Monitoramento De Ataques De Negação De Serviço: Um caso Prático Utilizando *Slowloris*

André Luiz Riccó Corrêa[1], Henrique Pachioni Martins[1].

[1]Curso de Tecnologia em Redes de Computadores – Faculdade de Tecnologia de Bauru (FATEC)
Rua Manoel Bento Cruz, n° 30 Quadra 3, Centro, 17.015-171 – Bauru, SP - Brasil

andrericorrea@gmail.com, henrique.martins01@fatec.sp.gov.br

Abstract. *Even with the great advance of technology related to computer networks, one of the biggest problems faced by the sectors responsible for information technology and infrastructure of computer networks, are denial of service attacks. This research aims to study the main types of denial of service attacks and ways to monitor these attacks. The research showed in a simulated attack, the monitoring of their characteristics through free software and the implementation of a possible defense solution. It was concluded that the softwares tested are efficient in monitoring and preventing a denial of service attack within the simulated environment.*

Resumo. *Mesmo com o grande avanço das tecnologias ligadas a redes de computadores, um dos maiores problemas enfrentados pelos responsáveis dos setores de tecnologia da informação e de infraestrutura de redes de computadores, são os ataques de negação de serviço. Essa pesquisa tem como objetivo estudar os principais tipos de ataques de negação de serviço e maneiras de monitorar esses ataques. A pesquisa mostrou em uma simulação de ataque, o monitoramento de suas características através de softwares gratuitos e a implementação de uma possível solução de defesa. Conclui-se que os softwares testados são eficientes no monitoramento e prevenção de um ataque de negação de serviço dentro do ambiente simulado.*

1. Introdução

Desde o início da Internet os responsáveis por manter em funcionamento serviços ligados a redes de computadores têm vários desafios, e um desses desafios é prevenir e evitar os ataques de negação de serviço. Esse tipo de ataque tem como objetivo impossibilitar o bom funcionamento de um serviço em uma rede de computadores, como por exemplo, serviços responsáveis por prover o funcionamento de sites hospedados na Internet.

Nos dias atuais o número de ataques de negação de serviço tem crescido e os alvos, que na maioria dos casos são empresas públicas ou privadas, têm sofrido com esses ataques. Pesquisas apontam que dentre 86% das empresas privadas situadas no

Brasil e que possuem mais de 200 funcionários, 15% já sofreram algum tipo de ataque de negação de serviço [Feitosa 2013].

Os ataques na maioria dos casos são realizados a partir de redes espalhadas por todo o globo. Eles são feitos normalmente por *hackers* que não possuem como objetivo o roubo de dados contidos nos servidores, mas sim o objetivo de impedir o funcionamento do serviço e deixá-los inacessíveis para os usuários comuns. Com o aumento desses ataques a serviços de bancos e empresas privadas, o prejuízo financeiro gerado pela falta de acesso a sistemas essenciais, tem aumentado a preocupação dessas organizações.

Os ataques de negação podem ser feitos a partir de computadores comuns ligados a Internet, utilizando *software*s específicos para essa função. Os *software*s utilizados nesse tipo de ataque, normalmente enviam varias solicitações ao mesmo tempo para a aplicação alvo e sobrecarregam o servidor que está disponibilizando o serviço.

Muitos *hackers* utilizam em seus ataques, computadores zumbis, que são vários computadores ligados a *Internet*, infectados com um vírus específico que possibilita o *hacker* controlar remotamente funções do computador infectado. Esses computadores formam uma grande rede dentro da própria Internet e enviam ao mesmo tempo um grande número de solicitações falsas para o servidor alvo do ataque. Esse tipo de ataque é conhecido como ataque distribuído de negação de serviço. Por ser um tipo de ataque eficiente e pela dificuldade de identificar a origem dos computadores principais, o ataque distribuído de negação de serviço tem se tornado popular entre *hackers* e sendo muito utilizado, gerando prejuízo a empresas privada e públicas.

Muitos órgãos governamentais vêm sendo atacados e seus serviços impossibilitados de funcionar, impedindo a população de ter acesso a funções básicas em sites. Ultimamente esses ataques na sua maioria são organizados por grupos em redes sociais algumas horas e às vezes dias antes de ocorrer. Podendo assim ser identificado e prevenido de maneira mais ágil e eficaz, trazendo menores consequências para essas organizações.

