UNIVERSIDADE DO SAGRADO CORAÇÃO

ROGÉRIO HANAWA

DETECÇÃO DE ANOMALIAS EM REDES DE COMPUTADORES COM A UTILIZAÇÃO DE APLICATIVOS ESPECÍFICOS

BAURU

2012

ROGÉRIO HANAWA

DETECÇÃO DE ANOMALIAS EM REDES DE COMPUTADORES COM A UTILIZAÇÃO DE APLICATIVOS ESPECÍFICOS

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para a obtenção do título de bacharel em Ciência da Computação, sob orientação do Prof. Dr. Kelton Augusto Pontara da Costa.

BAURU
2012

Hanawa, Rogério
H2338d

Detecção de anomalias em redes de computadores com a utilização de aplicativos específicos / Rogério Hanawa -- 2012.
42f. : il.

Orientador: Prof. Dr. Kelton Augusto Pontara da Costa.

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Universidade do Sagrado Coração - Bauru - SP

1. Anomalias. 2. Redes de computadores. 3. Tráfego. 4. Configurações. I. Costa, Kelton Augusto Pontara da. II. Título.

ROGÉRIO HANAWA

DETECÇÃO DE ANOMALIAS EM REDES DE COMPUTADORES COM A UTILIZAÇÃO DE APLICATIVOS ESPECÍFICOS

Qualificação para Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para a obtenção do título de bacharel em Ciência da Computação, sob orientação do Prof. Dr. Kelton Augusto Pontara da Costa.

Banca examinadora:

_____

Prof. Dr. Kelton Augusto Pontara da Costa

Universidade do Sagrado Coração

_____

Prof. Esp. Henrique Pachioni Martins

Universidade do Sagrado Coração

_____

Prof. Esp. André Luiz Ferraz Castro

Universidade do Sagrado Coração

Bauru, 19 de novembro de 2012.

AGRADECIMENTOS

Antes de tudo agradeço a Deus, por possibilitar essa oportunidade de estudo, ajudar nas horas difíceis e me dar forças para concluir esse objetivo.

Agradeço em especial a minha esposa que sempre esteve ao meu lado e teve paciência nos momentos necessários.

Um agradecimento especial aos Professores, Mestres e Doutores da Universidade do Sagrado Coração que sempre me trataram com muito respeito e profissionalismo, e que me proporcionaram um grande crescimento pessoal e educacional.

Em especial ao meu orientador Dr. Kelton Augusto Pontara da Costa, ao Prof. Esp. Henrique Pachioni Martins e ao Prof. Esp. André Luiz Ferraz Castro, pelos ensinamentos, pela confiança e disposição demonstrada sempre que precisei para conclusão desse estudo e por todos os ensinamentos e tratamento pessoal recebido.

Ao meu amigo de classe Luis Fernando Titon Pereira que sempre me auxiliou nos momentos de maior dificuldade e que levo comigo como um grande amigo para o resto de minha vida e a todos aqueles que me auxiliaram nesse projeto de maneira direta ou indiretamente, meus sinceros agradecimentos.

Muito Obrigado a todos!!!

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 *softwares* 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. Nesse estudo serão demonstrados conceitos e características da detecção de anomalias, as formas de ataques à rede de computadores, seus tipos e métodos de detecção.

Palavras-chave: Anomalias. Redes de computadores. Tráfego. Configurações.

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, *softwares* 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. This study will demonstrate concepts and characteristics of anomalies detection, forms of attacks on computer networks, their types and detection methods.

Keywords: Anomalies. Computer networks, Traffic, Configurations.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

CMIP	*Common Management Information Protocol*
BGP	*Border Gateway Protocol*
DDoS	*Distributed Denial of Service*
DMZ	*DeMilitarized Zone*
DNS	*Domain Name System*
DoS	*Denial of Service*
EGP	*External Gateway Protocol*
FTP	*File Transport Protocol*
HD	*Hard Disk*
IEEE	*Institute of Electrical and Electronics Engineers*
IGP	*Internal Gateway Protocol*
IP	*Internet Protocol*
LED	*Light Emitting Diode*
OSPF	*Open Shortest Path First*
RIP	*Router Information Protocol*
SDI	Sistema de Detecção de Intrusão
SYN	*Synchronize*
TCP	*Transmission Control Protocol*
TTL	*Time to Live*
XNS	*Xerox Network System*

SUMÁRIO

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 *softwares*[1]. 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 *softwares* com *firewalls*[2], analisadores de redes, dispositivos de *hardware*[3] e o estudo de vulnerabilidades nas configurações dos sistemas. (TITTEL, 2002).

O uso de aplicações comerciais desenvolvidas para essa finalidade, atualmente, oferecem informações que ao serem analisadas possibilitam verificar se está ocorrendo alguma movimentação indevida na rede; possibilitando ao gerenciador adotar medidas corretivas para evitar o problema.

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).

A segurança de rede é constantemente testada pelos *hackers*[4], os gerenciadores de redes foram testados e desafiados através dos ataques de negação de serviço, que deixaram inacessíveis alguns dos mais famosos *websites*, como o 'Piratebay', 'Banco do Brasil', entre outros. Os ataques de negação de serviço *(Denial of Service – DoS)*[5] consistem no envio indiscriminado de requisições a um endereço eletrônico alvo, ocorre que, os grandes números de solicitações simultâneas saturam o

[1] Programa de computador composto por uma sequência de instruções que é interpretada e executada.
[2] É um dispositivo que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.
[3] É usado para fazer referência a detalhes específicos de uma dada máquina, incluindo-se seu projeto lógico pormenorizado bem como a tecnologia de embalagem da máquina.
[4] Indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores.
[5] Termo usado na informática quando um *site* para de funcionar, prestar serviço por excesso de solicitação simultânea.

limite da rede fazendo com que o *site* fique temporariamente indisponível; esse tipo de ataque pode causar impactos financeiros e de imagem para empresas.(TELLES, 2008).

Seguindo a mesma linha surgiram os ataques de negação de serviço distribuídos *(Distributed Denial of Service* - DDoS)[6] que conjugam dois conceitos: a de navegação de serviço e intrusão distribuída. Esses ataques podem ser definidos como sendo um conjunto de ataques partindo de várias origens, disparados simultaneamente e de modo coordenado sobre um ou mais alvos. (TELLES, 2008).

1.1 OBJETIVOS GERAIS

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.

1.2 OBJETIVOS ESPECÍFICOS

- Estudar determinados tipos e exemplos de anomalias em redes, seus conteúdos teóricos;
- Encontrar métodos de detecção de anomalias;
- Utilizar ferramentas de gerenciamento de rede para verificação de anomalias.

[6] Termo usado na informática quando um *site* para de funcionar, prestar serviço por excesso de solicitação simultânea por um grupo.

1.3 JUSTIFICATIVA

A estabilidade na rede de computadores tornou-se algo indispensável nos tempos atuais; falhas de redes ou interrupções mesmo que momentâneas trazem sérias consequências.

Grandes empresas na área de telecomunicações e prestadoras de serviço fazem altos investimentos financeiros voltadas na prevenção e detecção de anomalias em rede; falhas nos sistemas podem prejudicar milhões de usuários e acarretar sérios danos financeiros ao mercado e seus clientes diretos e indiretos (SOBRE, 2012).

> O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira. Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato. (SOBRE....,c2012).

A Figura abaixo, demonstra o total de incidentes reportados pelo CERT.br nos anos de 1999 a 2012.

