UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CURSO DE ESPECIALIZAÇÃO SEMIPRESENCIAL EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

RAFAEL MACHADO BARDAL

ESTUDO SOBRE ATAQUES DE NEGAÇÃO DE SERVIÇO E UMA ABORDAGEM PRÁTICA

MONOGRAFIA

CURITIBA
2014

RAFAEL MACHADO BARDAL

ESTUDO SOBRE ATAQUES DE NEGAÇÃO DE SERVIÇO E UMA ABORDAGEM PRÁTICA

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de servidores e equipamentos de rede, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná – UTFPR

Orientador: Prof. Kleber Kendy Horikawa Nabas

CURITIBA

2014

Sumário

RESUMO

BARDAL, Rafael M. **Estudo sobre ataques de negação de serviço e uma abordagem prática.** 2014. 74 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

A presente monografia aborda o estudo dos ataques de negação de serviço e ataques distribuídos de negação de serviço, conhecidos como DoS e DDoS respectivamente, que acometem as redes conectadas a Internet. Apresenta um histórico das diversas formas de ataque a sistemas de comunicação desde antes da criação da Internet. Discorre sobre os diferentes tipos de ataques DoS que servem de base para o entendimento dos ataques distribuídos ou DDoS. Um panorama da situação atual da Internet em relação aos ataques é mostrado. Finalizando, são apresentadas propostas para simulações desses ataques em laboratório ou máquina virtual.

Palavras-chave: Internet.Ataque. DoS. DDoS. Hacker.

ABSTRACT

BARDAL, Rafael M. **Study about Denial of Service attacks and a pratical approach** 2014. 74 f. Monograph (Specialization in Server Configuration and Management and Network Equipment). Federal Technological University of Paraná. Curitiba, 2014 .

This monograph deals with the study of denial of service attacks and distributed denial of service attacks, known as DoS and DDoS respectively, affecting networks connected to the Internet. Shows a history of the numerous forms of attack on communication systems since before the creation of the Internet. It discusses the different types of DoS attacks that are the basis for understanding the distributed attacks or DDoS attacks. An overview of current Internet situation in relation to attacks is show. Finally, proposals are presented for simulations of these attacks in the laboratory or virtual machine.

Keywords: Internet. Attack. DoS. DDoS. Hacker.

LISTA DE SIGLAS

ACK – Acknowledment

ACL – Access Control List

ARPANET – Advanced Research Projects Agency Network

BBS – Bulletin Board System

BGP – Border Gateway Protocol

BIND – Berkley Internet Name Domain

BSD – Berkley Software Distribution

CERT – Computer Emergency Response Team

CIA – Central Intelligence Agency

CPU – Central Processing Unit

DDoS – Distributed Denial of Service

DNS – Domain Name System

DoS – Denial of Service

DST – Destination

FTP – File Transfer Protocol

HP-UX – Hewlett-Packard UNIX

HTTP – Hypertext Transfer Protocol

ICMP – Internet Control Message Protocol

ICMPv6 – Internet Control Message Protocol version 6

ICQ – “I seek you”

ID – Identification

IP – Internet Protocol

IPv6 – Internet Protocol version 6

IRC – Internet Relay Chat

MAC – Media Access Control

MIT – Massachusetts Institute of Technology

NCP – Network Control Protocol

NTP – Network Time Protocol

OS – Operational System

OSI – Open System Interconnection

OTAN – Organização do Tratado do Atlântico Norte

RFC – Request for Comments

RIP – Routing Information Protocol

SMB – Server Message Block

SMTP – Simple Mail Transfer Protocol

SRC – Source

SYN – Synchronize

TCP – Transmission Control Protocol

TI – Tecnologia da Informação

TFN – Tribe Flood Network

TFN2k – Tribe Flood Network 2000

UDP – User Datagram Protocol

VM – Virtual Machine

1 INTRODUÇÃO

Neste capítulo serão tratados os elementos introdutórios relacionados ao estudo de ataques de negação de serviço.

1.1 TEMA

No início, a Internet era formada por pequenas redes governamentais e acadêmicas interconectadas, utilizadas para fins principalmente de pesquisa. Em 1988, um estudante de uma universidade americana, escreveu um software que procurava determinadas falhas em computadores conectados na rede. Quando encontrava a falha, o software se copiava para o computador repetidas vezes, tornando seu alvo incapaz de outras tarefas. Este software ficou conhecido como Morris *Worm*, criado por Robert Tappan Morris e é considerado o primeiro *worm* da história. Apesar de ter sido criado como um experimento para estimar o tamanho da Internet, o resultado foi uma paralisação de muitos servidores e um prejuízo de centenas a milhares de dólares. Com o crescimento da Internet, esse tipo de ação tornou-se muito comum, mas não com objetivos nobres como o de Robert Morris. O ataque de negação de serviço, ou DoS, passou a ser usado como uma arma, executado de forma organizada e global. Entidades anônimas ou indivíduos, conhecidos como *hackers*, com conhecimentos técnicos sofisticados passaram a atacar grandes redes por motivações ideológicas, comerciais, financeiras ou somente por demonstração de poder e prestígio.

Ataque de negação de serviço, DoS ou *Denial of Service* é uma tentativa de fazer com que uma máquina, servidor ou toda uma rede de computadores fique indisponível para seus usuários. A técnica mais simples para realizar um ataque como esse é enviar a um host muitas requisições de comunicação externas falsas, fazendo com o que o servidor não consiga responder às requisições reais ou responda de maneira muito lenta. Em pouco tempo a máquina (computador) fica sem nenhum recurso computacional e os serviços oferecidos se tornam indisponíveis.

Com o crescimento da Internet e desenvolvimento dos vários sistemas operacionais disponíveis no mercado, outras maneiras e técnicas de ataque foram desenvolvidas pelos *hackers* e suas comunidades. Erros de configuração e falhas de segurança encontradas nos *softwares* de serviços como FTP, SMTP e HTTP são exploradas permitindo que o ataque seja executado com sucesso. Até mesmo limitações ou fraquezas na infraestrutura do alvo podem ser exploradas durante o ataque.

Entre os anos 1999 e 2000, uma nova categoria de ataque surgiu. Mais elaborado e organizado que o DoS, o DDoS, Ataque Distribuído de Negação de Serviço ou *Distributed Denial of Service*, passou a causar grande estrago na Internet. Os servidores de grandes empresas, como Yahoo, Ebay e Amazon foram afetados, ficando várias horas inacessíveis. Nesse tipo de ação, não existe apenas um atacante. Dezenas ou até milhares de computadores espalhadas por toda Internet podem ser utilizados para um ataque DDoS. Esses computadores são invadidos ou comprometidos através de um *trojan* ou *worm* e utilizados como um dos pontos de origem de um ataque sem o consentimento ou mesmo conhecimento de seu proprietário. A superioridade de um ataque DDoS reside no fato de sua origem ser praticamente irrastreável, devido à grande quantidade de *hosts* (computadores) usados como origem do ataque.

Atualmente, os ataques de negação de serviço afetam negócios e empresas em todo o mundo. O prejuízo financeiro, causado pela indisponibilidade aos sistemas, pelo consumo de tempo e recursos utilizados na detecção e recuperação dos ataques.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

O objetivo deste trabalho é desenvolver um estudo teórico sobre ataques de negação de serviço e propor um uma série de simulações possíveis de execução em laboratório ou máquinas virtuais.

1.2.2 Objetivo Específico

Inicialmente será traçado um histórico da Internet e as primeiras ameaças a sistemas de comunicação e segurança das redes. Os ataques de negação de serviço serão o foco principal do panorama e serão apresentados casos reais.

Posteriormente, serão descritas as diversas formas no qual um ataque pode acontecer. As diversas técnicas utilizadas serão detalhadas e analisadas, bem como os efeitos que causam.

No final, será proposto um ambiente de laboratório onde experimentos ataques DoS poderão ser executados de forma controlada e segura.

1.3 JUSTIFICATIVA

Notícias envolvendo casos de ataques de negação de serviço são cada vez mais comuns. Todos que utilizam e trabalham com computadores, principalmente os profissionais de TI, informática e telecomunicações podem ser afetados por um ataque, seja de forma direta ou indireta.

Segundo dados coletados e publicados pela empresa Arbor Networks ATLAS®, diariamente são observados mais de 2000 ataques DDoS. A mesma empresa afirma ainda que 1/3 do tempo de indisponibilidade dos serviços de Internet são atribuídos a estes ataques que podem ser facilmente comprados por U$150 no mercado negro virtual.

Cursos profissionalizantes ou de graduação nas áreas de rede e TI apenas mencionam o problema, sem entrar em detalhes técnicos. Apenas quem se dedica à área de segurança em redes acaba se aprofundando no assunto.

A intenção deste trabalho é prover uma base teórica para estudantes de graduação, especialização em redes e engenharia da computação, além de auxiliar na definição de um laboratório para testes e experimentos relacionados a ataques de negação de serviço.

1.4 METODOLOGIA

Para embasar o desenvolvimento desta metodologia foi feita uma pesquisa bibliográfica de materiais específicos do assunto ‘Ataques de Negação de Serviço’. O resultado desta pesquisa trouxe um maior entendimento sobre como se desenvolve um ataque, suas causas e efeitos. Isso abriu um leque de possibilidades de futuros estudos, como por exemplo, maneiras de identificar e/ou proteger possíveis alvos dessa prática.

Tendo em vista a escassez de estudos e maiores informações sobre o assunto ataques DoS em livros, foi feita uma pesquisa virtual a diversas fontes alternativas que são citadas na referência bibliográfica. Após o estudo acima descrito, foi desenvolvido um ambiente de ataque controlado e propostas simulações de ataques. Isso permitirá que os colegas do curso e qualquer outro estudante da área ou outros interessados, possam presenciar um ataque em funcionamento e desta maneira entender os danos causados por uma ação que pode ser simples, porém, gera prejuízos milionários a grandes empresas que dependem da disponibilidade completa de sua rede.