O objetivo dessa pesquisa é estudar alguns tipos de ataques de negação de serviço escolhidos de forma empírica e as melhores formas de prevenir esses ataques e diminuir os efeitos causados nos serviços de hospedagem de sites.

a) Estudar os principais tipos de ataques de negação de serviço;

b) Estudar *software*s gratuitos pra detecção de ataques de negação serviço;

c) Analisar os efeitos de ataques de negação de serviços em aplicações de rede de computadores;

d) Estudar as melhores práticas de monitoramento e prevenção de ataques de negação de serviços.

Tendo em vista o crescente número de ataques de negação de serviço a sites de instituições públicas e privadas e o prejuízo financeiro que esses ataques tem gerado a essas organizações. Justifica-se essa pesquisa que pretende estudar e demonstrar técnicas de analise e prevenção desses tipos de ataques para diminuir seus efeitos em serviços de hospedagem de sites.

2. Fundamentação teórica

2.1. Segurança da Informação

Com o aumento da tecnologia nas organizações é também necessário o aumento da preocupação com a segurança dos dados mantidos nos servidores. A segurança da informação é um item de extrema importância e deve ser visto como um passo principal para se manter um sistema tecnológico adequando dentro de uma organização.

As preocupações sobre a segurança variam desde um arquivo que não pode ser lido ou modificado por pessoas sem autorização até a entrada de pessoas não autorizadas na sala de ativos da organização.

É de responsabilidade do administrador da rede da organização prevenir possíveis eventos que podem ser evitados na questão de segurança da informação.

Tanenbaum (2003) divide em quatro áreas os problemas enfrentados na segurança de uma rede de computadores:

a) Sigilo: Manter arquivos e informações fora do alcance de usuários não autorizados;

b) Autenticação: Ter um controle sobre com quem se está comunicando ou trocando informações dentro da rede, se esse é um usuário autorizado a utilizar tais serviços ou acessar determinados diretórios e arquivos;

c) Não-repúdio: Controle de assinaturas de acesso e transições ou transferências na rede;

d) Controle de Integridade: Integridade das mensagens trafegadas na rede. Verificação da autenticidade das informações.

Outro ponto importante dentro da segurança da informação em uma rede de computadores é a disponibilidade dos serviços. O responsável pela rede deve se preocupar com as questões de segurança citas acima e com os efeitos que elas podem causar na disponibilidade de serviços na rede. É necessário que uma rede de computadores em uma organização esteja sempre disponível para seus usuários finais [Stallings 2008].

2.2. Software Livre

Softwares livres são sistemas que vão desde aplicativos a sistemas operacionais e possuem como objetivo a livre distribuição de seu código-fonte. Em muitos casos esses *softwares* possuem licenças para utilização, essas licenças podem determinar se os

usuários podem utilizar esse *software* para fins comerciais, empresarial e até se o usuário pode fazer modificações no código-fonte do sistema.

A utilização de *softwares* livre ou de código-fonte aberto tem aumentado significativamente nos últimos anos. Um dos exemplos de sistema que tem como base a filosofia do *software* livre são os sistemas operacionais *GNU/Linux*.

A maioria das distribuições *GNU/Linux* é distribuída gratuitamente. Entre essas distribuições podemos citar as distribuições *Debian*, *CentOS*, *Slackware* [Nemeth, Snyder e Hein 2007].

Além dos sistemas operacionais, existem os aplicativos livres. Os aplicativos livres estão cada vez mais incluídos dentro do departamento de tecnologia da informação de organizações e suas utilidades variam desde uma utilização mais simples como um aplicativo de edição de texto a utilizações mais complexas como servidores de sites e *software*s de identificação e prevenção de invasões.

2.3. Firewall

O *firewall* serve como uma maneira segura de ligar a rede interna de uma organização com a *Internet*. O *firewall* é um sistema que pode ser implementado na rede em forma de *hardware* específico ou *softwares*. Os *firewalls* podem ser apenas de filtro de pacotes, que utiliza um filtro com base no endereçamento *Internet Protocol* (IP) e números das portas *Transmission Control Protocol* (TCP) ou *User Datagram Protocol* (UDP). Ou podem ser utilizados na camada de aplicação, por exemplo, um *Proxy* [Stallings 2008].

Stallings (2008), cita quatro técnicas gerais utilizada pelos *firewalls* para controle de acesso e política de segurança de uma rede:

a) Controle de serviço: Define os serviços que podem entrar e sair da rede interna para a *Internet*;

b) Controle de direção: Define em qual direção as solicitações de serviço podem iniciar e passar pelo *firewall*;

c) Controle de usuário: Define o controle de acesso a serviços conforme os usuários que o estão acessando;

d) Controle de comportamento: Define como determinados serviços são utilizados dentro da rede.