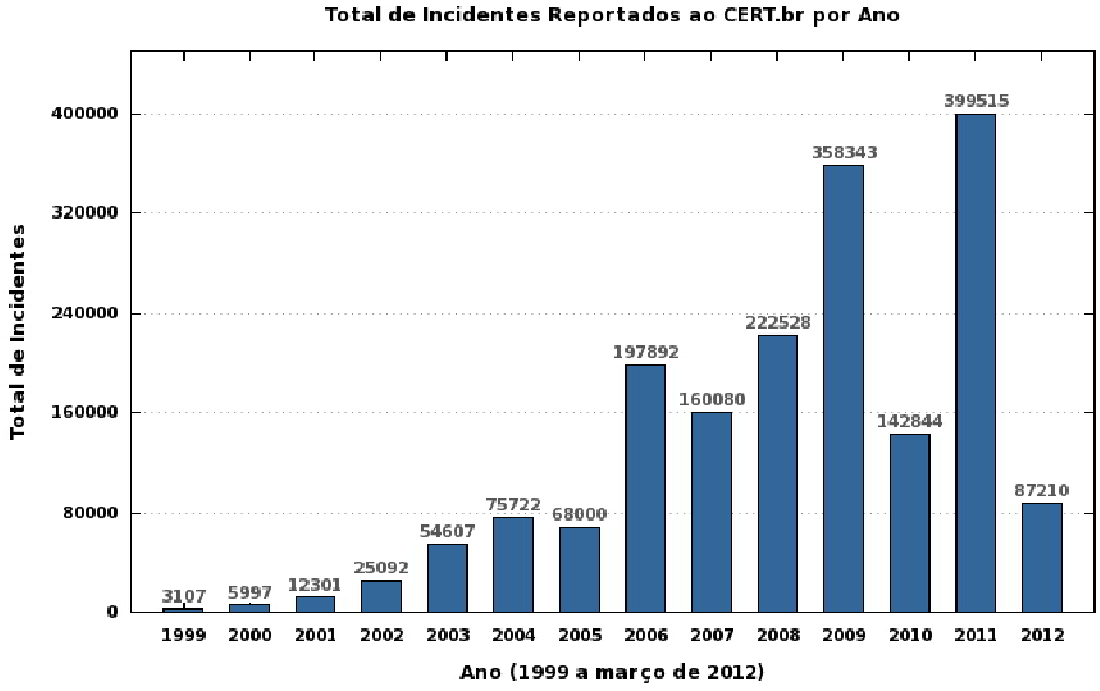

Figura 1 – Total de Incidentes reportados ao CERT.br por ano
Fonte: SOBRE (c2012).

A Agência Nacional de Telecomunicações (ANATEL, 2012) é o órgão que fiscaliza e acompanha as empresas prestadoras de serviço, bem como, a qualidade e problemas enfrentados pelos seus clientes.

1.4 ESTRUTURA DO TRABALHO

Esse estudo foi realizado e estruturado em tópicos e subtópicos de maneira a facilitar sua compreensão e leitura.

No capítulo 1, é descrita a Introdução do estudo descrevendo a importância do estudo de anomalias de redes, estudo de medidas preventivas e as formas de ataque.

Nos tópicos 1.1 e 1.2, o Objetivo Geral e os Objetivos Específicos a serem alcançados.

No tópico 1.3, a Justificativa desse estudo, ressaltando a importância crescente de um bom funcionamento de uma rede de computadores.

No capítulo 2, é descrito todo o Levantamento Bibliográfico que serviu de embasamento teórico para compreensão e possibilitar uma análise da parte prática do estudo. Foram abordados os conceitos e definições de anomalias de redes, tipos e exemplos de anomalias, formas e sistemas de detecção, os principais protocolos de rede, definição de rede interna e externa, enfim, a parte bibliográfica do estudo.

No capítulo 3, é descrito a Metodologia utilizada nos experimentos práticos, a topologia de rede, e dividido em subtópicos os experimentos realizados.

No capítulo 4, são descritos os Resultados Obtidos, ilustrações dos testes, *softwares* utilizados e conclusões dos testes.

No capítulo 5, é descrito a Conclusão Final do estudo.

2 LEVANTAMENTO BIBLIOGRÁFICO

2.1 ANOMALIA e DETECÇÃO

Segundo Ferreira (2012), define-se anomalia como o que se desvia da norma, da generalidade. Irregularidade.

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).

Conforme Roughan et al. (2004), 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.

“A detecção de anomalias consiste na tarefa de determinar a discrepância entre o comportamento realmente encontrado e o comportamento esperado na movimentação da rede [...]”. (HAJJI, 2003, p.301).

2.2 TIPOS E EXEMPLOS DE ANOMALIAS

Existem anomalias voltadas tanto para a parte do *hardware* do sistema, bem como aquelas ocasionadas por erros de *softwares*, como também as ocasionadas pelo ambiente externo como ataques DoS ou DDoS a um determinado servidor.

Exemplos:

- Tráfego excessivo em um determinado ponto da rede ou falhas no *link* ocasionando um congestionamento de pacotes;
- Número excessivo de requisições ftp a um determinado servidor ocasionando a queda do serviço;

- Configurações erradas nos dispositivos de rede; roteadores sem tabelas de roteamento corretas ou algoritmos de roteamento inadequados para a rede;
- Defeitos nos componentes físicos: roteadores com defeitos, cabeamento com resistência, impedância errada, montagem incorreta, entre outros...
- Defeitos nos *softwares* de roteamento: inconsistência em caso de queda de *links* ou determinados nós da rede, os *softwares* de roteamento devem ser capaz de resolver problemas de perda de caminhos através de seus algoritmos de roteamento e das tabelas de roteamento.
- Ataques DoS a um servidor ocasionando sua parada momentânea na prestação de serviços. (LYRA, 2008).

2.2.1 *Softwares* de Detecção de Intrusão

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).

Conforme Laufer (2002) trata-se de uma ferramenta composta de sensores capazes de disparar um alarme caso algum evento não esperado ou determinado venha a ocorrer na rede.

> O principal objetivo para se usar um sistema de detecção de intrusão é para possuir o conhecimento de que está em andamento ou ocorreu uma tentativa de invasão e de que possivelmente houve algum comprometimento de algum servidor ou estação. Essa informação é crucial quando se quer proteger a integridade, privacidade e autenticidade de dados em uma rede, que é o ponto principal para se usar qualquer tipo de ferramentas de segurança. Muitas vezes, mesmo depois de um ataque, é importante fazer uma análise dos dados obtidos para saber a origem do atacante, até onde ele conseguiu penetrar e ainda recolher informações para prevenir que outros tipos de ataque sejam efetivados. (LAUFER, 2002, p.2)

"Os SDIs são excelentes mecanismos que podem ser adicionados na arquitetura de defesa em profundidade de uma rede. Eles podem ser utilizados para identificar vulnerabilidades e fraquezas em seus dispositivos de proteção de perímetro [...]". (GUIMARÃES; LINS; OLIVEIRA, 2006, p.25).

A Figura 2 demonstra uma topologia de rede composta por um SDI.

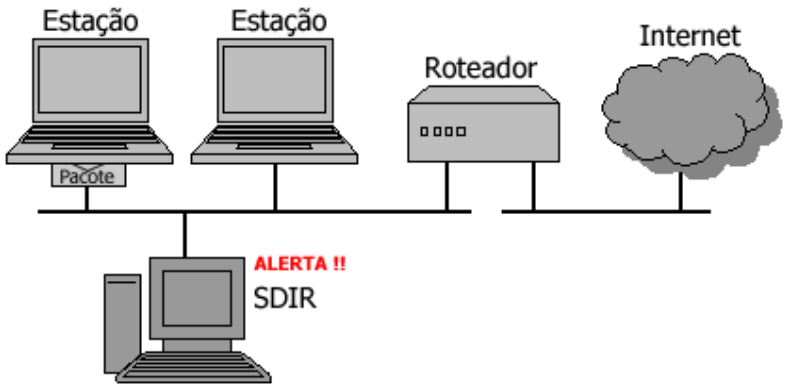

Figura 2 – Detecção de intrusão em uma rede local de difusão
Fonte: LAUFER (c2002).

Uma intrusão pode ocorrer em qualquer parte da rede, tanto em redes locais ou externas. Muitas vezes, a colocação de monitores nas entradas da rede não é suficiente, desse modo podemos implantar SDI em variados pontos da rede.

Exemplos:

- Máquinas próximas as zonas críticas[7];
- Em segmentos de redes desmilitarizadas *(*DMZ*)*[8] que mantém serviços públicos do tipo: servidores *Web*, transferência de ficheiros *(*FTP*),* resoluções de nomes *(*DNS*)*, ou servidores de comércio eletrônico;
- Na intranet empresarial onde encontram os serviços críticos;
- Nos pontos de junção da rede *intranet* com a rede *extranet* e a rede remota. (SISTEMA...,c2012).

De acordo com Cheswick, Belovin e Rubin (2005, p.33),

> Uma DMZ é um exemplo da nossa filosofia em geral de defesa em profundidade. Isto é múltiplas camadas de segurança fornecem um escudo melhor. Se o invasor passar pelo primeiro firewall ele ganhará acesso a DMZ, mas não necessariamente a rede interna.