1.5 CRONOGRAMA

Mês/Semana	Out 2014	Nov 2014	Dez 2014	Jav 2015	Fev 2015	Mar 2015	Abr 2015
Levantamento da literatura	X	X	X	X			
Elaboração do texto			X	X	X	X	X
Elaboração da proposta prática				X	X	X	
Organização do texto						X	X
Revisão da monografia							X
Defesa da monografia							X

1.6 ESTRUTURA

A monografia é composta por 8 capítulos. O primeiro capítulo trata da parte introdutória, onde o assunto é apresentado, os objetivos a serem atingidos, a justificativa da escolha do, procedimento metodológico adotado e a estrutura da monografia.

O capítulo 2 situa o leitor no contexto da Internet a partir de sua origem e faz um breve resumo das várias ameaças encontradas na grande rede. Segue então um histórico dessas ameaças, mas tendo como ponto de partida o início do século XX com a invasão e ataque em um dos mais antigos sistemas de comunicação. Outros fatos históricos são mencionados até chegar no surgimento da internet e os anos seguintes, dando ênfase nas ameaças, formas de invasão e ataque.

A partir do terceiro capítulo, o assunto ataques de negação de serviço é amplamente abordado. Uma classificação é descrita, bem como os vários tipos de ataques. O entendimento dos ataques DoS é essencial para se chegar na análise e estudo dos ataques DoS distribuídos. Grande parte do capítulo é voltado para este tipo de ataque.

No capítulo 4, são apresentados alguns dos piores e mais significativos ataques da história da Internet. É feita um breve resumo de cada um, bem como suas causas e efeitos. O capítulo seguinte expõe o panorama atual dos ataques de negação de serviço na Internet com alguns dados de empresas especializadas.

Finalizando a monografia, o capítulo 6 fornecesse algumas sugestões para simulações de ataques DoS realizáveis em laboratório ou ambientes virtuais. A este, segue as considerações finais, no capiítulo 7, bem como a relação das referências no capítulo 8.

2 DESENVOLVIMENTO TEÓRICO

2.1 AMEAÇAS NA INTERNET

Durante a Guerra Fria (1947-1953), o governo dos Estados Unidos, financiou a criação da primeira rede de comunicação de dados por pacote, a ARPANET (*Advanced Research Projects Agency Network*). Esta rede tinha o objetivo de conectar as bases militares e centros de pesquisas americanos, evitando assim uma perda total nas comunicações do país para o caso de um ataque bem sucedido da ex-União Soviética. A ARPANET surgiu dentro do Pentágono e em meados de 1975, através de um *Backbone*, conectava aproximadamente 100 redes, entre universidades, bases militares e centros de pesquisa, como pode ser visto na figura 1. Inicialmente usava o protocolo NCP (*Network Control Protocol*), porém com o crescimento da rede esse protocolo foi substituído pelo TCP/IP (*Transmition Control Protocol/Internet Protocol*), que é utilizado até hoje. A ARPANET é considerada a origem da Internet que cresceu de forma gigantesca e hoje conecta aproximadamente 500 milhões de redes, computadores e dispositivos móveis.

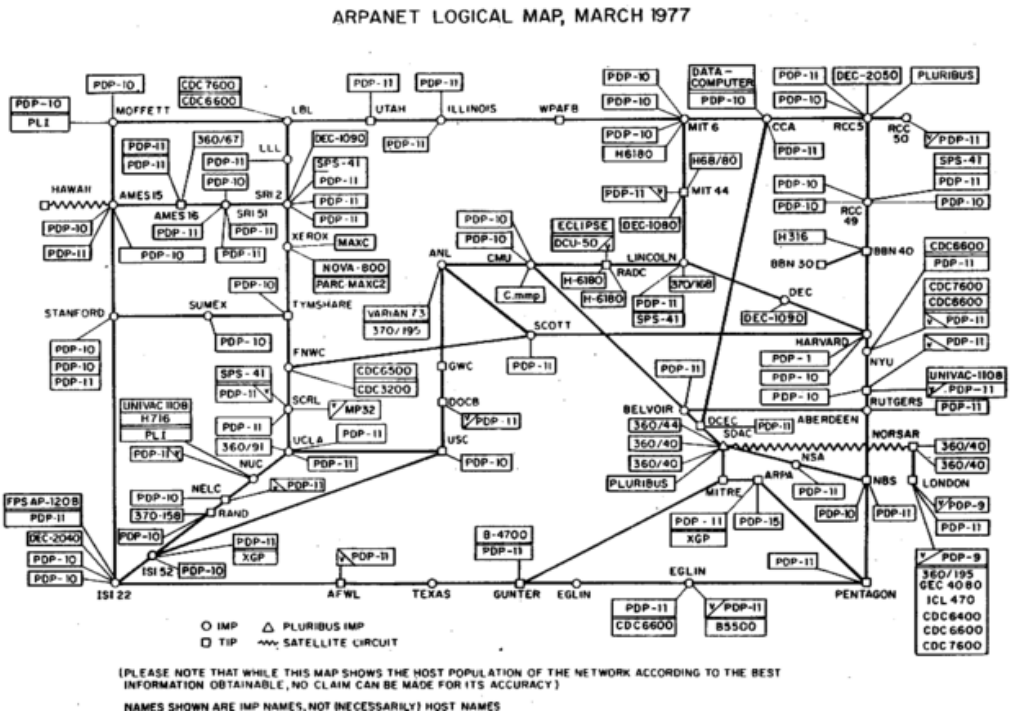

Figura 1 – Mapa lógico da ARPANET de março de 1977Fonte: ARPANET Maps - http://som.csudh.edu/fac/lpress/history/arpamaps/

A Internet está presente na vida de grande parte da população mundial, seja para o trabalho, estudo, entretenimento, comércio ou comunicação pessoal. Porém a grande rede esconde muitos perigos que vão desde simples sites com conteúdo impróprio, ilegal ou ofensivo, até grandes ataques que podem prejudicar provedores e usuários. A maioria das pessoas acha que não corre nenhum risco quando conectado à Internet. Alguns dos perigos aos quais os usuários estão susceptíveis podem ser chamados golpes da Internet e são:

- Furto de Identidade: é o ato de uma pessoa se passar por outra, utilizando nome, documentos, *e-mail* ou qualquer informação disponível na rede. O objetivo é tirar vantagens da vítima, de forma criminosa ou financeira.
- Fraude de Antecipação de Recursos: a vítima é induzida a fornecer informações confidenciais ou realizar pagamentos com a promessa de ganhos futuros.
- *Phishing*: através da combinação de tecnologia e engenharia social, a vítima é induzida a fornecer informações confidenciais. Ocorre principalmente por *e-mail*.
- *Pharming*: é um tipo específico de *phishing*, no qual a vítima é passa a acessar sites falsos, através da alteração de DNS (*Domain Name Server*).
- *Hoax* (boato): é uma mensagem, geralmente recebida por *e-mail*, com informações falsas ou alarmantes, em nome de entidades conhecidas. Tem como objetivos, desde espalhar desinformação até caluniar pessoas.

Além dessas ações, um computador pode ser “infectado” ou comprometido por códigos maliciosos, ou seja, pequenos programas que executam ações bem específicas. São eles:

- Vìrus - é um programa que se propaga de um computador para o outro, através de arquivos ou programas “infectados”, armazenados geralmente em mídias removíveis, como os antigos disquetes e os *pendrives*. Torna-se ativo, apenas quando o “hospedeiro” é executado. Executa ações específicas como apagar arquivos ou danificar componentes do computador.
- *Worm* - é um programa que se propaga de forma automática por uma rede. Explora falhas de segurança para invadir computadores e investigar a rede, enquanto esgota os recursos da máquina, até deixá-la indisponível.
- *Spyware* - é um programa que tem como objetivo coletar informações da vítima e enviá-las para terceiros
- *Backdoor* - é um programa que “abre uma porta” no computador da vítima. Permitindo acesso remoto as informações e arquivos, além de deixar disponível o computador para uso não autorizado.
- Cavalo de Tróia - é um programa que executa funções maliciosas, além daquela para a qual foi aparentemente projetado, sem o conhecimento do usuário.

Os grandes erros dos usuários é achar que nada de mal pode lhe acontecer e acaba não tomando os cuidados necessários. Porém os atacantes têm como objetivo conseguir acesso ao maior número de informações e computadores que for possível, sem levar em conta sua importância dentro da rede. Dessa maneira, além de tornar o computador inutilizável e colocar em risco seus dados pessoais, o invasor pode utilizar seus recursos para armazenar informações ilegais ou lançar ataques contra outras redes e computadores.

Muitos ataques ocorrem simultaneamente na Internet. Cada computador ou rede conectada pode ser alvo ou participar de um ataque. São vários os motivos que levam os atacantes a efetuar um ataque:

- Demonstração de poder

- Prestígio
- Motivações financeiras
- Motivações ideológicas
- Motivações comerciais

Os atacantes são conhecidos geralmente como *Hackers*, porém várias denominações são usadas dependendo da especialidade de cada uma. De acordo com a RFC2828, "*hacker* é alguém com um forte interesse em computadores, que gosta de aprender sobre eles e fazer experimentos". Muitas vezes é utilizado de maneira pejorativa, no lugar da denominação *Cracker*. Este "é alguém que tenta quebrar a segurança e ganhar acesso a sistemas que não lhe pertencem, sem ter autorização".

Um ataque é caracterizado quando um hacker, utilizando um ou mais computadores, ou até mesmo uma rede, coordena a execução de várias ações direcionadas a um ou mais computadores, servidores ou redes. Essas ações têm por objetivo causar algum dado ao alvo, como esgotamento dos seus recursos, desfiguração de conteúdo ou roubo de dados confidenciais. Para atingir seus objetivos os atacantes podem utilizar várias técnicas no ataque aos seus alvos:

- Exploração de vulnerabilidades - uma vulnerabilidade é uma falha em um sistema, seja de programação, configuração de sistemas operacionais, *softwares* ou serviços. Um atacante pode explorar essa falha e obter acesso ao sistema, às informações contidas neste ou simplesmente esgotar seus recursos.
- Varredura de portas (*scan port*) - é uma técnica na qual se utilizam *softwares* capazes de analisar se um ou mais hosts estão disponíveis na rede, quais os serviços disponibilizados, identificar o sistema operacional e outras informações. De posse desses dados, o atacante pode descobrir se o *host* analisado tem alguma vulnerabilidade que possa ser explorada.

