foi instalado o *Snort* em sua versão mais recente, atualmente v.3.2.4.

Para o funcionamento do mecanismo de comparação de assinaturas do *Snort*, é necessário popular o seu banco de dados de assinaturas instalando as *rules*. Para isso, foi criado um usuário no site da comunidade e então baixadas as assinaturas registradas, que são mantidas pela comunidade e possuem frequentes atualizações. Logo após, foi definida e configurada a interface *wan* para atuação do *Snort*, sendo esta a primeira interface de entrada de pacotes da instituição.

Em relação ao desempenho de detecção, considerando o *hardware* utilizado descrito na secção 3.1, ficou definido o uso do algoritmo AC-STD (*Aho-Cosarick*

Standard) devido a utilizar uma quantidade moderada de memória, porém com alta performance. O *Aho-Corasick* é um algoritmo inventando em 1975 pelos pesquisadores do Bell Labs Alfred V. Aho e Margaret J. Cosarick. Sua função é realizar pesquisas em *strings* com o objetivo de localizar palavras chaves em textos, a partir de uma única interação, utilizando como base um dicionário com um conjunto finito de palavras chave. [Aho e Corasick 1975].

Como critério para a escolha das *rules* a serem utilizadas no IDS em questão, foram tomadas como base as informações referentes aos tipos e frequência de ataques divulgadas pelo Cert.br e apresentadas na secção 2.1. Logo foram selecionadas as seguintes, *scan.rules*, *botnet-cnc.rules*, *phishing-spam.rules*, *spyware-put.rules*, *vírus.rules, trojan.rules*, *worm.rules, dos.rules, ddos.rules* e *sql.rules,* considerando as demais *rules* disponíveis para futura aplicação.

Para a utilização do sistema IPS, o pacote *Snort* instalado já acompanha a solução *barnyard2,* sendo que para sua ativação foi necessário apenas configurações basicamente relacionadas aos *logs* de eventos. O período de bloqueio definido para potenciais atacantes foi de 15 dias, tendo como critério utilizado a seguinte situação. Por exemplo, se for definido um prazo de bloqueio muito grande ou até indefinido, no momento do ataque há a possibilidade do atacante estar conectado a provedores de acesso à internet que forneçam endereços IP em modo dinâmico "DHCP Server", fato muito comum. Assim, logo após o atacante obter um novo endereço IP, seu antigo fica disponível para um novo usuário, que porventura poderá utilizá-lo e acessar serviços hospedados na instituição, mesmo considerado tráfego legítimo, não será possível estabelecer a comunicação por seu endereço IP já estar bloqueado. Entretanto, se for escolhido um prazo pequeno, como o definido, ainda manterá segurança e evitará perdas de conectividade.

Com o objetivo de monitorar e promover a segurança de toda a rede acadêmica do campus, foi escolhido a borda da infraestrutura como localização de instalação da solução IDS, assumindo assim a posição de roteador, firewall de perímetro e solução de detecção e prevenção de intrusos, em modo NIDS. A Figura 2 mostra a localização da solução na infraestrutura.

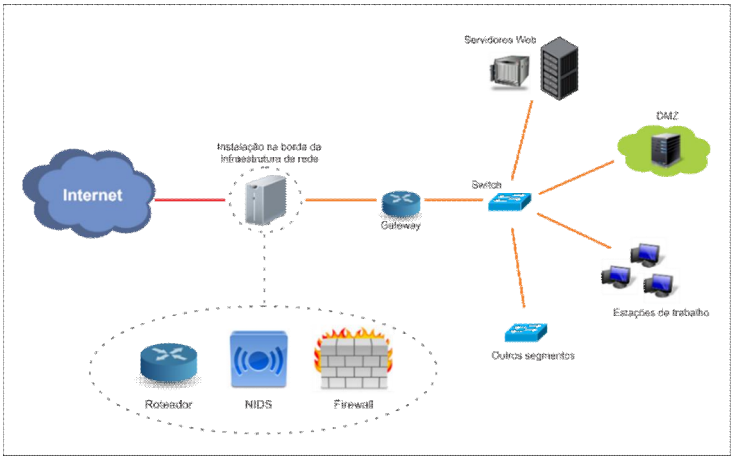

Figura 2. Localização da solução NIDS no IFFarroupilha-SVS

4. Resultados

A partir da implantação do sistema descrito, todo o tráfego entre a internet e o campus, passou a ser monitorado e analisado pelo IDS, estando em funcionamento desde então.