O *firewall* não pode assegurar que a rede está protegida, pois como lida apenas com entrada e saída de dados, ele não pode proteger a rede de outros ataques provindos da rede interna ou da *Internet*. Um exemplo que pode ser citado é o ataque de negação de serviços [Tanenbaum 2003].

Para a proteção da rede contra outros tipos de ataques é necessária a implantação de sistemas de prevenção e detecção de intrusos e analise de comportamento da rede.

2.4. Aplicações de Segurança

Para se evitar ataques que não são bloqueados pelas regras do *firewall*, é necessário manter aplicações de segurança e de gerenciamento para monitorar a saúde da rede e prevenir possíveis danos causados por esses ataques. Nesse tópico será analisado o sistema de detecção de intrusos e o sistema de monitoramento de rede baseado no protocolo *Simple Network Management Protocol* (SNMP).

2.4.1. IDS – Sistema de detecção de intrusos

Sistemas de detecção de intrusos (IDS) são *softwares* responsáveis por detectar intrusos ou certos tipos de ataques ao sistema. Esses *softwares* são capazes de analisar os sistemas para verificar se existem conexões feitas por computadores sem permissão na rede [Nassaro 2012].

Segundo Nassaro (2012), os sistemas IDS podem ser divididos em três categorias:

a) IDS baseado em *Host*: A análise é feita apenas com base em um computador especifico da rede normalmente o servidor principal e o levantamento das informações é feito por um *software* especifico ou através de dados de eventos do sistema;

b) IDS baseado em Rede: A análise é feita em toda a rede e de maneira mais detalhada. As informações são monitoradas por vários sensores espalhados pela rede e sistemas que monitoram a fundo pilhas de protocolos e cabeçalhos de pacotes que trafegam na rede;

c) IDS híbridos: É utilizado para a junção de sistemas baseados em *Host* e sistemas baseados em Redes. Essa união dos dois tipos de sistemas de detecção aumenta o controle e segurança da rede.

Um exemplo de *software* de detecção de intrusos mencionado por Kurose e Ross (2010), é o *software Snort*. O *Snort* é um aplicativo que verifica assinaturas de ataques contidas em um banco de dados e avisa o administrador sobre um possível ataque na rede.

2.4.2. Sistemas de Monitoramento

Os principais sistemas de monitoramento utilizam:

a) *Management Information Base* (MIB) de Sistema: São informações de objetos gerenciados em um sistema, essas informações ficam guardadas em um banco de dados e contem todos os dados dos objetos que são gerenciados no computador;

b) Protocolo SNMP: O protocolo SNMP é responsável por verificar as informações nas MIBs dos objetos gerenciados e enviar a um sistema de monitoramento.

Sistemas de monitoramento baseadas em SNMP ou aplicações SNMP são compostos por:

a) Gerente: Sistema que gerencia os agentes da rede, ele é composto por um gerador de comandos, receptor de notificações e um transmissor;

b) Agente: Os computadores gerenciados na rede e que produzem as informações para o gerente são denominadas agente. O agente é composto por um elemento respondedor de comandos e um elemento que envia as notificações [Kurose e Ross 2010].

Esses sistemas de monitoramento são capazes de verificar todos os tipos de informações contidos nas MIBs, por esse fato ele é de extrema eficácia para garantir a segurança da rede, pois é possível verificar serviços como tráfego em placas de rede, números de requisições e outras informações úteis para verificar se um computador está sofrendo algum tipo de ataque.

Como exemplo de *softwares* livre para gerenciamento e monitoramento de rede pode se citar os *softwares Nagios* e *Cacti*.

2.5. Tipos de Ataques de Negação de Serviço

2.5.1. DoS

O *Denial-of-Service* (DOS) ou ataque de negação de serviços tem como objetivo impedir um serviço de funcionar corretamente e assim impedir que os usuários utilizem esses serviços. O ataque de negação de serviços é muito utilizado para atacar servidores de hospedagem de sites na *Internet*. O DoS normalmente é feito através de múltiplas requisições feitas a um servidor. O atacante, que no caso seria o *hacker* que está tentando parar o serviço, utiliza de *software*s e técnicas para fazer múltiplas requisições automaticamente para o alvo, que é o serviço que o hacker deseja afetar. Umas das técnicas mais utilizadas é o *SYN flooding* [Nakamura e Geus 2007].