- Interceptação de tráfego (*sniffing*) - técnica utilizada quando o atacante tem acesso direto à rede ou *host*. Utilizando um *software* chamado *sniffer*, todo dado que trafega na rede pode ser interceptado, armazenado e analisado. Informações importantes como *logins* de acesso, senhas e contas de banco podem ser descobertos.
- Força bruta - *login* e senha de sistemas com controle de acesso, podem ser descobertos por tentativa e erro, ou seja, por força bruta. Isso pode ser feito de forma manual ou automática, através de *softwares* que utilizam listas de palavras nas tentativas.
- Negação de serviço (DoS) - ataque de negação de serviço é a forma de ataque mais comum na Internet. Tem como objetivo esgotar os recursos de um *host* ou uma rede, causando indisponibilidade dos serviços.

Um ataque não é iniciado, executado e finaliza em um curto espaço de tempo. Os atacantes precisam de muito tempo e paciência para preparar e organizá-lo. Vários métodos e técnicas podem ser empregados. Por exemplo, através de engenharia social, um *backdoor* pode ser disseminado por *e-mail* (*phishing*). Ataques de força bruta podem comprometer outros *hosts*. Assim o atacante tem acesso a muitas máquinas que podem ser utilizadas em um ataque. Através da varredura de portas é possível descobrir vulnerabilidades em servidores. Então um ataque de negação de serviço distribuído pode ser executado a partir dos hosts comprometidos anteriormente.

2.2 HISTORICO DAS AMEAÇAS AOS SISTEMAS DE COMUNICAÇÃO

Ataque e invasão aos sistemas de comunicação não é um conceito novo. Não surgiu na era da comunicação digital ou durante seu desenvolvimento. Muito menos após o surgimento e crescimento da Internet. Desde que o homem fez uso da tecnologia para criar aparelhos de comunicação à distância, surgiu também a intenção de interferir de forma negativa no processo. A interceptação ou bloqueio dos dados transmitidos e o envio de dados não confiáveis já é realidade desde o início do século XX.

2.2.1 O Caso Maskeline

Em 1903, o primeiro “ataque” a um sistema de comunicação foi perpetrado, pouco antes do início de uma demonstração pública de um telégrafo sem fio. O italiano Guglielmo Marconi e seu funcionário, o físico John Ambrose Fleming, pretendiam demonstrar o funcionamento de um aparelho que transmitia código morse, à distância, através de ondas eletromagnéticas. A estação transmissora (figura 2), instalada na cidade litorânea de Poldh, na Inglaterra, enviaria um sinal para a estação receptora (figura 3), localizada no Royal Institution, em Londres.

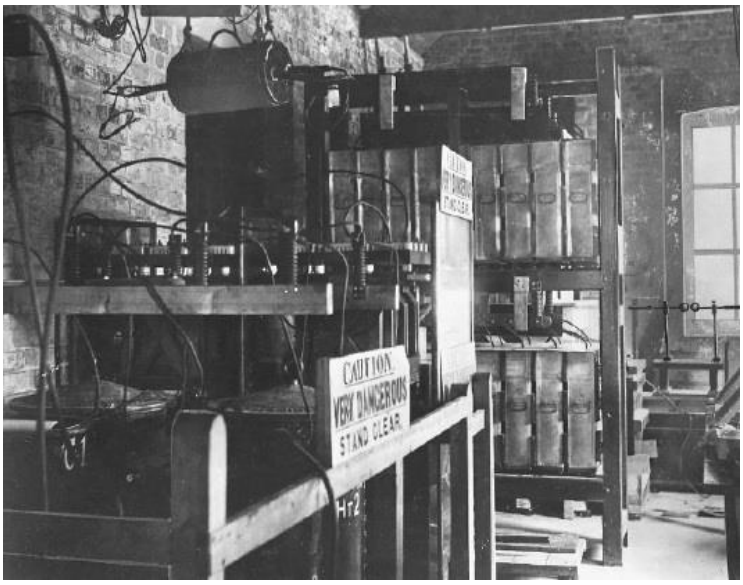

Figura 2 – Transmissor de Marconi na Estação de Poldhu

Fonte: Hong, Sungook. Wireless: From Marconi´s Back-Box to the audion, 2001, p.74.

A apresentação tinha por objetivo provar que a transmissão era totalmente sigilosa. O transmissor estaria calibrado de maneira a ser capaz de enviar mensagens apenas ao receptor e este ajustado apenas para receber dados do primeiro.

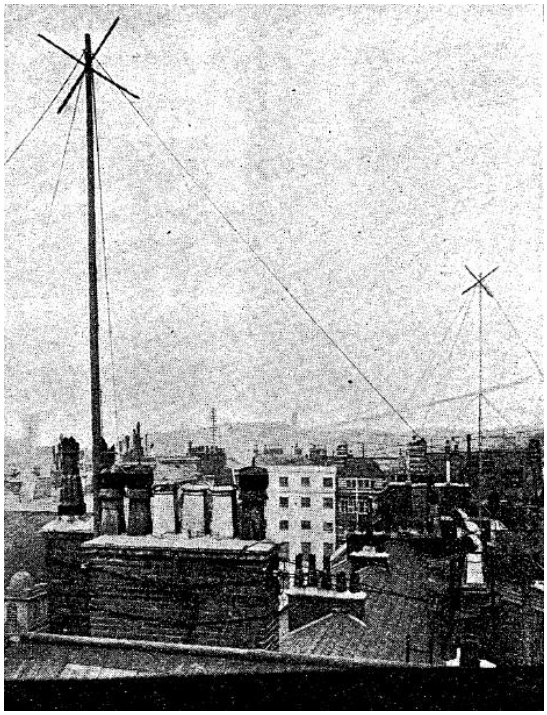

Figura 3 – Antena instalada no Royal Institute, em Londres

Fonte: Hong, Sungook. Wireless: From Marconi´s Back-Box to the audion, 2001, p.109.

Porém, antes de Marconi enviar sua mensagem para Londres, um sinal desconhecido foi recebido pelo aparelho de Fleming. A princípio pareceu ser uma forte interferência eletromagnética. Contudo, percebeu-se que uma mensagem em código morse estava sendo recebida. A palavra "*rats*" (ratos, em inglês) se repetiu várias vezes e em seguida a frase "*There was a young fellow of Italy, Who diddled the public quite prettily*" (Havia um jovem companheiro italiano, que enganou o público muito bem). A mensagem foi finalizada com outras frases e citações de Shakespeare. Logo após essa intervenção, a apresentação continuou com a recepção na mensagem de Marconi. Porém o estrago já estava feito. Fleming então envia uma carta ao jornal The Times com um pedido de ajuda para achar o culpado. Alguns dias depois, uma resposta é enviada ao jornal e publicada com uma confissão. O autor, Nevil Maskeline, mágico, cientista, rival de Marconi, assumiu a autoria pelo "ataque", afirmando que agiu pelo bem das pessoas e provando que o sistema não era seguro como seu inventor afirmava. Ele já havia utilizado técnicas de transmissão sem fio no acionamento de explosivos e para comunicação com um balão à uma altura de 15km, todas com sucesso. Mas suas ambições foram frustradas

porque Marconi patenteou a nova tecnologia. Assim, devido a uma rivalidade entre dois cientistas, uma nova “arma” surgiu e passou a ser utilizada massivamente, um século depois.

2.2.2 As ameaças através século XX

Durante todo o século XX, muitos ataques aconteceram aos mais variados meios de comunicação. Em 1932, um grupo de criptógrafos poloneses decifrou o código utilizado na máquina Enigma (figura 4). Esta era utilizada para codificar e decodificar mensagens através de rotores e foi muito usada pelo exército alemão.

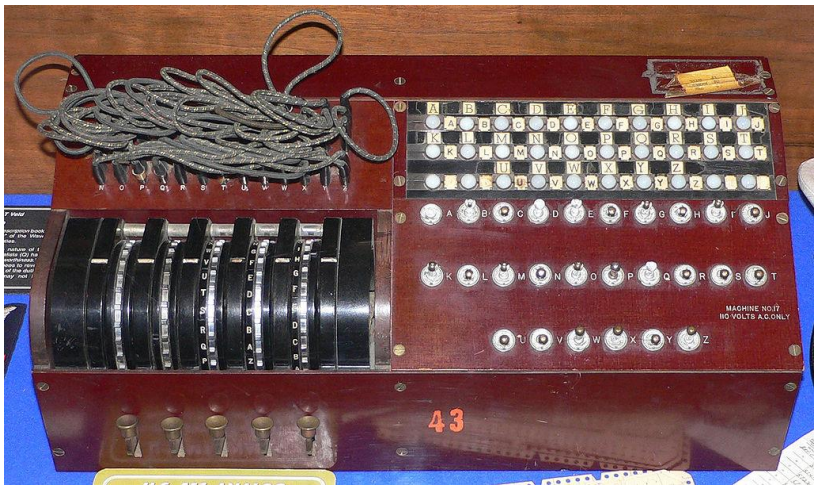

Figura 4 – Máquina Enigma

Fonte: Wikipedia

Em 1943, durante a Segunda Guerra Mundial, o Agente duplo francês René Carmille, sabotou os cartões perfurados alemães utilizados no censo da França. Conseguiu assim, salvar muitos judeus dos campos de concentração.

Em 1965, já na era dos grandes mainframes transistorizados, William D. Mathews do Instituto de Tecnologia de Massachusetts (MIT), descobriu uma

vulnerabilidade no sistema operacional de um mainframe IBM 7094 (figura 5) que permitia a fácil visualização das senhas dos usuários.