[7] Locais na rede que apresentam risco de segurança, acesso de informações restritas. Ex: banco de dados, servidores.
[8] Locais que oferecem uma proteção de múltiplas camadas, de difícil acesso ao usuário comum.

2.2.2 *Softwares* de Prevenção de Intrusão

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). Sistemas de prevenção de intrusão são considerados versões avançadas dos *softwares* de detecção de intrusão. (IERACE; URRITA; BASSET,2005).

De acordo com Ierace, Urrita e Basset (2005) os *softwares* de prevenção de intrusão realizam uma análise do tráfego da rede em tempo real comparando-a com um conjunto de regras pré-estabelecidas filtrando os pacotes maliciosos.

2.2.3 Detecção de anomalias usando análise de entropia

O conceito de entropia foi definido por Shannon (1948) 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 ou *bytes* trafegados em determinados pontos da rede.

Lucena e Moura (2008) apresentaram 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.

2.2.4 Detecção de anomalias de tráfego (DDoS)

Segundo Patrikakis, Micalis e Olga (2012), a *internet* consiste de centenas de milhões de computadores distribuídos em todo o mundo. Milhões de pessoas usam a *internet* diariamente, muitos se tornam um alvo fácil para os usuários mal intencionados que tentam esgotar seus recursos e lançar ataques *Denial-of-Service (*DoS*)* contra eles.

Um ataque DoS é uma tentativa mal-intencionada por uma única pessoa ou um grupo de pessoas para fazer um *site* como alvo, 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 coordenem para inundar a máquina da 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.

Os ataques DoS tentam esgotar os recursos da vítima. Esses recursos podem ser a banda da rede, potência de computação, ou dados operacionais estruturais do sistema. Para lançar um ataque DDoS, usuários mal-intencionados primeiro constroem uma rede de computadores que eles vão usar para produzir o volume de tráfego necessário para negar serviços aos usuários de computador. Para criar esta rede de ataque, os atacantes descobrir *sites* vulneráveis ou *hosts* da rede. As máquinas que estejam rodando essas ferramentas de ataque são conhecidas como zumbis, e eles podem realizar qualquer ataque sob o controle do atacante.

A Figura 3 apresenta o resultado desse processo automatizado, é a criação de uma rede de ataque DDoS que consiste em uma máquina denominada de manipulador (*master*) e outras denominadas de agentes escravo (*daemon*). O processo acontece enquanto a rede de alvos está sob ataque e cria uma quantidade significativa de tráfego.

> 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, p.45).

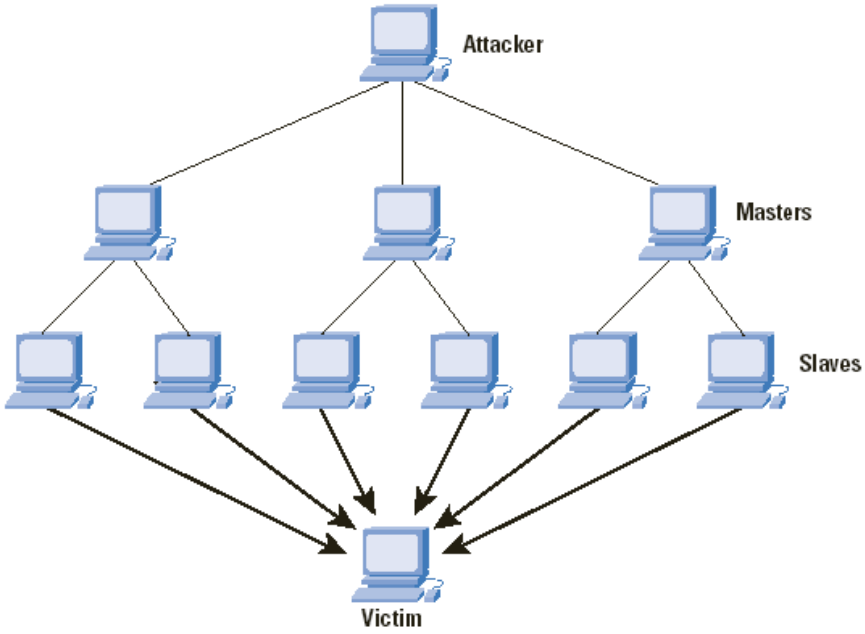

Figura 3 - Configuração do ataque DDoS
Fonte: SISTEMA (c2012)

2.2.5 Detecção de anomalia com assinaturas baseadas em heurísticas

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).

2.2.6 Detecção de anomalia baseada por análise de assinaturas

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).

De acordo com Laufer (2002, p.56), possíveis exemplos de assinaturas são,

> Endereço IP de origem participar da faixa de endereços reservados 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. É preciso verificar o endereço de origem do cabeçalho IP.

> Segmentos TCP com o flag SYN ativado para determinadas portas, por exemplo, portas 21, 22 e 23. Para isso, seria necessária somente uma verificação dos flags do cabeçalho TCP.
> Tentativa de acesso do usuário root a um servidor FTP, no qual ele não é permitido sua entrada. É necessário verificar o cabeçalho dos pacotes TCP certificando-se de que é um tráfego destinado à porta 21 do servidor. Ainda precisa-se analisar se o conteúdo destes pacotes é "USER root".

“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, p.12).

2.2.7 Defeito nos componentes físicos

As principais origens de falhas estão relacionadas 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).

De acordo com Webber (2002), a redundância de *hardware* está baseada na replicação de componentes físicos, onde há redundância de *hardware* passiva, neste tipo, componentes redundantes são utilizados para mascarar falhas, ou seja, corrige erros sem implicar ações do sistema.

Podemos citar como exemplo: cabeamento rompido, oxidação de conectores, roteadores com portas com funcionamento intermitente, entre outros...

2.2.8 Defeito nos *softwares* de redes

Os *softwares* de rede estão sujeitos a apresentar falhas e defeitos, afetando o funcionamento correto da rede.

> Em protocolos de roteamento as falhas se manifestam como rotas interrompidas e ocorrem devido a erros na comunicação ou defeitos no softwares. Ao detectar uma falha na rota, o protocolo de roteamento deve identificar uma nova rota operacional, permitindo assim que o tráfego entre dois nós seja restaurado. (MACEDO et al, 2005, p.15).

O ataque por vírus em rede de computadores pode se espalhar em questões de minutos danificando o funcionamento correto de *softwares* instalados e até de componentes de *hardwares*, ocasionando a interrupção parcial ou total do sistema, ocasionando perdas sociais e financeiras. Muitos dos ataques deixam a rede lenta e instável comprometendo o serviço dos usuários. (MENDES, 2007).

> 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, 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 resultado, os vírus passaram a atingir cada vez mais máquinas, embora com danos menores. (MORIMOTO, 2008, p.23).

2.3 CATEGORIAS DE PROTOCOLOS DE ROTEAMENTO

Atualmente, existem diversos tipos de protocolos de roteamento interno e externo. Os mais utilizados internos são os protocolos RIP e OSPF e externo o BGP. (FOROUZAN, 2012).

O Protocolo de informações sobre Rotas Versão – (RIP – *Router Information Protocol*) surgiu como uma derivação do protocolo de rotas do Sistema de Redes da Xerox (XNS – *Xerox Network System*) fazendo parte da suíte de protocolos TCP/IP.

O protocolo de Caminho Mínimo Aberto Primeiro – (OSTF – *Open Shortest Path First*) é baseado em um algoritmo de estado de ligações, o RIP, por outro lado, baseado em vetor de distância. (GALLO; HANCOCK; 2003).

O protocolo de Roteamento de Borda – (BGP – *Border Gateway Protocol*) é utilizado nos roteadores na propagação de informações e roteamento de pacotes IP aos seus destinos. (McCLURE; SCAMBRAY; KURTZ, 2003).

Conforme Commer (2007), os protocolos de roteamento de *internet* se encaixam em duas categorias: os protocolos de roteadores interno - IGP (*Internal Gateway Protocols*) e os protocolos de roteadores externos – EGP (*External Gateway Protocols*), que serão vistos nos subtópicos a seguir.