Apesar do *Snort* estar configurado para detecção de apenas algumas das assinaturas mais conhecidas, sua efetividade foi considerada satisfatória, analisando o ambiente desprotegido antes de utilizar o sistema de prevenção de intrusos, foco desta implementação.

Para apresentação dos resultados, foram coletados informações atualizadas, geradas a partir dos alertas do IDS em Agosto de 2015, mês de escrita deste artigo, no período de 01/08/2015 a 31/08/2015, totalizando 31 dias. Com base nessas informações foram detectados 7730 alertas, em sua maioria escaneamento de portas e serviços, incluindo algumas tentativas de conexões a banco de dados.

Após análise das informações obtidas, foi observado uma grande frequência de alertas dos tipos *"(spp_sip) Content length mismatch"* e *"ET SCAN Sipvicious User-Agent Detected,* ambos tendo como alvo a porta destino 5060 e utilizando o protocolo UDP. Com base nesta situação, percebeu que os atacantes estavam primeiramente tentando descobrir serviços ativos que permitam registros SIP (*Session Initiation Protocol*), para logo após, iniciar ataques com o objetivo de fazer ligações telefônicas sem custo para o intruso, utilizando a tecnologia VOIP (*Voice Over internet Protocol*). A Figura 3 apresenta as informações obtidas com base nos tipos de alertas gerados.

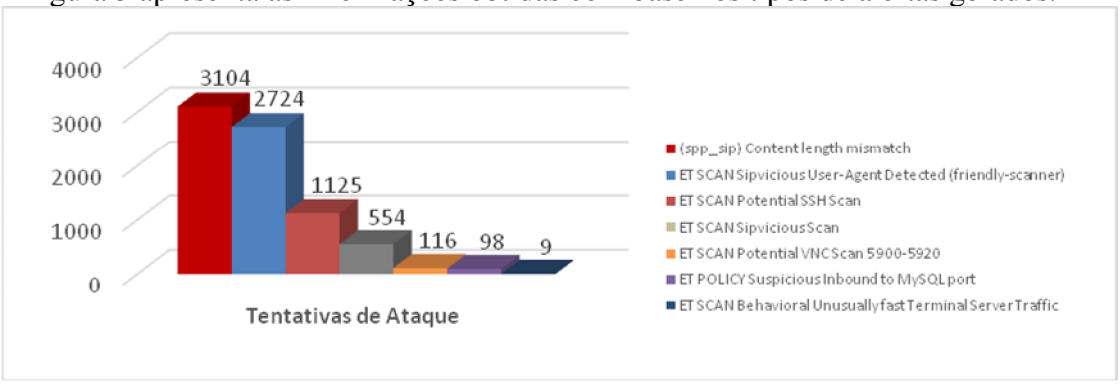

Figura 3. Tentativas de ataques sofridas entre 01/08/2015 a 31/08/2015

Todas as atividades consideradas tentativas de ataque que geraram alertas tiveram seus endereços IP de origem bloqueados pelo mecanismo IPS do *Snort*, conforme ação previamente configurada. Alguns tráfegos legítimos foram reconhecidos pelo IDS como atividade suspeita de ataque, aproximadamente 1% do total de alertas, tendo seus *hosts* de origem bloqueados e posteriormente sendo removidos manualmente. Esta ação conhecida como "falso positivo" torna-se uma dificuldade encontrada, ocasionando um grande impacto em relação a conectividade dos *hosts* que tem seu tráfego legítimo dentro da normalidade, porém bloqueados indevidamente.

A questão de falsos positivos ocorridos nos sistemas IDS em softwares livres está sendo minimizada pelos desenvolvedores de suas comunidades de acordo com as contribuições das regras de detecção mais aprimoradas, podendo ser considerado um trabalho futuro de pesquisa.

5. Trabalhos Relacionados

Uma análise bibliográfica e estudo de caso de comparação entre dois sistemas de detecção de intrusos baseados em assinaturas, *Snort* e *Suricata*, foi mostrado no trabalho de [Murini 2014], aonde utilizou dados sintéticos da DARPA para avaliação dos resultados.

Em [Cunha Neto 2005] é mostrado o *Snort* como ferramenta de detecção e prevenção de intrusos baseado no método de detecção por conhecimento de assinaturas, bem como sua instalação e configuração em ambiente *Linux*.