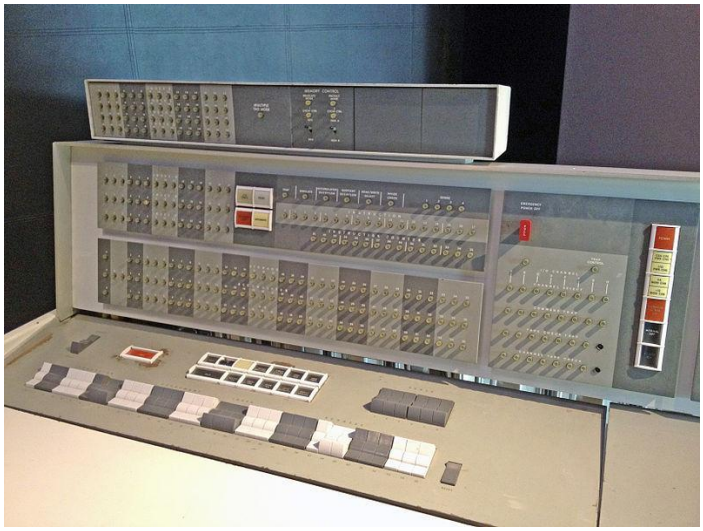

Figura 5 – Mainframe IBM 7094

Fonte: Wikipedia, http://en.wikipedia.org/wiki/IBM_7090

A década de 1970 foi dominada pelos *phone phreakers*, especialistas em explorar os sistemas de comunicação. Seu principal alvo era as companhias telefônicas. Utilizavam um dispositivo por eles criados, chamado Black-Box (caixa preta), que reproduzia os tons gerados pelas centrais telefônicas, permitindo ligações ilegais sem nenhum custo. Na década de 1980, muitos grupos foram formados, como o *Chaos Computer Club* na Alemanha e o *The Warelords* nos Estados Unidos. Os grupos serviam para trocar informações, organizar e executar ações em conjunto. Nessa época as BBS (*Bulletin Board System*) tornaram-se muito populares e viraram o principal alvo dos *hackers*, *phreakers* e outros especialistas no ataque e invasão de sistemas de comunicação. Com o surgimento e popularização da Internet, na metade da década, a atenção dos *hackers* caiu sobre a grande rede.

2.2.3 Os anos 80 e o Crescimento da Internet

Em 1983, o filme Jogos de Guerra, *War Games* como título original (figura 6), introduz ao público vários conceitos como invasão, *backdoor* (porta dos fundos), ataque de força bruta e todo o fenômeno do universo *hacker*. O filme conta como um adolescente consegue invadir o sistema militar americano, e achando que é um jogo, acaba ordenando um ataque a extinta URSS. O poder quase ilimitado do invasor é mostrado, assim como a histeria e paranoia que suas ações podem causar no governo e na população.

Figura 6 – Filme Jogos de Guerra

Fonte: Montagem feita com imagens do Google Images

Em 1988, Robbert Tappan Morris, estudante da Universidade de Cornell, do estado de Nova Iorque, desenvolveu um software que ficou conhecido como o primeiro grande *worm* da história (figura 7). Um *worm*, como já foi descrito anteriormente, é um programa que tem a capacidade de se espalhar em uma rede de computadores, aproveitando-se de falhas de segurança de serviços e sistemas operacionais. O objetivo do *worm* é coletar informações sobre o sistema infectado, transmiti-las para fora da rede local e podem ser usadas em outros ataques, além de consumir os recursos do computador infectado.

Antes do Morris Worm, em 1971, o *Creeper worm* infectou servidores da ARPANET, tendo sido desenvolvido por Bob Thomas. Sem nenhum efeito nocivo, apenas escrevia a frase “Eu sou o *Creeper*, pegue-me se for capaz” na tela dos usuários. No começo dos anos 1980, um programa desenvolvido por

John Shoch, para executar cálculos durante o tempo ocioso da máquina, se corrompeu e afetou vários computadores.

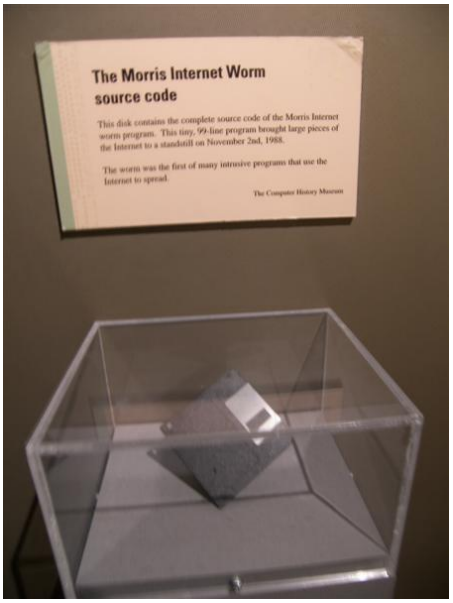

Figura 7 – Disquete com o código do Morris Worm

Fonte: Redmon, Jacques. The Morris Worm – 25 Years Later

No dia 2 de novembro de 1988, ocorreu o ataque. Perto das 6 horas da tarde, um programa foi executado em alguns computadores da Universidade de Berkley na Califórnia. O programa coletava informações da máquina, da rede e do usuário. Depois se replicava para outros computadores através de uma falha em alguns serviços como o *sendmail*, *fingerd* e *rsh*. O *worm*, que conseguia apenas infectar computadores da marca Sun Microsystem e Vax, com o sistema operacional BSD, derivado do Unix, se espalhou rapidamente e causou muita confusão entre administradores e usuários, quando esses perceberam que seus computadores estavam infectados. Arquivos incomuns e mensagens estranhas nos *logs* apareceram nas máquinas. O efeito mais notável foi sobrecarga no processamento dos computadores, causado pelo autor replicação e execução de muitas instâncias do *software*, o que os tornou praticamente inutilizáveis. O problema só foi controlado, depois que especialista da Universidade de Berkley e do Instituto de Tecnologia de

Massachusetts, conseguiram capturar o *worm*, analisá-lo e descobrir uma maneira de parar o espalhamento. Isso aconteceu 12 horas depois que a infecção foi descoberta.

O *Morris Worm*, como ficou conhecido, foi criado para mensurar o tamanho da Internet, porém a experiência saiu do controle e infectou muitos servidores, causando a paralisação de muitos serviços. Em torno de 6000 computadores foram infectados e o dano estimado foi algo em torno de 10 à 100 milhões de dólares.

2.2.4 Anos 90, a Década dos Vírus de computador

Na década de 1990, os vírus ficaram famosos, muitos deles utilizando nomes ainda mais famosos como Michelangelo, Leandro & Kelly, Freddy Krueger e Melissa. Os alvos foram principalmente os computadores pessoais baseados no sistema operacional MS-DOS. Foram facilmente espalhados através das BBS e programas *shareware*. Em 1994, *crackers* russos conseguem transferir 10 milhões de dólares de um banco para outros bancos do mundo todo. Em 1995 são lançados os filmes A Rede e *Hackers*. O primeiro conta a história de uma analista de sistemas que foi vítima de roubo de identidade através da Internet. O segundo mostra a vida de um grupo de jovens *hackers* que utilizam várias das técnicas de ataque e invasão, porém de forma fantasiosa. Nos anos seguintes vários ataques acontecem, como a invasão e alteração dos sites da CIA, Departamento de Justiça dos Estamos Unidos, da Força Aérea Americana e da Embaixada Americana na China.

2.3 TERMOS UTILIZADOS

Alguns termos são utilizados no decorrer deste trabalho e podem gerar confusão. Para evitar qualquer problema na interpretação desses, são consideradas algumas generalidades em algumas nomenclaturas.

Um dispositivo conectado à Internet, na maioria das vezes é um PC, Computador Pessoal ou *Desktop*, mas pode ser chamado também de máquina, computador ou *host*. Um computador mais robusto, de maior capacidade, utilizado em aplicações específicas e não utilizado a nível doméstico ou para trabalho, é chamado de servidor ou Server. Este também pode ser chamado de máquina ou host.

Os criminosos da Internet que executam os ataques são chamados de atacantes ou hackers. O uso deste último termo pode ser considerado incorreto em alguns casos. O porém o uso de *cracker* ou *phreaker* por causar ainda mais confusão.

2.4 AVISOS LEGAIS

Todas as informações aqui apresentadas, dados, comandos, tabelas, ilustrações, têm objetivo acadêmico. Este trabalho é apenas um estudo, uma compilação de informações sobre os ataques de negação de serviço e não deve ser tratado como um manual ou tutorial para realização de ataques.

Qualquer tipo de ataque ou invasão a computadores ou redes é considerado crime e sujeito a punições legais. As simulações práticas apresentadas no capítulo 6, devem ser executadas em uma rede isolada, em laboratório ou máquinas virtuais. O acesso à Internet ou a rede local deve ser bloqueado para evitar que os efeitos dos ataques simulados sejam propagados, causando prejuízos não esperados e desnecessários.

O autor não se responsabiliza por qualquer uso indevido das informações aqui contidas.

3 DESENVOLVIMENTO – ATAQUES DE NEGAÇÃO DE SERVIÇO

3.1 CATEGORIAS DOS ATAQUES DoS

De acordo com McClure, Scambray e Kurtz, os ataques DoS podem ser classificados em quatro categorias básicas: consumo de largura de banda, consumo de recursos, falhas de programação e ataques de roteamento ou DNS. Invasão e obtenção de acesso tornaram-se tipos secundários, pois é muita mais fácil tornar uma rede ou sistema indisponível do que obter acesso. Essa facilidade deve-se ao fato que os protocolos de rede, como TCP/IP, HTTP e FTP foram projetados para serem usados em um ambiente confiável e não são livres de falhas. Levando ainda em conta a enorme variedade de sistemas operacionais existentes no mercado e combinações entre esses e os serviços em rede, a exploração dessas falhas e fraquezas é muito simples, permitindo assim um ataque de negação de serviço. A seguir, as 4 categorias básicas de ataque são descritas.