2.3.1 Protocolos de roteadores interno

Os roteadores dentro de um sistema autônomo usam um protocolo de roteamento interno para trocar informações de roteamento. Existem diversos IGPs disponíveis; cada sistema autônomo está pronto para escolher seu próprio IGP. Usualmente, um IGP é fácil de instalar e de operar, mas pode limitar o tamanho ou complexidade de roteamento de um sistema autônomo. (COMMER, 2007).

2.3.2 Protocolos de roteamento externo

Um roteador de sistema autônomo usa um protocolo de roteador externo para trocar informações de roteamento com um roteador em outro sistema autônomo. EGPs normalmente são mais complexos de instalar e operar que os IGPs, mais oferecem maior flexibilidade e menos tráfego. Para economizar tráfego um EGP resume a informação de roteamento de um sistema autônomo antes de passá-la para outro sistema autônomo. Mais importante, um EGP implementa restrições nas políticas permitidas (*policy constraints)* que permitem a um administrador de sistema determinar exatamente que informações são liberadas para fora da organização. Na Figura 4 é demonstrado um exemplo de ligação EGP *e* IGP. (COMMER, 2007).

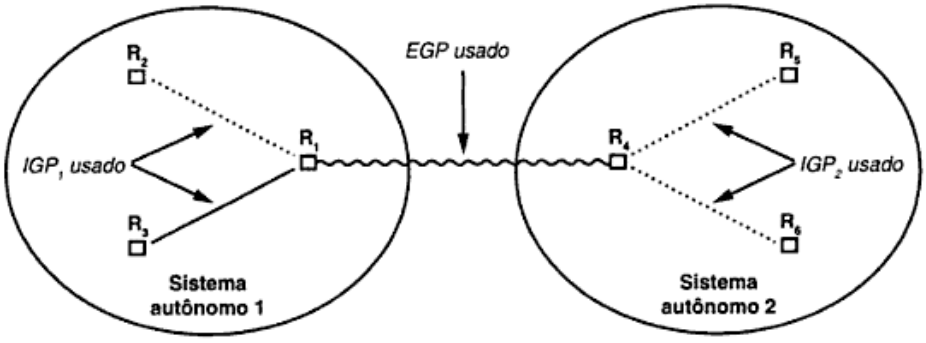

Figura 4 - Arquitetura de roteamento de Internet, cada sistema autônomo escolhe um IGP para usar internamente; um EGP é usado para comunicação entre sistemas autônomos.
Fonte: COMMER (c2007).

2.3.3 Filtragem de pacotes

Através do monitoramento do fluxo da rede é possível realizar a filtragem de pacotes. Recolhem-se os cabeçalhos de IP (*Internet Protocol*) de um determinado conjunto de pacotes para servir como amostragem. (THOTTAN, 2003).

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

2.3.4 Protocolo de gerenciamento SNMP

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

> Embora ele seja poderoso do ponto de vista de gerenciamento de rede, o SNMP introduz uma vulnerabilidade séria quando nenhum filtro de entrada é executado no tráfego da internet. Se for permitido que o tráfego SNMP entre e saia livremente de uma rede, é muito provável que um estranho à rede consiga emitir comandos GETs e SETs para algum dispositivo compatível com o SNMP. Na verdade, as "ferramentas de segurança" gratuitas disponíveis na *internet* simulam os recursos de detecção de rede dos sistemas de gerenciamento de rede e permitem que alguém faça download da base de informações de gerenciamento inteira de todos os dispositivos em uma rede. (SCHETINA; GREEN; CARLSON; 2002, p.112)

2.3.5 Protocolo *Finger*

Segundo Farmer e Venema (1993) o protocolo *finger* é utilizado para obter informações de usuários conectados ao sistema. O volume e a qualidade das informações obtidas causam preocupações aos administradores de rede. Ele contém

informações pessoais como senhas, bem como o último local que o usuário conectou-se na rede.

> O finger raramente é executado no firewall e, portanto, não é uma preocupação muito importante para *sites* protegidos por firewall. Se uma pessoa estiver no interior de seu firewall, provavelmente poderá obter um grande volume das mesmas informações de outras formas. No entanto, se você deixar máquinas expostas externamente, seria sábio desativar ou restrigir o daemon de finger. (CHESWICK; BELOVIN; RUBIN, 2005, p.117).

2.3.6 Protocolo *FTP*

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 protocolo FTP utiliza a porta 21 para conexão de controle em protocolos *IP* e a porta 20 para transferência de arquivos na rede. (TITTEL, 2002).

2.4 TIPOS DE TRANSMISSÕES DE DADOS

As quantidades de tráfego geradas em rede podem ser de três tipos:

2.4.1 *Unicast*

Quando transmitido o arquivo, as cópias dos dados são separadas e enviadas de sua origem para cada computador cliente. Nenhum outro computador na rede precisa processar o tráfego gerado. O *unicast* é bom para ser usado apenas em redes pequenas.

2.4.2 *Broadcast*

Esse tipo de transmissão, quem usa muito esse tipo de transmissão é quem gosta de ataques de *DENIAL OF SERVICE*. Esse tipo de transmissão os dados são enviados apenas uma vez, mas para toda a rede. Esse processo não é muito eficiente,

pois faz a velocidade cair bastante já que todos os computadores irão receber os dados. Mesmo os *hosts* que não fizeram o pedido receberão os dados.

2.4.3 *Multicast*

É uma mistura de *BROADCAST* E *UNICAST*. É enviada apenas uma cópia dos dados e somente os computadores que fizeram o pedido os recebem, assim evitando se causar um tráfego intenso e conseqüentemente um congestionamento na rede. (CARUSO; STEFFEN,1999)

2.5 FORMAS DE ATAQUE

A segurança na rede tem se tornado cada vez mais importante com o constante crescimento da *internet*, o desenvolvimento de ferramentas de *softwares* é cada vez maior. Outro grande problema enfrentado é o problema relacionado a vírus, *pharming, trojans e worms*. (MORIMOTO, 2008). A Figura 5 demonstra os incidentes ocorridos, de janeiro a março de 2012.

Incidentes Reportados ao CERT.br -- Janeiro a Março de 2012

Figura 5 – Incidentes Reportados ao CERT.br
Fonte: INCIDENTES (c2012).

O quadro abaixo descreve os tipos de incidentes ocasionados em rede e suas descrições:

Tipos de incidentes	Descrição
- *worm*:	notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- DoS :	notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- invasão:	um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- *web*:	um caso particular de ataque visando especificamente o comprometimento de servidores *Web* ou desfigurações de páginas na *internet.*
- *scan*:	notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- fraude:	esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
-outros:	notificações de incidentes que não se enquadram nas categorias anteriores.

Figura 6 – Descrição dos Tipos de Incidentes reportados pelo CERT.br – Jan. a Mar. 2012.
Fonte: INCIDENTES (c2012).

Obs.: Vale lembrar que não se deve confundir *scan* com *scam. Scams* (com "m") são quaisquer esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras. Ataques deste tipo são enquadrados na categoria fraude. Nos próximos subtópicos será realizado o estudo de algumas formas de ataque. (INCIDENTES...,c2012)

2.5.1 *Pharming*

De acordo com Thompson (2005, p.98) existem diversas formas de ataque a uma rede, entre eles,

> 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.

2.5.2 *Trojan*

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, 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. Uma vez plantado na máquina da vítima, o trojan fica aguardando um comando ou o momento programado para enviar a informação roubada ao malfeitor que o criou. (TELLES, 2008, p.243).

“O T25 – Trojan by Draco, é um pequeno trojan que entra pela porta 25, vasculha o sistema em busca do ficheiro ‘passwd’ e depois o reenvia pelo email. Ainda contém alguns bugs, mas funciona bem.” (OLIVEIRA, 2003, p.166).

2.5.3 *Sniffer*

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).

2.5.4 Biblioteca pcap

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[9] 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.

Os testes práticos dos tópicos 3.1 e 3.2 foram realizados com a utilização de quatro computadores interligados em rede através de um roteador[10]; onde 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.

Para o teste realizado no tópico 3.3 foi mantido a topologia de rede utilizada sendo substituído o roteador DLink por um *hub*[11] da marca 3COM, modelo SUPERSTACKII, composto por 24 portas *LAN*.

A gerência de uma rede está diretamente vinculada ao controle de atividades e monitoramento dos recursos da rede, obter informações possibilitando um diagnóstico e soluções para estes problemas.

