UNIVERSIDADE SAGRADO CORAÇÃO

EMERSON HENRIQUE MANSANO BARROS

ESTUDOS DE TÉCNICAS DE ATAQUE DoS: TESTES E ANÁLISES DOS ATAQUES

BAURU

2012

EMERSON HENRIQUE MANSANO BARROS

ESTUDOS DE TÉCNICAS DE ATAQUE DoS: TESTES E ANÁLISES DOS ATAQUES

Trabalho de Conclusão de Curso, apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do Título em Bacharel em Ciência da Computação sob orientação do Prof. Esp. Henrique Pachioni Martins.

BAURU

2012

Barros, Emerson Henrique Mansano
B2777e

Estudos de técnicas de ataques DoS: testes e análises dos ataques / Emerson Henrique Mansano Barros -- 2012.
46f. : il.

Orientador: Prof. Esp. Henrique Pachioni Martins.

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

1. Ataque de negação de serviço. 2. Tipos de ataques. 3. Realização de ataque de negação de serviço. I. Martins, Henrique Pachioni. II. Título.

EMERSON HENRIQUE MANSANO BARROS

ESTUDOS DE TÉCNICAS DE ATAQUE DoS: TESTES E ANÁLISES DOS ATAQUES

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do Título em Bacharel em Ciência da Computação sob orientação do Profº Esp. Henrique Pachioni Martins.

BANCA EXAMINADORA

_____

Prof. Esp. Henrique Pachioni Martins
Orientador

_____

Prof. Dr. Elvio Gilberto da Silva
Examinador

_____

Prof. Dr. Kelton Augusto Pontara da Costa
Examinador:

DATA:

AGRADECIMENTOS

Primeiramente agradeço a minha família, por sempre ter me apoiado e acreditarem em mim.

Aos amigos do curso, em especial Guilherme Trevisan e Fernando Schiavon.

A todos os meus professores e meu orientador Prof. Esp. Henrique Martins que me ajudou e incentivou nesta pesquisa.

RESUMO

Hoje em dia, em toda a mídia podemos ver diversas notícias de grandes empresas que tiveram suas *homepages* tiradas temporariamente fora do ar devido ao ataque de negação de serviço. Para tentar se proteger muitas empresas investem em *softwares* como *firewalls* e antivírus, porém até mesmo com essa segurança acabam sofrendo com este tipo de ataque, sendo que esses estão cada vez mais distribuídos e complexos. Um ataque para ser classificado como negação de serviço não pode ocorrer a invasão do *site*, ou seja, a informação contida no *site* não pode ser roubada, modificada ou eliminada, o que ocorre é a recusa de serviço. Este fato ocorre porque o sistema fica ocupado devido a inúmeras e contínuas solicitações ilegítimas, e deixa de atender solicitações legítimas de usuários.

Palavras-chave: Ataque de Negação de Serviço, Tipos de Ataques.

ABSTRACT

Today, throughout the news media can see several large companies that had their website taken down temporarily due to denial of service. To try to protect many companies invest in software like firewalls and antivirus, but even with this safety end up suffering with this type of invasion, this occurs because the attacks are increasingly complex and distributed. An attack to qualify as a denial of service will not occur the invasion site, or the information contained on this site can not be stolen, modified or eliminated, what happens is a denial of service. This occurs because the system is busy due to numerous illegitimate requests and continuous, and fails to meet legitimate demands of users.

Keywords: Denial of Service, Dos, Types of Denial of Service**.**

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

DoS - Ataque Negação de Serviço.
DDoS - Ataque de Negação de Serviço Distribuído
IDS - Sistema de detecção de Intrusos
TCP - Protocolo de Controle de Transmissão
UDP - Protocolo de Diagramas de Usuário
IP - Protocolo de Internet,
MAC - Media access control
IRC - Internet Relay Chat
DNS - Sistema de Nomes de Domínios
FTP - Protocolo de Transferência de Arquivos
HTTP - Hyper Text Transfer Protocol

SUMÁRIO

1 INTRODUÇÃO

Ultimamente vemos na mídia diversas reportagens sobre ataque do tipo negação de serviço, este tipo de ataque vem crescendo respectivamente devido a protestos de grupos *hackers*. Segundo estatísticas do CERT/BR, no ano de 2011, vários ataques de negação de serviço foram registrados diariamente, e envolvem principalmente novos vermes e ferramentas para esta prática. Um ataque para ser classificado como DOS (Denial Of Services) visa deixar inoperante serviços oferecidos pela empresa como servidor de rede, Web ou de *e-mail*. Vale salientar que indisponibilizar, significa retirar totalmente o servidor de operação ou deixá-lo lento ao ponto que o cliente abandone a utilização do serviço, devido ao alto tempo de resposta. Este tipo de ataque não implica na invasão do *site*, ou seja, a informação contida no *site* não pode ser roubada, modificada ou eliminada.

Esta técnica ficou conhecida popularmente a partir dos anos 2000 quando um adolescente canadense foi responsável pelo ataque bem-sucedido a grandes empresas como Amazon, Yahoo, eBay, CNN e outras, causando um prejuízo aproximado de US$ 1,7 bilhões por tirar temporariamente do ar os serviços desses importantes *sites*. (INFO, 2004). A partir de então os tipos de ataque foram se diversificando e evoluindo. Surgindo uma nova forma de ataque que é o DDOS *(Distributed Denial of service)*, que consiste na distribuição deste ataque através da rede.

Com esta nova técnica, este tipo de ataque se torna ainda mais preocupante, pois se trata de um ataque feito por várias máquinas e não necessariamente as máquinas precisam estar na mesma rede ou local. Esse fato dificulta a identificação de onde vêm as requisições (ataques). Pois é incomum uma máquina (cliente) enviar diversas requisições em um curto período de tempo, mas por outro lado, receber muitas requisições, de diversas máquinas diferentes é completamente natural, assim dificultando a identificação real do ataque. Diante deste cenário, esta pesquisa visa demonstrar o ataque de negação de serviço.

2 JUSTIFICATIVA

Atualmente vemos frequentemente na mídia, exemplos claros de ataques do tipo denial of service (negação de serviço), devido ao crescimento desse tipo de ataque, e as graves consequências que ele traz, se justifica a elaboração desta pesquisa.

3 Objetivos

3.1 Geral

Demostrar as técnicas usadas no ataque de negação de serviço, analisando os diferentes tipos de ataques e através disso efetuar o ataque de negação de serviço no ambiente de teste a ser criado.

3.2 Específicos

- Pesquisar em referencias bibliográficas sobre ataque de negação de serviço e negação de serviço distribuído.
- Analisar as técnicas de proteção para este tipo de ataque.
- Realizar o ataque de negação de serviço, monitorando o servidor e gerar gráficos sobre o ataque.
- Analisar tipos de ataque.

4 Fundamentação Teórica

4.1 Segurança da Informação

Com o passar do tempo, cada vez mais vivemos em um mundo competitivo e globalizado, onde a informação possui uma extrema importância, sendo essencial na vida das empresas. Segundo a norma NBR ISO/IEC 27002 (ABNT, 2005) a segurança da informação é definida como: “A proteção da informação de vários tipos de ameaças”, cujo objetivo é garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Vale salientar que a informação está em todos os segmentos de uma empresa, seja nos arquivos encontrados nos computadores, em papéis impressos ou até mesmo em um diálogo entre os funcionários. Assim sendo, a segurança da informação é de extrema importância e essencial para qualquer organização. Segundo a norma ABNT NBR ISO/IEC 27002, 2005 para garantir a segurança da informação, deve se respeitar alguns princípios que são:

Confidencialidade: Deve-se trazer a proteção em toda a informação impedindo a sua divulgação para pessoas que não são autorizadas, e impedindo cópias e distribuição não autorizada. Dessa forma, a informação deve ser confidencial e sua utilização deverá ser feita por pessoas previamente autorizadas.

Integridade: Toda a informação gerada não deve ser modificada sem a devida autorização da(s) pessoa(s) responsável por ela. Devido a isso não deve ser permitido que a informação original sofra nenhum tipo de violação, seja ela escrita, alteração de conteúdo, alteração de *status*, remoção e criação de novas informações.

Autenticidade: Não deve ser permitida a violação da origem da informação. Este controle de autenticidade está ligado ao fato de que a informação que está sendo trafegada seja de fato originada do proprietário a ela relacionada.

Disponibilidade: É garantir que a informação esteja disponível, sem nenhum tipo de modificação sempre que às pessoas autorizadas necessitem. Pode ser chamado também de continuidade do serviço. Através da garantia desses serviços, a segurança de informação poderá trazer benefícios relevantes para a organização.

4.2 Ferramentas para segurança da informação

4.2.1 Sistema de Identificação de Intruso

A definição dada para detecção de intruso segundo (NORTHCUTT, 2002, p.156).

> É um processo de coleta de informações que procura identificar sinais de que um ataque está iniciando ou ocorrendo. (...) a detecção de intrusão da rede permite identificar e reagir a ameaças contra o seu ambiente (...).

Os sistemas de detecção de intrusão são mecanismos de monitoramento que são capazes de perceber a ocorrência de um ataque ou algum comportamento anormal da sua rede, e, através disso, gerar resposta que possuam a função de alertar o administrador da rede.

O funcionamento da ferramenta de identificação de intruso pode variar, alguns modelos podem funcionar analisando e comparando o tráfego da rede (baseado em rede) ou podendo analisar uma determinada máquina (baseado em host) a procura de códigos maliciosos para identificar sinais de que um ataque está se iniciando.

A partir do momento que o IDS tiver evidências que está ocorrendo um ataque, ele irá registar o fato e acionar logo em seguida métodos de alertas, com isso respondendo a atividade suspeita e desconectando um usuário da rede, ou até mesmo reprogramando o *firewall* para que seja bloqueado o tráfego da rede no local suspeito. Na implementação do IDS deve ser definido todos os procedimentos a serem tomados, e quais os responsáveis pela segurança.

Hoje em dia existem diversos tipos de IDS para diferentes plataformas, porém o funcionamento básico de todos é o mesmo, sempre monitorar e analisar todos os pacotes que trafegam na rede, comparando com ataques já conhecidos. Segundo Bernardes (1999), todas as funcionalidades de um sistema de detecção tornam-se de vital importância na medida em que fornecem meios de inferir sobre o conteúdo das conexões permitidas e detectar as que apresentem um comportamento suspeito, ou não condizente com a política de segurança implantada.

4.2.2 Firewalls

A definição de *Firewalls* segundo Zwicky, Cooper e Chapman (2000, p. 104) é “um componente ou um conjunto de componentes que restringe o acesso entre uma rede protegida e a Internet, ou entre outros conjuntos de rede.” E de acordo com a Compy (2006) é um dispositivo constituído pela combinação de *software* e *hardware*, utilizados para dividir e controlar o acesso entre redes de computadores.

Em relação ao *firewall,* NIC (2003) relata que um *firewall* bem configurado é um instrumento de extrema importância para implantar a política de segurança da sua rede. Ele pode reduzir a informação disponível externamente sobre a sua rede ou, em alguns casos, até mesmo barrar ataques a vulnerabilidades ainda não divulgadas publicamente. Porém, por outro lado, *firewalls* não são infalíveis, a simples instalação de um *firewall* não garante que sua rede esteja segura contra invasores. Segundo Cert (2003), um *firewall* não pode ser a sua única linha de defesa, ele é mais um dentre os diversos mecanismos e procedimentos que aumentam a segurança de uma rede.

4.2.3 Tipos de Firewalls

Existem três tipos de *firewalls*, *a* nível de pacote, firewall a nível de pacotes baseado em estados, e o *firewall* a nível de aplicação, cada um possui vantagens e desvantagens um em relação ao outro, é muito comum as empresas utilizarem as duas tecnologias, *firewall* a nível de pacote e á nível de aplicação, em conjunto na sua infraestrutura de segurança, proporcionando um nível maior de segurança. (Junior, 2010).

4.2.4 Firewall a nível de pacotes

Esse tipo de *firewall* analisa e filtra pacotes enviados por redes distintas de comunicação. (INOKOSHI, 2007). Zwicky, Cooper e Chapman (2001, p. 105) definem filtragem de pacotes como,

> A ação de um dispositivo para controlar seletivamente o fluxo de dados de e para uma rede. Os filtros de pacotes deixam passar ou bloqueiam pacotes, em geral enquanto estão roteando (encaminhando) os pacotes de uma rede para outra (com maior frequência de uma rede interna e vice-versa). Para realizar a filtragem de pacotes, deve-se configurar um conjunto de regras que especificam que tipos de pacotes serão permitidos e que tipos deverão ser bloqueados. A filtragem de pacotes pode acontecer em um roteador, em uma ponte ou em um host individual. Às vezes ela é conhecida como triagem.

