UNIVERSIDADE SAGRADO CORAÇÃO

VINICIUS SANTOS SANCHEZ

NEGAÇÃO DE SERVIÇOS: ANÁLISE COMPARATIVA ENTRE PROGRAMAS DE ATAQUES DoS E PROPOSTA DE DEFESA

BAURU
2014

VINICIUS SANTOS SANCHEZ

NEGAÇÃO DE SERVIÇOS: ANÁLISE COMPARATIVA ENTRE PROGRAMAS DE ATAQUES DoS E PROPOSTA DE DEFESA

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

2014

Sanchez, Vinicius Santos.

S2118n

Negação de serviços: análise comparativa entre programas de ataques DoS e proposta de defesa / Vinicius Santos Sanchez. -- 2014.

42f. : il.

Orientador: Prof. Dr. Henrique Pachioni Martins.

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

1. Ataques. 2. Negação de serviços. 3. DoS. 4. Defesa. 5. Monitoramento. I. Martins, Henrique Pachioni. II. Título.

VINICIUS SANTOS SANCHEZ

NEGAÇÃO DE SERVIÇOS: ANÁLISE COMPARATIVA ENTRE PROGRAMAS DE ATAQUES DoS E PROPOSTA DE DEFESA

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. Me. Henrique Pachioni Martins.

BANCA EXAMINADORA

_____

Orientador: Prof. Me. Henrique Pachioni Martins

_____

Examinador: Prof. Dr. Elvio Gilberto da Silva

_____

Examinador: Prof. Esp. André Luiz Ferraz Castro

DATA: 10/12/2014

AGRADECIMENTOS

Primeiramente agradeço a minha família, por sempre ter me apoiado e acreditarem em mim, em especial Ana Rita Pronunciatti Pailo.

Aos amigos do curso, em especial Henrique Hiroshi Makita e Renan Rocha.

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

RESUMO

O ataque de negação de serviço começou a se tornar algo preocupante até mesmo para as grandes empresas como: The New York Times, Amazon.com, Mastercard, Visa, entre outros, que tiveram seus sites tirados do ar como foi demonstrado na mídia, devido algum ataque dessa natureza. Existem softwares como firewalls e antivírus que protegem, porem até mesmo estes estão sujeito a falhas devido à complexidade dos ataques ou software maliciosos, uma vez que estes estão se tornando cada vez mais utilizados. O ataque de negação de serviço, ao contrário de outros, não rouba, não altera e nem exclui as informações da vítima, ele sobrecarrega o serviço gerando requisições contínuas e ilegítimas deixando de atender as solicitações legitimas dos demais usuários. Dentro deste contexto este trabalho propôs uma solução para estes ataques, para aumentar e melhorar a segurança das empresas. Foi analisado duas ferramentas em funcionamento e uma defesa para os ataques. Como resultado obteve-se que uma das ferramentas de ataque demonstrou ser mais eficiente com relação a outra, fazendo com que o servidor não respondesse a novas requisições. Apesar disso a segunda ferramenta causou instabilidade do servidor elevando o uso do processamento do mesmo. A ferramenta de defesa se mostrou insatisfatória para o objetivo não cessando o ataque, apenas conseguiu diminuir o tráfego da rede pela metade.

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

ABSTRACT

The denial of service attack started to become something disturbing even for large companies such as The New York Times, Amazon.com, Mastercard, Visa, among others, who had taken down their sites as demonstrated in the media, due an attack of this nature. There antivirus software and firewalls and protecting, however even these are subject to failure due to the complexity of malicious software or attack, since they are becoming increasingly usefully. The denial of service attack, unlike others, does not steal, does not change and nor does it exclude the victim's information, it overloads the service generating continuous requests and illegitimate failing to meet the legitimate requests of other users. Within this context this paper proposed a solution to these attacks, to increase and improve the security of companies. Was analyzed two tools in operation and a defense for the attacks. As a result was obtained that one attack tools proved to be more efficient with respect to another , so that the server does not respond to new requests. Despite this, the second tool increasing instability caused server using the same processing. The defense tool proved unsatisfactory for the purpose not stopping the attack , only managed to reduce network traffic by half.

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

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

DoS - Denial of Service

DDoS - Distributed Denial of Service

FTP – File Transference Protocol

OSI – Open System Interconnection

TCP/IP – Transmission Control Protocol/Internet Protocol

SUMÁRIO

1 INTRODUÇÃO

A internet hoje proporciona conteúdo aos usuários que antes não se imaginavam, dentre eles estão: entretenimento, informação, serviços, educação e transações de dinheiro online. O que parece comum hoje, que temos acesso em um clique ou um toque na tela, antes não existia.

Porém, além de trazer muita coisa boa para a sociedade moderna, ela trouxe também sua dependência. Para comprovar isso, podemos citar as redes sociais, onde crianças, jovens e adultos passam horas conectados, seja interagindo com outras pessoas ou apenas verificando atualizações do seu círculo social.

No mundo econômico, as transações são de extrema importância, o que demanda disponibilidade total para abranger todas as empresas e clientes. Porém, se esses serviços fossem cortados ou derrubados por tempo indeterminado, acabaria gerando desconforto, revolta e etc.

Além disso a internet pode ser usada para diversos fins, tanto para produzir algo, quanto para degradar. Na internet as pessoas tem a liberdade de pesquisar o que quiserem, dar suas opiniões e usa-la a seu favor para diversos fins.

A internet muitas vezes se torna palco de conflitos de todos os gêneros, em redes sociais, servindo para auxiliar em crimes, derrubando os serviços (sites de bancos, do governo, de órgãos públicos, e etc.), muitas vezes como forma de protesto e algumas por vontade própria, e até como espionagem, como atualmente acontece entre os países.

É nesse contexto de conflitos que se encaixa o DoS. Apesar de não ser um tipo de ataque que rouba informações, ou que cause perda dos arquivos da vítima, ele causa a instabilidade e até a negação desse serviço, ou seja, se um site de um banco fosse atacado, este causaria a instabilidade, ou em alguns casos, iria derrubar o site, deixando o servidor sobrecarregado, e inacessível para os clientes e empresas conveniadas ao banco. Com o serviço fora do ar, geraria prejuízo para o banco e seus clientes.

Apesar desses ataques serem muitas vezes de origens desconhecidas e acontecerem sem aviso prévio, existem ferramentas que detectam essa sobrecarga no servidor e identificam o atacante, bloqueando assim seu acesso aos servidores, o que cancelaria um possível ataque.

A internet possibilita conhecimento nas mais diversas áreas atualmente. Quando se trata de técnicas hacker, existem muitas pessoas interessadas nesse assunto, sendo possível encontrar sem muita dificuldade, manuais e vídeos que demonstram como usar as mais variadas ferramentas existentes. Sendo assim, qualquer pessoa com um pouco de conhecimento sobre software e Linux, consegue executar de alguma forma um ataque.

Justifica-se então o desenvolvimento desse trabalho o intuito de contribuir para garantir maior segurança dos servidores que disponibilizam serviços pela internet, analisando a forma em que as ferramentas de ataques DoS agem e implantando o software que os protege desse tipo de ataque, visando manter o serviço sempre disponível, e seu funcionamento adequado.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Demonstrar ataques DoS (Denial of Service) em ação com duas ferramentas e elaborar um comparativo entra elas. Será apresentado também uma possibilidade de defesa desse tipo de ataque de negação de serviços.

1.1.2 Objetivos Específicos

- Simular duas ferramentas atacando um servidor apache (servidor web) instalado em outro computador.
- Comparar as duas ferramentas, analisando qual será mais rápida, mais eficaz e ao mesmo tempo analisar o nível de complexidade de implementação das mesmas.
- Realizar monitoramento do servidor por um software para analisar seu comportamento durante um ataque DoS.
- Implementar um software no servidor web, que defenda os ataques realizados e analisar a eficácia do software perante dois ataques de software diferentes.
- Elaborar um comparativo entre os dois softwares de ataque e monitorar o servidor antes e depois dos ataques com o software de defesa ativo.

2 REDES

O termo redes de computadores foi incialmente utilizado no século XX para denominar um conjunto de dispositivos interligados por meios de comunicação geralmente denominados como nós. Tudo o que conhecemos hoje em empresas e internet foi resultado de necessidade de requisição de informações a distância.

As redes de computadores servem de base para os softwares que são implementados em cima dessa estrutura que são os sistemas distribuídos.

O uso de sistemas distribuídos hoje são indispensáveis para empresas, que se baseiam em relatórios em tempo real de suas filiais, por exemplo, para tomada de decisões, para elaboração de um novo projeto e etc. Por essa interconexão é possível administrar com maior eficiência, possibilitando obter informações de filias mais remotas geograficamente sem dificuldades.

O termo sistemas distribuídos é diferente de rede de computadores, sistemas distribuídos caracteriza-se como a camada de software aplicada em cima de uma rede para manipular as informações que circulam entre os computadores interligados. Rede de computadores não possui uma ferramenta para mostrar para o usuário, por exemplo em forma de documento, como acontece nas páginas da internet. (TANEMBAUM, 2003).

O processamento distribuído é muito usado atualmente, pois ele executa uma tarefa entre workstations, ou estações de trabalho, o que se torna mais eficiente do que concentrar todo o processamento a uma única máquina responsável pelo controle da rede.

Segundo Fourouzan (2006), as redes podem também ser comparadas seguindo alguns critérios:

- Performance: ela pode ser medida de diversas formas, incluem-se o tempo de trânsito e o tempo de resposta. O tempo de trânsito é o tempo gasto para uma mensagem passar de um dispositivo para o outro. O tempo de resposta é o tempo decorrido entre uma solicitação e uma resposta.
- Confiabilidade: Além da garantia de entrega, a confiabilidade de uma rede é medida pela frequência de falhas, o tempo de reconfiguração de um link após uma falha, e a robusteza da rede em uma catástrofe.

- Segurança: é um critério cuja a finalidade é assegurar a proteção dos dados e das informações que trafegam na rede ao acesso não autorizado.

As redes possuem como meio de comunicação os links, por onde os dados passam de um dispositivo para outro, ou seja, para que a comunicação aconteça os dois dispositivos devem estar interligados através desse link. Há duas formas possíveis de conexão, a “ponto a ponto” e a “multiponto”.

A conexão ponto a ponto e determinada por possuir apenas um link interligando dois dispositivos, e através deste ocorre a transferência dos dados entre os “nós”, como são chamados os dispositivos conectados à rede.

A conexão multiponto é caracterizada por três ou mais computadores que compartilham o mesmo link de comunicação.

2.1 TOPOLOGIAS

Topologias são as formas como as estações ou hosts estão associados, existindo duas formas básicas: ponto-a-ponto e difusão (ou Multiponto).

A conexão “ponto-a-ponto” é considerada uma rede composta por diversas linhas de comunicação associadas a um par de estações de cada vez. A comunicação entre estações não adjacentes são feias por estações intermediárias, conhecido como “comutação de pacotes”, e é a topologia usada na maioria das redes WAN, MAN, e algumas LAN’s, como a topologia em anel e estrela por exemplo.

A difusão é considerada uma rede composta por uma única linha de comunicação compartilhada entre todas as estações. As mensagens são difundidas no canal ou linha e podem ser lidas por qualquer estação, porém a mensagem é identificada com o endereço do destinatário codificado na mensagem, sendo assim, é possível enviar mensagens para todas as estações (broadcasting) ou para um conjunto (multicasting) usando estes endereços reservados. Esta topologia é mais comum em LAN mas também é possível aplica-la em WAN, porem requer mecanismos de arbitragem de aceso para evitar conflitos. (ROSS, 2010).

2.1.1 Topologia em Anel

Na topologia em anel os componentes da rede são capazes de enviar e receber dados em qualquer direção, porém as mais utilizadas são as unidirecionais, ou seja, que se comunicam em um único sentido a fim de tornar os protocolos de comunicação menos complexos assegurando a entrega da mensagem corretamente e em sequência no destino.