3.1.1 Consumo de largura de banda

Forma mais simples de ser executar um ataque DoS é consumindo toda sua largura de banda disponível com a Internet ou. O ataque pode ser iniciado dentro da rede ou o que é mais comum, remotamente. Nesse tipo de ataque há duas situações possíveis. Na primeira, o atacante tem uma conexão com a rede ou Internet maior do que a da vítima. Por exemplo uma conexão E1 (2Mbps) sendo utilizada para atacar uma conexão discada de 126Kbps. Um artifício utilizado pelos atacantes é atacar uma rede privada com uma conexão de 100Mbps, onde será possível atacar redes conectadas através de E1 ou T1. Na segunda situação, o atacante possui controle sobre um ou vários *hosts* ou redes com conexão de banda estreita, como uma conexão discada à 56Kbps ou 128Kbps. Explorando vulnerabilidades, o atacante utiliza vários *hosts*, com um serviço em comum comprometido, em um ataque amplificado. Cada *host*

envia um pequeno tráfego para a vítima que terá sua conexão de banda larga saturada em pouco tempo.

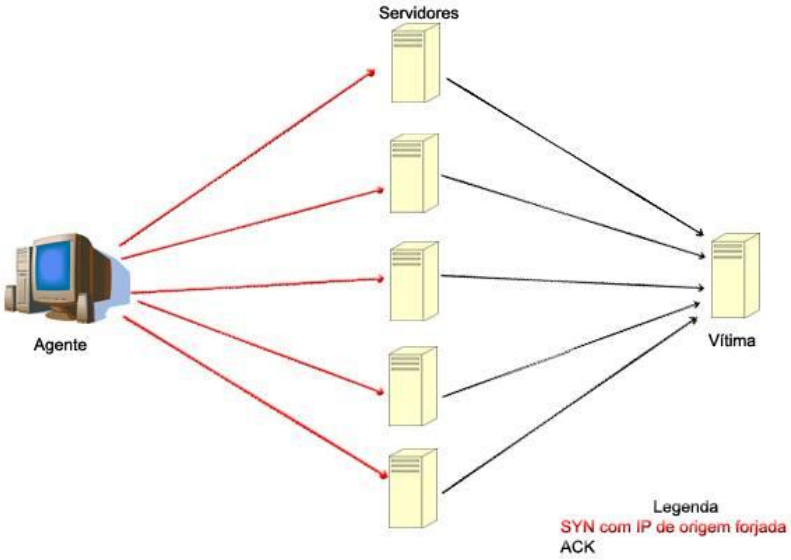

Figura 8 – Ataque com consumo de largura de banda

Fonte: Autoria Própria

3.1.2 Consumo de recursos

Nesse tipo de ataque, o objetivo é consumir os recursos de um sistema. Entende-se como recursos, uso de CPU, memória, espaço em disco ou processos. Durante o ataque, esses recursos serão levados ao seu limite máximo, até que o sistema fique impossibilitado de processar e fornecer os seus serviços ou fique totalmente inutilizável.

3.1.3 Falhas de programação

Qualquer *software*, sistema operacional e até mesmo processadores têm alguma falha em sua programação. Uma determinada condição, como uma instrução não programada ou não esperada, uma informação de tamanho muito grande pode acionar um processo que irá desencadear o esgotamento

de recursos do sistema. Os atacantes têm conhecimento dessas falhas e irão explorá-las em um ataque.

3.1.4 Ataque de roteamento ou DNS

Em um ataque baseado em roteamento, a tabela de roteamento de uma rede é manipulada. Fragilidade nos protocolos RIP e BPG podem ser exploradas, como a falta de autenticação. O atacante altera o roteamento de uma rede, desviando o tráfego originado dentro desta, para a rede do atacante ou para uma rede inexistente. Dessa maneira, a rede atacada fica impossibilitada de rotear seu tráfego corretamente, ficando totalmente congestionada e indisponível.

O ataque baseado no DNS consiste na manipulação da tabela de resolução de endereços. Nessa situação a rede vítima fica impossibilitada de resolver os endereços solicitados pelos seus *hosts* ou informa endereços incorretos.

3.2 TIPOS DE ATAQUES DoS

Ainda, de acordo com McClure, Scambray e Kurtz, alguns tipos de ataques DoS podem ser considerados genéricos, pois podem afetar uma variedade de sistemas. São ataques, principalmente das categorias de consumo de banda e recursos. O elemento comum entre esses tipos de ataque é a manipulação de um protocolo de camada 2 ou 3 do modelo OSI, como IP, ICMP, TCP e UDP. A seguir são descritos alguns desses tipos de ataque.

3.2.1 Smurf

Um ataque Smurf é o mais simples, porém é o pior ataque que pode ser executado. Isso é conseguido, através do uso do efeito da amplificação, onde uma rede é utilizada como fator amplificador. São três os elementos desse tipo

de ataque: o atacante, a rede amplificadora e a vítima. O ataque é iniciado quando o atacante envia um comando *ping* (pacote ICMP *Echo*) para o endereço de *broadcast* de uma rede (*directed broadcast ping request*). Por exemplo, para a rede 10.10.10.0/24, o endereço de broadcast é 10.10.10.255. Uma mensagem ICMP *Echo Request* é enviada para esse IP. Em uma situação normal, cada *host* da rede, enviaria uma mensagem de resposta E*cho Reply* para a origem, no caso o atacante. Mas isso não acontece. Nesse tipo de ataque, é utilizada uma técnica chamada de IP *spoofing*, onde o endereço de origem do pacote ICMP é mascarado. Através da manipulação do protocolo, o atacante muda o IP de origem para o IP da vítima. Dessa maneira, todos as respostas ao ping (*Echo Reply*), serão enviadas ao um só *host*. Se a rede tiver 100 *hosts*, esta terá um fator de amplificação 100. Quanto maior a rede, menor o tempo que leva para que toda a banda disponível para a vítima seja consumida. Dependendo da topologia e capacidade, a própria rede amplificadora poderá ser comprometida.

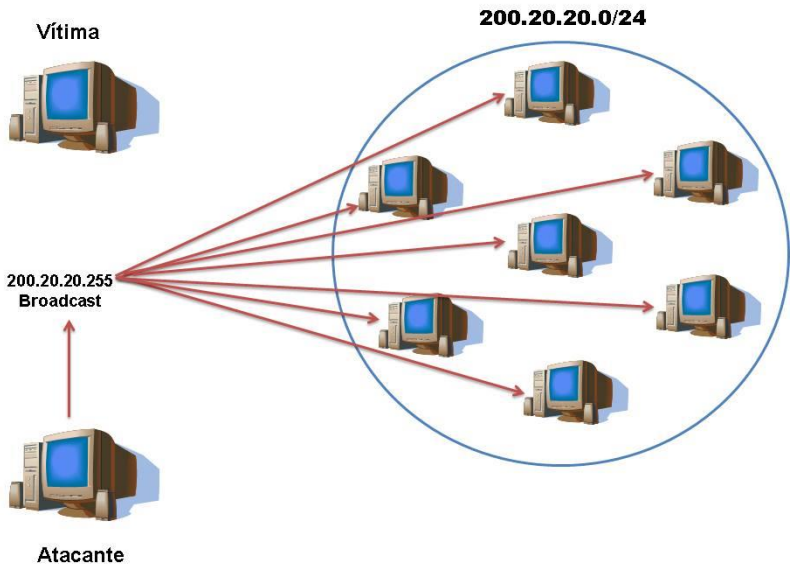

Figura 9 – Ataque Smurf

Fonte: Autoria Própria

Uma variação do ataque Smurf é o ataque Fraggle. A diferença entre eles é apenas o protocolo utilizado. No segundo caso, é utilizado o protocolo UDP em vez de ICMP.

Uma forma de prevenir um ataque Smurf, é desabilitar a funcionalidade *direct broadcast* no roteador de borda, através do comando: "*no ip directed-broadcast*".

O ataque Smurf é muito difícil de ser rastreado devido ao IP *spoofing*. Sem o conhecimento do IP real de origem, o atacante nunca será descoberto. A única maneira de isso acontecer, é fazer o rastreamento do endereço MAC da origem em cada *hop* da rede. Porém isso é muito difícil de ser feito, devido ao tamanho da rede.

3.2.2 Inundação SYN

Um ataque de inundação SYN (*SYN Flood*) é executado através da manipulação do protocolo TCP, em uma arquitetura cliente-servidor. O servidor é um *host* executando um serviço que terá uma porta específica no estado inicial LISTEN, como HTTP (porta 80), FTP (porta 21), TELNET (porta 23) e SSH (porta 21). O cliente estabelecerá uma conexão com esta porta para utilizar o serviço. Para entender como esse ataque ocorre, é necessário saber como uma conexão TCP é estabelecida em uma situação normal. O "aperto de mão tripo" (3-*Way Handshake*) ocorre antes que uma conexão TCP entre o cliente e o servidor seja estabelecida. Esse processo é composto por três etapas:

a. O cliente envia ao servidor uma mensagem SYN (*Synchronize*) à uma porta específica, estando este último no estado LISTEN.
b. O estado da porta no servidor, muda para SYN_RECV (*Synchronize Received*) e uma mensagem SYN-ACK (*Synchronize Acknowledge*) é enviada ao cliente
c. O cliente envia a mensagem ACK (*Acknowledge*) ao servidor. A conexão é ent estabelecida e o estado da porta do sevidor muda para ESTABLISHED (Estabelecida).

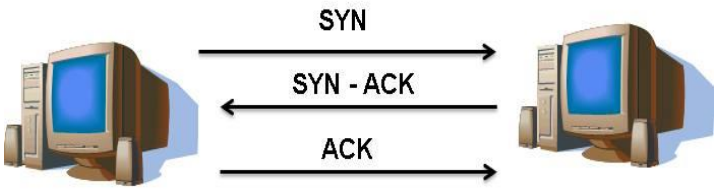

Figura 10 – 3 Way Handshake

Fonte: Autoria Própria

O tempo entre o envio do pacote SYN-ACK e do ACK pode variar e no servidor esse tempo pode ser configurado. Esse tempo varia de sistema para sistema, podendo ser de alguns segundos até vários minutos. Além disso, o servidor aloca um número finito de recursos para as requisições que são recebidas por uma porta. E é justamente esse limite que um atacante pode explorar durante um ataque de inundação SYN.

