Detecção de Anomalias em Redes de Computadores com a Utilização de Aplicativos Específicos

Rogério Hanawa[1], Kelton Augusto Pontara da Costa[2], Henrique Pachioni Martins[3], André Luiz Ferraz Castro[4]

Centro de Ciências Exatas e Sociais Aplicadas
Universidade do Sagrado Coração (USC) – Bauru, SP – Brasil
rogerio.hanawa@usc.edu.br, kelton.costa@usc.br

Abstract. *The large increase in the number of connected devices in computer networks has caused an increase in quality services demand, making the proper functioning of computer networks each time more important. The anomalies in computer networks are considered irregularity that occur on information traffic due to situations such as software defects, excessive traffic on the network, hardware equipment failure and configuration problems. These anomalies have caused major problems for businesses and individuals both financially and socially since they often make the internet usage temporarily unavailable. The studies devoted to detecting anomalies in computer networks try to find solutions with early detection of anomalies.*

Resumo. *O grande aumento no número de dispositivos ligados em redes de computadores tem ocasionado um aumento na demanda por serviços de qualidade, sendo cada vez mais importante o bom funcionamento das redes de computadores. As anomalias em redes de computadores são consideradas irregularidades que ocorrem no tráfego de informações devido a situações como defeitos de softwares, excesso de tráfego na rede, falhas de equipamentos de hardware e problemas de configurações. Essas anomalias têm ocasionado grandes problemas para empresas e pessoas físicas, tanto financeiramente como socialmente, já que muitas vezes essas anomalias indisponibilizam temporariamente o uso da internet. Os estudos voltados para detecção de anomalias em redes de computadores procuram encontrar soluções com detecções antecipadas das anomalias.*

1. Introdução

Com a expansão da *Internet* houve um grande aumento na exposição das redes de computadores, cada vez mais ocorrem situações que são consideradas como anomalias de rede; podem ser ataques às redes por grupos organizados, problemas de infraestrutura na rede ou de *Internet*. Diante desse contexto mundial criou-se a necessidade de identificar, analisar e prevenir essas anomalias no menor espaço de tempo possível; adotar medidas preventivas e utilizar corretamente ferramentas de monitoramento e detecção para garantir a segurança e bom funcionamento de todo o ambiente computacional. (TELLES, 2008).

Medidas de prevenção devem ser incluídas em toda a topologia do sistema, medidas de controles de acessos físicos e lógicos, utilização de ferramentas de *Internet* com *firewalls*, analisadores de redes, dispositivos de *hardware* e o estudo de vulnerabilidades nas configurações dos sistemas. (TITTEL, 2002).

A utilização de técnicas de reconhecimento de padrões do comportamento das redes são métodos que permitem detectar anomalias pelo tráfego da rede, tendo como objetivo principal a rápida detecção e se necessária recuperação da normalidade da rede.(HAJJI, 2003).

Esse estudo tem como objetivo principal: conhecer as técnicas de detecção de anomalias de redes, os conceitos de anomalias de redes, medidas preventivas, utilização de ferramentas para simulação de anomalias existentes em redes de computadores.

Como objetivos específicos: conhecer os tipos e exemplos de anomalias em redes, seus conteúdos teóricos; encontrar métodos de detecção de anomalias; e utilizar ferramentas de gerenciamento de rede para verificação de anomalias.

2. Anomalias de Rede e Detecção

Todos os sistemas de detecção de anomalias têm como o objetivo principal a detecção de um problema na rede da forma mais rápida possível; essa rapidez é essencial para a redução dos impactos e danos que o problema pode causar na rede. (THOTTAN, 2003).

A detecção de anomalias consiste na tarefa de distinguir ou descobrir dados cujo comportamento esteja fora dos padrões considerados normais e esperados para o conjunto ao qual ele pertence. (ROUGHAN et al. ,2004).

O Sistema de Detecção de Intrusão (SDI) é largamente utilizado para prover a segurança de ambientes interconectados, onde seu objetivo consiste em monitorar a rede em busca de indícios que identifiquem uma invasão e notificar o administrador da rede sobre o ocorrido. (XIAOPING; YU, 2004).