O *firewall* a nível de pacote analisa as informações contidas no cabeçalho dos pacotes, e de acordo com as regras especificadas pelo administrador, determinam se o pacote será aceito ou descartado. Isso torna o *firewall* transparente ao usuário e ganha um melhor desempenho se comparado ao *firewall* a nível de aplicação. (Junior, 2010).

4.2.5 Firewall a nível de pacotes baseado em estados

De acordo com Junior (2010), o *firewall* á nível de pacotes baseado em estado, também chamado de *stateful packet filter*, é semelhante ao *firewall* a nível de pacotes sendo que ele possui uma funcionalidade a mais. A tomada de decisão se o pacote será aceito ou descartado é feita com base em dois elementos: as Informações do cabeçalho do pacote (assim como o *firewall* a nível de pacotes) e ocorre a comparação de dados em uma tabela de estados que guarda todos os estados das conexões daquele pacote.

4.2.6 Firewall a nível de aplicação

Segundo Junior (2010), um *firewall* a nível de aplicação, também conhecido como servidor proxy, proporciona um nível mais refinado de segurança, ele faz mais do que analisar o cabeçalhos TCP, UDP e IP, ele toma decisões com base em dados da aplicação. Um servidor *proxy* funciona da seguinte maneira: Um cliente, que neste caso pode ser um navegador Web, se conecta ao servidor proxy e realiza uma requisição de um *site* qualquer, o servidor então recebe esta requisição e a encaminha para o servidor web de destino. O servidor Web irá responder a requisição ao servidor proxy que irá repassar os dados para o cliente que realizou a requisição.

Os serviços de *proxy* de um *firewall* são programas aplicativos ou servidores especializados que tomam as solicitações de usuários de serviços da Internet e os encaminham aos serviços reais. (Zwicky; Cooper; Chapman, 2000).

4.3 Ataques

Para entender sobre os diversos tipos de ataques, primeiramente se deve definir o que é um ataque e o que é uma intrusão. Segundo Crothers (2003), um ataque se define em uma tentativa de intrusão, já uma intrusão é um ataque que cumpriu com seu objetivo.

Os ataques na Internet podem ser realizados de diversas formas e com propósitos variados. Para a execução dos ataques o *hacker* utiliza-se de diversas ferramentas para invadir um sistema. Os principais tipos de ataques são.

4.3.1 Spoofing

Segundo Russel (2002), a técnica *Spoofing* é uma técnica de invasão, que visa usar uma máquina para representar o papel de outra na rede. Seu funcionamento ocorre através do uso de pacotes do protocolo TCP/IP. Esta técnica funciona falsificando o remetente dos pacotes de dados que trafegam na rede, para que o receptor deste pacote o enxergue como outra origem. Para este tipo de ataque existem basicamente três técnicas, que são:

- **IP Spoofing:** Técnica utilizada para ocultar a verdadeira origem dos pacotes da rede.

- **DNS Spoofing:** Esta técnica utiliza um servidor DNS falso, com isso este servidor é responsável por executar todas as resoluções de nomes, com isso quando o usuário for fazer uma consulta ao DNS, para saber qual é o endereço IP destino, este servidor responderá um IP falso, fazendo com que cliente pense que ele está na maquina requerida.

- **ARP Spoofing:** Funciona falsificando o endereço MAC da máquina, com isso o atacante se passa por um usuário de outra máquina na rede, tendo total acesso aos computadores.

4.3.2 SYN Flooding

SYN flooding é uma técnica usada para ataque de negação de serviço, o atacante aproveita as vulnerabilidades existentes entre o conceito de requisições de conexão e Internet. O ataque se inicia quando o cliente envia constantemente pacotes de sincronização para cada porta do servidor, utilizando falsos endereços IP, com isso o servidor irá responder cada tentativa feita pelo atacante para estabelecer á conexão, que é chamado de SYN / ACK (sincronização) das portas abertas, e RST (reset) de cada porta fechada.

Para se iniciar o processo normal de uma conexão entre um cliente e um servidor é chamado de aperto de mão em três fases *(three-way handshake)*, ou seja, a partir do momento que o cliente tentar iniciar uma conexão TCP com um servidor, ocorre a transferência de várias mensagens que por padrão são:

O Cliente solicita um pedido de SYN (conexão) ao servidor. Após solicitação de conexão confirmada pelo servido, ele envia uma resposta (SYN-ACK) de volta ao cliente. Quando o Cliente receber á resposta do servidor, responderá com um ACK, estabelecendo a conexão.

No ataque SYN são enviados ao servidor milhares de solicitações de conexão, devido a isso, a fila de solicitações será sobrecarregada, ocupando todos os recursos da máquina, devido a isso nenhuma outra conexão, legítima ou não, será feita, resultando no ataque de negação de serviço. Segundo Cert (1996), o pontencial para um SYN flooding ocorre quando o servidor emitiu uma confirmação de conexão (SYN-ACK) e não recebe de volta do usuário um ACK de resposta. Este procedimento é chamado de *half-open connection*, ou seja, uma metade de conexão é feita.

4.3.3 Worm

De acordo com Symantec (2006), *Worm* é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador, semelhante ao vírus são programas que infectam a maquina, porem não altera arquivos, possui a capacidade de se duplicarem com isso passando de um sistema para outro. O *Worm* pode residir na memória e ser copiado pela rede, utilizando o recurso do Sistema Operacional, invisíveis para o usuário deixando a máquina lenta e aumentando o tráfego na rede.

4.3.4 Botnets

Os *botnets*, são mais conhecido como computadores zumbis, é uma rede de máquinas que são infectadas, o termo Bot é denominado um vírus do tipo *Worm* que possui a capacidade de se comunicar com um atacante. Já o botnets é uma coleção de Bots sob o domínio de um controlador (atacante).

Conforme explica o Cert (2006), o Bot se conecta a um servidor de IRC e entra em um canal determinado. Então, ele aguarda por instruções do invasor, monitorando as mensagens que estão sendo enviadas neste canal.

Quando o invasor consegue a comunicação com o Bot, pode enviar as instruções para que ele realize diversas atividades como:

- Desferir ataques na Internet;

- executar um ataque de negação de serviço;

- furtar dados do computador;

- enviar e-mails e Spam.

É importante destacar também que os vírus podem se reproduzir, já os botnets não. Os Botnets, uma vez executado, eles só fazem lançar a sua ação maliciosa, não possuindo funções de reprodução, devido a esta característica eles não podem ser considerados como vírus.

4.3.5 Vírus

De acordo com CERT (2006) e Mcaffee (2006), um vírus é um código de computador que se anexa a um programa ou arquivo para poder se espalhar entre os computadores, infectando-os à medida que se desloca, quando a vitima irá executar o programa, consequentemente irá executar o vírus, com isso ele é carregado na memória do computador à espera que outros arquivos sejam executados para serem infectados.

Segundo Forristal (2002), quando o vírus é ativado, além de infectar outros arquivos, podem realizar tarefas pré-determinadas que vão desde formatar o disco rígido até baixar a performance da máquina.

4.3.6 Cavalo de Tróia

De acordo com a Symantec (2006), um cavalo de tróia ou *trojan horse* é um programa, que normalmente a vitima recebe, como por exemplo, um cartão virtual, álbum de fotos, etc. Este arquivo recebido executa as funções desejadas, porem possui um código malicioso contido dentro da aplicação.

O cavalo de tróia é diferente de um vírus ou de um *worm* por não infectar outros arquivos, nem propagar cópias de si mesmo automaticamente. De acordo com Symantec (2006) e Cert (2006), o cavalo de tróia possui diversas funções maliciosas como, instalação de *keyloggers*, alteração ou destruição de arquivos, e inclusão de *backdoors*, para permitir que um *hacker* tenha total controle sobre o computador.

4.3.7 Smurf

O Smurf é um tipo de ataque de negação de serviço que funciona devido à existência do endereço *broadcast* na rede, ou seja, ele solicita uma resposta para todas as estações da rede, com isso todos os computadores existentes naquela rede responderão a solicitação e enviarão pacote para o endereço IP da vítima, fazendo com que a conexão da mesma se torne indisponível, ou até mesmo lenta. Para que o ataque ocorra, o endereço da estação conectada tem que ser alterado, com isso emitindo um grande fluxo de requisições, um único pacote enviado na rede pelo atacante pode facilmente ser multiplicado por mais de 100 vezes. Segundo o Cert (1998), os dois componentes principais para que ocorra o ataque Smurf é o uso de falsos pacotes ICMP de *echo request* e da direção de pacotes para endereços de broadcast IP.

4.3.8 DoS (Denial of Service)

Este tipo de ataque tem a finalidade de provocar a negação de serviço. Esta recusa do serviço ocorre porque o sistema fica ocupado devido a inúmeras e contínuas solicitações ilegítimas, e deixa de atender solicitações legítimas de usuários. Segundo Russel (2002.p.38), “O ataque pode se concentrar em dificultar processos, diminuir a capacidade de processamento, destruir arquivos para tornar o recurso inutilizável ou desativar partes do sistema ou processos”.

Os ataques de negação de serviço mais comuns partem do princípio que o cliente tem que efetuar á autorização, para ser aceito na conexão, este processo é chamado de *3-way handshake*, que consiste na troca de três mensagens para iniciar ou finalizar a conexão.

Todo o servidor possui um limite para processar essas requisições de conexão, se um cliente requisitar diversas conexões simultâneas e chegar até o limite máximo suportado pelo servidor, sem enviar a confirmação para acesso, o servidor ficará impossibilitado de receber novas requisições até que o tempo limite das conexões em aberto se esgote (Lopes, 2002).

Um exemplo de ataque de negação de serviço ocorreu em 21 de outubro de 2002, onde nove dos treze computadores responsáveis pelo sistema de resolução de nomes da Internet (DNS) pararam de responder às requisições por aproximadamente uma hora (Wired News Report, 2002).

4.3.9 Como detectar o ataque

Para tentar detectar e evitar o ataque de negação de serviço em uma rede deve se notar algumas irregularidades que estão ocorrendo no exato momento, como:

- **Excesso de tráfego**: A banda da rede irá atingir e exceder o numero máximo de conexões autorizadas, ultrapassando o número máximo de acesso permitido.
- **Tamanho dos pacotes da rede acima do normal**: Pacotes com seu tamanho superior ao normal da rede são considerados suspeitos, pois podem conter mensagens de controle, o conteúdo do pacote do atacante pode estar alterado porém, o endereço final desse pacote é verdadeiro, com isso pode-se localizar o agente que está realizando o ataque se baseando no fluxo de mensagens enviadas.
- **Pacotes TCP e UDP não fazem parte de uma conexão**: Diversos tipos de ataques DDOS utilizam aleatoriamente diferentes protocolos de conexão. Podendo com isso ser detectado com a utilização de um *firewall* que monitore o estado das conexões.
- **Tipos de pacotes devem ser analisados:** Todos os pacotes que tem como destino final as portas de FTP ou HTTP e forem do tipo binário deve ser excluídos imediatamente.

4.3.10 Distributed Denial of Service (DDoS)

O ataque de negação de serviço distribuído possui o mesmo conceito de um ataque básico de negação de serviço, porém a sua única diferença é que a origem do ataque não parte apenas de um computador, mas sim de milhares de outros computadores ligados na rede. Para que ocorra o ataque de negação de serviço distribuído, primeiramente é necessário invadir a quantidade de maquinas desejada, e instalar um *software* malicioso que quando for ativado irá iniciar o ataque simultaneamente de todas as máquinas que foram infectadas em um mesmo alvo (servidor). Na Figura 2, podemos ver o funcionamento de um ataque.

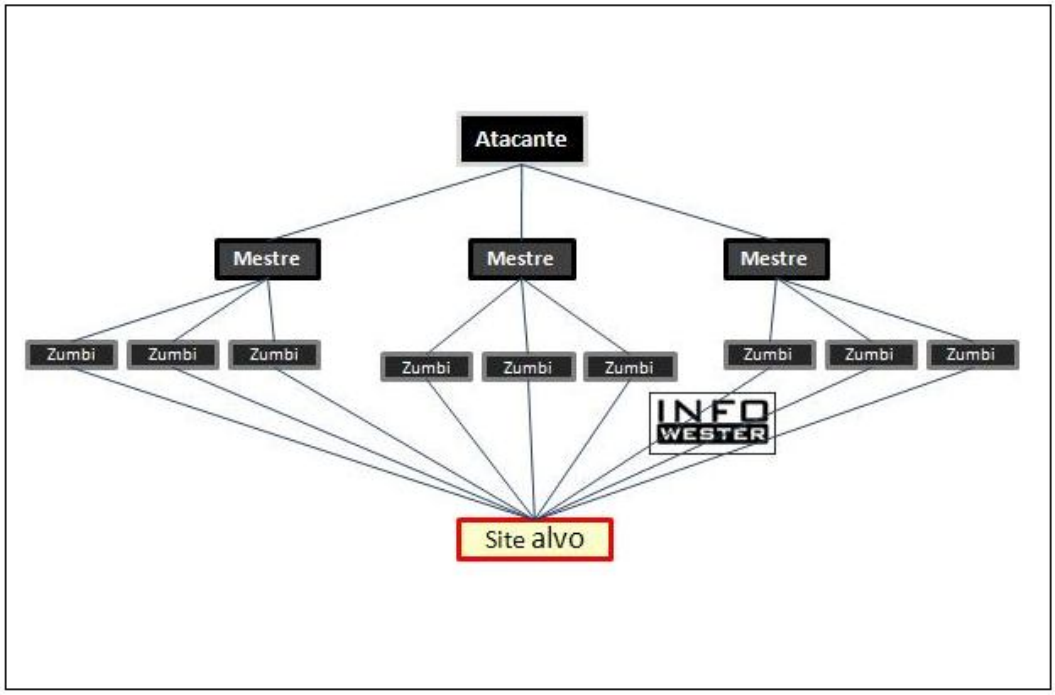

Figura 1- Ataque de Negação de Serviço.