2.5.2. DDoS

Distributed Denial-of-Service (DDoS) ou ataque distribuído de negação de serviços é um tipo de ataque de negação. Atualmente ele vem se difundido entre a comunidade *hacker* e se tornando um dos tipos de ataque de negação mais utilizados, principalmente por possuir uma arquitetura de ataque que dificulta e muita das vezes impossibilita a identificação da origem do ataque.

Esse tipo de ataque utiliza uma arquitetura feita de maneira que os ataques sejam efetuados a partir de vários computadores distribuídos em toda a *Internet*. A arquitetura utilizada atualmente possui diferentes níveis de funcionalidades:

a) Alvo: Serviço que será alvo do ataque;

b) Refletor: São computadores não infectados, que são utilizados para aumentar o ataque;

c) Zumbis: Os computadores zumbis são computadores infectados com um vírus capaz de mandar ataques de negação de serviços sem que o usuário perceba. Os computadores zumbis são utilizados em *Botnets* para aumentar o número de locais de ataques ao alvo;

d) Mestres: Os computadores mestres são responsáveis por manter uma lista de todos os computadores zumbis que o atacante infectou para fazer os ataques. Os computadores mestres também são infectados com um vírus especifico para essa função;

e) Atacante: O atacante é o responsável pelos ataques. Ele é o primeiro nível de ataque, responsável por enviar as informações de ataques, como por exemplo, o endereço do alvo. Essas informações são passadas para o mestre e então para seus outros níveis.

O ataque DDoS pode ser classificado em dois tipos. Segundo Stallings (2008) esses tipos são:

a) Ataque direto: O ataque direto é feito quando um computador atacante envia as informações de ataque para os computadores mestres e estes enviam para os computadores zumbis que fazem o ataque ao computador alvo;

b) Ataque refletor: O ataque refletor insere em sua arquitetura mais um nível, os computadores refletores. Nesse ataque o computador atacante envia as informações de ataque para os computadores mestres e estes para os computadores zumbis. Os computadores zumbis então enviam pacotes solicitando o endereço IP do computador alvo para os computadores refletores e estes respondem estas solicitações inundando o computador alvo de solicitações. Esse ataque é mais prejudicial e é mais difícil de ter a origem identificada do que um ataque de DDoS direto, pois ele envolve mais computadores, inclusive computadores que não foram infectados com nenhum tipo de vírus de ataque.

2.5.3. SYN Flooding

SYN *flooding* é uma técnica de ataque de negação de serviço. Esse ataque explora o estabelecimento de conexões TCP [Nakamura e Geus 2007]. O ataque é feito através de inúmeras requisições de conexões enviadas para o servidor alvo. Com um grande número de requisições para processar o servidor não consegue responder a todas e a pilha de memória sofre um transbordamento e as requisições autênticas começam a ser negadas impedindo os usuários terem acesso aos serviços.

2.5.4. Smurf

A técnica de ataque *Smurf* utiliza pacotes *Internet Control Message Protocol* (ICMP) *echo* (*ping*) para atacar um computador alvo. O ataque é feito quando um computador

envia vários pacotes falsos de ICMP *echo request* para o IP de *broadcast* de uma rede, essas requisições possuem a origem falsificada com o endereço IP do computador alvo utilizando a técnica de IP *Spoofing*. Após o envio dessas requisições para o endereço de *broadcast* da rede, todos os computadores conectados a essa rede enviam a resposta para o endereço IP do alvo. Esse tipo de ataque utiliza a rede para amplificar o ataque de negação ao alvo que com os vários pacotes de respostas recebidos tem seus serviços prejudicados [Nakamura e Geus 2007].

2.5.5. Fraggle

O ataque *Fraggle* funciona de forma quase idêntica ao ataque *Smurf*. A diferença entre os dois tipos de ataque são os tipos de pacotes utilizados para atacar o computador alvo [Nakamura e Geus 2007]. No *Fraggle* o computador que está fazendo o ataque utiliza-se de pacotes UDP *echo* para enviar solicitações falsas para o endereço de *broadcast* da rede. Da mesma forma que o ataque *Smurf* os pacotes enviados tem o endereço de origem falsificado com o endereço IP do computador alvo, que recebe pacotes de respostas de todos os computadores da rede prejudicando assim seus serviços.