Os Sistemas de Prevenção de Intrusão (SPI) atuam na rede de modo passivo e de forma pró ativa, possibilitando que ataques conhecidos ou não sejam identificados com antecedência, possibilitando ao administrador da rede tomar medidas preventivas. (SEQUEIRA, 2003).

O conceito de entropia foi definido como uma medida ligada à quantidade de informações e de incerteza em um determinado sistema com base na probabilidade de um determinado evento acontecer. Na detecção de anomalias a entropia pode ser usada através da avaliação do padrão do comportamento do tráfego da rede; mensurando o fluxo de *IP (Internet Protcol)* ou *bytes* trafegados em determinados pontos da rede. (SHANNON, 1948).

Um método que faz uso de análise de entropia para detecção de anomalias baseada numa assinatura estatística de tráfego. É utilizada a análise para a detecção e classificação da anomalia em uma lista de tipos. A metodologia consegue inferir um padrão de tráfego normal através do uso de técnicas de estruturação e agrupamento de dados para mineração, aprendizado e classificação do tráfego. (LUCENA; MOURA, 2008).

Um ataque *DoS* é uma tentativa mal-intencionada por uma única pessoa ou um grupo de pessoas para fazer um site com alvo, ou nó para negar serviço a seus clientes. Quando esta tentativa deriva de uma única máquina da rede ou um pequeno grupo de

máquinas, constitui-se um ataque *DoS*. Por outro lado, também é possível que uma grande quantidade de hospedeiros maliciosos se coordene para inundar a vítima com uma abundância de pacotes de ataque, de modo que o ataque ocorra simultaneamente a partir de pontos múltiplos. Este tipo de ataque é chamado de *DoS* distribuído, ou um ataque *DDoS*.

Podemos fazer uma analogia quando falamos de anomalias de tráfego e *DDoS* e chegamos a conclusão que se trata da mesma coisa. A principal característica das anomalias de tráfego são as alterações danosas que estas podem ocasionar à rede. A Entropia Não-Extensiva analisa esse tipo de problema e existem formas de Entropia (que é a avaliação do padrão de comportamento do tráfego) como a de Shannon e a de Tsallis. Vários estudos foram feitos e concluiu-se que este tipo de detecção é flexível e permite um bom desempenho. (EVANGELISTA, 2008).

O método baseado em heurística consiste essencialmente em estabelecer um conjunto de regras e instruções simples em uma linguagem de programação para encontrar possíveis soluções para problemas complexos ou mal definidos. Embora não seja considerado o melhor método, a programação heurística propicia bons resultados. (MAXION; TAN, 2000).

Uma assinatura em um sistema de detecção de intrusão consiste em um padrão que verifica o tráfego com o objetivo de localizar alguma anomalia. Para ter certeza que um pacote de dados é confiável é necessário que este seja testado contra todas as assinaturas configuradas. (LAUFER, 2002).

Uma análise por assinaturas utiliza todos esses padrões estabelecidos para verificar se cada pacote os apresenta. É uma simples comparação do conteúdo dos pacotes com o conteúdo das assinaturas. (LAUFER, 2002).

As principais origens de falhas estão relacionados com problemas de especificação, implementação, componentes defeituosos, desgaste dos componentes físicos, interferência eletromagnética e variações ambientais. Também não podemos desconsiderar as falhas de natureza humana. (ANDERSON; LEE, 1981).

A redundância de *hardware* está baseada na replicação de componentes físicos, onde a redundância de *hardware* passiva, neste tipo, componentes redundantes são utilizados para mascararem falhas, ou seja, corrige erros sem implicar ações do sistema. (WEBBER, 2002).

Os vírus moderadamente inofensivos são normalmente os que conseguem se espalhar mais rápido e se manter ativos durante mais tempo, já que são os menos notados e os menos combatidos. Com isso, os criadores de vírus lentamente foram mudando de foco, deixando de produzir vírus espetaculares, que apagam todos os dados do *HD (Hard Disk)*, para produzirem vírus mais discretos, capazes de se replicarem rapidamente, usando técnicas criativas, como enviar mensagens para a lista de contatos pessoais ou postar mensagens usando seu *login* em redes sociais. Como resultados disso, os vírus passaram a atingir cada vez mais máquinas, embora com danos menores. (MORIMOTO, 2008).