Quando uma mensagem é enviada, ela caminha pelo anel que é um caminho fechado, até chegar no destino ou quando não encontra o destino ela retorna a fonte, dependendo do protocolo utilizado. A vantagem desta topologia que ela permite o envio simultâneo. (ROSS, 2008).

2.1.2 Topologia em Estrela

Nesta topologia os nós que compõem a rede são interligados através de um controlador que geralmente é denominado hub, sendo este responsável por fazer envio das informações para o nó correto de acordo com seu endereço na rede. Uma das grandes vantagens desta topologia é que se algum dos nós ou algum link estiver fora de operação, isto não comprometerá a comunicação entre os outros nós que estão ligados neste hub. (MARIMOTO, 2014).

2.1.3 Topologia em Barramento

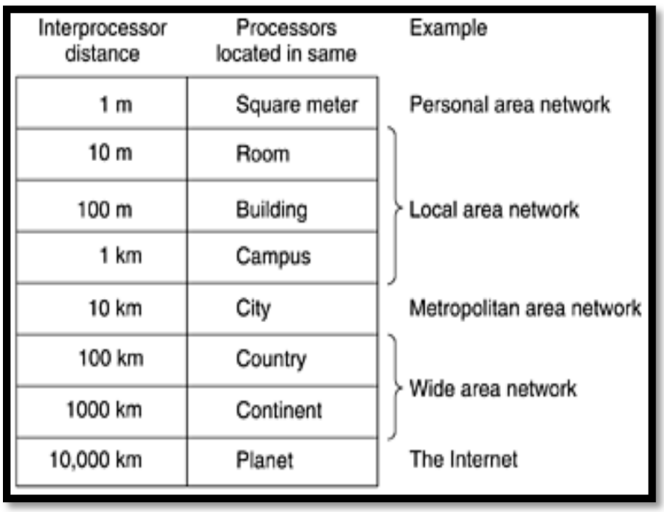
Esta topologia possui como elemento central da estrutura um backbone (espinha dorsal), onde todos os nós da rede são interligados. Este é um fio onde dele saem pequenos segmentos de cabos que vão até o nó que será interligado na rede. Esta é uma característica que determina que esta topologia seja geralmente multiponto. (ALENCAR, 2012).

2.1.4 Topologia em Malha

Nesta topologia cada nó da rede possui um link dedicado, o que significado que a comunicação é exclusiva entre os dois nós interligados. Geralmente cada nó é interligado diretamente aos outros que estão na rede. (FOROUZAN, 2006).

2.2 CLASSIFICAÇÃO DAS REDES

Hoje, podemos considerar três tipos básicos de redes: a rede local, a rede metropolitana e a rede geograficamente distribuída. Sendo que o que as diferenciam são tecnologias de transmissão, topologia e tamanho.



Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Figura 1 – Classificação das redes por escala.
Fonte: Tanembaum (2003).

Na Figura 1 pode-se observar uma classificação das redes de acordo com a distância que ela se alonga para interligar os elementos que a compõem. No caso de da distância atingir 10 metros a 1 quilômetro ela é considerada uma LAN, se for de 10 quilômetros aproximadamente ele é uma MAN, ou se ainda for de 100 quilômetros até 1.000 quilômetros ela passa a ser WAN, se caso foi maior que a WAN ela é considerada a Internet em si.

2.2.1 Rede Local (LAN – Local Area Network)

É um conjunto de dispositivos interligados dentro de campus, empresas ou escritórios, compartilhando informações e dispositivos, como por exemplo impressoras. As redes LAN's como o próprio nome sugere, são redes locais que possuem tamanho restrito e por esse limite permite a utilização de determinados projetos que em outras circunstâncias seriam inviáveis, simplificando também seu gerenciamento e possibilitando implementar topologias diferentes dependendo do que se pretende elaborar.

A velocidade dessas LAN's variam de 1 Mbps (megabytes por segundo), até 100 Mbps. Porém com as evoluções das redes essas velocidades foram melhoradas e hoje, dependendo do equipamento de transmissão em que a rede está interligada, pode chegar até 10 Gbps (gigabytes por segundo) ou até mais, dependendo da tecnologia.

2.2.2 Redes Metropolitanas (MAN – Metropolitan Are Network)

As redes MAN's abrangem uma área muito maior que uma LAN, conectando um maior número de dispositivos abrangendo até um cidade. Possuem como característica uma área de abrangência de 10 Km.

2.2.3 Redes Geograficamente Distribuídas (WAN – Wide Area Network)

São redes capazes de interligar países e até continentes com distâncias de 100 até 1000 Km. Tanembaum (2003) descreve a WAN como uma rede que contém um conjunto de máquinas com a finalidade de executar programas/aplicações do usuário. Os hosts são as máquinas que pertencem ao usuário e são conectados a uma sub-rede que geralmente são as operadoras de telefonia ou provedores de acesso à internet. A tarefa da sub-rede é transportar mensagens de um host para o outro. A ligação dessas sub-redes é que formam a WAN, assim como a ligação das redes LAN's formam as redes MAN.

2.3 MODELOS DE REFERÊNCIAS

Existem dois modelos importantes de arquiteturas de rede, o modelo OSI e o TCP/IP. Essas arquiteturas são padrões definidos que possibilitam a comunicação de diversos equipamentos para diferentes fins. Hoje existem uma variedade de dispositivos, seja a nível corporativo ou até mesmo residencial.

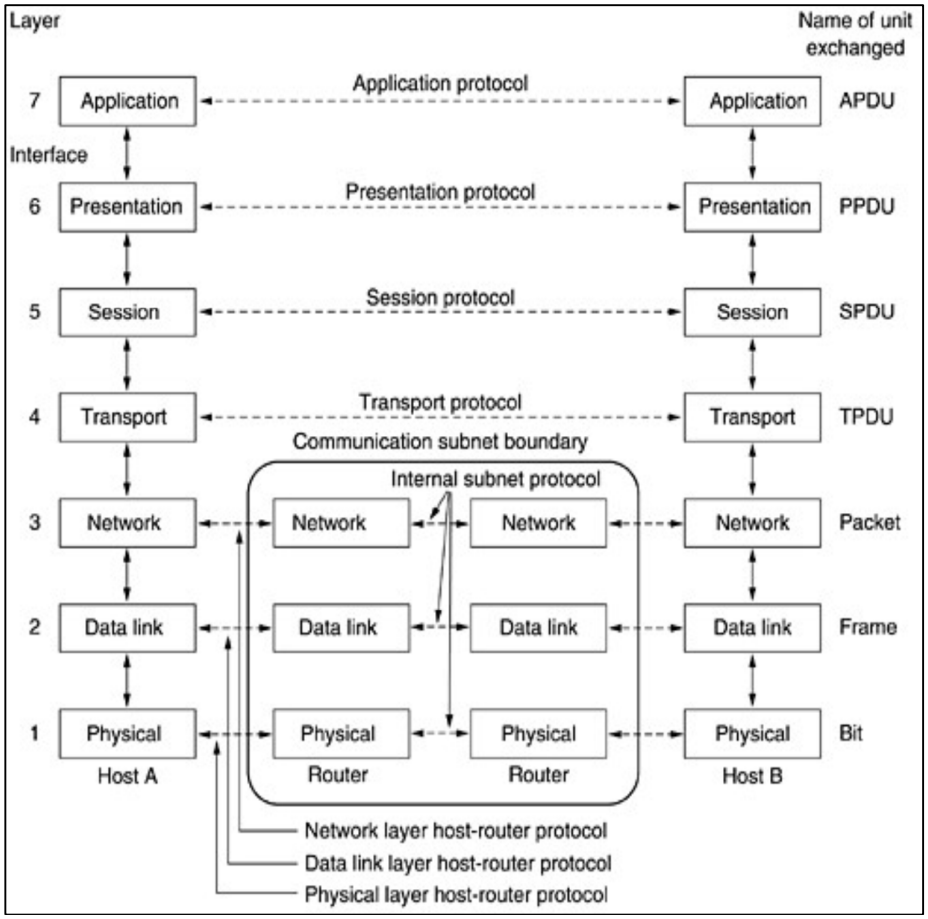
Estes dispositivos necessitam se comunicar para realizar as mais diversas funções para as quais foram criados, temos impressoras, celulares, tablet's, televisores, entre outros que possuem a capacidade de se conectar à internet, ou trocar informações entre si. Isso só é possível por seguirem um padrão de comunicação. (PINHEIRO, 2002).

2.3.1 Modelo de Referência OSI

O modelo OSI (Open Systems Interconnection) foi uma proposta desenvolvida pela ISO (International Standards Organization) com a intenção de padronizar os protocolos empregados nas diversas camadas em que as redes se dividem. O modelo de referência OSI trata de interconexão de sistemas abertos, ou seja, sistema que estão abertos a comunicação com outros sistemas, para abreviar pode ser chamado simplesmente de modelo OSI. (TANEMBAUM, 2003).

Este modelo possui sete camadas, são elas: física, enlace de dados, rede, transporte, sessão, apresentação e aplicação. As camadas são definidas na sequencia como pode ser visto na Figura 2, onde cada camada possui sua função específica.

Figura 2 – Modelo OSI.



2.3.1.1 Camada física

Está é responsável pela transmissão dos bits pelo canal de comunicação. Está camada possibilita a transmissão de pulsos elétricos que representam os bits, e é responsável por controlar se os bits podem trafegar nos dois sentidos, quantidade de tempo que este ficará ativo, forma de conexão inicial (sincronização) e a função de controlar a quantidade de pinos que o conector deve ter e a função de cada um. (PINHEIRO, 2002).

2.3.1.2 Camada de enlace de dados

Responsável por transformar um canal de transmissão em uma linha que pareça livre de erros de comunicação para a camada de rede. Eles dividem os bytes em quadros de uma certa quantidade para tornar mais fácil a confirmação de recebimento, enviando o quadro recebido. (ALENCAR, 2012).

2.3.1.3 Camada de rede

Controla a operação da sub-rede, determinando a maneira de como os

Fonte: Tanembaum (2003).

pacotes são roteados até a origem de destino. As rotas podem ser baseadas em tabelas estáticas, pré-definidas pela rede ou altamente dinâmicas sendo definidas a cada pacote, refletindo a carga atual da rede. Se houver muitos pacotes trafegando na sub-rede ao mesmo tempo, eles dividem o mesmo caminho provocando gargalos. (MORIMOTO, 2014).

2.3.1.4 Camada de transporte

Aceita os dados da camada acima dela, dividindo-os em unidades menores se necessário repassando para a camada de rede. Ela deve assegurar que todos os dados cheguem até a outra extremidade. Isso deve ser feito de modo que as camadas superiores fiquem isoladas das inevitáveis mudanças de tecnologia de hardware. (TANEMBAUM, 2003).

2.3.1.5 Camada de sessão

Permite que os usuários de diferentes máquinas estabeleçam sessões entre eles, possibilitando a troca de informações. (ALENCAR, 2012).

2.3.1.6 Camada de apresentação

Está relacionada a sintaxe e semântica das informações transmitidas. Para elementos da rede que tratam de representações de dados diferentes, as estruturas desses dados podem ser abstraídas juntamente com uma codificação padrão que será usada durante a conexão. (MORIMOTO, 2014).

2.3.1.7 Camada de aplicação

Contém uma série de protocolos comumente necessários para os usuários, como por exemplo o HTTP, POP3, IMAP, RSS, FTP, entre outros. (TANEMBAUM, 2003).

2.3.2 Modelo de Referência TCP/IP

Figura 3 – Modelo de camadas TCP/IP.

Fonte: Forouzan (2006).