Para o teste prático foi utilizada a seguinte topologia de rede, conforme demonstra a Figura 7:

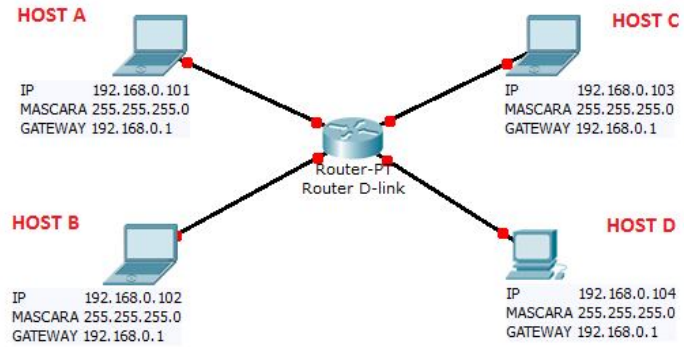

Figura 7 – Topologia de rede utilizada nos testes práticos 3.1 e 3.2.
Fonte: Elaborado pelo autor.

[9] Trata-se de um ambiente de desenvolvimento de aplicações, orientados a objetos, que permite a criação de aplicações para sistemas operacionais.
[10] É um elemento intermediário em uma rede de computadores que permitem a troca de informações entre redes internas e externas.
[11] O *Hub* funciona como a peça central, que recebe os sinais transmitidos pelas estações e os retransmite para todas as demais

Conforme a Figura 7 tem-se os *host(s)*[12]*:* A, B, C e D; o roteador da marca D-Link, modelo DIR-600 com quatro portas *LAN* utilizando barramento de comunicação de 10/100Mbp/s, padrão IEEE 802.11n; IEEE 802.11g e uma porta de *WLAN* para conexões de *internet*. O *host* A foi configurado com o IP 192.168.0.101, máscara de rede classe C 255.255.255.0 e *gateway* 192.168.0.1; O *host* B foi configurado com o IP 192.168.0.102, máscara de rede classe C 255.255.255.0 e *gateway* 192.168.0.1; O *host* C foi configurado com o IP 192.168.0.101, máscara de rede classe C 255.255.255.0 e *gateway* 192.168.0.1; O *host* D foi configurado com o IP 192.168.0.101, máscara de rede classe C 255.255.255.0 e *gateway* 192.168.0.1.

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

As análises foram realizadas e divididas em subtópicos bem como os resultados obtidos.

3.1 ANÁLISE DE ANOMALIA DE REDE BASEADO EM PROTOCOLOS

Nesse tópico foi utilizada a topologia de rede conforme demonstra a Figura 7, através do componente IdIcmpClient[13] da linguagem *Delphi* foi utilizado o componente, sendo disparado eventos de solicitação ao *gateway*[14] da rede 192.168.0.1 a um ciclo de 1 Hertz (1 ciclo por segundo).

Primeiramente, 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.

---

[12] É qualquer máquina ou computador conectado a uma rede, podendo oferecer informações, recursos, serviços e aplicações aos usuários ou outros nós na rede

[13] Componente da linguagem Delphi que disponibiliza procedimentos próprios de rede.

[14] Pode ser traduzido como "portão de entrada". O *gateway* pode ser um PC com duas (ou mais) placas de rede, ou um dispositivo dedicado, utilizado para unir duas redes. Existem vários usos possíveis, desde interligar duas redes que utilizam protocolos diferentes, até compartilhar a conexão com a Internet entre várias estações.

3.2 ANÁLISE DE ANOMALIA DE REDE SOB INFLUÊNCIA DE APLICATIVO *SNIFFER* (FAREJADORES)

Nessa análise utilizou-se a topologia de rede, conforme a Figura 7. Foi utilizada conexão com a *internet*, acessada através do *host* D.

Foi escolhido o *software* Cain[15] 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 roteador estava configurado para rede *internet* trabalhando com IP dinâmico entre 192.168.0.100 ao 192.168.0.110; a conexão externa está sobre um IP fixo com velocidade de 2 *Megabytes* por segundo.

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.

3.3 ANÁLISE DE ANOMALIA DE REDE COM *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.

[15] Aplicativo utilizado por administradores de rede e auditores de segurança para monitorar o tráfego, ver por onde os usuários navegam capturar pacotes de dados para verificar se são suspeitos e testar a robusteza da estrutura de segurança da rede.

Abaixo, a Figura 8 demonstra a topologia de rede local.

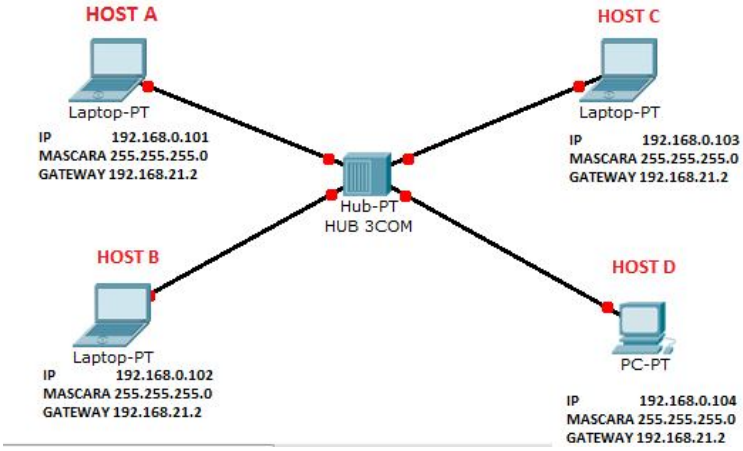

Figura 8 – Topologia de rede utilizada no teste prático 3.3
Fonte: Elaborado pelo autor.

4 RESULTADOS OBTIDOS

4.1 ANÁLISE DE ANOMALIA DE REDE BASEADO EM PROTOCOLOS

Para a análise dos resultados foi utilizado o *software* Colasoft Ping Toll, uma ferramenta de análise de rede que ficou monitorando o IP 192.168.0.1 (*gateway* da rede), sendo que ao ser executado o *software* desenvolvido em linguagem Delphi, denominado de programa ‘T’1 que disparava solicitações ao *gateway* da rede a um ciclo por segundo, notou-se que houve uma alteração progressiva no tempo de resposta, de acordo com a execução sequencial 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) milissegundo atingiu 412 (ms) milissegundos.

As alterações encontradas durante a realizações dos testes foram destacadas em cor vermelha nas telas de resultados.

A Figura 9 demonstra o *software* Colasoft Ping Toll monitorando o *gateway* da rede mostrando estabilidade com tempo de resposta em 1ms.

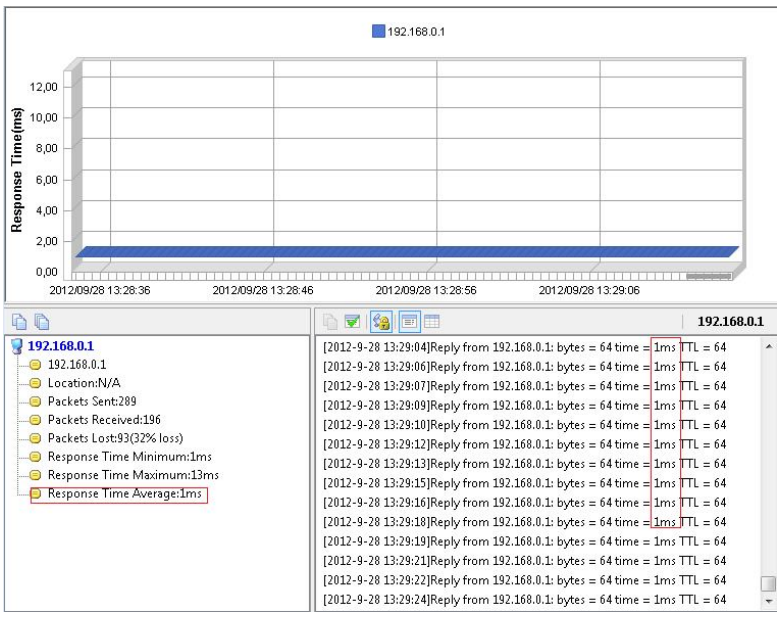

Figura 9 – Resultado obtido sem nenhum computador com o programa T1 em execução.
Fonte: Elaborado pelo autor.