Fonte: Infowester (2012).

4.3.11 Motivação dos ataques

Os ataques virtuais podem ocorrer por diversos fatores, seja positivo ou negativo, um usuário bem-intencionado pode iniciar um ataque com o objetivo de provar que a segurança da empresa possui falhas e vulnerabilidades. Neste caso, pode-se tentar encontrar uma solução para evitar ataques de usuários mal-intencionados e, quando encontrada a solução, ela pode ser amplamente divulgada para acelerar o processo de proteção.

Porém o tipo de ataque mais frequente geralmente é feito por grupos de *hackers*, que usam desta prática para protestar ou para terem reconhecimento na comunidade virtual. Está ocorrendo diversos ataques de negação de serviço pelo grupo *hackers* denominado anônimos, esse grupo conseguiu concretizar ataques de negação de serviço em vários *sites*, com o objetivo de protestar contra a lei SOPA, isso trouxe um reconhecimento do grupo, pois um atacante que consegue forçar um *site* bem conhecido a sair do ar ganha certa visibilidade e é bem considerado pelos colegas, podendo inclusive ser admitido em um determinado grupo de ataque de mais alto nível.

Outro grande motivo do ataque de negação de serviço é o lucro financeiro, uma pessoa com habilidade suficiente para iniciar um ataque pode interromper um determinado servidor por certo período em troca de uma remuneração paga por terceiros.

Com isso uma empresa poderia contratar esse “serviço” e usar este tipo de ataque para prejudicar seus concorrentes. Antes de atacar um determinado alvo, um *hacker* competente toma várias precauções antes de realizar um ataque, ele realiza um estudo do alvo, sempre buscando o máximo de informações possíveis sobre á vitima. Segundo Forristal (2002), existem cinco fases para uma invasão, que são:

- **Criação do mapa de ataque:** Os *hackers* procuram conhecer informações sobre o alvo. Usam ferramentas como o *nslookup (Name Space Lookup)* que fornecem informações iniciais importantes;

- **Elaborar um plano de execução:** O *hacker* tem que ter em mente qual serviço está vulnerável, qual o Sistema Operacional, e qual a vulnerabilidade encontrada.

- **Estabelecer um ponto de entrada:** A vulnerabilidade mais recente é a menos defendida, o atacante na primeira tentativa se baseará nesse princípio.

- **Acesso ininterrupto e adicional:** Quando determinado qual o método de ataque, ele testa a vulnerabilidade em potencial, para saber se o ataque será bem sucedido e se não gerará nenhum alerta;

- **Execução do ataque:** O *hacker* terá um ponto de apoio no ataque através do serviço comprometido, mas seu sucesso dependerá da eficácia do rastreamento após a invasão inicial.

4.4 Incidentes

Segundo o Cert (2011), as notificações de incidentes de segurança virtual cresceram quase três vezes em um ano. O centro de estudos também notou, em 2011, o aumento de 78% nas notificações de ataques nos servidores em comparação com 2010, totalizando 15.491 notificações.

Em relação ao trimestre anterior, houve uma queda de 38% no número de notificações, mas um aumento de 43% em relação ao quarto trimestre de 2010. Conforme mostrado na Figura 2 podemos ver o gráfico de incidentes no ano de 2011.

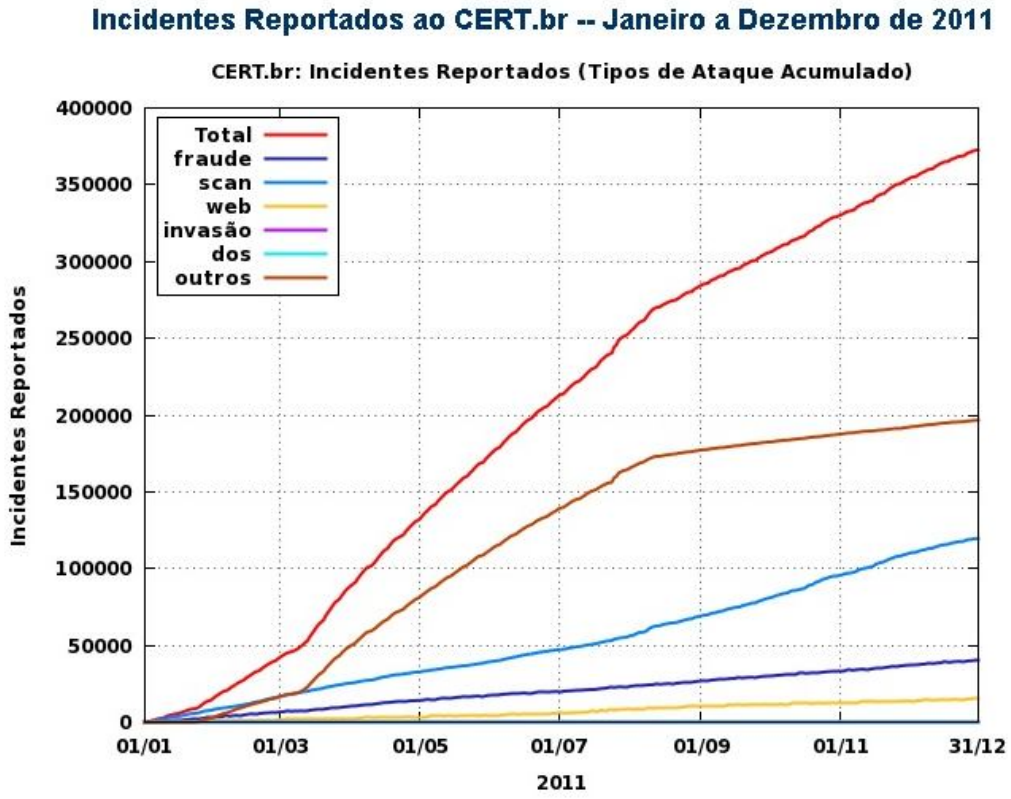

Figura 2 - Incidentes reportados.

Fonte: Cert, (2011)

5 Metodologia

5.1 Ambiente de teste

Para a configuração do ambiente de teste e a criação do servidor de hospedagem, primeiramente foi instalado o sistema operacional Linux Ubuntu 12.04. Este sistema foi escolhido pelo fato de possuir diversos recursos prontos para serem instalados e por ser um sistema operacional livre, não necessitando de grandes *hardwares* para a instalação.

Após a instalação do sistema operacional, foi determinado e configurado um endereço IP fixo para o servidor Web (192.168.0.118). Após esta configuração se iniciou a instalação dos programas necessários para o funcionamento do servidor Web, entre eles o pacote LAMP-SERVER, que é uma ferramenta gratuita para sistema operacional Linux que funciona com a união de PHP, MYSQL e APACHE.

Para derrubar uma página em um servidor Web, é necessário primeiramente que está pagina Web esteja disponível para acesso. Para isso foi desenvolvida uma pagina web utilizando a ferramenta Wordpress, por ser uma ferramenta de fácil uso, com diversos recursos e vasta documentação disponíveis na Internet. A página de exemplo criada foi acessada por dois clientes, ficando disponível apenas para acesso a rede interna, ou seja, uma pagina de Intranet, servindo apenas como alvo para que ocorra a demonstração do ataque de negação de serviço.

Antes de realizar o ataque foi preciso configurar uma ferramenta de monitoramento para poder coletar os dados do ataque. A ferramenta de monitoramento de servidor escolhida foi o Zabbix, que é um *software* livre que possui todas as informações necessárias em gráficos através de uma *interface* Web. O Zabbix irá monitorar os dados físicos do servidor, ou seja, o uso do *hardware* do servidor, como o uso de memória, o uso do disco rígido, e o uso do processador. Além disso, irá monitorar e analisar os dados e informações que estão trafegando pela placa de rede.

O *hardware* utilizado para criação do servidor, classificado como “ubuntu_server” foi um Notebook da Amazom PC, com processador Core Duo de 2ghz, 1Gb de memória RAM e 160Gb de HD.

O computador classificado como “VM_atacante”, é uma máquina virtual, que segundo Laureano (2006), uma máquina virtual (Virtual Machine – VM) é uma duplicata eficiente e isolada de uma máquina real, realizando uma cópia isolada de um sistema físico, a qual é totalmente protegida.

O *software* utilizado para criar a máquina virtual foi o Vmware. Já o sistema operacional escolhido para ser instalado foi o Linux Ubuntu 12.04, junto com a ferramenta que usada no ataque (T50). Toda a estrutura desenvolvida está ilustrada na figura 3.

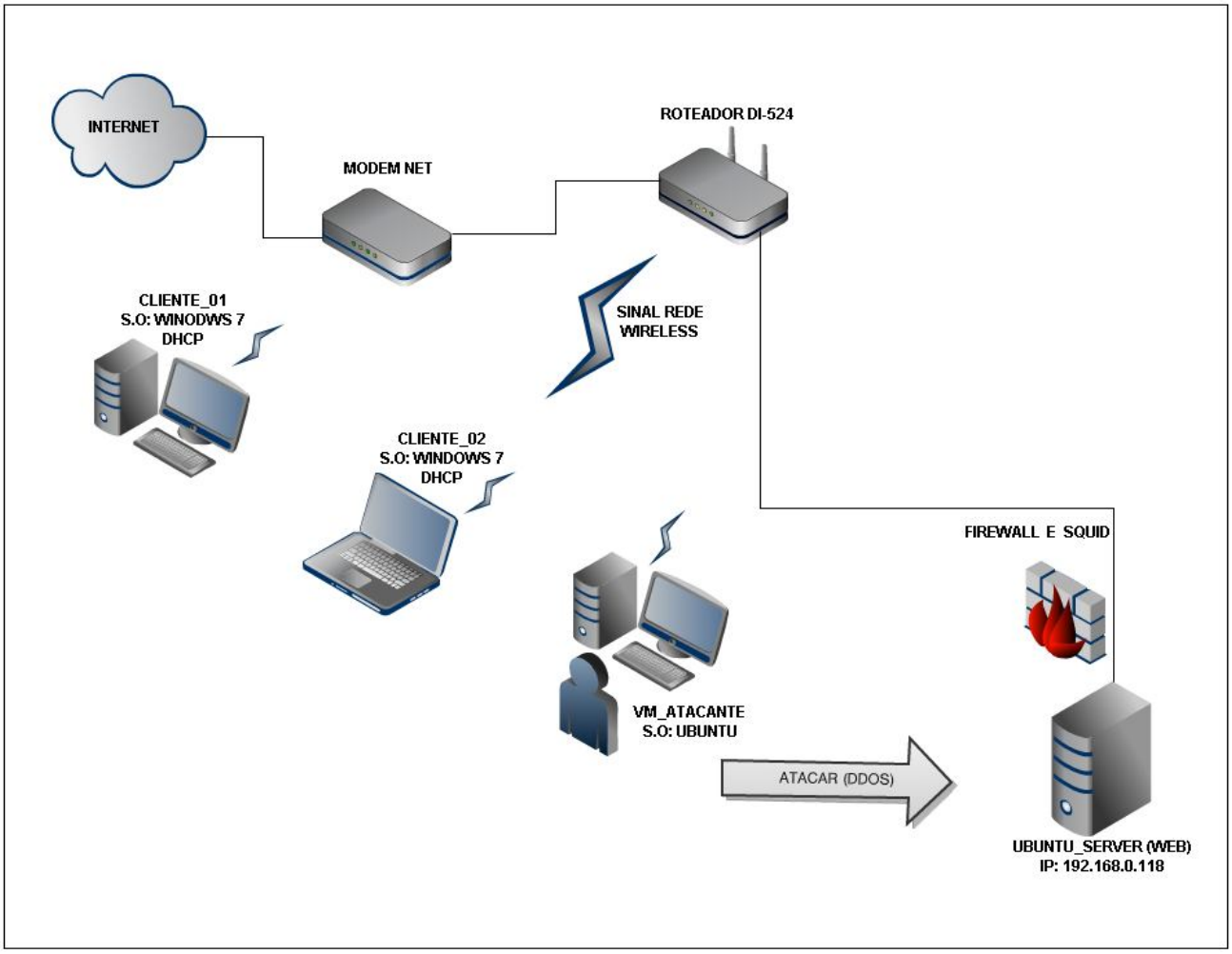

Figura 3 - Ambiente de teste criado.