Esse modelo é composto de cinco camadas diferente do modelo OSI, e são organizadas como pode ser visto na Figura 3. É suportado por praticamente todos os sistemas operacionais e permite que computadores de arquiteturas totalmente diferentes como, PC's, Mac's, Mainframes e até telefones celulares, tablets e demais dispositivos que tenham conexão com a internet atualmente.

2.3.2.1 Camada física

É responsável por transmitir uma cadeia de bits num meio físico específico. Nesta também são tratadas as especificações elétricas e mecânicas de uma interface e do meio de transmissão. (FOROUZAN, 2006).

2.3.2.2 Camada de enlace de dados

A camada de enlace de dados é responsável por converter os mais variados tipos de bits que vem da camada física, em um link seguro para passar este dados a camada acima, a de rede. (ALENCAR, 2012).

2.3.2.3 Camada de rede

Uma das funções principais da camada de rede, é possibilitar o roteamento dos pacotes da rede para que estes possam sair da fonte e chegar ao seu destino. Este roteamento é feito por dispositivos como roteador e switch, eles possuem tabelas com os endereços de cada elemento da rede, e com isso elabora rotas eficientes para que o pacote trafegue de um dispositivo para o outro. (ALENCAR, 2012).

2.3.2.4 Camada de transporte

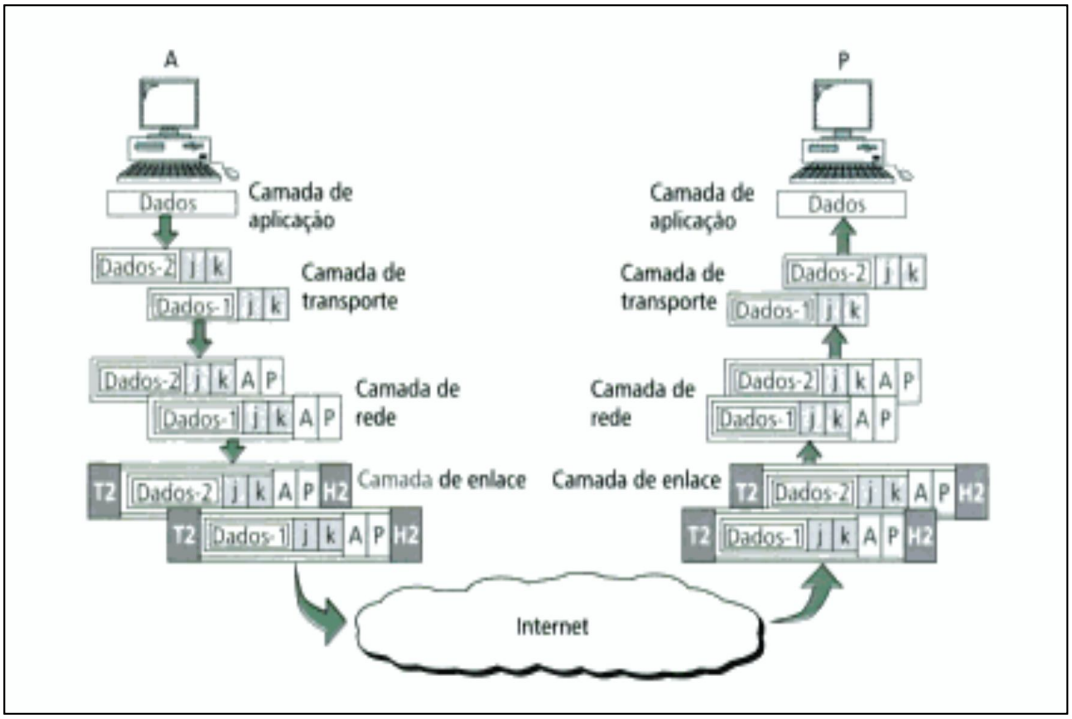
Está camada assegura que a informação ou pacotes cheguem intactos e livres de erros para o dispositivo que irá receber. Ela controla o fluxo do link e também faz endereçamento das portas, que é um endereço em cada pacote que trefega na rede recebe, para serem encaminhados para um processo especifico em seu destino. (MORIMOTO, 2014).

2.3.2.5 Camada de aplicação

Esta camada permite o acesso a rede pelos usuários finais, tanto softwares ou humanos. Ela suporta serviços como transferência de arquivos, acesso a World Wide Web, log-in remoto (acesso a computadores sem estar próximo do mesmo), e-mails, entre outros. (MORIMOTO, 2014).

A Figura 4 mostra onde cada camada do protocolo se encontra em uma simulação de tráfico de dados pela rede. A camada de aplicação é a mais próxima do usuário, onde executa as requisições de informações ou o envio delas, estes dados são encaminhados para a camada de transporte controla o fluxo do link e endereça os pacotes com o seu respectivo destino. A camada de enlace de dados cria uma caminho seguro livre de erros para os dados seguirem para a internet.

Figura 4 - Funcionamento do TCP/IP.



Fonte: Forouzan (2006).

Quando estes pacotes chegam no dispositivo de destino acontece o processo inverso, até chegar na camada de aplicação onde o usuário final poderá ver o resultado de sua requisição. (FOROUZAN, 2006).

3 GERENCIAMENTO DE REDES

O objetivo do gerenciamento das redes é garantir que a mesma tenha seu funcionamento adequado e com a melhor qualidade possível. Para isso é necessário monitorar os elementos que a compõem para ter um diagnóstico de como está seu funcionamento para então tomar providências se necessário.

Para realizar esse monitoramento dos elementos (físicos ou lógicos) da rede, são necessários softwares que são capazes de medir a qualidade e a estabilidade da rede. Existem hoje software com propósitos gerais de monitoramento, e também para monitoramentos específicos, sendo possível gerenciar configurações, falhas, segurança, contabilização, entre outros.

O gerenciamento pode ser definido como coordenação de recursos matérias ou lógicos, fisicamente distribuídos na rede afim de assegurar o tempo de resposta aceitáveis confiabilidade e segurança da informação.

Pode ainda se resumir em três etapas:

1. Coleta de dados: processo que monitora os recursos gerenciados.
2. Diagnóstico: Trata e analisa as informações adquiridas na coleta de dados.
3. Ação/Controle: Uma vez detectado uma anomalia é necessária uma ação ou controle caso o evento não tenha sido resolvido, ou voltar a aparecer.

O gerenciamento em si pode ser centralizado em um processador central ou distribuídas em diversos locais. Dentro deste contexto, é importante se destacar as MIB's (Management Information Base) que segundo Pinheiro (2002) é um banco de dados que armazena informações referentes a todos os recursos gerenciados.

As MIB's são definidas em termos de atributos (propriedades dos objetos gerenciados), operações que são as ações que os agentes submetem ao gerente para informar sobre a ocorrência de eventos, notificações que os agentes enviam aos gerentes para informar eventos e relações que são as formas de comunicações entre os objetos. (PINHEIRO, 2002).

3.1 SNMP

O SNMP (Simple Network Management Protocol) é um protocolo da camada de aplicação usado para efetuar o gerenciamento de redes. Através deste protocolo é possível obter informações sobre os elementos que compõem a rede através de um computador chamado de "gerente".

Ao invés de utilizar o modelo cliente/servidor, o SNMP utiliza o conceito de gerentes e agentes. O gerente será o responsável por adquirir as informações dos agentes que são os dispositivos conectados na rede, e atualizar o gerenciamento local baseado nas informações adquiridas com os pedidos feitos aos agentes, gerando gráficos e enviando notificações no caso de anomalias para o administrador. (MAURO, 2005).

Os agentes enviam informações do estado atual da máquina como uso de CPU, uso de memória, uso de recursos de rede. Essas informações chegam ao gerente onde geralmente possui um software que manipula essas informações gerando gráficos para o administrador analisar e tomar as devidas providencias. (MAURO, 2005).

Atualmente o SNMP pode ser usado tanto no sistema operacional Windows como no Linux. Para a versão Windows, é preciso adicionar o recurso no painel do controle do sistema na opção de programas e recursos, e adiciona-lo. Para o Linux é necessário executar alguns comandos para efetuar a instalação deste protocolo.

Os materiais necessários sobre o protocolo podem ser acessados no site da Microsoft, que também é a criadora do WinSNMP API, que é uma biblioteca que possui comandos encapsulados para auxiliar no desenvolvimento de programas que gerenciam o SNMP.

O protocolo possui 3 versões, o SNMPv1, SNMPv2 e SNMPv3. O que muda entre as versões são algumas melhorias e concertos de bugs que foram encontrados no uso. Apesar disso, na prática ele responde aos comandos perfeitamente em qualquer umas das versões. (MICROSOFT, 2014).

3.2 CACTI

O software Cacti é uma ferramenta para gerenciamento de redes muito eficaz, mostrando o estado atual da rede através de gráficos. Esta ferramenta utiliza o protocolo SNMP para envio de requisições aos elementos da rede e recebe como resposta o estado atual, como uso de banda e CPU, do elemento em questão e o Apache PHP[1].

Assim como todas as ferramentas administrativas de rede, o Cacti é importante para manter a rede segura e disponível, pois qualquer anomalia identificada nos elementos que estão sob controle deste software, será reportada para o administrador da rede, ou a pessoa responsável pela estrutura da mesma, e este será responsável por tomar as devidas decisões para normalizar os serviços. (COSTA, 2008).

Além de adquirir informações do estado das máquinas, a ferramenta ainda monta gráficos com estas informações para tornar o monitoramento mais fácil de ser interpretado, sendo necessário apenas se atentar aos gráficos para detectar possíveis anomalias na rede.

Este software utiliza a ferramenta RRDTool que pega os dados armazenados dos agentes, e transforma essas informações em gráficos para fácil gerenciamento e para servir de base também a outros sistemas com a mesma finalidade do Cacti.

O software possui toda a sua interface orientada em PHP (Personal Home Page) e as informações são passadas para ele através de scripts, ou de softwares personalizados pelo usuário. Os dados recebidos são armazenados no banco de

[1] O Apache é compatível com o protocolo HTTP e geralmente ativado em servidores para hospedagem de sites. Suas funcionalidades são mantidas através de uma estrutura de módulos envolvendo tecnologias de transmissão via web.

dados, que no caso é o MySQL, e os gráficos são montados a partir dos resultados registrados no banco de dados. (CACTI, 2014).

4 SOFTWARE LIVRE

Software é um conjunto de linhas/comandos, que são interpretados pelo computador, que tem uma determinada função para a qual foi desenvolvido. Segundo Anunciação (2007), para ser considerado software livre, o mesmo deve respeitar o senso de comunidade dos usuários assim como a liberdade de modifica-lo se for de interesse do usuário.

Hoje utilizamos os softwares para realizar qualquer tarefa diária, desde o aplicativo do celular até o programa que é usado nas empresas. É uma variedade muito vasta de categorias existentes hoje, que são capazes de fazer diversas tarefas do dia-a-dia, tanto para o meio corporativo quanto para o de entretenimento. (ANUNCIAÇÃO, 2007).

A característica do software livre é a capacidade de poder modifica-lo, controlando-o e aprimorando o que este faz pelo usuário. Muitas pessoas entendem software livre como preço quando na verdade deve ser entendido como liberdade de expressão. Quando o usuário não possui a capacidade de controlar o que o software faz, o programa o faz. Logo o respectivo desenvolvedor deste o controla, passando assim a ideia de que manipula o usuário de certa forma. (OLIVEIRA, 2009).

Como exemplos de softwares livres existentes hoje, pode-se citar o Linux e suas derivadas distribuições, LibreOffice ou BrOffice que é uma alternativa aos software da empresa Microsoft, Blender que é uma ótima ferramenta de modelagem e animação 3D, entre outros.

4.1 LINUX

O Linux possui como base o Unix, que é um sistema operacional de grande porte. Seu nome vem do seu criador Linus Torvalds, logo a junção de Linus + Unix originou o nome Linux.