Atualmente, existem diversos tipos e categorias de protocolos de roteamento interno e externo. Os mais utilizados internos são os protocolos *RIP(Routing Information Protocol)*, e *OSPF(Open Shortest Path First)* e externo o *BGP (Border Gateway Protocol)* .(FOROUZAN, 2012).

Com determinados softwares é possível detectar uma anomalia pela filtragem de pacotes; exemplo: um crescimento rápido no fluxo de um determinado protocolo (*FTP* -

File Transmission Protocol, por exemplo) e crescimento de fluxo acelerado a um destino na rede. (BARFORD; PLONKA, 2001).

A filtragem de pacotes é um método que exige um conjunto *hardwares* de alto nível, sendo sua utilização mais adequada em redes de grande porte e locais que disponham de bons recursos financeiros. (BARFORD; PLONKA, 2001).

O protocolo de gerenciamento *SNMP (Simple Network Management Protocol)* desenvolvido na década de 80 para resolver problemas de gerenciamentos em ambientes de rede *TCP/IP (Transmission Control Protocol / Internet Protocol*) heterogêneas. Primeiramente foi desenvolvido como uma solução provisória o *CMIP (Common Management Information Protocol)*. Desde então o protocolo *SNMP* passou a ser o mais utilizado. (ODA, 2012).

O protocolo *FTP (File Transfer Protocol)* possui a capacidade de transferências de arquivos entre máquinas com sistemas operacionais diferentes. O *FTP* também tem a capacidade de manipular as transferências interativas de arquivos e por pilhas. O *FTP* utiliza a porta 21 para conexão de controle *FTP* em protocolos *IP* e a porta 20 utilizada para transferência de arquivos na rede. (TITTEL, 2002).

O *pharming* consiste em alterar a tabela de *DNS* de um ou mais servidores, fazendo com que toda a requisição de página, como por exemplo 'www.banco.com.br', seja desviada para outro endereço controlado pelo *scammer*. Se a página for uma cópia fiel da página verdadeira, é possível até que profissionais experientes sejam vítimas desse golpe.(THOMPSON, 2005).

O arquivo conhecido como cavalo de tróia ou *trojan* geralmente ocorre quando funcionários de uma rede corporativa têm acesso pela *internet* a sites não confiáveis, se a rede não possuir um *firewall* ou um *proxy* eficiente o registro da máquina do usuário pode ser infectado e é carregado toda vez que a máquina reinicia. Existem diversos tipos de *trojans*, alguns simplesmente comprometem o funcionamento correto do sistema operacional, outros podem fazer com que a máquina execute operações automaticamente como, por exemplo, conectar-se com servidores de *IRC*; deixando toda a rede vulnerável e exposta a um controle externo. (OLIVEIRA, 2003).

Um *Trojan Horse* ou Cavalo de Tróia ou simplesmente *trojan* é um programa que age como a lenda do cavalo de Tróia, entrando no computador e liberando uma porta para um possível invasor. (TELLES, 2008).

O método de intrusão *sniffer* ou 'farejador' trabalha interagindo com a placa de rede, realiza a leitura dos pacotes que transitam pela rede. Quando implantado um *software sniffer* ele é executado em modo promíscuo (misturado) e é muito utilizado para coletar informações que não tenha como destino somente o *MAC-Adress* associado a essa porta. (ASHLEY, 2006).

A biblioteca *'pcap'* é destinada a captura de pacotes, podendo funcionar de modo oculto. A *pcap* trabalha com algumas funções para recebimento e processamento de cada pacote. Normalmente utiliza-se a biblioteca *pcap* em conjunto com um aplicativo *sniffer*.(JACOBSON; LERES; MCCANNE, 2002).