2.6. Ferramentas de Ataque de Negação de Serviço

A maioria dos ataques de negação de serviços é feita através de *softwares* ou ferramentas específicas para essa função. Abordaremos prioritariamente as ferramentas mais conhecidas, como por exemplo, a Botnet, ferramenta que é utilizada tanto para ataques de distribuídos de negação de serviços como para diversas outras funções.

2.6.1. Botnet

Botnet é o termo utilizado para determinar uma rede de computadores infectados com um vírus que o tornem um computador zumbis. Esse vírus pode ser denominado com sendo um *software* robô, que utiliza esses computadores sem que o usuário tome conhecimento [CSO/EUA 2013].

Uma *Botnet* pode ser utilizada para comandar ataques distribuídos de negação, mas possui outras funcionalidades, como por exemplo, enviar spams e espalhar vírus [Microsoft 2013].

O número crescente de computadores infectados com vírus específicos para o tornarem parte de uma *Botnet*, tem se tornado preocupante para as empresas de segurança da tecnologia. No ano de 2010 um levantamento de dados feito pela empresa *Prolexic Technologies* encontrou mais de 4 milhões de computadores infectados com algum vírus para o tornar zumbi [CSO/EUA 2013].

2.6.2. TFN

O *Tribe Flood Network* (TFN) utiliza a arquitetura de ataque de DDoS direto. Ele realiza os ataques de negação através do envio de pacotes TCP. Essa ferramenta pode ser utilizada em diversos tipos de ataques diferentes, entre eles, IP *Spoofing*, SYN *Flooding* e *Smurf* [Nakamura e Geus 2007].

2.6.3. TFN2K

O *Tribe Flood Network 2000* (TFN2K) é uma ferramenta que surgiu da evolução do TFN. Uma de suas características é que ele utiliza de vários protocolos entre eles UDP, TCP e ICMP. Com a utilização de vários protocolos, o tráfego do TFN2K tende a ser mais difícil de ser reconhecido e filtrado [Nakamura e Geus 2007].

2.6.4. Trinoo

O *Trinoo* é uma ferramenta mais simples de ataques distribuídos de negação de serviços. O *Trinoo* igualmente o TFN e o TFN2K utiliza o ataque DDoS direto e como característica, necessita de uma senha para se conectar aos computadores mestres. O *Trinoo* pode fazer apenas um tipo de ataque, o UPD *flood* [Solha, Texeira e Piccolini 2013].

2.6.5. Slowloris

O *Slowloris* é uma ferramenta de negação com uso específico em servidores de *Hypertext Transfer Protocol* (HTTP). O ataque feito pelo *Slowloris* consiste em requisitar a abertura de um grande número de conexões no servidor alvo, com isso o servidor tem seu processamento prejudicado e não consegue efetuar todas as requisições de conexão.

2.6.6. T50

Outra ferramenta que tem sido utilizada para ataques de negação de serviço é o T50. O T50 a princípio foi criado para testar a qualidade de diferentes tipos de estruturas de redes de computadores. Porém com a abertura de seu código-fonte *hackers* o modificaram para poder efetuar ataques de DDoS. A grande diferença do T50 é a

possibilidade dele utilizar um grande número de protocolos, aumentando assim suas funções para ataques.

2.7. Ferramentas de prevenção de ataques de negação de serviço

2.7.1. (D)DoS Deflate

O *software (D)DoS Deflate* é um *script* desenvolvido em *Shell Bash* utilizado para auxiliar no bloqueio de um ataque de negação de serviço. Esse *software* utiliza o comando *netstat* para verificar as conexões realizadas no servidor e se o numero de conexões ultrapassarem o limite definido pelo usuário ele bloqueia o endereço IP referente a essas conexões. Esse bloqueio do endereço IP pode ser realizado pelo *software iptables* ou pelo *software Advanced Policy Firewall* (APF). As configurações do *software (D)DoS Deflate* podem ser realizadas pelo arquivo "ddos.conf" encontrado no diretório "/usr/local/ddos/" [Medialayer 2013].

O *software (D)DoS Deflate* por padrão é executado pela função *crontab* do sistema operacional *GNU/Linux* podendo ser definido o tempo de execução pelas configurações do *software*.

3. Materiais e Métodos

Para alcançar o objetivo proposto de analisar os efeitos de ataque de negação de serviços e as melhores praticas de prevenção e monitoramento desses ataques, foi feito uma pesquisa bibliográfica contendo os principais tópicos sobre o tema proposto. Para alcançar o objetivo pratico foi realizado uma simulação de um ataque de negação de serviço em um ambiente virtual e uma possível solução de defesa.