5.2 Execução do Ataque

Para realizar o ataque de negação de serviço da forma convencional seria impossível, pois não iria conseguir atingir o número necessário de computadores para acessar simultaneamente o servidor e com isso faze-lo negar o serviço.

Devido a esse fato foram pesquisada ferramentas para a realização deste ataque. A ferramenta com maior poder de ataque e própria para efetuar testes de negação de serviço é a ferramenta conhecida como T50. Esta ferramenta foi desenvolvida pelo brasileiro Nelson Brito. Ela é capaz de realizar ataques DoS e DDoS usando o conceito de "*stress testing*". Atualmente o T50 está na versão 5.3, disponível apenas para o sistema operacional Linux, sendo uma ferramenta gratuita e de código aberto com a capacidade de emitir as seguintes requisições do servidor:

- Mais de 1.000.000 pacotes por segundo de SYN Flood (+50% do uplink da rede) em uma rede 1000BASE-T (Gigabit Ethernet).
- Mais de 120.000 pacotes por segundo de SYN Flood (+60% do uplink da rede) em uma rede 100BASE-TX (Fast Ethernet).

A ferramenta T50, está integrada na lista de *Backtrack* que é uma distribuição do Linux, que tem como objetivo a distribuição de diversos instrumentos centrados apenas para a segurança da rede. Segundo (remote-exploit) a distribuição de *Backtrack* possui mais de 300 ferramentas diferentes e tem como foco principal ajudar a penetração em redes seguras, podendo permitir a realização de testes e analisar o nível de segurança da própria empresa. A interação da ferramental T50 na distribuição Backtrack prova o seu real poder e seu verdadeiro funcionamento.

O ataque realizado foi exclusivamente na porta 80 do servidor, pois esta porta é o principal protocolo da Internet (http), e está reservada para acesso as páginas de servidor Web. O ataque foi do tipo SYN flood ou ataque SYN, que é uma forma de ataque de negação de serviço. É um dos tipos mais comuns de DoS e também um dos mais efetivos, pois consiste em enviar um grande volume de pacotes SYN, até que o seu alvo (servidor) seja inundado por requisições, não conseguindo responder todas ao mesmo tempo e com isso negando serviço. Para realizar o ataque, utilizando a ferramenta T50, foi usado o seguinte comando:

./t50 192.168.0.118 --flood -S --turbo --dport 80

Sendo que:

./t50 - Parâmetro inicial da ferramenta T50 para execução do ataque.

192.168.0.118 - È o endereço de IP fixo que foi determinado no servidor.

--flood - Seleciona o tipo do ataque que será realizado (SYN flood).

-S - Parâmetro usado para o ataque do tipo SYN flood.

--turbo - Objetivo de acelerar os pacotes enviados para o servidor.

-- dport 80 - Ataque redirecionado exclusivamente na porta 80.

Foram realizados três ataques, com duração de aproximadamente cinco minutos, e consequentemente três coletas de dados, com o objetivo de verificar e comparar a mudança dos gráficos durante o ataque.

5.3 Resultados

Para gerar os resultados, foram realizados ao todo três ataques de negação de serviço, em três datas e horários diferentes. Antes da realização do primeiro ataque foram coletados os gráficos do servidor Web funcionando de forma convencional, ou seja, sem a presença de atacantes. Esta coleta inicial de dados ocorreu no dia 05/11/2012 podendo ser visualizada através dos gráficos de *hardware*, como o processamento do CPU (Figura B), uso de memória do sistema (Figura F), utilização de arquivos de paginação (Figura D), e o estado do software de monitoramento Zabbix (Figura E).

Nesta coleta inicial dos gráficos, mostra que o tráfego de entrada e saída na interface de rede Eth0 (Figura A e C) estão estáveis, ocorrendo a navegação normal dos pacotes de rede pelo dispositivo Eth0.

Antes de iniciar o primeiro ataque de negação de serviço, o servidor web foi reiniciado e consequentemente todo o processo da máquina foi zerado, para visualizar o verdadeiro impacto do ataque. Como descrito abaixo na figura 4 está sendo mostrado o gráfico de entrada e saída de dados da Eth0 antes do período de ataque.

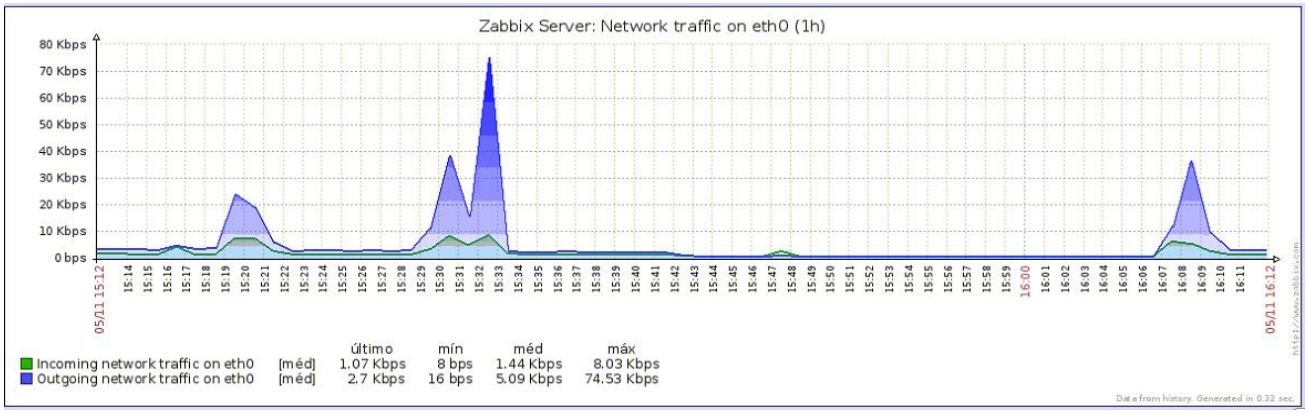

Figura 4 - Gráfico Eth0 antes do ataque Ddos.

O primeiro ataque de negação de serviço teve inicio dia 05/11/2012 as 19h:20m. Após esse horário, visualizando os gráficos de entrada e saída da *interface* de rede durante o ataque, podemos perceber claramente a grande mudança que ocorreu no trafego de dados da interface de rede Eth0. O tráfego de dados na *interface* de rede passou a ser alto, chegando ao ponto de ultrapassar a quantidade de barramento de 120kbps de entrada de dados e mais de 100kps de saída de dados na interface de rede, como mostrado na Figura 5.

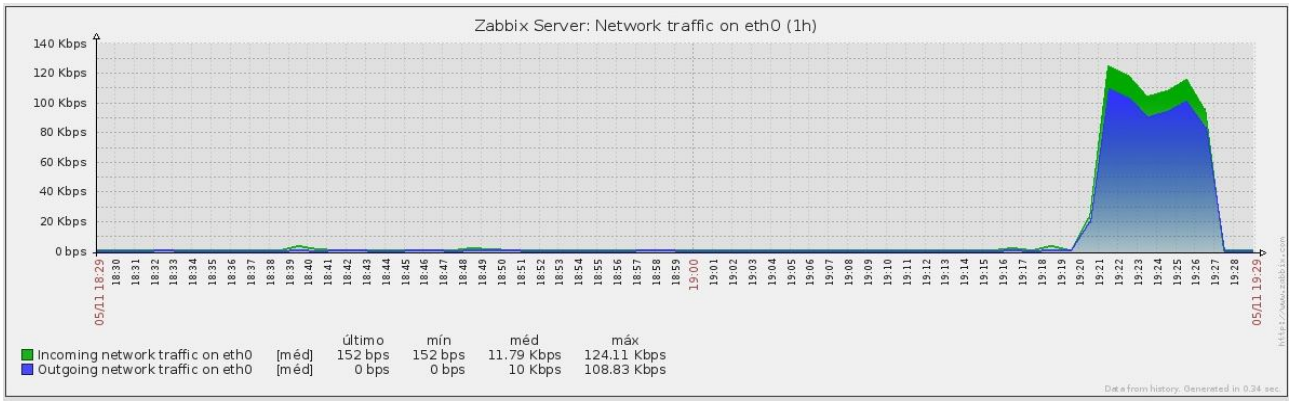

Figura 5 - Gráfico Eth0 durante o ataque.

Para comparar os dados foram realizados três ataques. Todos os ataques foram realizados com êxito, atingindo o objetivo que era deixar a página Web off-line, através da negação de serviço.

Quando o ataque estava em andamento o servidor Web ficou instável e com leves travamentos, e toda a conexão da Internet ficou fora do ar em todos os equipamentos descritos no ambiente de teste criado.

As grandes mudanças ocorridas nos gráficos da Eth0, durante o segundo e terceiro ataque pode ser visualizada nos apêndices.

Para analisar e visualizar melhor os dados da *interface* de rede Eth0 foi criado uma tabela comparativa de tráfego de entrada e saída de dados do dispositivo, podendo ser visualizada abaixo.

Ataque	**Data**	**Dados de entrada Eth0(Kbps)**	**Dados de saída Eth0(Kbps)**	**Duração (Minutos)**
01	05/11/2012	124.11	108.83	8
02	06/11/2012	41.9	76.66	7
03	10/11/2012	47.84	39.23	7

Tabela 6 - Comparativa dos Ataque

Na tabela acima é mostrado os três ataques, junto com seu tempo de duração e a quantidade de acessos que teve no dispositivo de rede Eth0. O primeiro ataque foi o mais longo e o que obteve mais acesso a *interface* de rede do servidor.

5.4 Defesa do ataque de Negação de Serviço

Através dessa pesquisa pode-se perceber que não existe como se defender totalmente do ataque de negação de serviço, devido ao seu poder de ataque e sua arquitetura. Pelo fato de não ter uma solução definitiva contra ataques DDoS, existem várias maneiras de se minimizar os dados causados pelo ataque. O melhor modo de proteção é a elaboração de uma politica de segurança funcional, e com frequentes atualizações. Segundo o RFC 2196 (The Site Security Handbook), “uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos usuários dos recursos de uma organização”. Em conjunto com a politica de segurança tem que estabelecer um plano de contingência que é a melhor solução contra ataques do tipo força-bruta que consomem todos os recursos da maquina e da rede. Segundo Amaro (2004), o plano de contingência deve ser parte da política de segurança de uma organização complementando assim o seu planejamento estratégico. A defesa para o ataque de negação de serviço consiste na junção de todas as ferramentas de segurança citadas na pesquisa, como ferramenta de identificação de intruso, *Firewall, Proxy*, o uso de monitoramento (Zabbix), junto com politica de segurança e plano de contingencia atualizados.

5.5 Perspectivas Futuras

Através dessa pesquisa pode-se perceber a força que o ataque de negação de serviço possui. Apesar da extrema necessidade de haver uma solução definitiva para sanar os ataques de negação de serviço, ainda é muito difícil encontrar uma solução específica e concreta para esse tipo de ataque.

A defesa consiste na junção de inúmeras ferramentas de seguranças, porém, isto não impede totalmente que o ataque ocorra. Torna-se necessário que haja mais pesquisas sobre ataques Dos e DDos, formando com isso mais informações e melhores forma de defesa, buscando acabar totalmente com os ataques.

6 Considerações Finais

O ataque de negação de serviço é uma grande ameaça para empresas e sociedade, pois sua execução ocorre pela rede de computadores. Hoje em dia existem milhares de ferramentas disponíveis na Internet para que qualquer pessoa possa realizar um ataque, como demonstrado com a ferramenta T50.

A possibilidade de acabar com ataque de negação de serviço é impossível, pois se qualquer equipamento estiver conectado à rede, sempre terá a possibilidade de receber dados em quantidade acima do limite suportado.

Os recentes ataques, ocorridos esse ano pelo grupo Hacker Anonymus nos mostra que não é apenas as empresas que são atingidas, mas toda a infraestrutura da Internet está vulnerável. Devido a isso é de extrema importância a iniciação de novos estudos sobre os ataques DDoS, para poder garantir mais segurança e estabilidade na rede.