O sistema Unix teve origem na década de 1960, envolvendo empresas, universidades e laboratórios, entre eles o MIT (Massachusets Institute of Technology), a GE (General Eletric), a AT&T (American Telephone and Telegraph) entre outros, que desenvolveram um sistema chamado Multics. O sistema não

atingiu seus objetivos, e algumas empresas envolvidas no projeto acabaram saindo. (BRASIL..., 2014).

Após o desenvolvimento do Unix, surgiu um outro sistema que também o possui como base que é o Minix, que era totalmente gratuito e com seu código fonte aberto, ou seja, sendo possível um programador experiente alterar seu código, modificando suas funções conforme a vontade do mesmo. (ANUNCIAÇÃO, 2007).

Linus Torvalds que era um estudante de Ciências da computação da Universidade de Helsinki, na Finlândia, por hobby decidiu fazer um sistema mais poderoso que o Minix. No mesmo ano, Linus desenvolveu o kernel, que é a base dos sistemas operacionais, de seu sistema. Porem em si ele só era um kernel, foi então que ele começou usar programas da GNU (que é um projeto com objetivo de desenvolver um sistema operacional compatível com o Unix).

Foi nesse contexto em que o Linux começou a ganhar notoriedade, juntando o kernel desenvolvido pelo Linus com os programas do projeto GNU (. O Linux também está sob a licença GPL, que permite que qualquer pessoa possa usar os programas que estão sobre ela, com o compromisso de não tornar os programas fechados e comercializados. Resumindo, pode-se alterar os programas e até vende-lo, porém não pode ser fechado (o código do mesmo) nem vendido. (ANUNCIAÇÃO, 2007).

4.2 BackTrack

É uma ferramenta Linux baseada no WHAX, Whoppix e Auditor (ferramentas para auditoria, testes de sistemas e redes) voltada para testes de penetração, usada por analistas de segurança de redes e sistemas, hackers “éticos”, auditores, entre outros.

As primeiras versões do sistema foram lançadas no ano de 2006 e 2007, com poucas ferramentas de testes. Atualmente, em sua última versão lançada em 2012 (BackTrack 5 R3), possui mais de 300 ferramentas para testes de penetração.

Existem algumas certificações que se baseiam no BackTrack como ferramenta principal como OSWP (Offensive Security Wireless Professional), OSCE (Offensive Security Certified Expert) e OCSP (Offensive Security Certified Professional). Essas certificações são oferecidas pela Offensive Security, empresa responsável por manter o BackTrack.

A última versão do BackTrack foi a versão 5 R3, após esta versão, foi desenvolvida uma nova versão, com mais ferramentas chamada Kali Linux, apesar disso, mantem as mesmas ferramentas da antiga versão em funcionamento. (GIAVAROTO, 2013).

4.3 CentOS

É uma distribuição do sistema Linux voltada para servidores, sendo considerada estável por ser sistema “clone” da distribuição paga do Linux Red Hat Enterprise Linux (RHEL). É compatível com os mesmos pacotes de atualização do RHEL e é derivado de código fonte livremente prestados ao público pela Red Hat.

Este sistema começou a ser desenvolvido com um grupo pequeno de desenvolvedores, porém como toda distribuição Linux, possui uma grande comunidade de usuários e desenvolvedores dispostos a realizar testes, melhorias e elaborar o feedback para os desenvolvedores responsáveis, com isso eles desenvolvem versões melhores do sistema com qualidade maior e mais estável.

Algumas empresas já adotaram o sistema para prestar serviços de hospedagem, como por exemplo a HostGator, que já oferecem sistema para seus clientes. Apesar de ser relativamente novo, já se mostra digno de confiança. (CENTOS, 2014).

4.4 PERL

É uma linguagem de programação criada por Larry Wall enquanto ele trabalhava no laboratório da NASA (Jet Propulsion Labs). É uma linguagem estável e multiplataforma, e é um software livre disponível sobre a licença GPL (General Public License).

Inicialmente foi projetada para manipulação de textos e para ser prática, ou seja, de fácil uso, eficiente e completa. Hoje é usada para as mais variadas tarefas como administrar sistemas, desenvolvimento WEB, programação de redes, desenvolvimento de interfaces gráficas entre outros.

Ela herda características das linguagens C, BASIC entre outras. Possui uma interface de integração com o banco de dados (DBI) suportando vários tipos de bancos como o MySQL, Postgre, Oracle, Sybase entre outros. Possui suporte à programação procedural (execução via console) e também a orientação de objetos (interfaces gráficas). (PERL...,2014).

5 SEGURANÇA DA INFORMAÇÃO

Hoje com a influência da internet, com tudo o que ela pode nos oferecer, fica impossível de pensar em não usufruir das oportunidade e benefícios que ela nos traz, isso tanto para o lado corporativo, como para o lado dos usuários normais. Com ela é possível fazer movimentação da conta bancária, administrar sem estar no local, vídeo conferencias, entretenimento, entre outros.

Dentro deste contexto a informação é considerada algo muito importante. As empresas estão vivendo um momento globalizado e competitivo, tornando a informação algo essencial para sua existência. Com as informações é possível elaborar planejamento, ter controle do estado atual da empresa e elaborar plano de contingências.

Sendo assim a informação pode ser considerada um ativo da empresa de suma importância para seus negócios, logo esta deve ser devidamente protegida. Segundo a norma NBR ISO/IEC 27002 (CUNHA, 2014), essa proteção ou segurança pode ser obtida a partir de um conjunto de controles adequados.

Esses controles se referem aos procedimentos, políticas, processos, estruturas organizacionais funções de hardware e redes, entre outros. Eles precisam ser estabelecidos, monitorados, implementados, analisados e melhorados. Este controle garante o atendimento do objetivo do negócio e preza a segurança da organização.

Resumidamente segurança da informação é a proteção da informação em si de diversos tipos de ameaças. Esta proteção garante a continuidade do negócio, minimiza os riscos, maximiza o retorno sobre os investimentos e maximiza também as oportunidades de negócio. (CUNHA, 2014).

6 ATAQUE DoS

O ataque DoS (Denial of Service, em português, Negação de serviço) é um tipo de ataque de internet feito para sobrecarregar o servidor em que a aplicação alvo está hospedada, como por exemplo sites de governo, bancos, entre outros, impedindo que outros usuários tenham acesso a este serviço.

Este tipo de ataque é feito por uma máquina utilizando técnicas específicas para forçar o servidor a responder solicitações, ou seja, o atacante tem como objetivo fazer com que os serviços tenham acesso impossibilitado.

Uma das técnicas utilizadas é o SYN Flooding, em que o computador tenta estabelecer comunicação com o servidor com o sinal (SYN – syncronize), quando a conexão está ativa o servidor envia como resposta um sinal chamado de ACK (acknowledgement - reconhecimento). O problema é que o servidor possui limite para responder às solicitações que chegam até ele. Quando este é atingido ele passa a recusar novos pedidos, impossibilitando novos acessos de outros usuários.

Apesar de deixar o servidor instável, este tipo de ataque não rouba, altera ou exclui as informações do alvo, ao contrário de outros ataques. O que torna esse tipo de ataque mais preocupante é que as ferramentas utilizadas para este fim são encontradas com muita facilidade hoje, estando disponível não apenas para hacker, mas para qualquer pessoa que consiga seguir um breve manual na internet. (DUARTE, 2014).

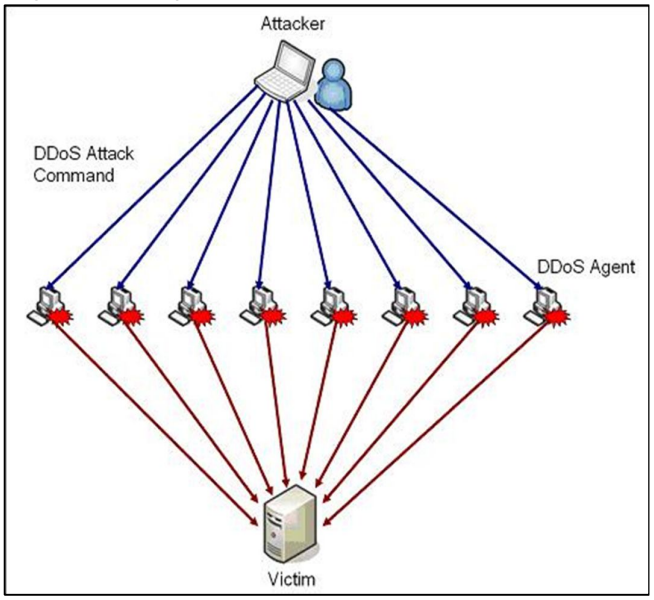
6.1 ATAQUE DDoS

Este tipo de ataque é parecido com o DoS, porém com o diferencial de usar várias máquinas infectadas para ajudar no ataque, ampliando a capacidade do mesmo. Hoje, com avanço da tecnologia, principalmente dos servidores, em alguns casos apenas atacando de uma única máquina, não é possível impedir o funcionamento do mesmo. É nesse contexto em que o DDoS (Distributed Denial of Service) se torna necessário.

Nele o atacante tem que infectar outras máquinas conectadas na internet (que são chamadas de zumbis) geralmente com softwares maliciosos, como vírus por exemplo, para poder controla-las e usa-las para efetuar o ataque à vítima. Nesses ataques são esgotados os recursos de rede da vítima fazendo com que perca conexão com a internet, esgotando o bandwidth (largura de banda de acesso à internet) quando o ataque está em execução.

A Figura 5 ilustra de forma resumida como o ataque acontece, o Attacker (atacante), infecta as demais maquinas conectadas a internet e instalam as ferramentas necessárias para usa-las a seu favor quando ativadas. Quando o atacante dispara o comando para iniciar o ataque, eles entram em ação mandando requisições para o servidor que no caso é o Victim (vitima), sobrecarregando o mesmo e assim derrubando o serviço que nele está hospedado. (LIMA, 2014).

Figura 5 – Ataque DDOS.



Fonte: Lima (2014).

6.2 FERRAMENTAS DE ATAQUE E DEFESA DE NEGAÇÃO DE SERVIÇOS

6.2.1 Slowloris

Esta ferramenta foi desenvolvida na linguagem de programação Perl e é usada para efetuar ataques a servidores com intenção de sobrecarrega-lo, causando instabilidade do mesmo e até fazendo com que este deixe de responder.

O software mantem o máximo de conexões abertas no servidor alvo e mantem elas o máximo possível. Também envia cabeçalhos HTTP que não possui conclusão de solicitação, com isso os servidores vão manter estas conexões simultâneas até a sua capacidade máxima, quando isso acontece, as novas tentativas de conexões de demais clientes são negadas.

Tal ferramenta funciona em sistemas Linux/UNIX e Windows, porém no sistema da Microsoft possui limite da quantidade de soquetes abertos você pode ter

em um determinado tempo, devido a isso o sucesso é maior com os sistemas Linux/Unix. (SLOWLORIS, 2014).

6.2.2 T-50

Esta ferramenta foi desenvolvida pelo brasileiro Nelson Brito, ela utiliza o método de injeção de pacotes realizando stress tests, podendo utilizar vários protocolos diferentes como TCP, UDP, ICMP entre outros.

Diferente do Slowloris, o T-50 utiliza apenas um soquete para efetuar a sobrecarga do servidor. O sistema utilizado para implementar essa ferramenta é o Linux/Unix. (BRITO, 2014).

Esta ferramenta foi desenvolvida originalmente para testar redes TCP/IP com o objetivo de baratear o custo de teste de tráfego em uma rede economizando na obtenção de novos equipamentos para este fim. Nelson (2014) alerta que o mal uso desta ferramenta pode causar oportunidades de ataques DoS e DDoS, porem o software é indicado apenas para pesquisas, e se isenta da utilização para estes fins.