A figura 10 demonstra o resultado com a execução do programa T1 no *host* A, fazendo com que o tempo de resposta fique instável alternando entre 1ms a 2ms.

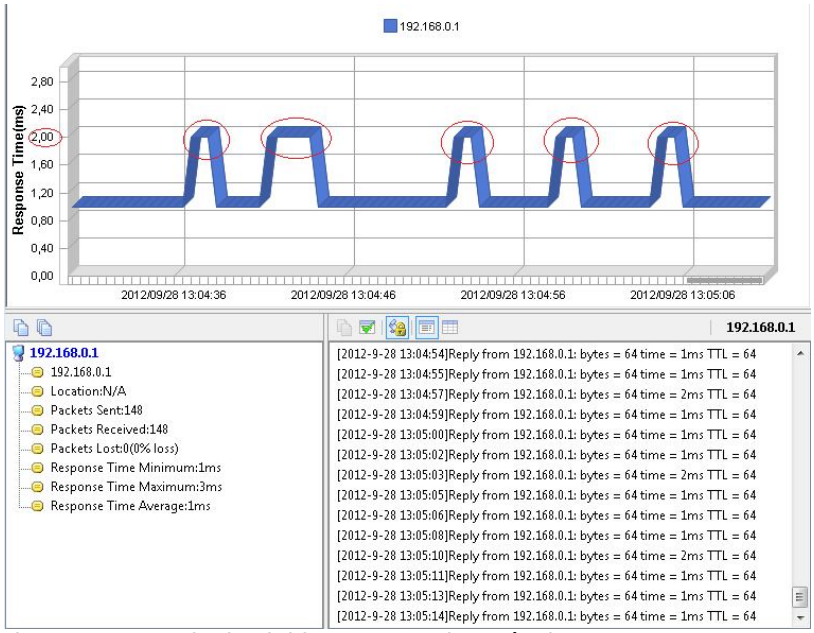

Figura 10 – Resultado obtido com uma das máquinas com o programa T1 em execução.
Fonte: Elaborado pelo autor.

A Figura 11 demonstra o resultado com a execução do programa T1 no *host* A e B, fazendo com que o tempo de resposta fique instável alternando entre 1ms a 2ms por períodos maiores.

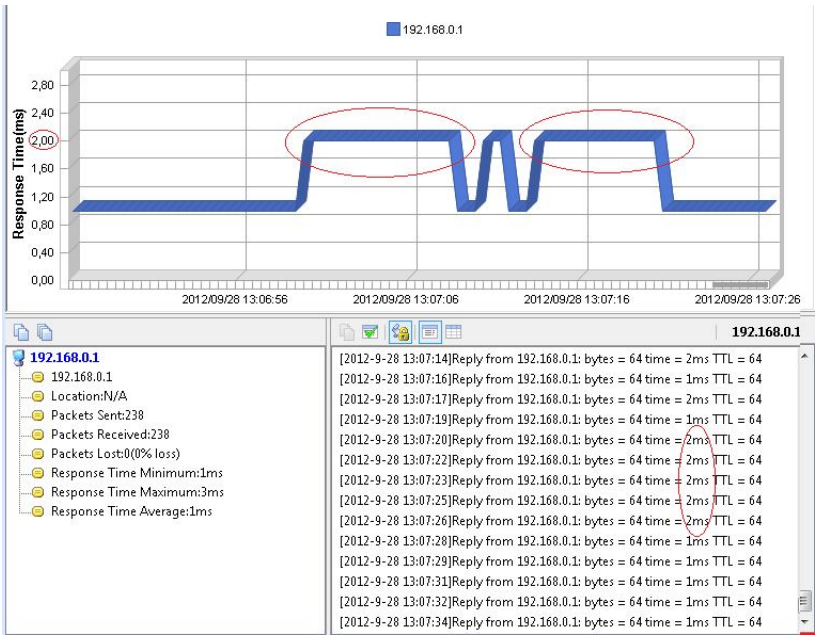

Figura 11 – Resultado obtido com dois computadores com o programa T1 em execução.
Fonte: Elaborado pelo autor.

A Figura 12 demonstra o resultado com a execução do programa T1 nos *host(s)* A, B e C fazendo com que o tempo de resposta fique instável alternando entre 1ms a 3ms.

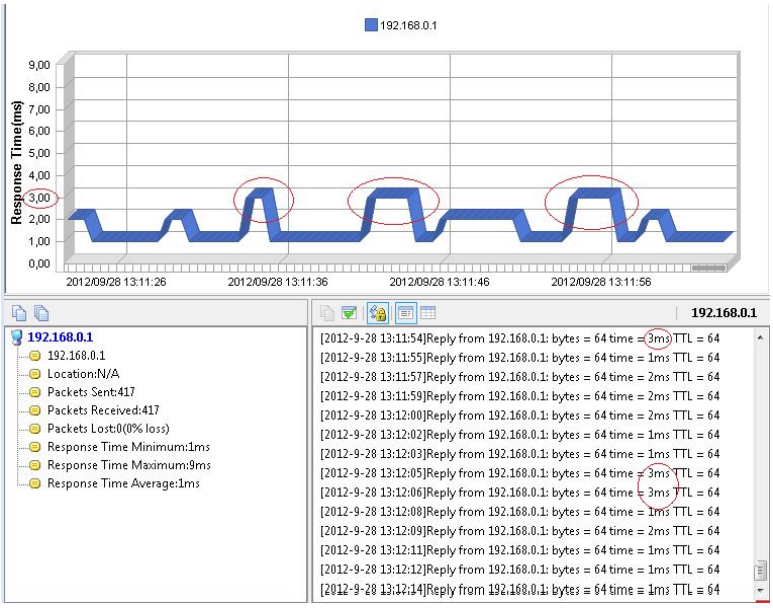

Figura 12 – Resultado obtido com três computadores com o programa T1 em execução.
Fonte: Elaborado pelo autor.

A Figura 13 demonstra o resultado com a execução do programa T1 nos *host(s)* A, B, C e D fazendo com que o tempo de resposta fique instável alternando entre 1ms a 6ms.

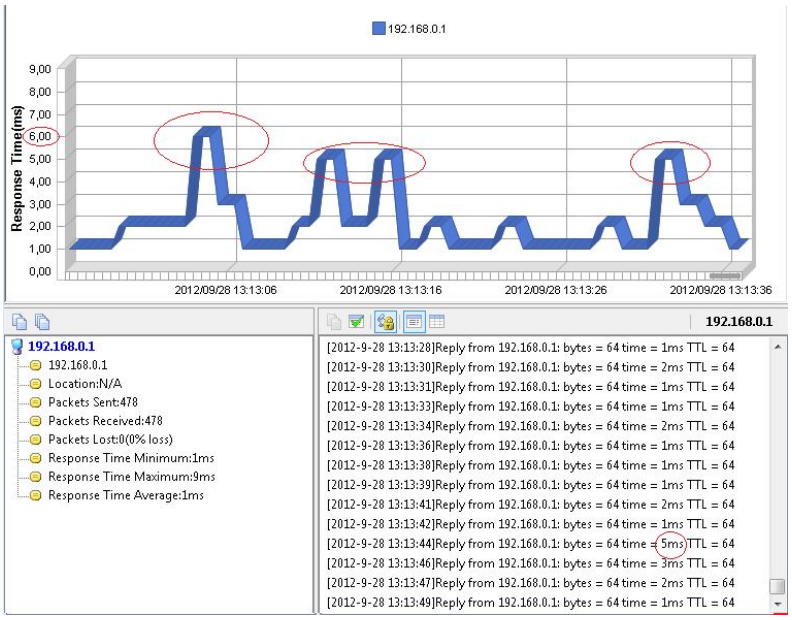

Figura 13 – Resultado obtido com quatro computadores com o programa T1em execução.
Fonte: Elaborado pelo autor.

A Figura 14 demonstra o resultado mais esperado o pico de 412ms alcançado com a execução do programa T1 nos *host(s)* A, B, C e D simultaneamente.