Quando o ataque tem início, o servidor vítima recebe um pacote SYN com IP de origem forjado (IP *Spoofing*). O servidor responde com a mensagem SYN-ACK normalmente. Se este IP existir, o host do IP forjado envia ao servidor uma mensagem RST, indicando que não foi ele que iniciou a conexão. Porém, o atacante deve escolhe um IP de origem inalcançável para o servidor. Dessa maneira, o servidor envia a mensagem, mas nunca recebe uma posta ACK ou RST. Como o servidor recebeu uma requisição para uma conexão em potencial, esta passa para o estado SYN_RECV e é colocada em uma fila de conexões (*Connection Queue*). Mas como a conexão não é estabelecida, ela não sairá da fila antes que o tempo de espera se esgote. Se o atacante enviar várias requisições SYN em intervalos menores que o tempo de espera, a fila de conexões irá crescer. Geralmente, a fila é muita pequena, e em pouco tempo, a porta não responderá mais nenhuma tentativa de conexão, seja real ou não.

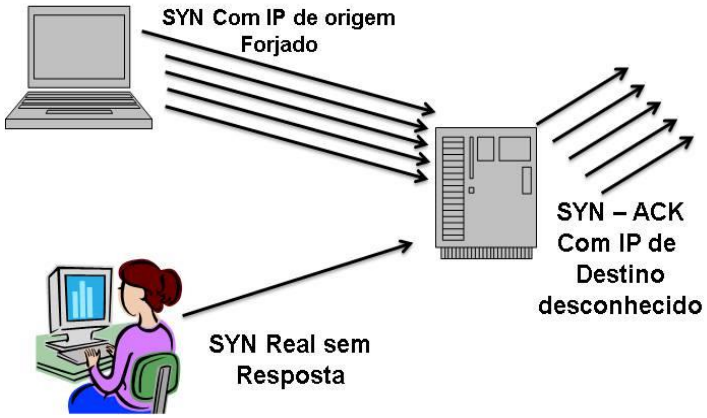

Figura 11 – Ataque de inundação SYN

Fonte: Autoria Própria

Uma maneira para se determinar quando um ataque SYN está em progresso, é através do comando “*netstat*”, presente na maioria dos sistemas operacionais. Se um grande número de conexões no estado SYN_RECV estiver presente, a chance de um ataque estar sendo executado é grande.

```
c:\netstat -n -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1030         127.0.0.1:1032         ESTABLISHED
  TCP    127.0.0.1:1032         127.0.0.1:1030         ESTABLISHED
  TCP    10.1.1.19:21           10.1.1.4:1256          SYN_RECEIVED
  TCP    10.1.1.19:21           10.1.1.4:1257          SYN_RECEIVED
  TCP    10.1.1.19:21           10.1.1.4:1258          SYN_RECEIVED
  TCP    10.1.1.19:21           10.1.1.4:1259          SYN_RECEIVED
  TCP    10.1.1.19:21           10.1.1.4:1260          SYN_RECEIVED
  TCP    10.1.1.19:21           10.1.1.4:1261          SYN_RECEIVED
  TCP    10.1.1.19:21           10.1.1.4:1262          SYN_RECEIVED
  TCP    10.1.1.19:21           10.1.1.4:1263          SYN_RECEIVED
  TCP    10.1.1.19:21           10.1.1.4:1264          SYN_RECEIVED
  TCP    10.1.1.19:21           10.1.1.4:1265          SYN_RECEIVED
  TCP    10.1.1.19:21           10.1.1.4:1266          SYN_RECEIVED
  TCP    10.1.1.19:4801         10.57.14.221:139       TIME_WAIT
```

Figura 12 – Comando netstat com conexões no estado SYNC_RECV

Fonte: Google Images

Da mesma maneira que um ataque Smurf, o ataque SYN não pode ter sua origem identificada com facilidade, devido ao IP de origem ser forjado. Para minimizar os efeitos desse tipo de ataque, alguns cuidados podem ser tomados:

- Aumentar o tamanho da fila de conexões.

- Diminuir o tempo de espera para estabelecimento da conexão.
- Manter o sistema operacional e serviços atualizados e livre de falhas.

Essas medidas podem minimizar os efeitos de um ataque ou até mesmo evitá-los, porem como custo de utilizar recursos adicionais do sistema e diminuir sua performance.

3.2.3 Ataque de fragmentação

Também chamado de *Teardrop*, este tipo de ataque explora uma falha no protocolo IP. Foi bastante utilizado para provocar instabilidade de algumas versões do O.S Microsoft Windows, como 3.1x, 95, NT e versões antigas do *Kernel* do Linux.

Este tipo de ataque utiliza a manipulação dos campos *Header Length* (tamanho do cabeçalho) e *Fragment Offset* (defasagem de fragmento) do cabeçalho do protocolo IP (IP *Header*). Esses campos (figura 7) são utilizados pelo receptor, para reordenar os pacotes recebidos. O *Offset* indica a posição inicial dos dados e o final do pacote é calculado utilizando o campo tamanho. O próximo pacote terá o campo *offset* igual a soma do *offset* e tamanho do pacote anterior.

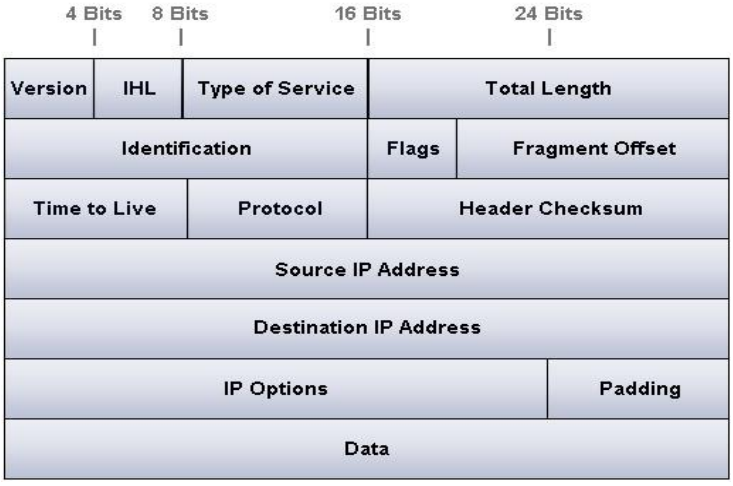

Figura 13 – Cabeçalho do protocolo IP

Fonte: Google Images

Durante o ataque, o atacante envia para o host vítima, uma série de pacote IP fragmentados, com valores incorretos de tamanho e *offset*. Em uma situação normal, o receptor, utilizando os campos já citados para reordenar os pacotes. Porém a vítima não consegue fazer a reordenação dos pacotes devido a manipulação feita pelo atacante. Os pacotes são sobrepostos e o host receptor acaba ficando instável devido alto processamento ou falta de memória na tentativa de ordenar os pacotes.

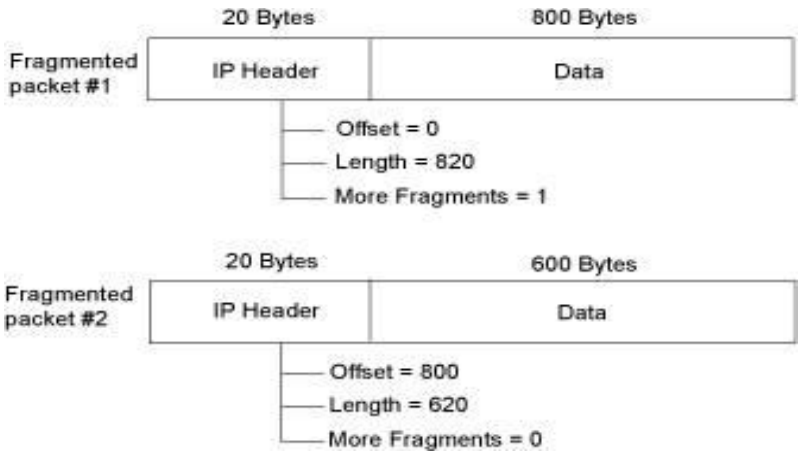

Figura 14 – Pacotes IP manipulados

Fonte: Google Images

Atualmente, as falhas exploradas no ataque de fragmentação foram identificadas e corrigidas. Porém, alguns sistemas operacionais recentes, como Windows Vista e 7 podem ser vulneráveis, quando em condições específicas, como por exemplo, quando o serviço de compartilhamento de arquivos SMB (*Server Message Block*) está habilitado. A solução para estes casos é simples, bastante uma correção na configuração ou atualização do sistema operacional.

3.2.4 Ping da Morte

O famoso ataque *Ping* na morte (*Ping of Death*) foi muito usado nos primórdios da Internet e é o tipo de ataque mais antigo que se conhece.

Atualmente, os sistemas operacionais recentes, não são afetados. O ataque era executado enviando um *ping* mal formado para um *host*.

O tamanho máximo permitido de um pacote IP é de 64k *bytes* ou 65635 *bytes*. O ataque consiste em enviar um pacote com tamanho superior ao permitido para um *host*. Quando esse datagrama for recebido, causará um transbordamento de dados ou buffer overflow. Isso causará uma instabilidade no sistema, paralisação ou reinicialização do sistema operacional.

Essa vulnerabilidade do protocolo IP não era limitada aos sistemas operacionais Windows e Unix. Outros O.S como Mac, Netware e dispositivos como impressoras e roteadores também podiam ser afetados. Sua execução é extremamente fácil, não sendo necessário nenhum conhecimento, além do comando ping com alguns parâmetros adicionais: "*ping* -i 1 -l 65500 ip_do_destino –t".

Atualmente, essa falha não ocorre, pois nenhum sistema ou dispositivo, envia ou recebe pacotes com mais de 64k bytes.

3.3 ATAQUE DISTRIBUIDO DE NEGAÇÃO DE SERVIÇO

3.3.1 Introdução ao DDoS

A virado do século XX para o século XXI, viu o nascimento de uma nova categoria de ataque de negação de serviço, o DDoS, *Distributed Denial of Service* ou Ataque Distribuído de Negação de Serviço. Esse tipo de ataque é uma evolução do DoS que foi usado por décadas. O primeiro DDoS bem documentado, ocorreu em agosto de 1999, quando mais de 200 máquinas foram "infectadas" com uma ferramenta chamada *Trinoo* e atacaram um único servidor da Universidade de Minnesota, o deixando indisponível por mais de dois dias. No ano seguinte, em fevereiro, o primeiro ataque mundialmente noticiado, durou 3 dias e afetou os servidores de importantes empresas de comercio eletrônico. O site Yahoo foi a primeira vítima, no dia 7, ficando inacessível por aproximadamente 3 horas e causando um prejuízo de 500 mil

dólares. No dia 8, foi a vítima foi a maior livraria online do mundo. A Amazon foi atacada, juntamente com o Ebay e a CNN. Este ataque causou uma dificuldade no acesso desses sites, alguns ficando indisponível por horas. O prejuízo somado passou da casa dos milhões de dólares. No terceiro dia, o E-Trade e ZDNet também foram atacados.