6.2.3 (D)DoS Deflate

Quando se trata de ataques DoS e DDoS, não há nenhuma proteção completa contra este tipo de ataque, mas existem plataformas de segurança e ferramentas para amenizar seu efeito. Grandes empresas estão investindo pesado para assegurar que seus serviços não sejam interrompidos com este tipo de ataque. Porem empresas pequenas não possuem o mesmo potencial para investir.

Para este tipo de ameaça foi criado o (D)DoS Deflate, lançado como software de proteção para DDoS livres. Ele é um script (linguagens de programação executadas de dentro dos programas), shell bash (um interpretador de comandos entre o sistema e o usuário). É leve e auxilia no processo de bloquear um ataque DDoS criando uma lista dos IP’s conectados ao servidor e o seu respectivo número de conexões. Se o número de conexões for maior que 100 por exemplo, esse IP é bloqueado a fazer novas conexões, com isso interrompendo um possível ataque.

Esta ferramenta possui algumas peculiaridades como, aviso de IP’s bloqueados, arquivo de configuração simples, criação de lista de IP’s que não serão afetados pelo script (em caso de algum serviço especifico no servidor) e os endereços IP bloqueados são desbloqueados automaticamente após um certo tempo pré-configurado (por padrão este tempo é de 600 segundos). (MEDIA, 2014).

7 METODOLOGIA

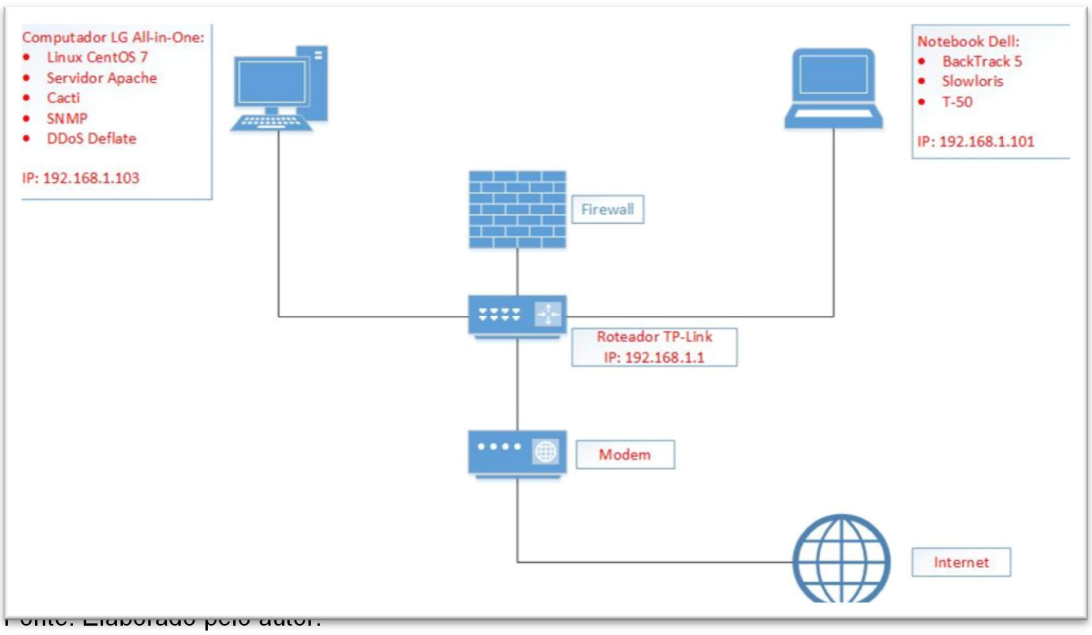
Para o desenvolvimento deste trabalho, foram feitos levantamentos bibliográficos sobre os assuntos que englobam o tema, como redes, software livre, Linux, entre outros, para compreender o propósito deste trabalho.

Foi utilizado um computador e um notebook com o sistema de virtualização da Oracle, o VitualBox, para instalar os sistemas que serão utilizados.

Em uma das maquinas virtuais[2] foi utilizado o sistema BackTrack 5 (que é uma distribuição do Linux para realizar testes dos mais variados tipos) para utilizar as ferramentas citadas neste trabalho para ataques DoS (Slowloris e T-50) e o Cacti para monitorar o servidor durante o ataque. Em outra máquina virtual foi instalado o Linux CentOS 7 com o (D)DoS Deflate, que ficou configurado como servidor web, e foi ativado o protocolo SNMP para enviar informações ao Cacti sobre seus recursos monitorados.

Como mostra a figura 6, para fazer a ligação desta rede foi utilizado um roteador da marca TP-Link, este conectado aos dois computadores, e ao modem da marca SpeedyTouch que faz conexão com a internet.

Figura 6 – Metodologia.



Fonte: Elaborado pelo autor.

[2] Maquinas virtuais são uma cópia de um computador isolado rodando em um software especifico dentro do sistema operacional.

O computador LG All-in-One possui as configurações: processador Intel core i5 (3ª geração), memória de 4 gigabytes e Hard Disk de 500 gigabytes. O notebook Dell possui um processador Intel Core i5 (4ª geração), memória de 4 gigabytes, Hard Disk de 500 gigabytes e placa gráfica da nVidia Gforce 740M com 2 gigabytes de memória.

A rede foi configurada com os seguintes endereços IP: O Computador LG que teve a máquina virtual com o servidor web ficou 192.168.1.103. O notebook Dell que foi o responsável por realizar os ataques ficou com o IP de 192.168.1.101. O roteador TP-Link ficou com o IP 192.168.1.1.

8 RESULTADOS

A primeira ferramenta utilizada foi o T-50, ele necessita instalação dependendo da versão do Linux que será utilizada, ou no caso da versão Linux BackTrack 5 ele já vem com os pacotes necessários pré-configurados, neste caso basta abrir o promt de comando do Linux e executar um comando para ativa-lo. O servidor estava configurado no IP: 192.168.1.103 como citado acima, e foi direcionado na porta 80, que é responsável por páginas web (http). O tipo de ataque utilizado foi o SYN flood que é uma das formas de ataque de negação de serviço.

Todas essas informações são passadas por parâmetro no terminal do BackTrack 5 através do seguinte comando:

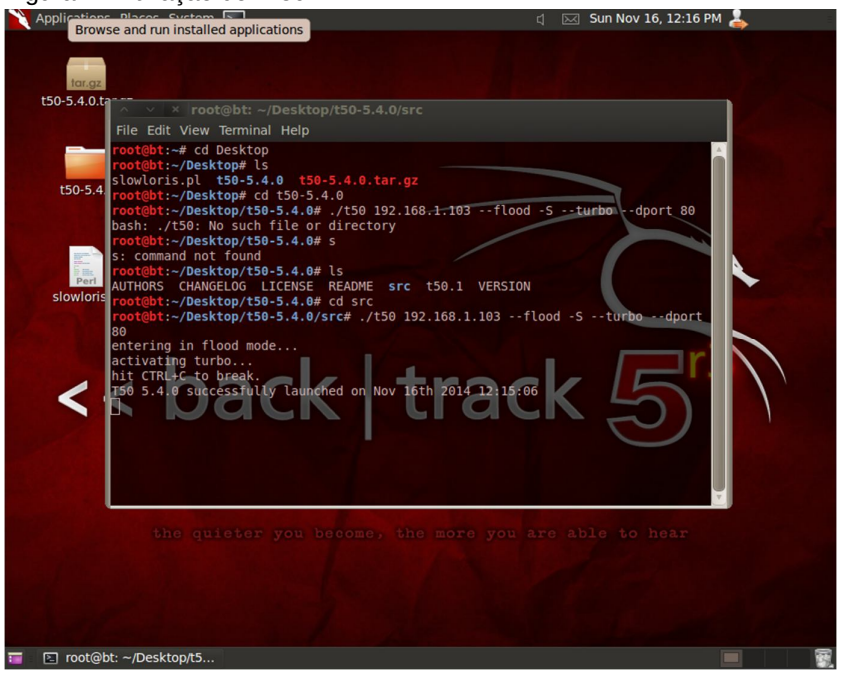
./t50 192.168.1.103 --flood -S --turbo --dport 80

- **./t50**: é o parâmetro inicial da ferramenta para a execução do ataque;
- **192.168.1.103**: é o endereço do servidor que será atacado, nesta parte poderia ser utilizado também um domínio (site) que funcionaria da mesma forma
- **--flood –S**: é o tipo e parâmetro do ataque que será realizado, neste caso é o SYN flood.
- **--turbo**: este parâmetro é responsável por acelerar os pacotes que são enviados ao servidor.
- **--dport 80**: é o parâmetro que direciona o ataque para um porta específica do servidor, neste caso é a porta 80.

A execução do código é bem simples e após digitar o comando os parâmetros são iniciados como pode ser visto na Figura 7, ativando o modo flood e o modo turbo. Após ativar os parâmetros a ferramenta inicia a conexão com o servidor disparando requisições para sobrecarregá-lo.

A segunda ferramenta utilizada foi o Slowloris, esta não vem pré-configurada, porém para instalá-la basta obter o código fonte através do site do desenvolvedor e salvá-lo como arquivo de texto com a extensão “.pl” da linguagem Perl, depois basta abrir o prompt de comando do Linux, ir até a pasta onde este arquivo foi salvo, e executar o comando para ativá-lo.

Figura 7 - Ativação do T-50



Fonte: Elaborado pelo autor

Assim como no T-50 as informações referente ao ataque são passadas por parâmetros no terminal do BackTrack 5 da seguinte forma:

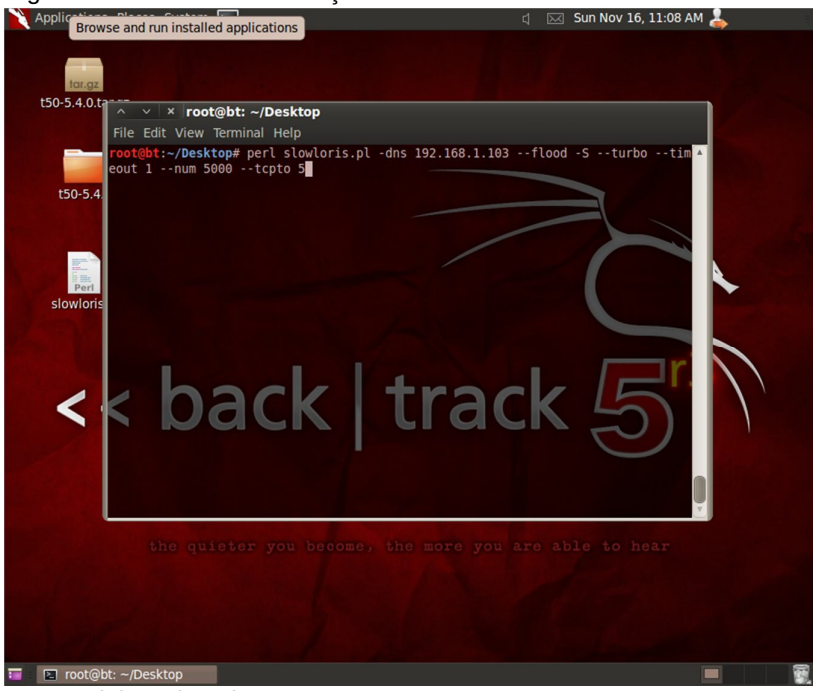
perl slowloris.pl -dns 192.168.1.103 -port 80 -timeout 1 -num 500 -tcpto 5

- perl slowloris.pl: é o parâmetro inicial para iniciar o ataque;
- -dns 192.168.1.103: é o endereço do servidor que será atacado;
- -port 80: este parâmetro define que a porta 80 do servidor que será atacada;
- -timeout 1 –num 500: estes dois parâmetros indicam que a cada 1 segundo ele enviará 500 requisições para o servidor, estes valores podem ser alterados, porém quanto maior a quantidade de requisições, maior será a largura da sua banda que o software irá utilizar;
- -tcpto 5: informa o tipo de interface.