3. Metodologia

Foram realizadas pesquisas experimentais baseadas nos estudos bibliográficos com a aplicação de testes diferenciados utilizando a linguagem de programação *Delphi* com aplicativos prontos para comprovação dos resultados.

Pesquisados e estudados os métodos e formas que ocorrem as anomalias de rede para embasamento e aplicação em ambiente prático.

Foram realizados três testes práticos onde foram realizados com a utilização de quatro computadores interligados em rede através de um roteador; foram aplicados métodos com o intuito de alcançar os resultados mais próximos da realidade dos ataques, identificação das anomalias e medidas práticas que auxiliem um gerenciador de rede a identificar de modo mais rápido possível uma anomalia de rede.

Na realização do último teste foi mantido a topologia de rede utilizada sendo substituído o roteador DLink por um *hub* da marca 3COM, modelo SUPERSTACKII, composto por 24 portas LAN.

Para os testes práticos foi utilizada a seguinte topologia de rede, conforme demonstra a figura 1:

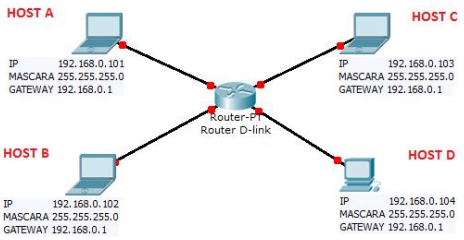

Figura 1 – Topologia de rede utilizada nos testes práticos 3.1 e 3.2.
Fonte: Elaborado pelo autor.

Na topologia utilizada nos experimentos práticos, os computadores foram interligados em um ambiente de rede interna, sendo que o *router* ligado com acesso a *internet*, sendo que, de acordo como os experimentos realizados houve o desligamento da conexão da *internet* de acordo com a necessidade da análise a ser realizada.

O primeiro teste realizado no estudo foi voltado à análise de detecção de anomalia de rede baseada em protocolos, sendo utilizada a topologia de rede conforme demonstra a Figura 1, através da linguagem *Delphi* foi utilizado o componente *IdIcmpClient*, sendo disparado eventos de solicitação ao *gateway* da rede 192.168.0.1 a um ciclo de 1 *Hertz* (1 ciclo por segundo).

O *software* foi executado sequencialmente, ou seja, computador após computador, colhendo os resultados e por último executado simultaneamente em todos os computadores da rede.

O intuito dessa análise foi ver como a rede se comporta quando recebe requisições simultâneas, as alterações no tempo de resposta e procurar algum padrão que se diferencie do normal.

A segunda análise realizada foi analisa anomalia de rede sob influência de um aplicativo *sniffer* (farejador de rede), utilizou-se a topologia de rede, conforme a figura 1. Foi utilizado conexão com a *Internet*, acessada através do *host* D. Foi escolhido o *software* Cain que ficou ativo na rede realizando a leitura e captura de pacotes que trafegavam pela rede. Nessa análise foram realizados testes na rede interna com o *software* Cain em execução, verificado a influência no *gateway* da rede e no roteador quando acessado a rede *internet*.

O intuito dessa análise foi verificar o comportamento da rede sob a influência de um aplicativo que faz a leitura e captura de pacotes, detectar algum padrão de anomalia, haja vista, que esse tipo aplicativo pode ser utilizado de modo prejudicial.

A terceira análise foi baseada em anomalia de rede através de *hardware* defeituoso; para a realização dessa análise foi mantida a topologia de rede, sendo apenas substituído o roteador Dlink por um *hub* 3COM, modelo SUPERSTACKII composto por 24 portas *LAN*. Durante a análise verificou-se que a rede apresentava queda de conexão de modo intermitente, foram monitorados individualmente as máquinas e seus respectivos *IP(s)* e monitorado simultaneamente o *gateway* da rede para identificação da anomalia. Abaixo, a figura 2 demonstra a topologia de rede local.