Diferente do ataque DoS que parte de um único host, o DDoS pode ter origem em dezenas, centenas ou milhares de hosts. As ferramentas utilizadas até então na defesa e detecção de ataques DoS, se tornaram ineficazes diante da nova ameaça, pois eram baseados na monitoração do volume de pacotes recebidos de um único endereço. Outro fato que torna o DDoS ainda mais agressivo é a dificuldade de se descobrir sua origem. O ataque DoS já era extremamente difícil de ser rastreado devido a técnica de ip spoofing de origem. Em um ataque distribuído, a tarefa de determinar a origem de centenas de endereços forjados é um trabalho praticamente impossível. Um dos hosts que originou o ataque pode ser rastreado através da captura de pacotes em cada roteador por onde o pacote passou e o endereço mac de origem identificado, roteador a roteador, até chegar ao atacante. Para dificultar, isso precisa ser feito enquanto o ataque ocorre. Mesmo que isso seja feito e o host identificado, o real responsável pelo ataque não poderá ser descoberto. Isso porque todas as máquinas utilizadas no ataque foram invadidas e comprometidas, tendo o invasor, tomado todas as medidas necessárias para cobrir os seus rastros.

Um ataque DDoS é mais difícil de ser executado do que um DoS. Antes do ataque ser iniciado, algumas etapas devem ser seguidas. Um DDoS típico é antecedido pela invasão de um *host*, através de uma exploração de alguma vulnerabilidade ou de senha roubada, de preferência com uma conexão com a Internet de alta capacidade. Esse host será utilizado como o DDoS Mestre ou *Master*, ou seja, o controlador de toda a rede DDoS. O sistema operacional desse *host* é preparado e ferramentas de *hacking* são instaladas. O atacante usa então *scanners* de porta, detectores de sistema operacional, ferramentas de *exploit* para invadir muitas máquinas. São instalados então, programas para DoS/DDoS, no maior número de *hosts* possível. Essas ferramentas que serão utilizadas no ataque propriamente dito. Essa tarefa é feita de forma automática,

através de scaneamento de uma grande faixa de endereços IP afim de encontrar hosts com falhas e vulnerabilidades que permitam a invasão e o comprometimento do sistema. Esses *hosts* são conhecimento como Agentes, *deamons* ou *zombies* e são as primeiras vítimas de um ataque DDoS. O proprietário ou administrador do *host* Agente pode nunca saber que o sistema foi invadido e será utilizado em um ataque. Mesmo que o software malicioso seja identificado e removido, a localização do Mestre DDoS, da onde a invasão foi efetuada, não será identificada. Esse é um dos motivos que torna um ataque DDoS praticamente impossível de ter sua origem reconhecida, pois será extremamente difícil para a vítima chegar em um host Agente, quanto mais no *host* Mestre. Dessa maneira, o responsável pelo ataque está totalmente protegido e escondido dentro da Internet, podendo executar um ou mais ataques sem se preocupar em ser descoberto. Após ter muitos Agentes sob o seu controle, o atacante pode então iniciar o ataque à vítima escolhida. Através do *host* Mestre, o atacante envia para todos os seus Agentes um comando que fará que o ataque DDoS propriamente dito seja iniciado. Cada Agente irá executar um simples ataque DoS contra a vítima. Porém, como muitos Agentes fazem o mesmo ataque ao mesmo tempo, o sistema atacado ficará sobrecarregado em pouco tempo e seus serviços ficarão indisponíveis.

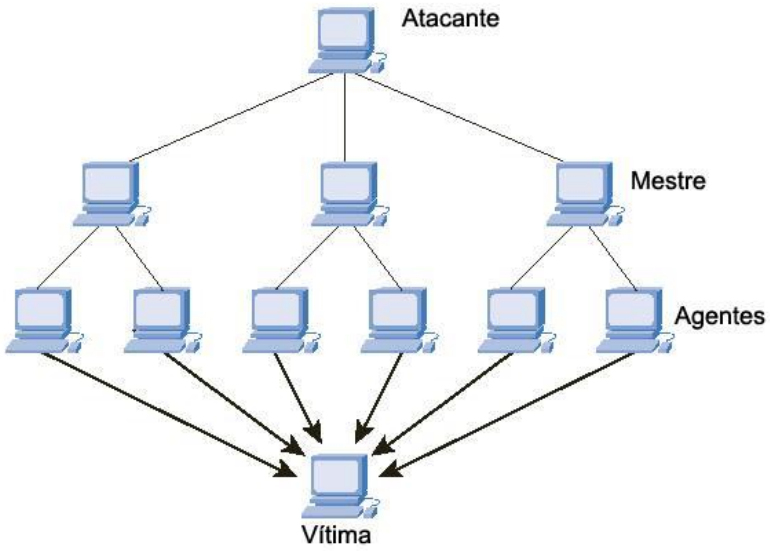

Figura 15 – Ataque DDoS

Fonte: Autoria Própria

A mecânica de um ataque DDoS é muito simples, porém exige muito tempo e paciência para ser preparado. O *hacker* deve ter um vasto conhecimento em sistemas operacionais (Unix, Linux, Windows, Mac), programação, nos vários protocolos utilizados na Internet, principalmente TCP, IP, UPD, ICMP, além das vários programas e ferramentas utilizadas nas etapas de invasão e comprometimento do Mestre e dos Agentes.

3.3.2 Categorias de ataques DDoS

Assim como o ataque DoS, o DDoS pode ser executado utilizando-se diferentes técnicas, porém sempre seguindo a estrutura apresentada anteriormente. Pode-se classificar os ataques distribuídos, da mesma maneira como os não distribuídos, em categorias:

3.3.2.1 Ataque baseado em conexões

A intensão do atacante é exaurir toda as conexões TCP disponíveis da vítima, seja de um *Firewall*, servidor HTTP ou outro serviço baseado em conexões.

3.3.2.2 Ataque volumétrico

A banda disponível na conexão da vítima é ocupada por tráfego originado na rede DDoS com o objetivo de isolar o serviço oferecido do resto da Internet.

3.3.2.3 Ataque de fragmentação

A vítima recebe uma infinidade de pacotes TCP ou UDP fragmentados que necessitam de reordenação. Esse processo acaba por reduzir a performance do host vítima, de maneira a afetar o serviço oferecido.

3.3.2.4 Ataques à aplicação

Aplicações ou serviços específicos podem ser prejudicados através de alguma falha ou vulnerabilidade.

3.3.3 Amplificação

O efeito causado por um ataque DDoS pode ser aumentado ainda mais, utilizando-se técnicas também já utilizadas nos ataques DoS. A amplificação é um artifício simples, porém de grande poder destrutivo. A maneira mais comum de executar um ataque amplificado é através do uso de servidores DNS espalhados pela Internet e com pouca ou sem nenhuma restrição de uso. Forjando o endereço IP da vítima, o atacante envia uma solicitação ao serviço através de um pequeno pacote TCP. A resposta do servidor pode ser um grande pacote direcionado à vítima. Quando utilizado em um ataque não distribuído, o efeito amplificador é enorme. Sendo um ataque distribuído, com vários Agentes realizando requisições a inúmeros servidores DNS, o tráfego recebido pela vítima será gigantesco. Esse tipo de ataque é um dos mais potentes, podendo derrubar um serviço ou toda uma rede em muito pouco tempo.

3.3.4 CLASSIFICAÇÃO DE ACORDO O SOFTWARE UTILIZADO

Pode-se classificar os ataques DDoS através das ferramentas utilizadas na execução do ataque. A seguir serão apresentadas algumas destas ferramentas que se tornaram modelos para outras ferramentas desenvolvidas nos últimos anos.

3.3.4.1 Trinoo

Também chamado de *Trin00*, foi o primeiro *software* desenvolvido especificamente para ataques DDoS. Começou a aparecer na Internet em meados de 1999. É baseado em um ataque DoS do tipo inundação SYN (este tipo de ataque já explicado no capítulo anterior). A comunicação entre o DDoS Mestre e os Agentes é feita utilizando-se algumas portas específicas. Ver tabela 1 para detalhe das portas utilizadas.

3.3.4.2 Tribe Flood Network

Mais conhecido como TFN. É uma ferramenta mais poderosa e elaborada que o *Trin00*. É utilizada para formar uma grande rede DDoS capaz de executar vários tipos de ataque DoS como inundação SYN, inundação ICMP, inundação UDP e ataques do tipo SMURF. Além da variedade de ataques em sua implementação, sua rastreabilidade é fortemente dificultada, pois toda comunicação entre o atacante, Mestre e Agentes é feita através de pacotes ICMP ECHO e ICMP REPLAY. A ausência de pacotes TCP ou UDP torna esse tráfego praticamente invisível na Internet, devido a maioria das ferramentas de monitoração serem programadas para ignorar esse tipo de mensagem.

3.3.4.3 Stacheldraht

Ferramenta batizada com o nome alemão para arame farpado. É uma combinação do *Trin00* e TFN com alguns aperfeiçoamentos. Utiliza encriptação na comunicação entre o Mestre e os Agentes, assim como alguns processos automatizados. Os ataques executados são os mesmos do TFN.

3.3.4.4 Trinity

Assim como as outras ferramentas, é utilizado para executar vários ataques DoS de inundação. A grande diferença para as demais ferramentas encontra-se na forma de comunicação entre o Mestre e os Agentes, feita através do protocolo IRC (Internet Chat Relay) ou o ICQ (antigo software para troca de mensagens instantâneas).