7 Apêndices

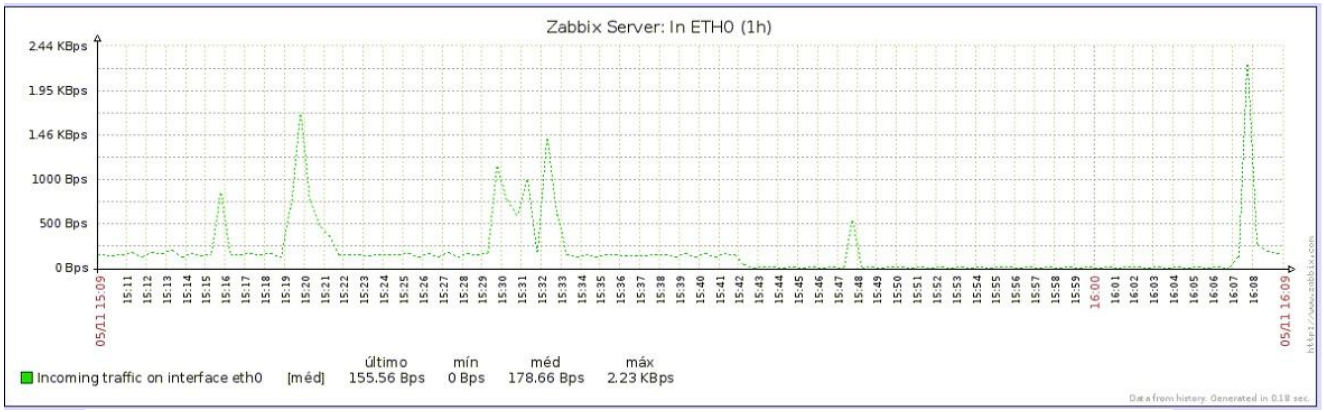

Figura A – Tráfego de entrada na interface Eth0

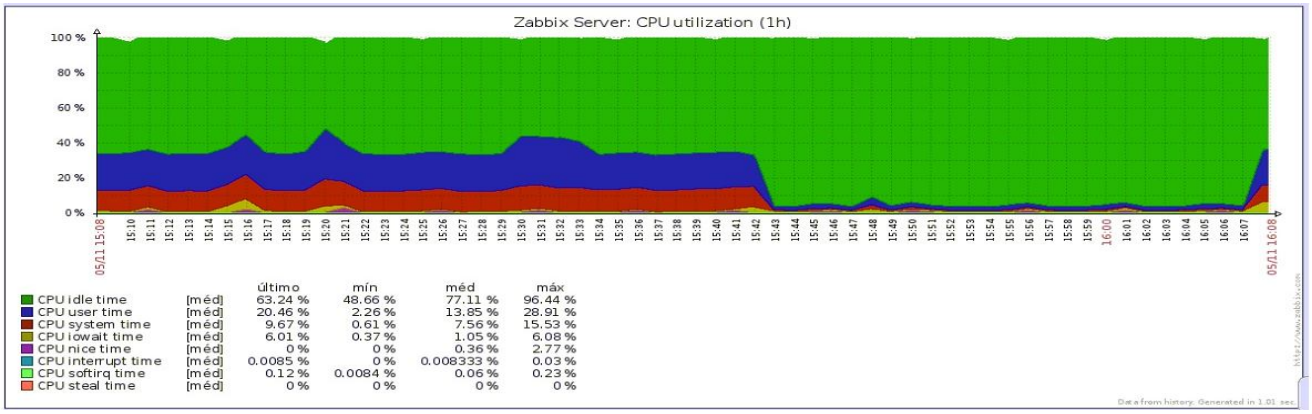

Figura B – Utilização do processador.

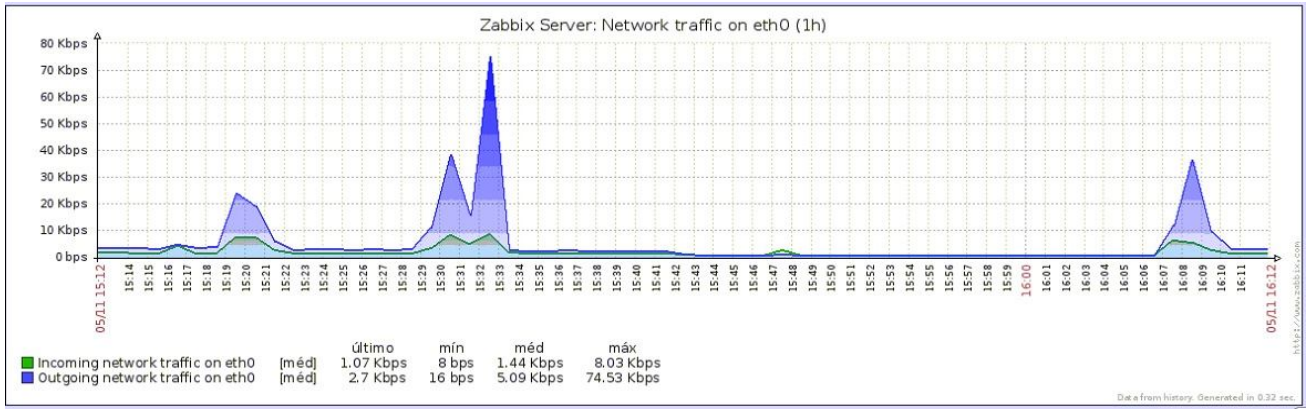

Figura C – Tráfego de entrada e saída na interface Eth0.

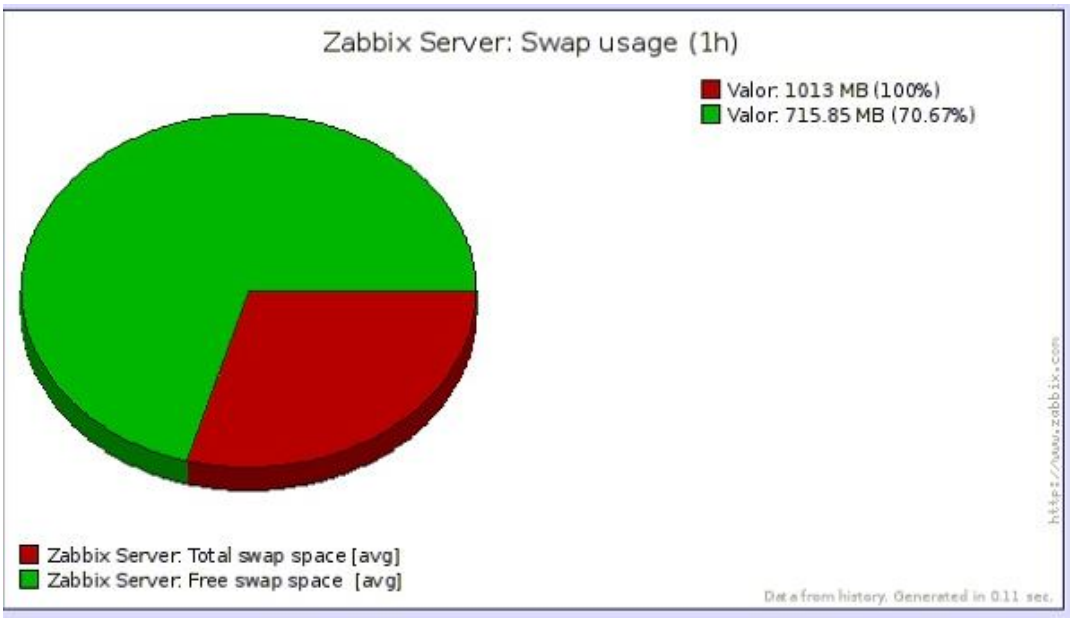

Figura D – Uso da utilização Swap.

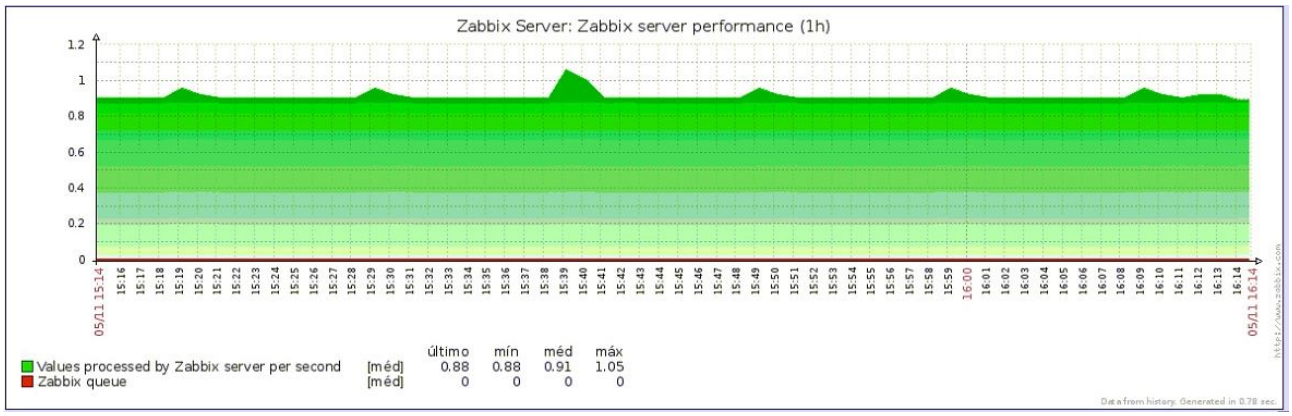

Figura E – Desempenho do Zabbix.

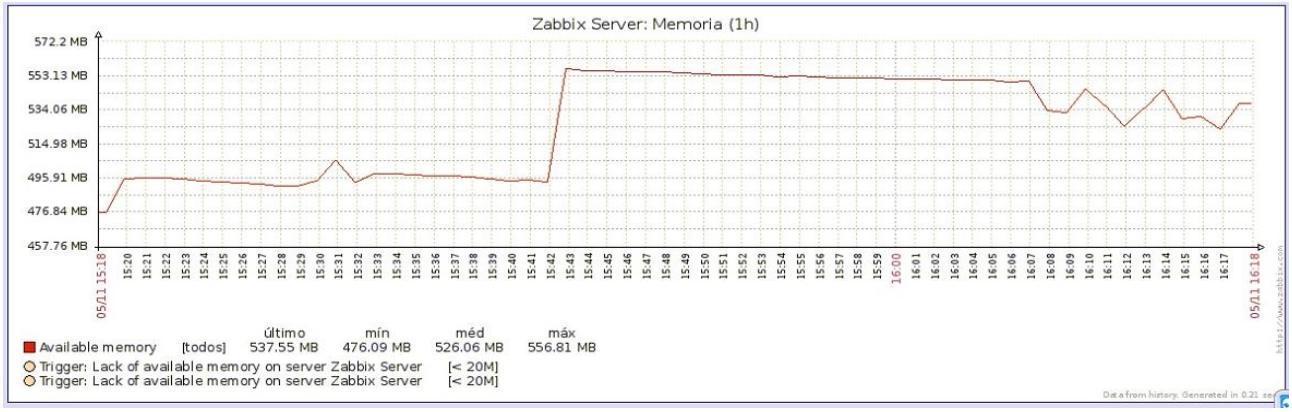

Figura F – Uso de memoria do sistema.

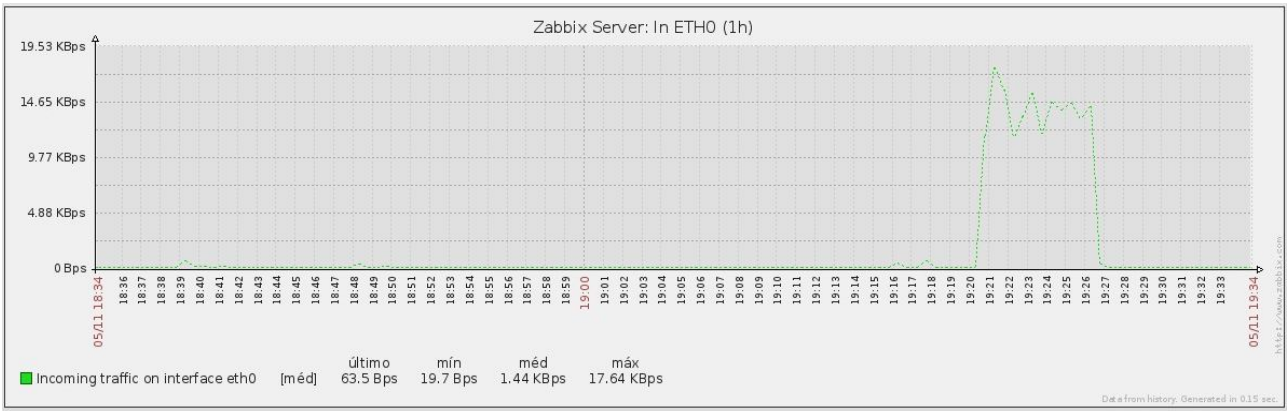

Figura G – Tráfego de entrada na interface Eth0 (Primeiro ataque).