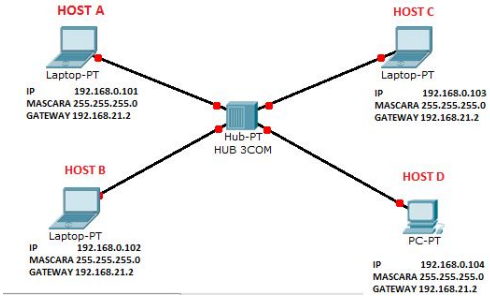

Figura 2 – Topologia de rede utilizada no teste prático 3.3
Fonte: Elaborado pelo autor.

4 Resultados obtidos

Para a análise dos resultados do primeiro experimento de rede baseado em protocolos foi utilizado o *software* Colasoft Ping Toll, uma ferramenta de análise de rede que ficou monitorando *gateway* da rede, sendo que ao ser executado o *software* desenvolvido em linguagem *Delphi*, denominado de programa T1, notou-se que houve uma alteração progressiva no tempo de resposta, de acordo com a execução progressiva do *software* nos computadores da rede; sendo constatado como ponto mais interessante o "pico" obtido quando os quatros computadores executaram simultaneamente o programa, de aproximadamente 400, onde o tempo de resposta que se mantinha estável em 1(ms) milisegundo atingiu 412 (ms) millissegundos.

Fazendo-se uma análise comparativa, esse "pico" simula a anomalia de negação de serviço, onde vários computadores requisitam uma mesma página ou *IP* sobrecarregando a rede fazendo-a com que a mesma não consiga responder a todas as solicitações e ficando temporariamente indisponível até a regularização do sistema.

Na segunda análise de rede, sob a influência de um aplicativo *sniffer* para obtenção dos resultados foi utilizado o *software* Colasoft Ping Toll, uma ferramenta de análise de rede, a rede interna quando executado o *software* Cain não apresentou alterações tanto na comunicação entre os *host(s)*, bem como, no *gateway* da rede. Foi detectado alterações no comportamento da rede quando verificado a comunicação via *Internet* através do monitoramento do *IP* atribuído pelo roteador para comunicação externa na rede.

É possível verificar pelas áreas destacadas em vermelho que com a execução do aplicativo *sniffer* a rede ficou instável chegando a determinados momentos a perder momentaneamente a conexão, nesse experimento o *site* acessado para estudo foi o mesmo.

A captura de pacotes realizada pelo *software* Cain na rede influenciou diretamente a conexão com a *Internet*, ocasionando visivelmente perda de pacotes e lentidão na rede.

Para a realização da terceira análise de anomalia da rede sob a influência de equipamentos de *hardware* com defeito dos resultados foi utilizado o *software* Colasoft Ping Toll, uma ferramenta de análise de rede que ficou monitorando a rede. Devido ao problema ser intermitente foram realizados vários testes, sendo que a causa da anomalia veio a ser encontrada quando monitorado o *gateway* da rede que fazia com que o *TTL - Time to Live* atingisse o valor máximo de 255, impossibilitado o tráfego de dados.

5. Considerações finais

Com base em todo levantamento bibliográfico e os diversos autores pesquisados a metodologia sugerida nesse contexto com a realização de testes em uma topologia de rede, descrita nos capítulos anteriores, foram obtidos resultados indicativos para que fosse possível identificar e simular anomalias em redes de computadores.

Esse estudo pretendia auxiliar gerentes, profissionais da área de rede e administradores de rede, ou entusiastas da área de rede para compreender o que vem a serem anomalias de rede de uma forma geral.

Os resultados servem como subsídio para auxiliar profissionais da área da rede a identificar anomalias e tomar medidas que regularize de modo mais rápido possível a normalidade da rede; aos programadores que desejam desenvolverem softwares através da análise dos resultados, de acordo com os valores obtidos nas análises experimentais, utilizando-se como exemplo: alterações nos parâmetros encontrados no gateway da rede quando está ocorrendo um ataque *DoS* ou *DDoS*, alterações no *Time to Live – TTL* da rede, e no comportamento da rede quando utilizado os *softwares* denominados *sniffers*.

Referências

ANDERSON, T.; LEE, P. A. Fault tolerance -principles and practice. Englewood Cliffs, Prentice-Hall, 1981.