A simulação do ataque de negação foi direcionada a um site fictício hospedado em um servidor alvo dentro de um ambiente virtualizado com base em *softwares* livres.

Para este ataque simulado foi utilizado o *software Oracle VM VirtualBox* para virtualizar as maquinas utilizadas. Conforme descrito na figura 1 para realizar a simulação foi virtualizados um servidor com o sistema operacional *Debian* e a aplicação *Apache* HTTP *Server* servindo de hospedagem para o site que foi atacado, para simulação esse computador alvo recebeu o nome *APACHE*. Também foi virtualizado dentro desse ambiente um computador com sistemas de gerenciamento de redes baseado em SNMP, para verificação da saúde do computador alvo, nesse computador de monitoramento nomeado como *MONITORAMENTO* foi instalado o sistema operacional *Debian* e os *softwares Cacti* e *Nagios*, ambos configurados para monitorar o computador *APACHE*. O computador nomeado como *ATACANTE* foi utilizado para efetuar os ataques simulados ao site hospedado no computador *APACHE*, neste computador foi utilizada a distribuição GNU/Linux Back Track e a aplicação Slowloris para efetuar os ataques.

Figura 1. Ambiente virtualizado utilizado na simulação do ataque.

Fonte: Elaborado pelo próprio autor (2013)

A simulação foi realizada em duas etapas. Na primeira etapa foi realizado um ataque pelo computador *ATACANTE* através do *software Slowloris*, este ataque foi direcionado a porta 80 do computador *APACHE*.

Na segunda etapa da simulação foi utilizado o *software (D)DoS Deflate* no computador *APACHE*. Para uma maior precisão na coleta dos dados da simulação o *software* foi iniciado manualmente através do comando "*ddos.sh -k*" que é utilizado para verificar o numero de conexões realizadas por um endereço IP e o bloqueio automático do endereço que excede o limite de conexões configuradas no *software* e foi definido o limite máximo de 100 conexões por endereço IP.

Durante a simulação de ataque o computador *MONITORAMENTO* armazenou dados de fluxo de dados através do protocolo SNMP com o *software Cacti* e dados do estado do serviço HTTP com o *software Nagios*.

4. Resultados Obtidos

Durante a simulação do ataque foram coletados dados dos softwares de monitoramento do período de 10 minutos antes do inicio do ataque e dos minutos 5 e 10 após o inicio do ataque feito pelo computador *ATACANTE*, assim como os dados das atualizações dos *softwares* de monitoramento após o inicio da defesa.

O resultado coletado através do *software* de monitoramento *Cacti* de acordo com a figura 2, mostra o fluxo de dados na placa de rede do computador *APACHE* durante os 10 (minutos) que antecederam o ataque.

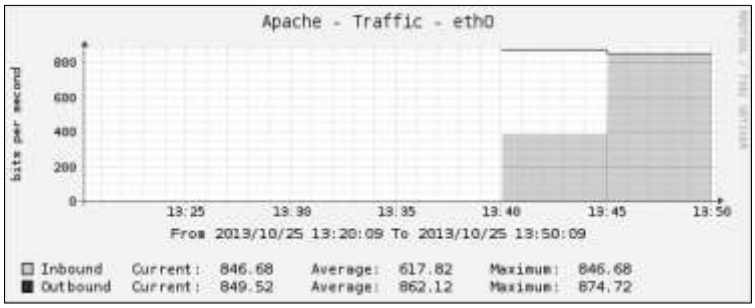

Figura 2. Gráfico de fluxo de dados da placa de rede do computador *APACHE* dos 10 minutos antecedentes ao ataque

Fonte: Elaborado pelo próprio autor (2013)

Após iniciado o ataque foram coletados novamente os dados dos *softwares Cacti* e *Nagios* após 5 minutos do seu inicio. Na figura 3 é possível verificar o aumento no fluxo de dados na placa de rede do computador *APACHE* indicado pelo *software Cacti*. Na figura 4 é possível verificar que após 4 minutos do inicio do ataque uma atualização do software *Nagios* indica um estado crítico do serviço HTTP do computador *APACHE*.