Após ativar o comando do Slowloris ele começa a construir os pacotes de requisição, faz a conexão com o servidor e começa a disparar os pacotes, como foi descrito no comando. A Figura 8 mostra o comando sendo ativado para disparar cinco

mil requisições por segundo, quando é pressionado a tecla “enter” ele começa a construção das requisições e tenta se conectar com o servidor.

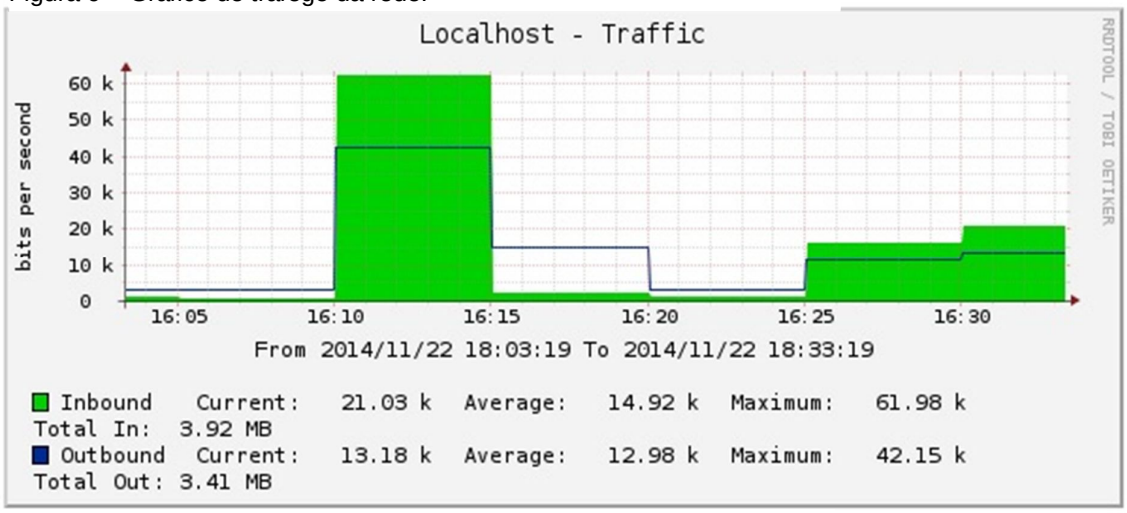
Figura 8 – Comando de ativação do Slowloris



Fonte: Elaborado pelo autor

Cada ferramenta foi testada com cinco minutos de duração, verificando-se no software Cacti o uso da CPU, memória e tráfego da rede durante os ataques.

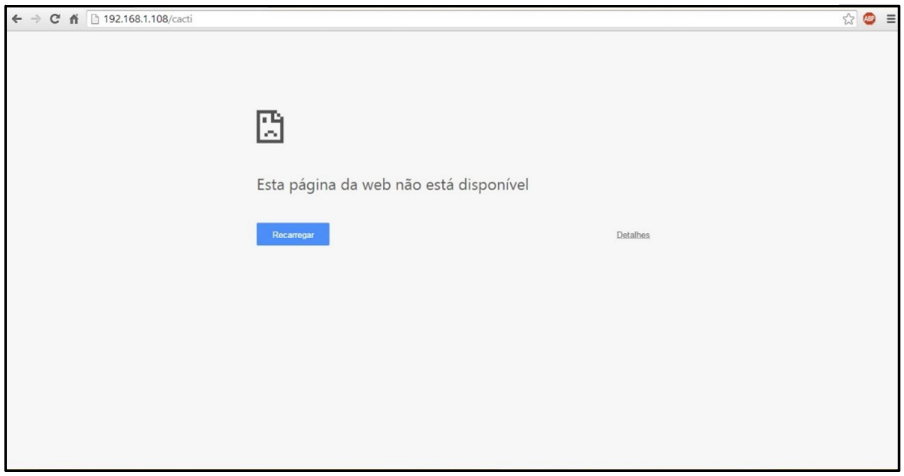
Figura 9 – Gráfico de trafego da rede.



Fonte: Elaborado pelo autor.

Primeiro foi usada a ferramenta T50 e depois foi usada a ferramenta Slowloris. Havia no servidor uma página HTML simples que foi usada para testar se o servidor ainda respondia as requisições durante os ataques. O T50 foi ativado das 16:10 às 16:15 como pode ser visto na Figura 9, ele elevou o trafego da rede do servidor ao limite, com isso este deixou de responder as novas requisições. Ao tentar carregar a página de teste, o navegador exibiu a mensagem “Esta página da web não está disponível” como mostra a Figura 10.

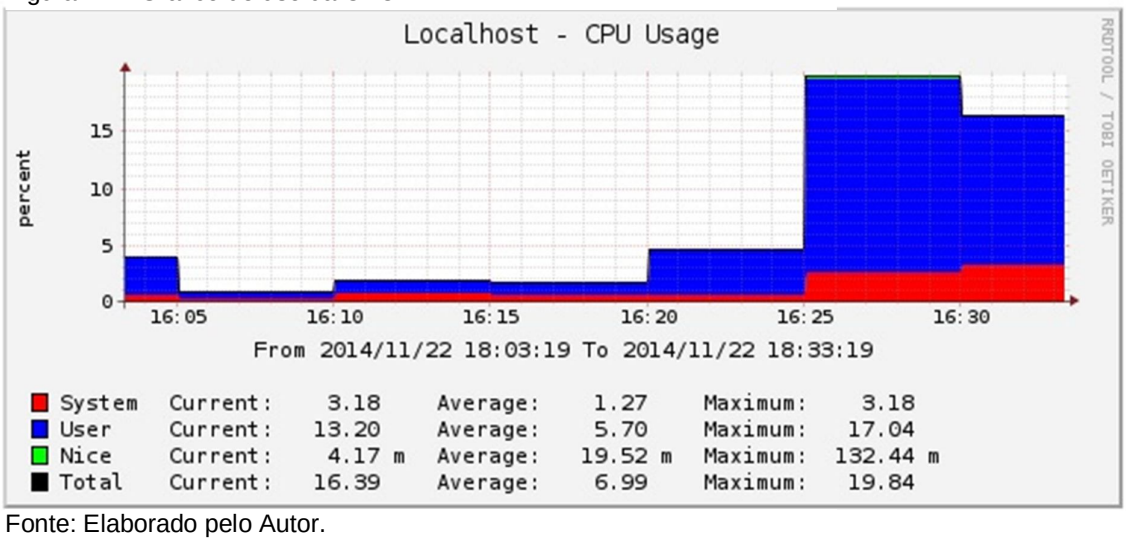
Figura 10 – Pagina de teste indisponível.



Fonte: Elaborado pelo Autor.

O Slowloris foi ativado das 16:25 às 16:30, ele também elevou o tráfego da rede do servidor, porém teve efeito bem menor se comparado a primeira ferramenta

Figura 11 – Gráfico de uso da CPU.



Fonte: Elaborado pelo Autor.

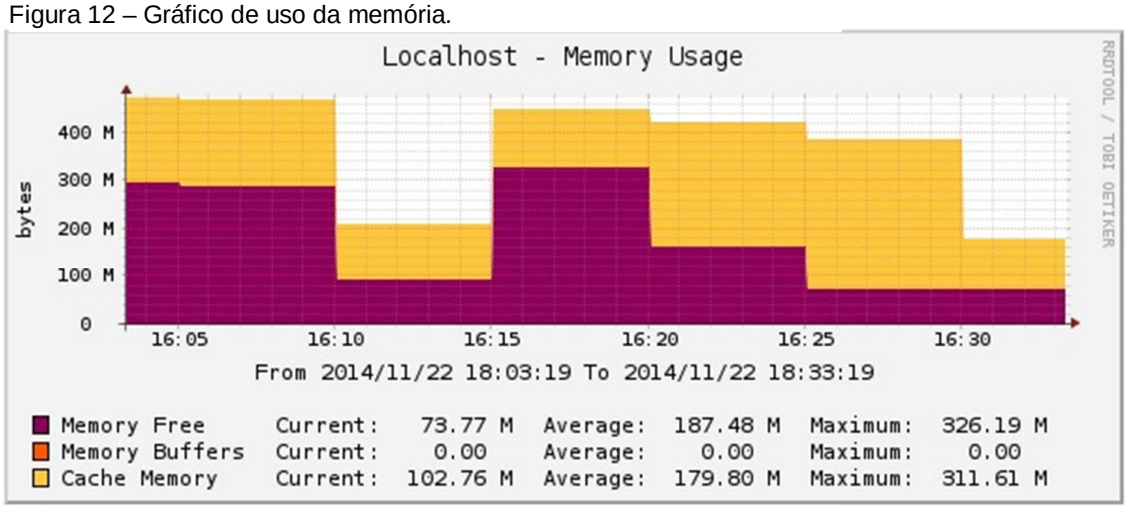
utilizada. Apesar disso, considerando o uso da CPU, ele teve um efeito maior, como pode ser visto na Figura 11, ele aumentou muito o processamento do mesmo.

Mesmo assim o servidor não deixou de responder, ao tentar carregar a página de teste, o servidor respondeu a solicitação, porém com um tempo muito maior. Em questão de eficácia o T-50 se destacou pois cumpriu o objetivo de sobrecarregar o servidor a ponto de parar de atender a novas requisições.

Com relação ao uso da memória do servidor, não houve alterações durante os ataques, nenhuma das duas ferramentas elevou o uso de memória do mesmo, isso

pode ser visto na Figura 12, durante o período dos ataques a memória permaneceu normal.

Figura 12 – Gráfico de uso da memória.



Fonte: Elaborado pelo Autor

Após as implementações das ferramentas de ataque, foi utilizado o software (D)Dos Deflate no servidor para testar durante cada ferramenta de ataque em ação. Primeiramente, foi iniciado o ataque novamente com o T-50 e foi ativado o software de defesa no servidor, depois foi ativado o Slowloris.

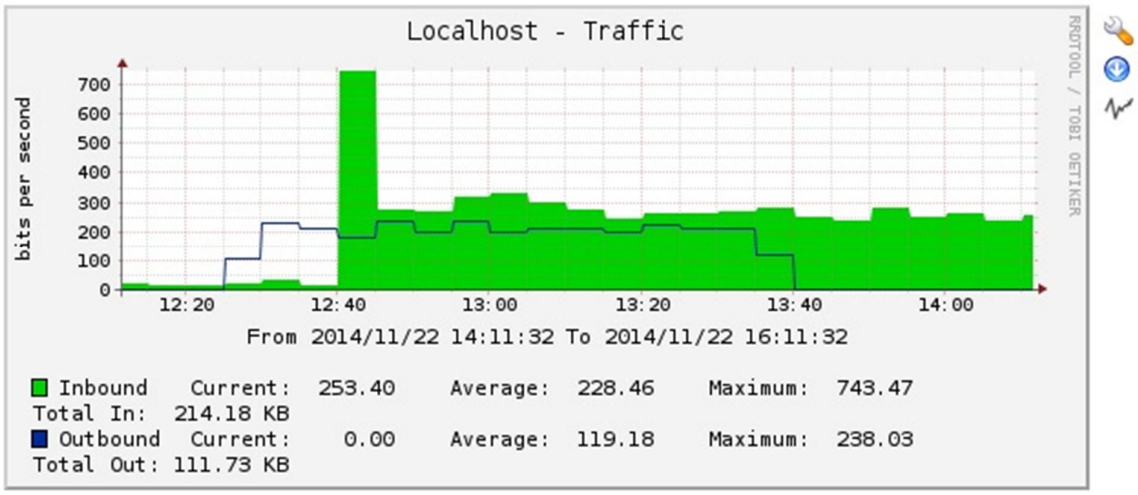
A primeira ferramenta foi ativada às 12:40 horas, ativou-se o software de defesa em conjunto. O ataque começou a sobrecarregar o servidor, e após 5 minutos esta sobrecarga começou a diminuir.