ASHLEY, M. Fine-tune your IDS/IPS, 2006. Disponível em :<http://www.comnews.com/stories/articles/0706/0706fine_tune.htm>. Acesso em 02 Jun 2012.

BARFORD, P.; PLONKA, D. “Characteristics of Network Traffic Flow Anomalies” , p.69-73, nov 2001.

EVANGELISTA, S. V. B. Sistema de Detecção de Intruso e Sistema de Prevenção de Intruso. Petrópolis: Laboratório Nacional de Computação Científica, 2008, 75p.

FERREIRA, A. B. H. Web Dicionário, 2012. Disponível em :< http://www.webdicionario.com/anomalia>. Acesso em 9 maio 2012.

FOROUZAN, B. A. Comunicação de Dados e Redes de Computadores. 3 ed. Porto Alegre: Bookman, 2012, pg.485.

HAJJI H. “Baselining Network Traffic and Online Faults Detection”. Communications, 2003, ICC 03. IEEE International Conference on, v.:1, p.301-308, maio 2003.

JACOBSON, V.; LERES C.; MCCANNE,S. PCAP Library, 2002. Disponível em:<http://www.tcpdump.org/pcap.htm.>. Acesso em 02 Jun 2012.

LAUFER, R. P. Introdução a Sistemas de Detecção de Intrusão. Rio de Janeiro UFRJ, 2002. Trabalho para a disciplina de redes de computadores.

LUCENA, S. C.; MOURA, A. S. Detecção de Anomalias Baseada em Análise de Entropia no Tráfego da RNP. In: 13º Workshop de Gerência e Operação de Redes e Serviços. 2008, Rio de Janeiro. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/wgrs/2008/012.pdf>. Acesso em 15 jun 12.

MAXION, R.; TAN, K. Benchmarking Anomaly-Based Detection Systems, 1st. International Conference on Dependable Systems & Networks, 2000. Disponível em:<http://www.cs.cmu.edu/afs/cs.cmu.edu/user/maxion/www/pubs/maxiontan00.pdf >. Acesso em 02 Jun 2012.

MORIMOTO, C. E. Redes Guia Prático. São Paulo: GDH Press e Sul Editores, 2008.

ODA, C. S. Gerenciamento de redes de computadores. Disponível em:<http://www.gt-er.cg.org.br/operacoes/gerencia-redes>. Acesso em 04 Jun.2012.

OLIVEIRA, W. Técnicas para Hackers – Soluções para segurança – versão 2. Porto – Lisboa. Portugual: Centro Atlântico, 2003.

ROUGHAN, M.; GRIFFIN, T. MAO, Z.M.; GREENBERG, A., FREEMAN, B. IP Forwarding Anomalies and Imporoving their Detection Using Multiple Data Sources. SIGCOMM'04 Workshops, p.307-312, set 2004.

SEQUEIRA, D. 2003. Intrusion Prevention Systems - Securitys Silver Bullet?. Disponível em :< http://whitepapers.zdnet.co.uk/0,39025945,60070694p-39000677q,00.htm.> Acesso em 1 jun 2012.

SHANNON, C. E. 1948. A mathematical theory of communication. Bell System Technical Journal, 27:379–423 and 623–656.

TELLES, R. Descomplicando a Informática. Rio de Janeiro. Ed: Campus, 2008.

THOMPSON, M. A. INVASÃO.BR. Salvador: ABSI – Associação Brasileira de Segurança na Internet, 2005.

THOTTAN, M.;JI, C. Anomaly detection in IP networks. IEEE Transactions on Signal Processing, v.51, n.8, p.2191-2204, 2003.

TITTEL, E. Rede de Computadores. Porto Alegre. Ed. Bookman, 2002.

WEBER, Taisy Silva. Tolerância a Falhas: Conceitos e Exemplos. Programa de Pós-Graduação, UFRGS, 2002.

XIAOPING, Y.; YU, D. 2004. An Auto-configuration Cooperative Distributed Intrusion Detection System. Disponível em:<http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=\&arnumber=1342340\&i%snumber=29576.>. Acesso em 01 jun 12.