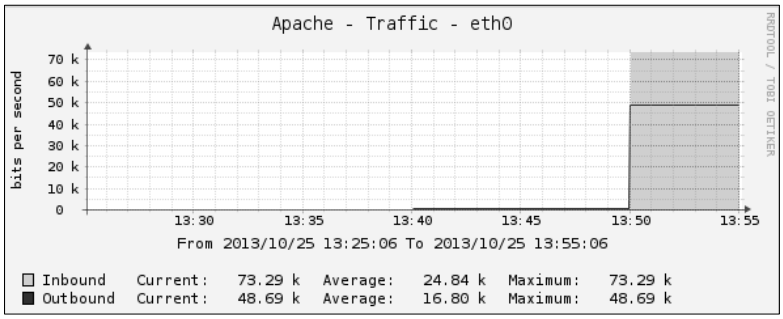

Figura 3. Gráfico de fluxo de dados da placa de rede do computador APACHE após 5 minutos do inicio do ataque

Fonte: Elaborado pelo próprio autor (2013)

Host	Service	Status	Last Check	Duration	Attempt	Status Information
apache	HTTP	CRITICAL	2013-10-25 13:54:28	0d 0h 0m 47s	1/4	CRITICAL - Socket timeout after 10 seconds

Figura 4. Aviso de estado crítico do serviço HTTP do computador *APACHE*

Fonte: Elaborado pelo próprio autor (2013)

Após os 10 minutos iniciais do ataque, foi possível notar no *software Cacti* apenas um pequeno aumento no fluxo de dados na placa de rede do computador *APACHE,*como pode ser visto na figura 5.

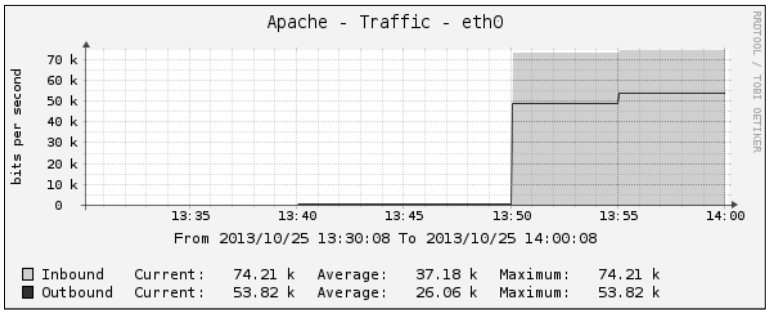

Figura 5. Gráfico de fluxo de dados da placa de rede do computador *APACHE* após 10 minutos do inicio do ataque

Fonte: Elaborado pelo próprio autor (2013)

Posteriormente a coleta dos dados iniciais e dos dados do ataque, foi iniciado o *software (D)DoS Deflate* para verificar o seu funcionamento no bloqueio de um ataque de negação. Como pode se notar na figura 6 o *software* indicou 402 conexões realizadas pelo computador *ATACANTE*. Após a inicialização do *software* pode-se notar que o mesmo bloqueou o endereço IP do computador *ATACANTE.* Na figura 7 podemos notar o IP bloqueado no *software IPTABLES* através do comando "*iptables -- list*".

```
Sex Out 25 14:00:41 BRST 2013
root@apache:/usr/local/ddos# ./ddos.sh -k
    402 192.168.0.4
```

Figura 6. Conexões realizadas pelo endereço IP do computador *ATACANTE*

Fonte: Elaborado pelo próprio autor (2013)

```
Sex Out 25 14:01:05 BRST 2013
root@apache:/usr/local/ddos# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.0.4          anywhere
```

Figura 7. Lista de endereços IPs bloqueados no *software IPTABLES*

Fonte: Elaborado pelo próprio autor (2013)

Após a inicialização do *software (D)DoS Deflate*, foi colhido novamente os dados dos *softwares* de monitoramento. Como pode ser verificado na figura 8, após 2 minutos do inicio da defesa, uma atualização do *software Nagios* indica um estado de normalidade do serviço HTTP no computador *APACHE*. E após 5 minutos do inicio da defesa, pode-se notar na figura 9 uma atualização do *software Cacti* mostrando uma diminuição no fluxo de dados na placa de rede do computador *APACHE*.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
apache	HTTP	OK	2013-10-25 14:02:28	0d 0h 0m 2s	1/4	HTTP OK: HTTP/1.1 200 OK - 583 bytes in 0,052 second response time

Figura 8. Estado normal do serviço HTTP do computador *APACHE*

Fonte: Elaborado pelo próprio autor (2013)