Em [Perlin, Nunes e Kozakevicius 2011] é apresentado os principais conceitos relacionados ao desenvolvimento de sistemas detectores de intrusão em redes de computadores, com foco voltado para detecção de intrusão por anomalias, um dos métodos utilizados nos IDS, baseada na transformada *Wavelet*.

Esta pesquisa demonstra a eficácia do *Snort* como sistema IDS baseado na detecção por assinaturas, apresentando resultados obtidos com dados das tentativas de intrusões sofridas no ambiente acadêmico em questão, contribuindo assim, com os administradores de redes e pesquisadores da área de tecnologia em segurança da informação.

6. Considerações finais

Apesar do campus de São Vicente do Sul manter na sua infraestrutura de redes diferentes mecanismos de segurança, como *firewalls*, soluções antivírus, *VPN*, *DMZ*, dentre outros, não estavam sendo suficiente para prevenir alguns tipos de ameaças.

Esta pesquisa e implementação do sistema de detecção e prevenção de intrusos baseada em rede utilizando assinaturas, proporcionou uma camada extra de segurança para a rede acadêmica do local, tornando possível detectar e prevenir diversos métodos de ataques, protegendo assim todos os sistemas e *hosts* internos. Além disso, permitiu o monitoramento e documentação dos possíveis ataques futuros, auxiliando e orientando o administrador de redes do local como proceder com os incidentes de segurança.

Algumas assinaturas desenvolvidas pela comunidade do *Snort* ainda estão gerando falsos positivos, causando bloqueios indesejados. Análise e testes com essas regras estão sendo efetuadas para que não ocorram indisponibilidade de algum sistema e ao mesmo tempo possam somar a base de dados de conhecimento do IDS.

6.1. Trabalhos futuros

Os conhecimentos obtidos através da implementação descrita neste artigo bem como a efetividade do sistema IDS podem ser ampliados através de futuras pesquisas, sendo algumas apontadas a seguir:

Modificar e/ou parametrizar as assinaturas do *Snort* para otimizar suas detecções a fim de minimizar os falsos positivos.

Aplicar as demais *rules* disponíveis da comunidade do *Snort* e verificar seu funcionamento e efetividade.

Comparar o *Snort* com outros sistemas de detecção de intrusos como o Suricata.

Referências

Aho, A. V. e Corasick, M. J. (1975) "Efficient String Matching: An aid to bibliographic search", Comm. Of the ACM 18, n.6: 333-340.

Cert br (2015) "Centro de Estudos, Resposta e Tratamento de Incidente de Segurança no Brasil", http://www.Cert, Julho.

Cunha Neto, R. P. (2005) "Implementação de Ferramenta para detecção de Intrusão", em Caderno de Estudos Ciência e Empresa, FAETE, v.02, p. 01-06.

Kizza, J. M. (2005) "Guide to Computer Network Security", New York, NY:Springer.

Laskoski, J. (2015) "O que é pfSense", http://goo.gl/eIsL3L, Setembro.

Murini, C. T. (2014) "Análise dos Sistemas de Detecção de Intrusão em Redes: Snort e Suricata Comparando com Dados da Darpa", UFSM, TCC, Janeiro.

Nakamura, E. T. (2007) "Segurança de Redes em Ambiente Corporativos", Novatec Editora, São Paulo.

NetScreen Technologies, Inc. (2002) "Intrusion Detection and Prevention – Protecting Your Network From Attacks".

Perlin, T., Nunes, R. C. e Kozakevicius, A. J. (2011) "Detecção de Anomalias em Redes de Computadores através de Transformadas Wavelet", em Revista Brasileira de Computação Aplicada (ISSN 2176-6649), Passo Fundo, v. 3, n 1, p. 02-15, mar. 2011.

Pfsense (2015) "pfSense Open Source Security", https://www.pfsense.org, Agosto.

Ranum, M. J. (2001) "Coverage in Intrusion Detection Systems", NFR Security, 26 de Agosto.

Shah, B. (2001) "How to Choose Intrusion Detection Solution", Sans Institute, 24 de Julho.

Snort (2015) "The Open Source Network Intrusion Detection System", https://www.Snort.org, Julho.

Tanenbaum, A. S. (2003) "Redes de Computadores", 4. ed. Elsevier, Rio de Janeiro.