Já a segunda ferramenta foi ativada às 13:40 horas e novamente foi ativado o software de defesa. Em relação ao Slowloris, não houve alteração, ele manteve a

sobrecarga (em um nível menor que o T-50), e o DDoS Deflate não bloqueou o ataque como deveria.

No primeiro ataque, a defesa levou aproximadamente 5 minutos para começar a surtir efeito. No segundo ataque, como não houve alteração, não obteve-se nenhum resultado significativo. Essas informações podem ser vistas na Figura 13.

Figura 13 – Ativação do DDos Deflate



Fonte: Elaborado pelo Autor

Fonte: Elaborado pelo Autor

As ferramentas de ataque funcionaram normalmente, sendo que o T-50 se destacou por tirar o servidor do ar por completo, ao contrário do Slowloris que apenas o deixou lento. Pode ser visto na Figura 14 o comparativo entre as duas ferramentas de ataque utilizadas. O software de defesa não se mostrou eficaz, e não correspondeu ao planejado. Em conjunto com a primeira ferramenta de ataque ele fez efeito, porém não sessou o ataque, já com a segunda ferramenta, não teve alteração.

Ferramentas	Causou instabilidade	Causou negação do serviço	Nível de complexidade	Tempo (ativada)
T-50	Sim	Sim	Alto	5 minutos
Slowloris	Sim	Não	Baixo	5 minutos

9 CONCLUSÕES

Através dessa pesquisa pode-se perceber que não foi possível 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 DoS e DDoS principalmente, existem várias maneiras de se minimizar os danos causados pelo ataque. O melhor modo de proteção é a elaboração de um ambiente monitorado com planos de contingências eficazes para que, se necessário, sejam ativados de forma rápida e segura, não comprometendo o serviço por muito tempo.

A defesa dos ataques desta natureza consiste em um conjunto de ferramentas que possibilitam monitorar os recursos do servidor e intervir quando houver necessidade. Cada empresa deve possuir um planejamento com relação a sua segurança pois essa é a melhor forma de se prevenir contra esses ataques.

Como possibilidade para trabalhos futuros, uma hipótese a ser explorada seria a implementação de um outro tipo de software de defesa, testando sua eficácia e constatando se demonstrar-se-ia superior ou inferior ao que foi obtido no presente trabalho.

REFERÊNCIAS

ALENCAR, M. S. **Engenharia de redes de Computadores**. Érica, 2012.

ANUNCIAÇÂO, H. **Linux Total e Software Livre**. Ciência Moderna, 2007.

BRASIL ESCOLA. **História do Linux**. Disponível em: < http://www.brasilescola.com/informatica/historia-do-linux.htm >. Acesso em: 14 de mai. 2014.

BRITO, N. **Uso irresponsável do T50**. Disponível em: < http://fnstenv.blogspot.com.br/2012/02/uso-irresponsavel-do-t50.html#more >. Acesso em: 17 de mai. 2014.

CACTI. **O que é Cacti**. Disponível em: < http://www.cacti.net/what_is_cacti.php >. Acesso em: 14 de mai. 2014.

CENTOS**. CentOS**. Disponível em: < http://www.centos.org/about/ >. Acesso em: 22 de nov. 2014.

COSTA, F. **Ambiente de rede monitorado com Nagios e Cacti**. Ciência Moderna, 2008

CUNHA, W. **ABNT NBR ISO/IEC 27002:2005**. Disponível em: <http://waltercunha.com/blog/wpcontent/uploads/2009/06/resumo_abnt_nbr_iso_27002_2005.pdf >. Acesso em: 08 mai. 2014.

DUARTE, O. C. M. B. **Negação de serviço**. Disponível em: < http://www.gta.ufrj.br/grad/06_1/dos/intro.html >. Acesso em: 17 de mai. 2014.

FOROUZAN, B. A. **Comunicação de Dados e Redes de Computadores** 3. ed. Artmed, 2006.

GIAVAROTO, S. C. R. **BackTrack Linux Auditoria e Teste de Invasão em Redes de Computadores**. Ciência Moderna, 2013.

LIMA, G. **Simular um ataque DDos**. Disponível em:< ww.blog.corujadeti.com.br/que-tal-simular-um-ataque-ddos-para-testar-seu-weblab/ > Acesso em: 05 mai. 2014.

MAURO, D. **Essential SNMP** 2. ed. O'Reilly, 2005.

MEDIA. **(D)DoS Deflate**. Disponível em: < http://www.deflate.mediaplayer.com > Acesso em: 28 de mai. 2014.

MICROSOFT. **Protocolo SNMP**. Disponível em: < http://msdn.microsoft.com/en-us/library/ms950400.aspx >. Acesso em: 05 mai. 2014.

MORIMOTO, C. E. **Redes – Guia Completo** 3. ed. Disponível em: < http://www.guiadohardware.net/redes-guia-completo-3 >. Acesso em: 24 de nov. 2014

OLIVEIRA R. A. **Software Livre e Broffice**. Academia, 2009.

PERL BRASIL. **Perl**. Disponível em: < www.perl.org.br/Main/WebHome >. Acesso em: 17 de mai. 2014.

PINHEIRO, J. M. S. **Gerenciamento de redes de Computadores.** 2002.

ROSS, J. **Redes de computadores**. Antenna, 2008.

ROSS, K. **Computer Networking: A Top-Down Approach Featuring the Internet.** Pearson, 2010.

SLOWLORIS. **Slowloris**. Disponível em: < http://ha.ckers.org/slowloris/ >. Acesso em: 17 de mai. 2014.

TANEMBAUM, A. S. **Redes de Computadores** 4. ed. Campus, 2003.

Negação de Serviços: Análise comparativa entre dois programas de ataques DoS e proposta de defesa

Vinicius Santos Sanchez[1], Henrique Pachioni Martins[2], Elvio Gilberto da Silva[3], André Luiz Ferraz Castro[4]

[1]Centro de Ciências Exatas e Sociais Aplicadas – Universidade Sagrado Coração (USC)
Bauru 17.011-970 – São Paulo – SP – Brasil

viniciusanchez@gmail.com

Abstract. *The internet has revolutionized the way in which we have access to information of all kinds, despite the great progress that it provides, can also pose risks when used by malicious people seeking ways to cause damage to systems such as DoS attack. This article aims to describe two DoS attack tools in action services, elaborating a comparison between them and implement a defense software checking its effectiveness before the attack tools.*

Resumo. *A internet revolucionou o modo em que temos acesso a informações dos mais variados tipos, apesar do grande avanço que ela proporciona, pode também oferecer riscos quando utilizada por pessoas mal intencionadas que buscam formas de causar danos em sistemas como por exemplo o ataque DoS. O presente artigo teve como objetivo descrever duas ferramentas de ataque de negação de serviços em ação, elaborando um comparativo entre elas bem como implementar um software de defesa verificando sua eficácia perante as ferramentas de ataque.*

Introdução

A internet hoje proporciona conteúdo aos usuários que antes não se imaginavam, dentre eles estão: entretenimento, informação, serviços, educação e transações de dinheiro online. O que parece comum hoje, que temos acesso em um clique ou um toque na tela, antes não existia.

Porém, além de trazer muita coisa boa para a sociedade moderna, ela trouxe também sua dependência. Para comprovar isso, podemos citar as redes sociais, onde crianças, jovens e adultos passam horas conectados, seja interagindo com outras pessoas ou apenas verificando atualizações do seu círculo social.

No mundo econômico, as transações são de extrema importância, o que demanda disponibilidade total para abranger todas as empresas e clientes. Porém, se esses serviços fossem cortados ou derrubados por tempo indeterminado, acabaria gerando desconforto, revolta e etc.

Além disso a internet pode ser usada para diversos fins, tanto para produzir algo, quanto para degradar. Na internet as pessoas tem a liberdade de pesquisar o que quiserem, dar suas opiniões e usa-la a seu favor para diversos fins.

A internet muitas vezes se torna palco de conflitos de todos os gêneros, em redes sociais, servindo para auxiliar em crimes, derrubando os serviços (sites de bancos, do governo, de órgãos públicos, e etc.), muitas vezes como forma de protesto e algumas por vontade própria, e até como espionagem, como atualmente acontece entre os países.

É nesse contexto de conflitos que se encaixa o DoS. Apesar de não ser um tipo de ataque que rouba informações, ou que cause perda dos arquivos da vítima, ele causa a instabilidade e até a negação desse serviço, ou seja, se um site de um banco fosse atacado, este causaria a instabilidade, ou em alguns casos, iria derrubar o site, deixando o servidor sobrecarregado, e inacessível para os clientes e empresas conveniadas ao banco. Com o serviço fora do ar, geraria prejuízo para o banco e seus clientes.

Gerenciamento de redes

O objetivo do gerenciamento das redes é garantir que a mesma tenha seu funcionamento adequado e com a melhor qualidade possível. Para isso é necessário monitorar os elementos que a compõem para ter um diagnóstico de como está seu funcionamento para então tomar providências se necessário.

Para realizar esse monitoramento dos elementos (físicos ou lógicos) da rede, são necessários softwares que são capazes de medir a qualidade e a estabilidade da rede. Existem hoje software com propósitos gerais de monitoramento, e também para monitoramentos específicos, sendo possível gerenciar configurações, falhas, segurança, contabilização, entre outros. (PINHEIRO, 2002).

SNMP

O SNMP (Simple Network Management Protocol) é um protocolo da camada de aplicação usado para efetuar o gerenciamento de redes. Através deste protocolo é possível obter informações sobre os elementos que compõem a rede através de um computador chamado de “gerente”.

Ao invés de utilizar o modelo cliente/servidor, o SNMP utiliza o conceito de gerentes e agentes. O gerente será o responsável por adquirir as informações dos agentes que são os dispositivos conectados na rede, e atualizar o gerenciamento local baseado nas informações adquiridas com os pedidos feitos aos agentes,

gerando gráficos e enviando notificações no caso de anomalias para o administrador. (MAURO, 2005).

Cacti

O software Cacti é uma ferramenta para gerenciamento de redes muito eficaz, mostrando o estado atual da rede através de gráficos. Esta ferramenta utiliza o protocolo SNMP para envio de requisições aos elementos da rede e recebe como resposta o estado atual, como uso de banda e CPU, do elemento em questão.

Assim como todas as ferramentas administrativas de rede, o Cacti é importante para manter a rede segura e disponível, pois qualquer anomalia identificada nos elementos que estão sob controle deste software, será reportada para o administrador da rede, ou a pessoa responsável pela estrutura da mesma, e este será responsável por tomar as devidas decisões para normalizar os serviços. (COSTA, 2008).

Linux

O Linux possui como base o Unix, que é um sistema operacional de grande porte. Seu nome vem do seu criador Linus Torvalds, logo a junção de Linus + Unix originou o nome Linux.

O sistema Unix teve origem na década de 1960, envolvendo empresas, universidades e laboratórios, entre eles o MIT (Massachusets Institute of Technology), a GE (General Eletric), a AT&T (American Telephone and Telegraph) entre outros, que desenvolveram um sistema chamado Multics. O sistema não atingiu seus objetivos, e algumas empresas envolvidas no projeto acabaram saindo. (BRASIL..., 2014).

Após o desenvolvimento do Unix, surgiu um outro sistema que também o possui como base que é o Minix, que era totalmente gratuito e com seu código fonte aberto, ou seja, sendo possível um programador experiente alterar seu código, modificando suas funções conforme a vontade do mesmo. (ANUNCIAÇÃO, 2007).

BackTrack

É uma ferramenta Linux baseada no WHAX, Whoppix e Auditor (ferramentas para auditoria, testes de sistemas e redes) voltada para testes de penetração, usada

por analistas de segurança de redes e sistemas, hackers “éticos”, auditores, entre outros (GIAVAROTO, 2013).