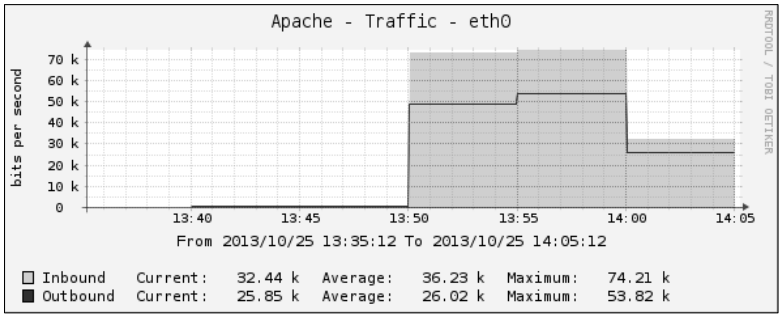

Figura 9. Gráfico de fluxo de dados da placa de rede do computador *APACHE* após 5 minutos do inicio da defesa

Fonte: Elaborado pelo próprio autor (2013)

5. Conclusão

Através da pesquisa bibliográfica realizada pode ser feito o estudo dos tipos mais comuns de ataques de negação de serviço, assim como verificada a importância da prevenção e do monitoramento destes ataques.

Na simulação de ataque de negação realizada, foi demonstrado através dos resultados gerados, que um ataque de negação de serviço, mesmo feito em pequena escala, ocasiona grande prejuízo ao funcionamento de um serviço de rede de computadores. Através dos dados coletados por *softwares* gratuitos de monitoramento, foi possível notar a eficiência do *software Slowloris* para efetuar o ataque direcionado ao serviço HTTP do computador alvo, impossibilitando o funcionamento do serviço, assim como um aumento expressivo no fluxo de dados na placa de rede do computador alvo.

Concluiu-se através dos dados analisados, que o *software (D)DoS Deflate* é eficaz no combate a ataques provindos do *software Slowloris*, pois houve uma significativa mudança no fluxo de dados na placa de rede do computador alvo, assim como o restabelecimento do funcionamento do serviço HTTP.

Para futuros trabalhos de pesquisa, pode ser realizada a verificação da eficiência de outros programas de defesa de ataques de negação de serviço, assim como de outros *softwares* de monitoramento.

Referências

CSO/EUA. (2010) “Ataques DDoS estão mais fortes do que nunca”. <http://computerworld.uol.com.br/seguranca/2010/01/15/ataques-ddos-estao-mais-fortes-do-que-nunca/>. Acesso em: 25 maio 2013.

Feitosa, M. (2013) “Mais de 70% das empresas no Brasil são vítimas de ataques virtuais, diz pesquisa”**.** http://computerworld.uol.com.br/seguranca/2013/04/02/mais-de-70-das-empresas-no-brasil-sao-vitimas-de-ataques-virtuais-diz-pesquisa/>. Acesso em: 20 maio 2013.

Kurose, J. F.; Ross, K. W. (2010) “Redes de computadores e a Internet: Uma abordagem top-down”. São Paulo: Addison Wesley. 5ª edição.

Medialayer, “(D)DoS Deflate”. (2013) <http://deflate.medialayer.com/>. Acesso em: 22 Out. 2013

Microsoft. (2013) “O que é botnet?”. <http://www.microsoft.com/pt-br/security/resources/botnet-whatis.aspx>. Acesso em: 25 maio 2013.

Nakamura, E. T.; Geus, P. L. de. (2007) “Segurança de redes em ambientes corporativos”. São Paulo-SP: Novatec.

Nassaro, D. (2012) “Sistemas de Detecção e Proteção Contra Invasões a Ambientes informatizados – IDS e IPS”. Brasília: Segurança Digital, n. 009, p.34-39. <http://segurancadigital.info/sdinfo_downloads/revista_sd/9_edicao_novembro_30_11_2012.pdf>. Acesso em: 20 maio 2013.

Nemeth, E.; Snyder, G.; Hein, T. R. (2007) “Manual Completo Linux”. São Paulo: Pearson Prentice Hall.

Solha, L. E. V. A.; Teixeira, R. C.; Piccolini, J. D. B. (2013) “Tudo que você precisa saber sobre os ataques DDoS”. <http://www.rnp.br/newsgen/0003/ddos.html>. Acesso em: 25 maio 2013.

Stallings, W. (2008) “Criptografia e segurança de rede”. São Paulo: Prentice Hall. 4ª edição.

Tanenbaum, A. S. (2003) “Redes de computadores”. Rio de Janeiro: Elsevier. 4ª edição.