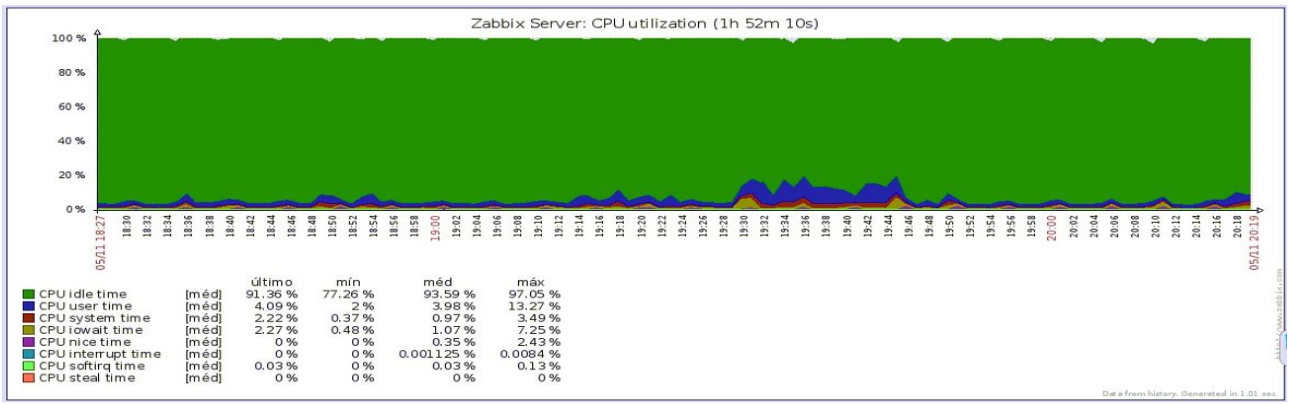

Figura H – Utilização do processador (Primeiro ataque).

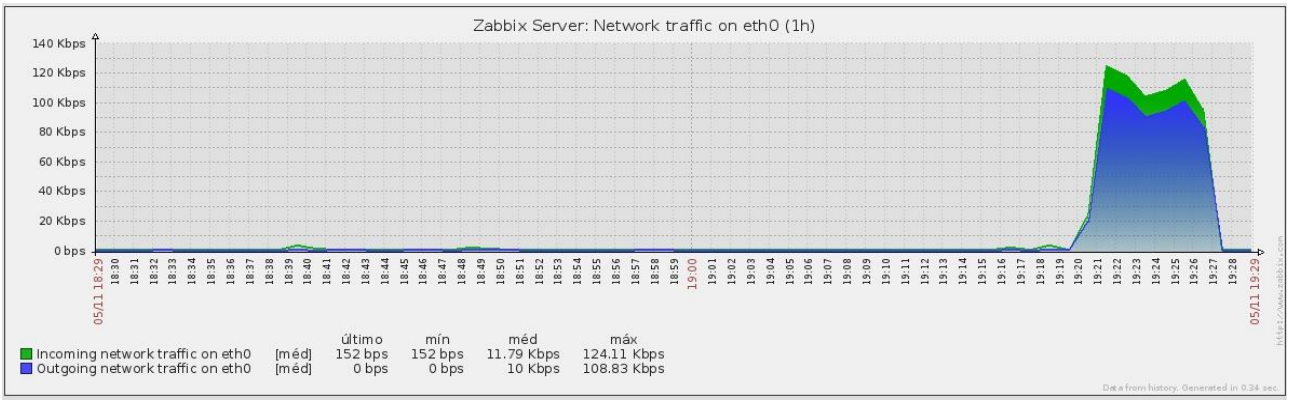

Figura I – Tráfego de entrada e saída na interface Eth0 (Primeiro ataque).

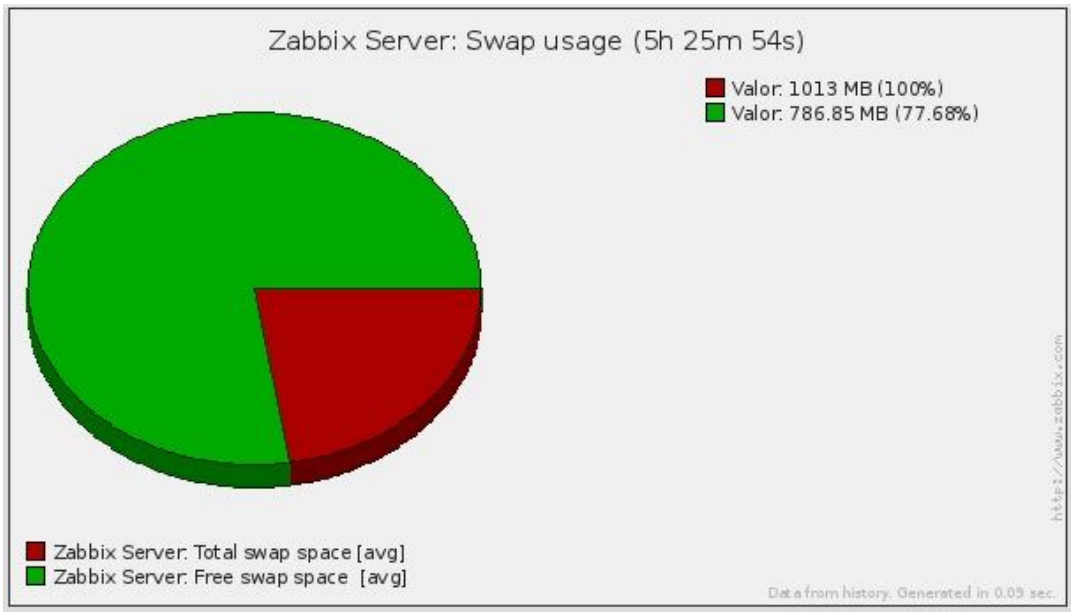

Figura J – Uso da utilização Swap (Primeiro ataque).

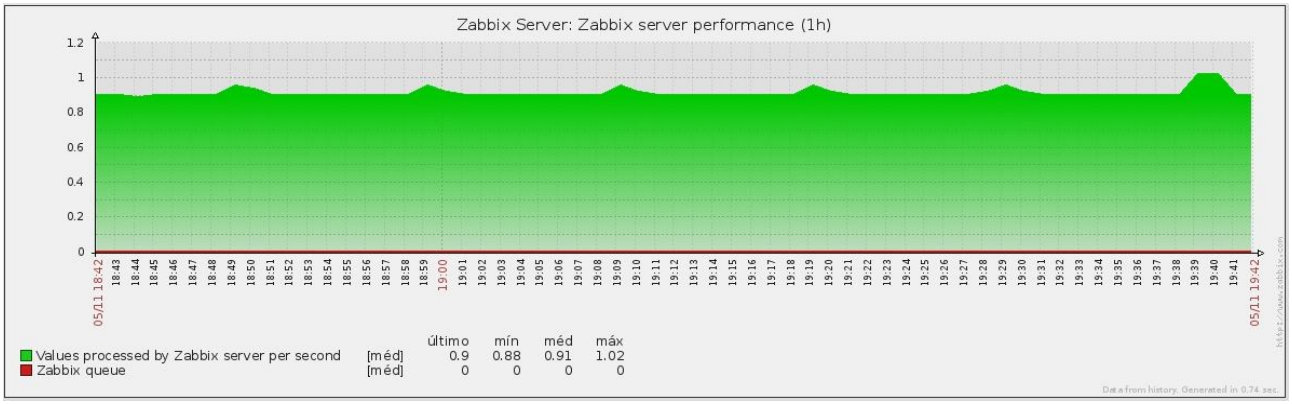

Figura K – Desempenho do Zabbix (Primeiro ataque).

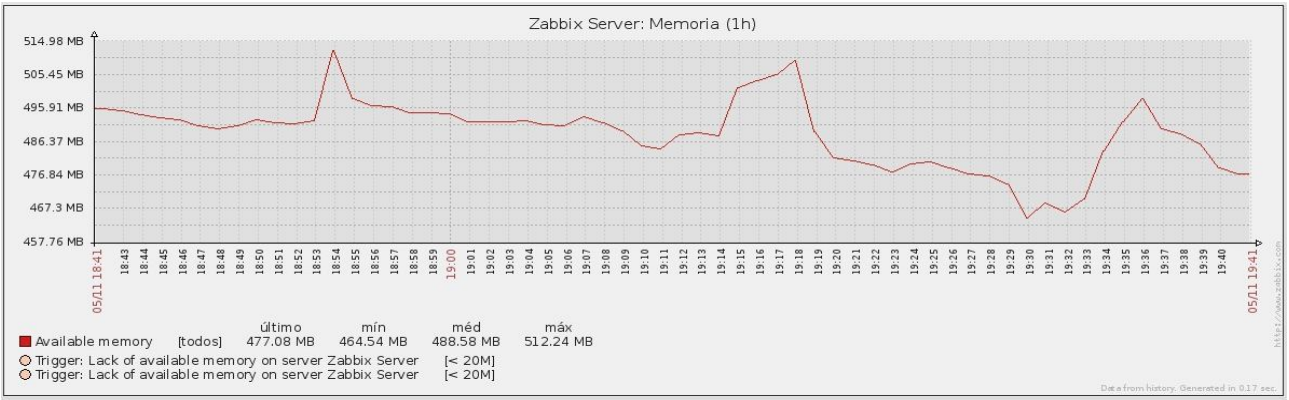

Figura L – Uso de memoria do sistema (Primeiro ataque).

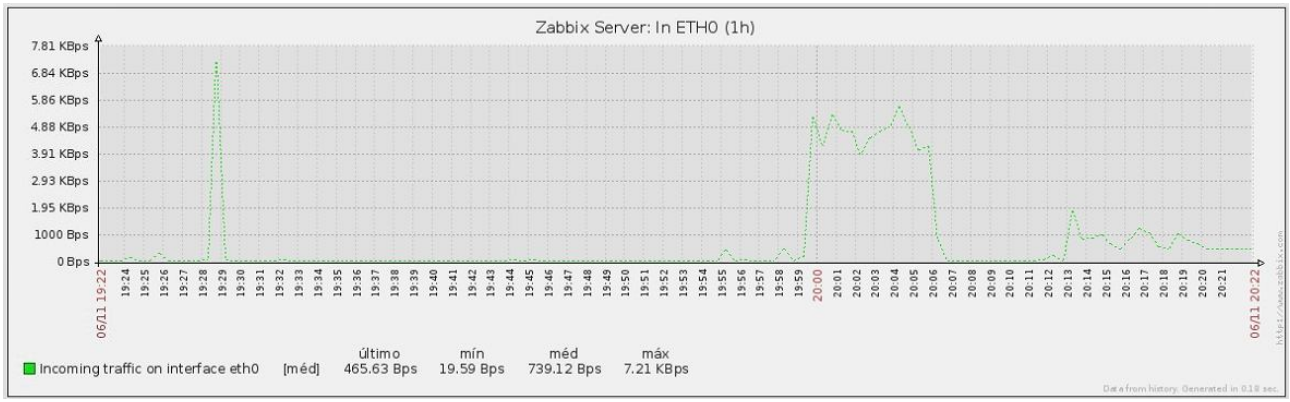

Figura M – Tráfego de entrada na interface Eth0 (Segundo ataque).

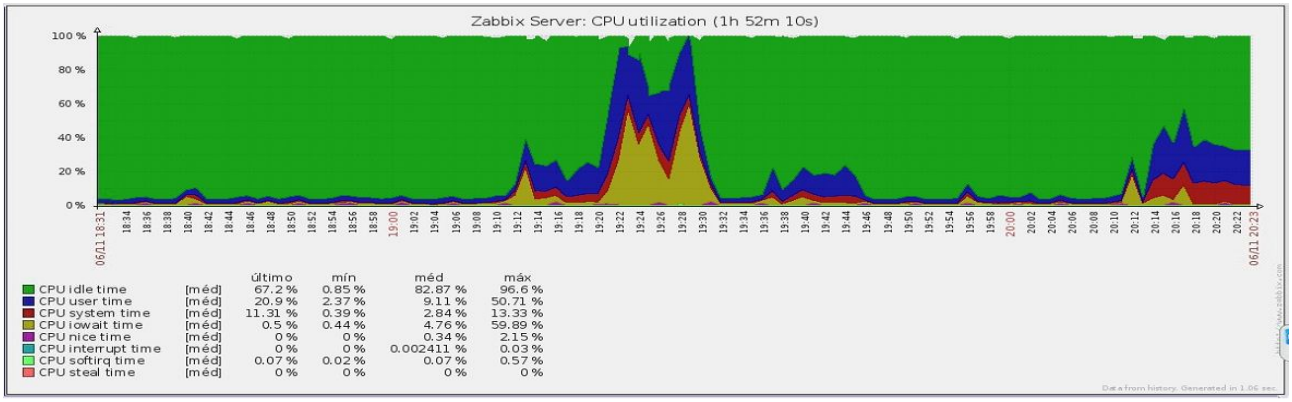

Figura N – Utilização do processador (Segundo ataque).