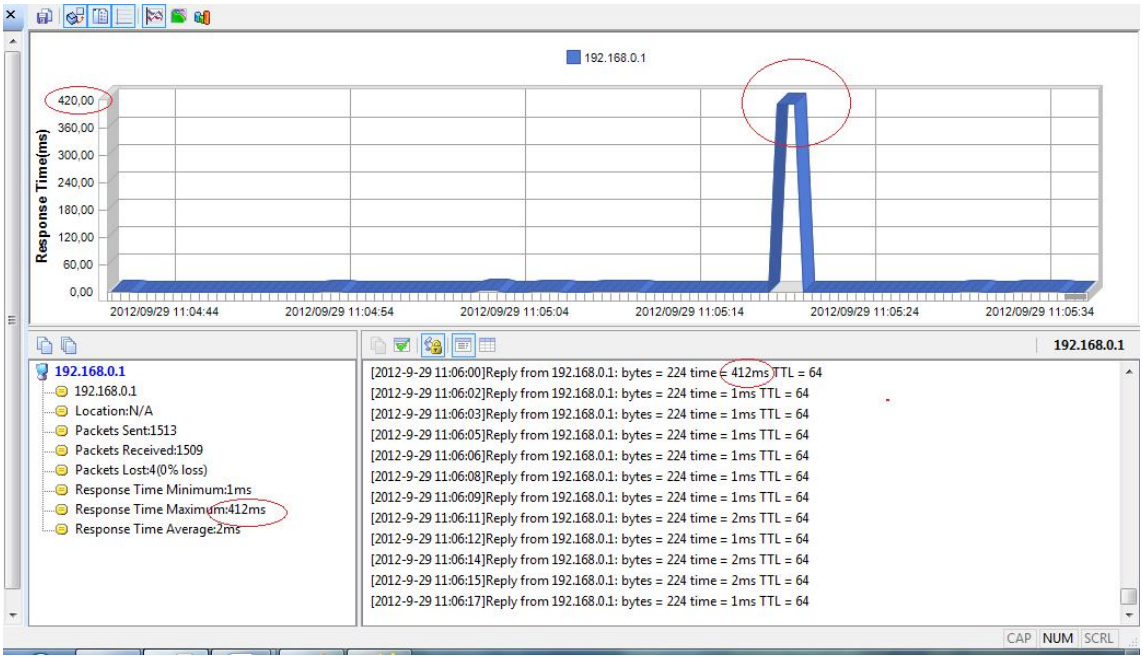

Figura 14 – Resultado obtido com os computadores iniciando o programa simultaneamente.
Fonte: Elaborado pelo autor.

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.

4.2 ANÁLISE DE ANOMALIA DE REDE SOB INFLUÊNCIA DE UM APLICATIVO *SNIFFER* (FAREJADOR)

Para a análise dos resultados foi utilizado o *software* Colasoft Ping Toll, uma ferramenta de análise de rede, quando executado o *software* Cain na rede interna não apresentou alterações tanto na comunicação entre os hosts, 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.

A Figura 15 demonstra o comportamento da rede quando acessada a *internet* sem o *software* Cain sendo executado, a rede mantém um padrão quando acessado um *site* externo na rede.

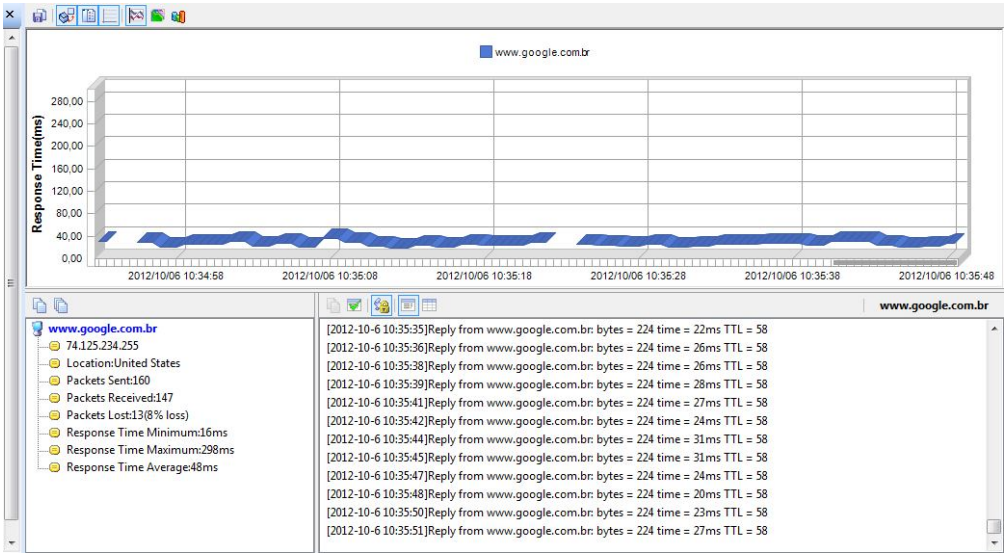

Figura 15 – Análise da rede acessando um *site* externo sem a execução do aplicativo Cain.
Fonte: Elaborado pelo autor.

A Figura 16 demonstra o comportamento da rede quando acessada a *internet* com o *software* Cain sendo executado, a rede mantém um padrão quando acessado um *site* externo na rede.

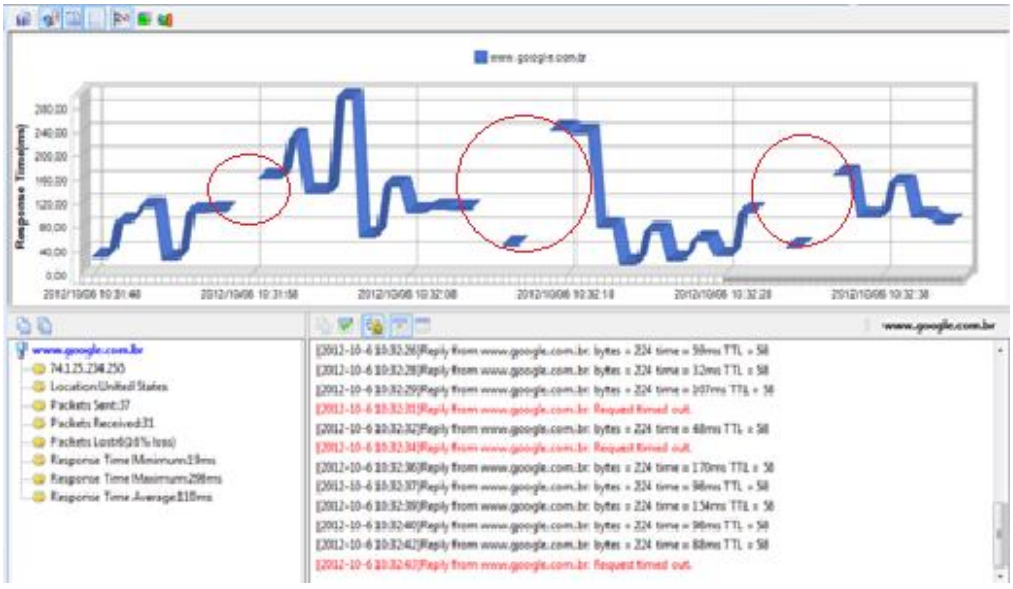

Figura 16 – *Software* Cain em execução.
Fonte: Elaborado pelo autor.

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.

4.3 ANÁLISE DA ANOMALIA DA REDE SOB INFLUÊNCIA DE EQUIPAMENTO DE *HARDWARE* COM DEFEITO

Para a análise 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 *Time to Live* – TTL atingisse o valor máximo de 255, impossibilitado o tráfego de dados. A Figura 18 demonstra a mudança de estado do TTL, a Figura 19 demonstra o *hardware* acusando no seu painel central com o item grifado em vermelho, que estaria ocorrendo conflito de pacotes no tráfego da rede. Foram realizadas novas configurações locais, porém o problema persistiu, sendo resolvido somente com a substituição do *hub.* A Figura 17 demonstra a mensagem de erro apresentada quando ocorria a anomalia na rede.

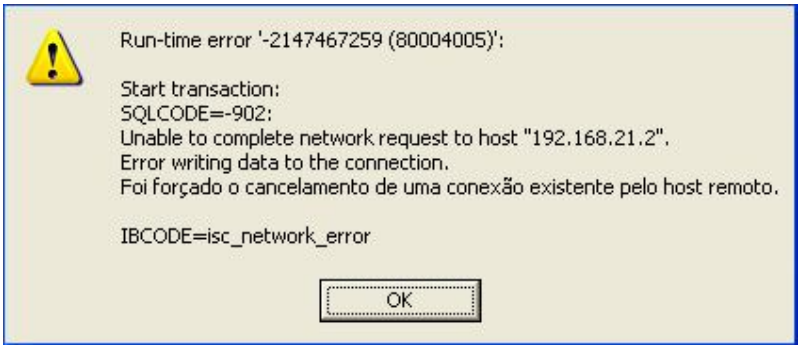

Figura 17 – Mensagem de erro, conexão de rede interrompida.
Fonte: Elaborado pelo autor.