CentOS

É uma distribuição do sistema Linux voltada para servidores, sendo considerada estável por ser sistema “clone” da distribuição paga do Linux Red Hat Enterprise Linux (RHEL). É compatível com os mesmos pacotes de atualização do RHEL e é derivado de código fonte livremente prestados ao público pela Red Hat. (CENTOS, 2014).

Ataque DoS

O ataque DoS (Denial of Service, em português, Negação de serviço) é um tipo de ataque de internet feito para sobrecarregar o servidor em que a aplicação alvo está hospedada, como por exemplo sites de governo, bancos, entre outros, impedindo que outros usuários tenham acesso a este serviço.

Este tipo de ataque é feito por uma máquina utilizando técnicas específicas para forçar o servidor a responder solicitações, ou seja, o atacante tem como objetivo fazer com que os serviços tenham acesso impossibilitado. (DUARTE, 2014).

T-50

Esta ferramenta foi desenvolvida pelo brasileiro Nelson Brito, se baseia no método de injeção de pacotes realizando stress tests, podendo utilizar vários protocolos diferentes como TCP, UDP, ICMP entre outros.

Diferente do Slowloris, o T-50 utiliza apenas um soquete para efetuar a sobrecarga do servidor. O sistema utilizado para implementar essa ferramenta é o Linux/Unix. (BRITO, 2014).

Slowloris

Esta ferramenta foi desenvolvida na linguagem de programação Perl, e é usada para efetuar ataques a servidores com intenção de sobrecarrega-lo causando instabilidade do mesmo, e até fazendo com que este deixe de responder.

O software mantem o máximo de conexões abertas no servidor alvo e mantem elas o máximo possível. Também envia cabeçalhos HTTP que não possui conclusão de solicitação, com isso os servidores vão manter estas conexões simultâneas até a sua capacidade máxima, quando isso acontece as novas tentativas de conexões de demais clientes são negadas. (SLOWLORIS, 2014).

Métodos

Para o desenvolvimento deste trabalho, foram feitos levantamentos bibliográficos sobre os assuntos que englobam o tema, como redes, software livre, Linux, entre outros, para compreender o propósito deste trabalho.

Utilizou-se um computador e um notebook com o sistema de virtualização da Oracle, o VitualBox, para instalar os sistemas que serão utilizados.Em uma das maquinas virtuais[3] foi utilizado o sistema BackTrack 5 para utilizar as ferramentas citadas neste trabalho para ataques DoS (Slowloris e T-50) e o Cacti para monitorar o servidor durante o ataque. Em outra máquina virtual foi instalado o Linux CentOS 7 com o (D)DoS Deflate, que ficou configurado como servidor web e foi ativado o protocolo SNMP para enviar informações ao Cacti sobre seus recursos monitorados.

Para fazer a ligação desta rede utilizou-se um roteador da marca TP-Link, este conectado aos dois computadores e a um modem que faz conexão com a internet.

O computador LG All-in-One possui as configurações: processador Intel core i5 (3ª geração), memória de 4 gigabytes e Hard Disk de 500 gigabytes. O notebook Dell possui um processador Intel Core i5 (4ª geração), memória de 4 gigabytes, Hard Disk de 500 gigabytes e placa gráfica da nVidia Gforce 740M com 2 gigabytes de memória.

A rede foi configurada com os seguintes endereços IP: O Computador LG que teve a máquina virtual com o servidor web ficou 192.168.1.103. O notebook Dell que foi o responsável por realizar os ataques ficou com o IP de 192.168.1.101. O roteador TP-Link ficou com o IP 192.168.1.1.

[3] Maquinas virtuais são uma cópia de um computador isolado rodando em um software especifico dentro do sistema operacional.

Resultados

A primeira ferramenta utilizada foi o T-50, ele necessita instalação dependendo da versão do Linux que será utilizada, ou no caso da versão Linux BackTrack 5 ele já vem com os pacotes necessários pré-configurados, neste caso basta abrir o promt de comando do Linux e executar um comando para ativa-lo. O servidor estava configurado no IP: 192.168.1.103 como citado acima, e foi direcionado na porta 80, que é responsável por páginas web (http). O tipo de ataque utilizado foi o SYN flood que é uma das formas de ataque de negação de serviço.

Todas essas informações são passadas por parâmetro através do seguinte comando:

./t50 192.168.1.103 --flood -S --turbo --dport 80

- **./t50**: é o parâmetro inicial da ferramenta para a execução do ataque;
- **192.168.1.103**: é o endereço do servidor que será atacado, nesta parte poderia ser utilizado também um domínio (site) que funcionaria da mesma forma
- **--flood –S**: é o tipo e parâmetro do ataque que será realizado, neste caso é o SYN flood.
- **--turbo**: este parâmetro é responsável por acelerar os pacotes que são enviados ao servidor.
- **--dport 80**: é o parâmetro que direciona o ataque para um porta específica do servidor, neste caso é a porta 80.

A execução do código é bem simples e após digitar o comando ele inicia os parâmetros, ativando o modo flood e o modo turbo. Após ativado os parâmetros, a ferramenta inicia a conexão com o servidor disparando requisições para sobrecarrega-lo.

A segunda ferramenta utilizada foi o Slowloris, esta não vem pré-configurada, porem para instala-la basta obter o código fonte através do site do desenvolvedor e salva-lo como arquivo de texto com a extensão “.pl” da linguagem Perl, depois basta abrir o promt de comando do Linux, ir até a pasta onde este arquivo foi salvo, e executar o comando para ativa-lo.

Assim como no T-50 as informações referente ao ataque são passadas por parâmetros da seguinte forma:

perl slowloris.pl -dns 192.168.1.103 -port 80 -timeout 1 -num 500 -tcpto 5

- perl slowloris.pl: é o parâmetro inicial para iniciar o ataque;
- -dns 192.168.1.103: é o endereço do servidor que será atacado;
- -port 80: este parâmetro define que a porta 80 do servidor que será

atacada;

- -timeout 1 –num 500: estes dois parâmetros indicam que a cada 1 segundo ele enviará 500 requisições para o servidor, estes valores podem ser alterados, porém quanto maior a quantidade de requisições, maior será a largura da sua banda que o software irá utilizar;
- -tcpto 5: informa o tipo de interface.

Cada ferramenta foi testada com cinco minutos de duração, verificando-se no software Cacti o uso da CPU, memória e trafego da rede durante os ataques. Primeiro foi usada a ferramenta T50 e depois foi usada a ferramenta Slowloris.

Havia no servidor uma página HTML simples que foi usada para testar se o servidor ainda respondia as requisições durante os ataques. O T50 foi ativado das 16:10 às 16:15. Esta ferramenta elevou o trafego da rede do servidor ao limite, com isso este deixou de responder as novas requisições. Ao tentar carregar a página de teste, o navegador exibiu a mensagem “Esta página da web não está disponível”.

O Slowloris foi ativado das 16:25 às 16:30 e também elevou o tráfego da rede do servidor, porém teve efeito bem menor se comparado a primeira ferramenta utilizada. Apesar disso, considerando o uso da CPU, ele teve um efeito maior, aumentando muito o processamento.

Mesmo assim o servidor não deixou de responder, ao tentar carregar a página de teste, o servidor respondeu a solicitação, porém com um tempo muito maior. Em questão de eficácia o T-50 se destacou pois cumpriu o objetivo de sobrecarregar o servidor a ponto de parar de atender a novas requisições.

Com relação ao uso da memória do servidor, não houve alterações durante os ataques, nenhuma das duas ferramentas elevou o uso de memória, durante o período dos ataques a memória permaneceu normal. O comparativo entre as ferramentas de ataque pode ser visto na Figura 1 abaixo.

Figura 1 - Tabela comparativa entre as ferramentas de ataque.

Ferramentas	Causou instabilidade	Causou negação do serviço	Nível de complexidade	Tempo (ativada)
T-50	Sim	Sim	Alto	5 minutos
Slowloris	Sim	Não	Baixo	5 minutos

Fonte: Elaborado pelo Autor

Após as implementações das ferramentas de ataque, foi utilizado o software (D)Dos Deflate no servidor para testar durante cada ferramenta de ataque em ação.

Primeiramente, foi iniciado o ataque novamente com o T-50 e foi ativado o software de defesa no servidor, depois foi ativado o Slowloris.

A primeira ferramenta foi ativada às 12:40 horas, ativou-se o software de defesa em conjunto. O ataque começou a sobrecarregar o servidor, e após 5 minutos esta sobrecarga começou a diminuir.

Já a segunda ferramenta foi ativada às 13:40 horas e novamente foi ativado o software de defesa. Em ralação ao Slowloris, não houve alteração, ele manteve a sobrecarga (em um nível menor que o T-50), e o DDoS Deflate não bloqueou o ataque como deveria.

No primeiro ataque, a defesa levou aproximadamente 5 minutos para começar a surtir efeito. No segundo ataque, como não houve alteração, não obteve-se nenhum resultado significativo.

As ferramentas de ataque funcionaram normalmente, sendo que o T-50 se destacou por tirar o servidor do ar por completo, ao contrário do Slowloris que apenas o deixou lento. O software de defesa não se mostrou eficaz, e não correspondeu ao planejado. Em conjunto com a primeira ferramenta de ataque ele fez efeito, porém não sessou o ataque, já com a segunda ferramenta, não teve alteração.

Considerações Finais

Através dessa pesquisa pode-se perceber que não foi possível 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 DoS e DDoS principalmente, existem várias maneiras de se minimizar os danos causados pelo ataque. O melhor modo de proteção é a elaboração de um ambiente monitorado com planos de contingências eficazes para que, se necessário, sejam ativados de forma rápida e segura, não comprometendo o serviço por muito tempo.

A defesa dos ataques desta natureza consiste em um conjunto de ferramentas que possibilitam monitorar os recursos do servidor e intervir quando houver necessidade. Cada empresa deve possuir um planejamento com relação a sua segurança pois essa é a melhor forma de se prevenir contra esses ataques.

Como possibilidade para trabalhos futuros, uma hipótese a ser explorada seria a implementação de um outro tipo de software de defesa, testando sua eficácia

e constatando se demonstrar-se-ia superior ou inferior ao que foi obtido no presente trabalho.

Referencias

ANUNCIAÇÂO, H. **Linux Total e Software Livre**. Ciência Moderna, 2007.

BRASIL ESCOLA. **História do Linux**. Disponível em: < http://www.brasilescola.com/informatica/historia-do-linux.htm >. Acesso em: 14 de mai. 2014.

BRITO, N. **Uso irresponsável do T50**. Disponível em: < http://fnstenv.blogspot.com.br/2012/02/uso-irresponsavel-do-t50.html#more >. Acesso em: 17 de mai. 2014.

CENTOS**. CentOS**. Disponível em: < http://www.centos.org/about/ >. Acesso em: 22 de nov. 2014.

COSTA, F. **Ambiente de rede monitorado com Nagios e Cacti**. Ciência Moderna, 2008.

DUARTE, O. C. M. B. **Negação de serviço**. Disponível em: < http://www.gta.ufrj.br/grad/06_1/dos/intro.html >. Acesso em: 17 de mai. 2014.

GIAVAROTO, S. C. R. **BackTrack Linux Auditoria e Teste de Invasão em Redes de Computadores**. Ciência Moderna, 2013.

MAURO, D. **Essential SNMP** 2. ed. O'Reilly, 2005.

OLIVEIRA R. A. **Software Livre e Broffice**. Academia, 2009.

PINHEIRO, J. M. S. **Gerenciamento de redes de Computadores.** 2002.

SLOWLORIS. **Slowloris**. Disponível em: < http://ha.ckers.org/slowloris/ >. Acesso em: 17 de mai. 2014.