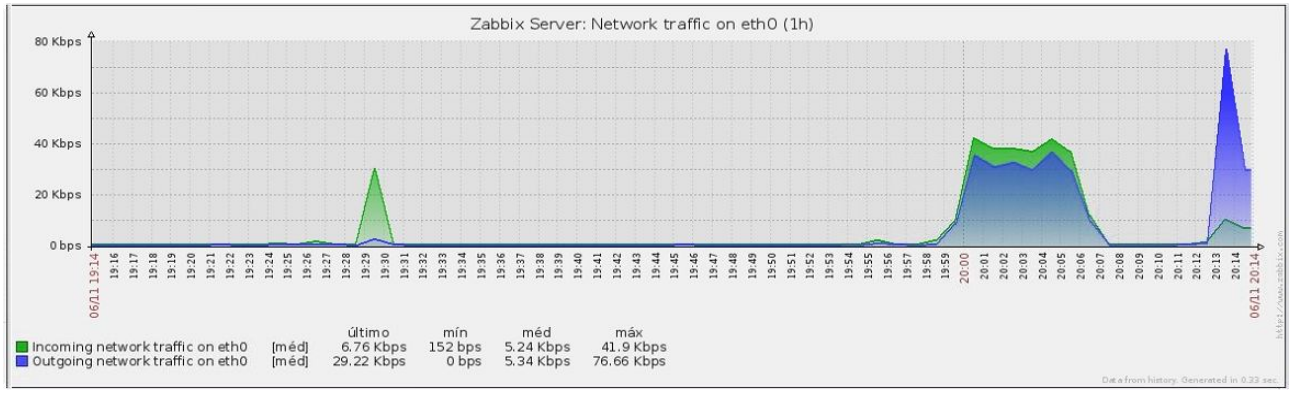

Figura O – Tráfego de entrada e saída na interface Eth0 (Segundo ataque).

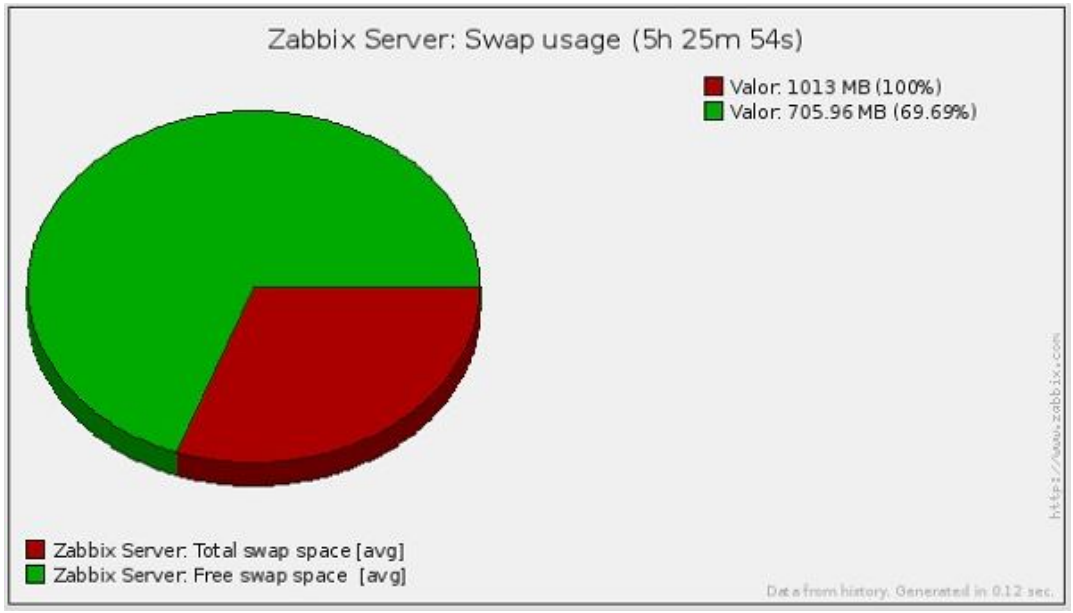

Figura P – Uso da utilização Swap (Segundo ataque).

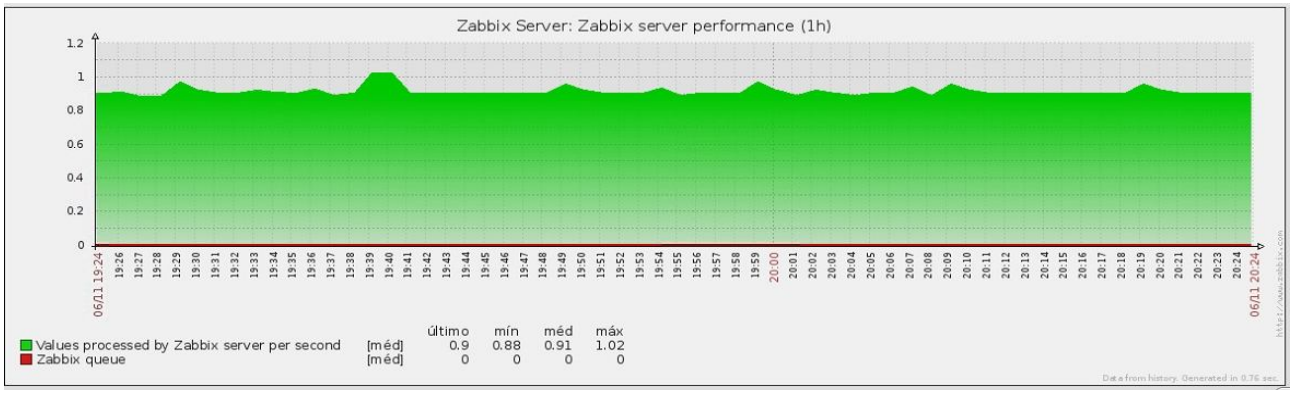

Figura Q – Desempenho do Zabbix (Segundo ataque).

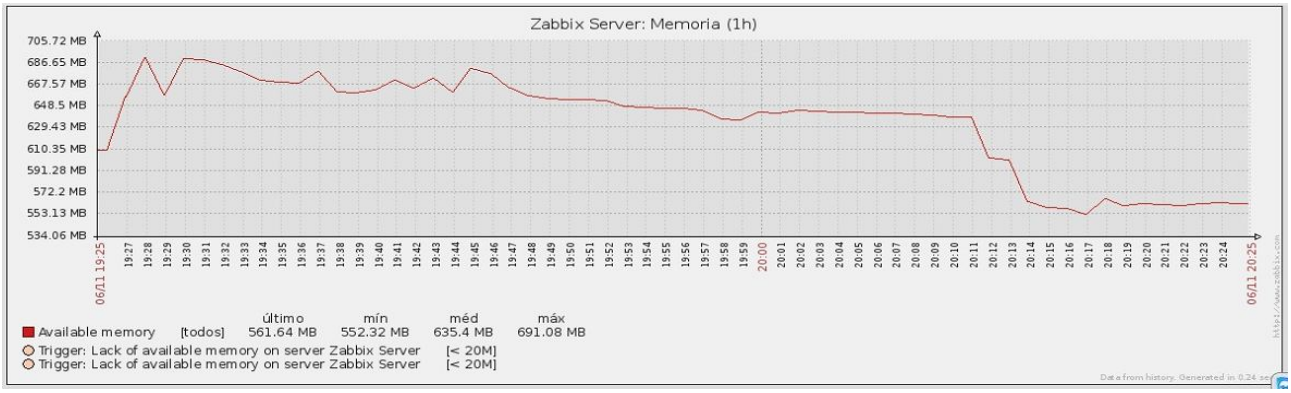

Figura R – Uso de memoria do sistema (Segundo ataque).

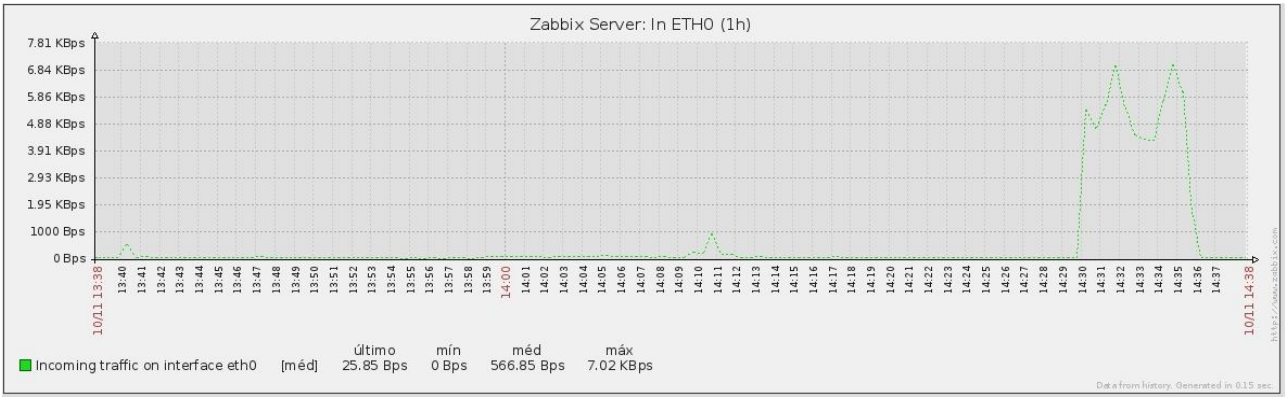

Figura S – Tráfego de entrada na interface Eth0 (Terceiro ataque).

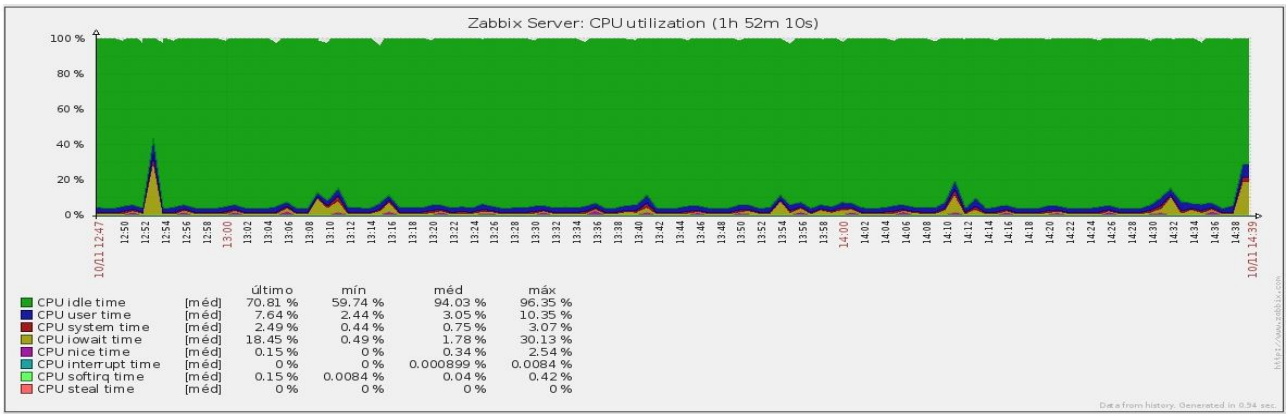

Figura U – Utilização do processador (Terceiro ataque).

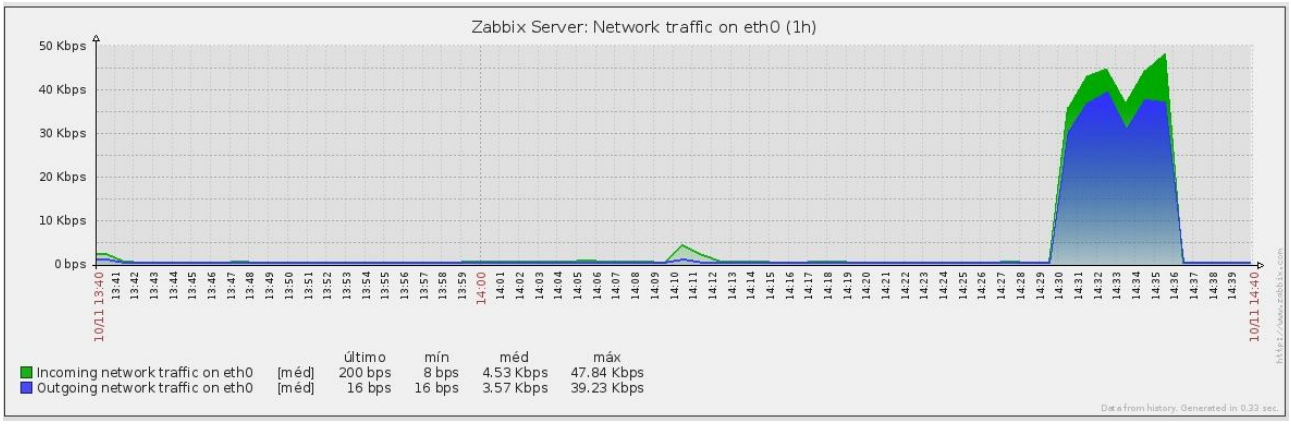

Figura V – Tráfego de entrada e saída na interface Eth0 (Terceiro ataque).