A figura 18 demonstra o momento do defeito na rede através do *software* Colasoft PING Tool, nota-se que *o Time to Live*-TTL da rede chega ao seu valor máximo 255 indisponibilizando o tráfego de pacotes na rede.

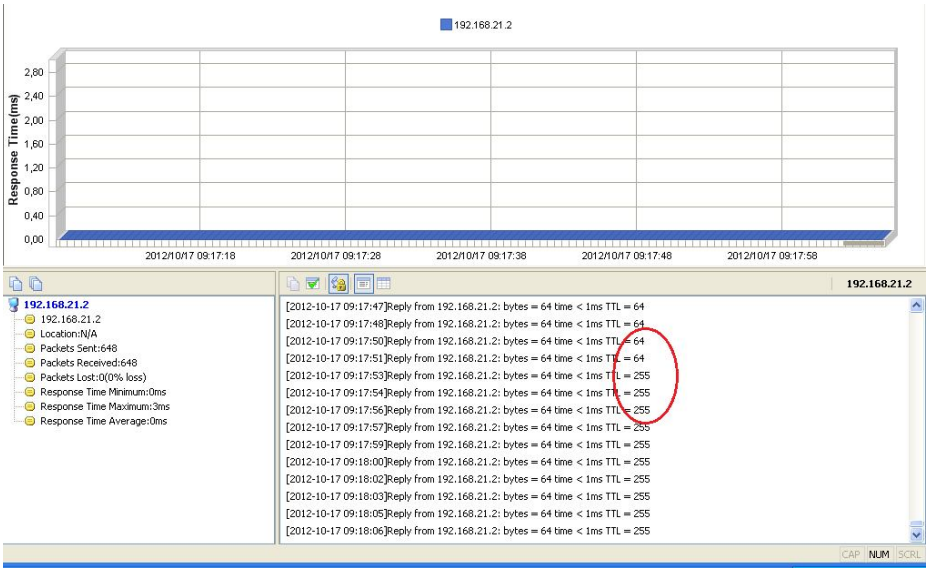

Figura 18 – *Time to Live* – TTL com valor máximo.
Fonte: Elaborado pelo autor.

A Figura 19 ilustra o acusamento de conflito de pacotes, com o led[16] indicador grifado em vermelho, após revisar toda a topologia da rede, o problema foi resolvido com a substituição do equipamento que mantinha a conexão em funcionamento, porém, não permitia o tráfego de dados.

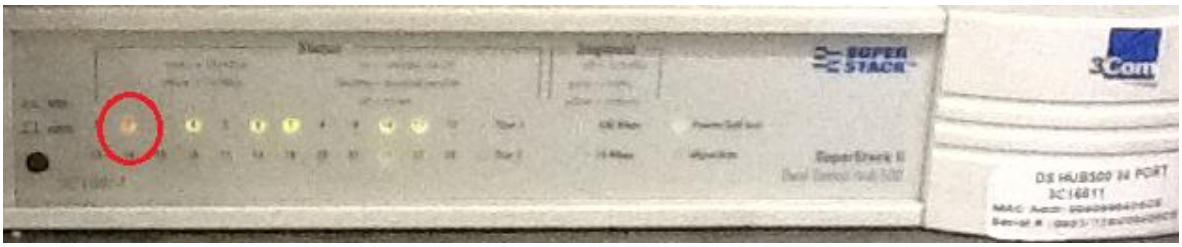

Figura 19 – Led acesso na cor laranja, indicando conflito de pacotes na rede.
Fonte: Elaborado pelo autor.

[16] LED é a sigla em inglês para *Light Emitting Diode*, ou Diodo Emissor de Luz.

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, foi percebido que o estudo alcançou os seus objetivos demonstrando situações que ocorrem no cotidiano em anomalias e formas para detecção.

Conclui-se com esse estudo, que a proposta de adquirir conhecimentos teóricos referentes a anomalias de redes, seus tipos e métodos; e realizar testes experimentais que permitam diferenciação de uma rede normal para situações de anomalia; foi conseguida com êxito com os testes realizados.

Os resultados servem como subsídio para auxiliar profissionais da área da rede de computadores 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, 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 (*farejadores*).*

Em trabalhos futuros a ser desenvolvido, utilizar os parâmetros encontrados nos testes práticos em um *software* funcional e prático, utilizando-se os parâmetros de TTL, monitoração do *gateway* da rede, e a inconsistência da rede com perda de pacotes de dados.

REFERÊNCIAS

ANATEL. **Portal da ANATEL**, 2012. Disponível em :< http://www.anatel.gov.br/Portal/exibirPortalInternet.do>. Acesso em 02Jun 2012.

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.

CARUSO, C. A. A.; STEFFEN, F.D. **Segurança em informática e de informações**. São Paulo: SENAC, 1999.

CHESWIKC, W. R.; BELOVIN, S. V.; RUBIN, A. D. **FIREWALLS E SEGURANÇA NA INTERNET: REPELINDO O HACKER ARDILOSO**. Porto Alegre: Bookman, 2005.

COMMER, D. E. **Redes de Computadores e a Internet**. São Paulo: Bookman, 2007.

CROVELLA, M., LAKHINA, A.; DIOT, C. (2005a**). Mining anomalies using traffic feature distributions**. SIGCOMM.

CROVELLA, M., LAKHINA, A.; DIOT, C. (2005b**). Mining anomalies using traffic feature distributions - technical report**. BUCS-TR.

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

FARMER, D.; VENEMA, W. **"Improving the securityof your site by breaking into it**," 1993. Disponível em:<http://www.cerias.purdue.edu>. Acesso em 03 Jun 2012

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.

GALLO, M. A.; HANCOCK, W. M. **Comunicação entre computadores e tecnologias de rede**. São Paulo: Thomsom, 2003.

GUIMARÃES, A.G.; LINS, R. D.; OLIVEIRA, R. **Segurança com redes privadas virtuais.** Rio de Janeiro: Eletrônica, 2006.

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

IERACE, N.; URRITA, C.;BASSETT, R. 2005. **Intrusion Prevention systems**.Disponível em:< http://www.acm.org/ubiquity/views/v6i19_ierace.html/.>. Acesso em 1 jun 12.

INCIDENTES reportados ao CERT.br. **CERT.br**, c2012. Disponível em :< http://www.cert.br/stats/incidentes/2012-jan-mar/tipos-ataque.html>. Acesso em 1 jun 2012.

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.

LYRA, M.R. **Segurança e Auditória em Sistemas de Informação**. Rio de Janeiro: Ciência Moderna, 2008. 253 p.

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.

MACEDO et al. **Avaliando aspectos de tolerância a falhas em protocolos de roteamento para redes de sensores sem fio.** 2005. Disponível em: < http://www.lbd.dcc.ufmg.br/ colecoes/wtf/2005/002.pdf> . Acesso em 12 maio 12.

McCLURE, S.; SCAMBRAY, J.; KURTZ, G. **HACKERS EXPOSTO**. 4 ed. Rio de Janeiro: Elsevier, 2003.

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.

MENDES, D. R.; **Redes de Computadores**. São Paulo: Novatec, 2007.

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.

PATRIAKIS,C.; MICHALIS,M.; OLGA, Z. **Distributed Denial of Service Attacks**,2012. Disponível em :<http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html>. Acesso em 15 maio 12.

ROUGHAN et al. **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.

SCHETINA, E.; GREEN, K.; CARLSON J**. Aprenda a desenvolver e construir sites seguros**. Rio de Janeiro: Campus, 2002.

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

SISTEMA de Monitoração, Análise e Resposta de segurança da CISCO, **CISCO**, 2012. Disponível em http://www.cisco.com/web/BR/produtos_destaque/MARS_Brochure.pdf. Acesso em 25 maio 2012.

SOBRE o CERT.br. **CERT.br,** c2012. Disponível em :< http://www.cert.br/sobre/>. Acesso em 1 jun 2012.

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.