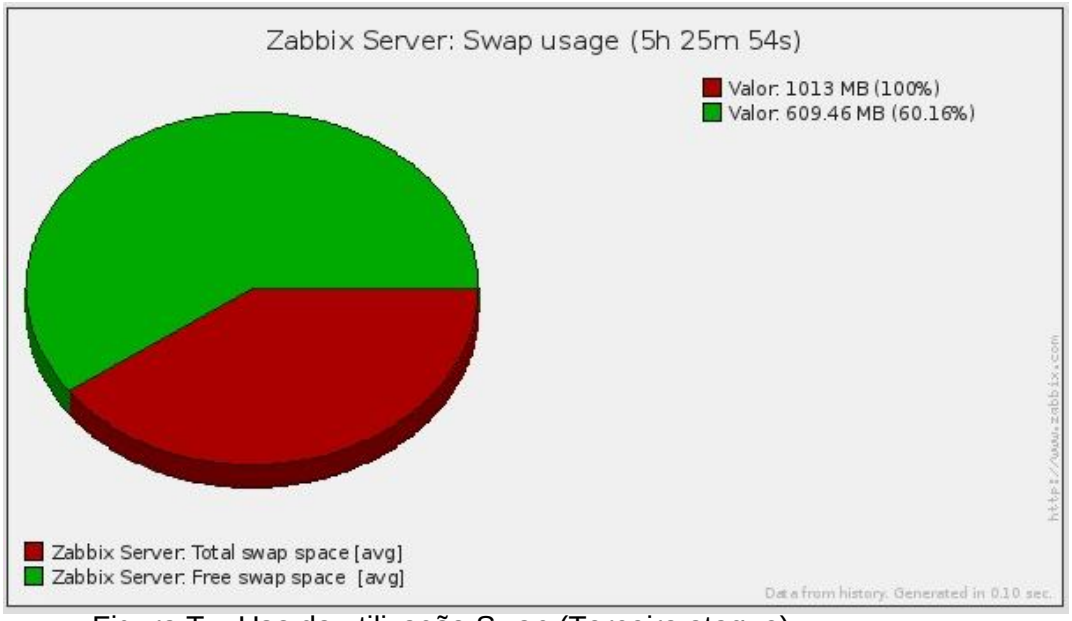

Figura T – Uso da utilização Swap (Terceiro ataque).

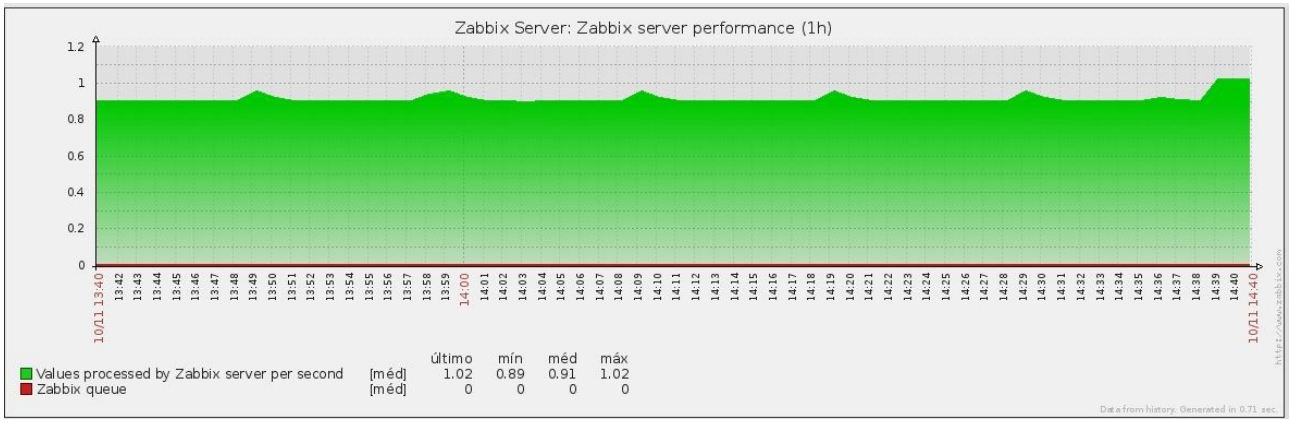

Figura X – Desempenho do Zabbix (Terceiro ataque).

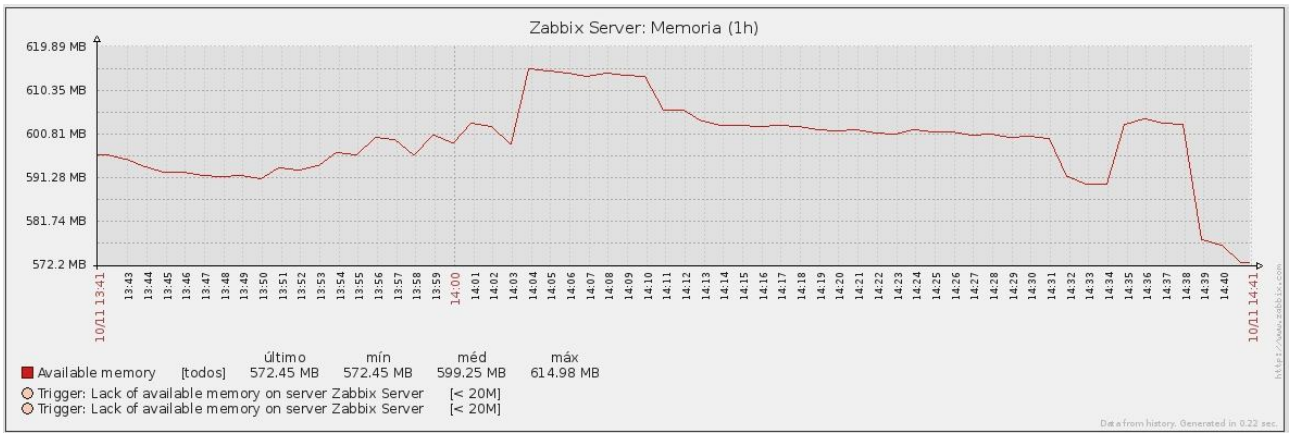

Figura W – Uso de memoria do sistema (Terceiro ataque).

REFERÊNCIAS

ARAUJO, Camila Gonzaga de. **Mecanismo de Defesa Contra Ataque DDoS.**Disponível em: <http://200.255.167.162/pesquisa/pdf_monografias/sistemas/2008/4071.pdf>. Acesso em: 13 abr. 2012.

AMARO, Mariza de O. S. **Sua organização está preparada para uma contingência?** Programa de Pós-Graduação de Engenharia de Sistemas e Computação. Rio de Janeiro: UFRJ, 2004. Disponível em:<https://www.mar.mil.br/sdms/artigos/6816.pdf>. Acesso em 12/11/2012.

AMORIM, Rodrigo Diego Melo; JAHANIAN, Farnam. **Ataques Denial-of-Service.** Disponível em: <http://www.cin.ufpe.br/~fab/cursos/metodologia-graduacao/2006-2/monografias/rodrigo-diego.doc>. Acesso em: 06 fev. 2012.

BERNARDES, M. C. **Avaliação do Uso de Agentes Móveis em Segurança Computacional.** Dissertação (Mestrado) — Instituto de Ciências Matemáticas e de Computação (ICMC - USP), São Carlos, SP, 1999.

BERTHOLDO, Leandro Márcio; ANDREOLI, Andrey Vedana; TAROUCO, Liane. **Compreendendo Ataques Denial of Services.** Disponível em: <http://www.cert-rs.tche.br/docs_html/ddos-errc-2003.pdf>. Acesso em: 05 fev. 2012.

BERTHOLDO, Leandro Márcio; ANDREOLI, Andrey Vedana. Ddos - **distributed denial of service (ataques distribuídos)**. , 2010. Disponível em: <http://www.cert-rs.tche.br/docs_html/ddos.html>. Acesso em: 10 maio 2012.

BARBOSA, : André Sarmento; MORAES, Luís Felipe M. de.**Fundamentos de Sistemas de Segurança da Informação.**Disponível em: <http://www.land.ufrj.br/~verissimo/cos871/bibref/biblio02.pdf>. Acesso em: 24 mar. 2012.

CERT ADVISORY CA-1998-01. **Smurf IP Denial-of-Service Attacks.** Disponível em: <http://www.cert.org/advisories/CA-1998-01.html>. Acesso em: 23 maio 2012.

COMPY, Carlos A. A.; STTEFEN, Flávio Deny. **Segurança em Informática e de Informações**. 2a ed. rev. e ampl. São Paulo: Senac, 1999.

CERT ADVISORY. **Cartilha de Segurança para Internet.** Disponível em: <http://cartilha.cert.br/malware/sec7.html>. Acesso em: 12 abr. 2012.

COOKE, Evan; JAHANIAN, Farnam. **The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets.** Disponível em: <http://static.usenix.org/events/sruti05/tech/full_papers/cooke/cooke_html/>. Acesso em: 06 fev. 2012.

GOMES, Norma Rodrigues; MATTOS, Luiz Antonio da Frota. **Detecção de Ataques pela Constatação de Violação dos Protocolos IP e TCP.** Disponível em: <http://www.sbrc2007.ufpa.br/anais/2004/2090.pdf>. Acesso em: 12 mar. 2012.

INOKOSHI, Rodrigo Kiyoshi. **Avaliação de *Firewall* e Sistema de Detecção de Intrusão baseado em software livre**. Jaguariúna, 2007.

JUNIOR, Vamberto de Freitas Rocha. **Estudo e implementação de *Firewall* em ambientes corporativos**. João Pessoa, 2010.

KUMARASAMY, Saravanan. **Distributed denial of service (ddos) attacks detection mechanism**. , 2011. Disponível em: <http://www.airccse.org/journal/ijcseit/papers/1211ijcseit04.pdf>. Acesso em: 05 fev. 2012.

LAUFER, Rafael P. et al. **Negação de Serviço: Ataques e Contramedidas.** Disponível em: <http://www.gta.ufrj.br/ftp/gta/TechReports/LMVB05a.pdf>. Acesso em: 13 mar. 2012.

LAUREANO, M., 2006. **Máquinas Virtuais e Emuladores: Conceitos, Técnicas e Aplicações.** 1ª edição. São Paulo: Novatec Editora.

MCCLUE, Stuart; SCAMBRAY, Joel; KURTZ, George. ***Hackers expostos segredos e soluções para a segurança de redes:*** **Segredos e Soluções para a segurança de redes**. 4. ed. Rio de Janeiro: Campus, 2003.

MACAFFE disponível em http://www.mcafee.com/br/ acesso em 30 março de 2012

NORTHCUTT, S.; et al. **Desvendando segurança em redes.** Rio de Janeiro: Editora Campus, 2002.

NOGUEIRA, Toniclay Andrade; BATISTA, Othon Marcelo Nunes.**Negação de Serviço: Implementação, Defesas e Repercuções.**Disponível em: <http://www.linuxsecurity.com.br/info/DoS/DoS.doc>. Acesso em: 10 mar. 2012.

OLIVEIRA, Luis. et al. **Avaliação de proteção contra ataques de negação de serviço distribuídos (ddos) utilizando lista de ips confiáveis** . , 2007. Disponível em:

<http://http://www.lbd.dcc.ufmg.br/colecoes/sbseg/2007/008.pdf>. Acesso em: 05 fev. 2012.

PHILIPP SCHROEDEL. Backtrack. , 2012. Disponível em: <http://www.remote-exploit.org/articles/backtrack/index.html>. Acesso em: 06 nov. 2012.

STEFFEN JUNIOR, Julio. **Sistema de Detecção de Intruso.** Disponível em: <http://graficashayene.com/bysined.com/13/cursos/SistemasdeDeteccaode%20ntrusao.pdf>. Acesso em: 11 abr. 2012

SIEWERT, Vanderson C.. ***Firewall*** **suas características e vulnerabilidades**. Florianópolis, 2008.

SHARMA, Kapil. Ip spoofing. , 2001. Disponível em: <http://www.gazetadolinux.com/pr/lg/issue63/sharma.html>. Acesso em: 10 mar. 2012.

SYMANTEC disponível em http://www.symantec.com.br/ acesso em 12 de março de 2012.

WHALEN, Sean. An **introduction to arp spoofing** . , 2001. Disponível em: <http://www.rootsecure.net/content/downloads/pdf/arp_spoofing_intro.pdf>. Acesso em: 12 mar. 2012.

ZWICKY, Elizabeth D.; COOPER, Simon; CHAPMAN, D. Brent (2001). **Construindo Firewalls para a Internet.** 2ª edição. Editora O´Reilly. Tradução Editora Campus.