3.3.4.5 Shaft

Similar ao *Trin00*, porém com a diferença que o software cliente, através da qual a rede DDoS é controlada, pode altarar o tamanho dos pacotes enviados em um ataque de inundação DoS, assim como o tempo de duração do ataque. Uma característica da ferramenta é o uso do mesmo número de sequência para os pacotes TCP: 0x28374839.

3.3.4.6 Tribe Flood Network 2K

Conhecido também como TFN2K. É uma variante mais complexa do TFN. Possui algumas funcionalidades específicas para dificultar sua identificação e rastreio, para executar comandos remotamente, gerar endereços IP da origem através da técnica de IP *spoofing* e transportar o tráfego dentro da rede DDoS utilizando vários protocolos como TCP, UDP e ICMP. Executa ataques DoS de inundação, além de ataques que enviam pacotes inválidos ou mal formados para a vítima, como o ataque *Teardrop*.

3.3.5 Utilização de portas TCP e UDP

Na tabela seguinte, encontram-se as portas utilizadas na comunicação entre o atacante, Mestre e Agentes nas ferramentas já apresentadas.

Ferramenta	Atacante-Mestre	Mestre-Agente	Agente-Mestre
Trinoo	27665/TCP	27444/UDP	31335/UDP
TFN	ICMP Echo/Echo Reply	ICMP Echo Reply	ICMP Echo/Echo Reply
Stacheldraht	16660/TCP	65000/TCP	ICMP Echo Reply
Trinity	6667/TCP	6667/TCP e 33270/TCP	
Shaft	20432/TCP	18753/UDP	20433/UDP

Tabela 1 – Utilização de portas nas ferramentas DDoS

Fonte: Kessler, Gary C. Defenses Against Distributed Denial of Service Attacks.

As ferramentas descritas são as mais utilizadas e as mais conhecidas. Existem inúmeras outras alternativas para a preparação de uma rede DDoS e execução do ataque. Algumas são amplamente distribuídas e utilizadas entre as comunidades *hackers*. A evolução desse tipo de software acompanha a evolução dos sistemas operacionais e dos serviços disponíveis na Internet. Diariamente falhas e vulnerabilidades são detectadas e corrigidas. Dessa maneira os hackers precisam descobrir novas maneiras de invadir e atacar os sistemas, por mais modernos e seguros que sejam.

3.3.6 Defesa Contra Ataques DDoS

Não existe uma técnica ou ferramenta contra os ataques distribuídos de negação de serviço. Uma só entidade ou administrador de rede não consegue se defender sozinho de um ataque tão poderoso. Esse deve ser um esforço de todas as organizações que desempenham funções básicas dentro da Internet. Provedores de acesso, centros de pesquisa, grandes empresas do ramo devem se unir com o objetivo único de proteger a rede. Existem ferramentas que auxiliam na defesa e procedimentos recomendáveis que devem ser seguidos em qualquer rede conectada à Internet.

3.3.6.1 Procedimentos recomentados para defesa

a. Aplicar sempre que disponíveis e de forma rápida, correções e atualizações de hardware, sistemas operacionais, serviços e aplicativos.
b. Analisar periodicamente os logs do sistema e procurar por atividade suspeita, como tentativas frustradas de acesso e excesso de conexões.
c. Monitorar periodicamente o sistema, testando-o contra vulnerabilidades conhecidas. Todas as portas TCP e UDP abertas, devem ser associadas a algum serviço disponível na rede.
d. Monitorar o tráfego dentro da rede, procurando por comportamentos fora do normal.
e. Utilizar ferramentas de auditoria que verifiquem inconsistências em todo o sistema.
f. Evitar uso de softwares de fontes desconhecidas e não confiáveis.
g. Educar os usuários para que estes sejam capazes de detectar ameaças e reportar irregularidades.

Todas estas ações e procedimentos servem para evitar que redes e sistemas sejam usadas em um ataque ou sejam vítimas. Manter toda rede segura é a chave para não sofrer os danos causados por um DDoS. É possível ainda, utilizar um *Firewall*, um elemento que irá impedir que um ataque atinja a rede através da filtragem de pacotes. Os principais filtros utilizados para manter uma rede a salvo dos ataques DDoS são descritos a seguir.

3.3.6.2 Filtros de Rede Recomendados

a. Filtro de saída - todos os pacotes saintes da rede devem ter o endereço IP de origem analisado e identificado com um *Network* ID conhecido,

caso contrário, devem ser descartados. Isso evita que um ataque utilizando endereço de origem forjado (IP *Spoofing*) seja originado na rede.

b. Endereços de *broadcast* - não há nenhuma razão para que endereços de *broadcast* sejam enviados para uma rede. Esse tipo de tráfego é de uso exclusivo da rede local e deve ser bloqueado na entrada.
c. Portas sem uso - qualquer porta TCP ou UDP que não esteja em uso ou não seja disponibilizada para a rede externa, deve ser bloqueada no *Firewall*.
d. Endereços privados - algumas faixas de IP são utilizadas internamente pelas redes e não devem ser roteadas para fora da rede. Nem mesmo pacotes com endereços de origem iguais aos endereços privados devem entrar na rede, devendo ser descartados pelo *Firewall*. Muitas vezes os IPs privados são utilizados como endereços de origem forjados (IP *Spoofing*). Segundo a RFC 1918, os endereços privados são: 10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16. Alguns endereços IP reservados, definidos na RFC 5735, também podem ser utilizados como origem forjada: 0.0.0.0/32, 127.0.0.0/8, 169.254.0.0/16, 192.0.2.0/24, 224.0.0.0/4, 240.0.0.0/5, 248.0.0.0/5, 255.255.255.252/32.

Estas são algumas ações possíveis contra os ataques de negação de serviço. Não existe uma regra ou uma receita para evitar, muito menos para defesa contra um ataque DDoS. Os métodos e técnicas utilizadas pelos *hackers* estão em constante evolução. Dessa maneira, as formas de defesa necessitam também evoluir. E quanto mais rápido isso acontecer melhor. Como já foi dito, provedores de acesso, empresas do ramo e centro de pesquisa precisam trabalhar junto para conseguirem proteger as redes que fazem parte da Internet, desenvolvendo métodos e tecnologias para prever ataques, proteger redes e identificar os atacantes. Esse mal nunca será extinguido, pois a cada nova forma de defesa encontrada, novas formas de ataque serão criadas. Mas precisa ser minimizado o quanto antes.

4 PIORES ATAQUES DA HISTÓRIA

Ataques de negação de serviço acontecem todos os dias, a qualquer hora. Alguns são imperceptíveis e causam pouco ou nenhum dano. Outros causam lentidão ou instabilidade em servidores e serviços. Já outros são tão poderosos que derrubam ou paralisam toda uma rede durante horas. A seguir são apresentados alguns dos piores e mais significativos ataques que se tem notícia e aparecem em várias reportagens, artigos e fazem parte de listas dos piores ataques da história. Alguns deles, se executados novamente, poderiam não ser uma grande ameaça. Porém na época em que ocorreram tiveram grande importância e impacto.

4.1 1988 - MORRIS WORM

O *Morris Worm* foi o responsável por um dos primeiros ataques de negação de serviço. Já citado anteriormente nesse trabalho, em novembro de 1998, Robbert Tappan Morris, estudante da Universidade de Cornell, do estado de Nova Iorque, desenvolveu um software com a intenção de mensurar o tamanho da Internet. Porém seu experimento saiu do controle e muitos servidores com o sistema operacional BSD foram infectados pelo *Morris Worm*, como ficou conhecido. Os servidores atingidos ficaram sobrecarregados, devido a replicação automática do software, e só voltaram ao normal depois de 12 horas, quando especialistas da universidade conseguiram eliminar o *worm* de toda rede.

4.2 2000 – MAFIABOY

Em fevereiro de 2000, um estudante canadense chamado Michael Demon Calce executou uma série de ataques DDoS ao site de 11 grandes empresas, como Yahoo, CNN e Ebay. Esta série de ataques, como citado anteriormente nesse trabalho, é o primeiro ataque DDoS noticiado da história.

O estudante, ficou conhecido mundialmente como Mafiaboy. Na época, então com apenas 15 anos, permaneceu anônimo devido às leis canadenses. Seu projeto, batizado de Rivolta, derrubou servidores e deixou indisponíveis os serviços de grandes empresas de comercio eletrônico, durante três dias. O prejuízo estimado pelos investigadores do caso foi da ordem de 1,7 bilhões de dólares, devido à indisponibilidade das redes e perda nas vendas. Pouco tempo depois, Mafiaboy foi preso pelas autoridades canadenses. Á princípio negou as acusações, porém acabou confessando ser autor dos ataques. Anos mais tarde, em uma entrevista para uma rádio canadense, ele tentou se redimir. Nessa ocasião, afirmou que não tinha intenção de executar os ataques e havia deixado seu computador executando um software configurado com alguns endereços IP conhecidos enquanto ia à escola. Porém, essa informação nunca foi confirmada. De qualquer maneira, ele foi condenado pelas leis canadenses e ficou proibido de usar um computador por muito tempo.

De acordo com as investigações, pois o garoto nunca entrou em detalhes sobre seus ataques, ele utilizou uma ferramenta, chamada IMP Tool, para ataques DoS, desenvolvida pelo *hacker* conhecido como Sinkhole. Antes dos ataques, Mafiaboy invadiu 75 computadores, em 54 redes diferentes, sendo 48 universidades dos Estados Unidos, Canadá, Coreia e Dinamarca e implantou o software que seria utilizado nos ataques. Os alvos foram servidores com sistema operacional Solaris, HP-UX e Linux. O serviço mais atingido foi o DNS, nos servidores que executavam o *software* BIND (Berkley Internet Name Domain). Para atingir os servidores *web* (serviço HTTP), enviou solicitações com informação inútil que exigiam resposta, o que causou um enorme consumo de banda. Foi um ataque poderoso, porém simples. Mafiaboy só foi descoberto porque passou a espalhar, nas salas de bate papo da rede IRC, que era o responsável pelo ataque à empresa Dell. Porém esse ataque não havia sido noticiado, o que levou as autoridades a considerarem o hacker suspeito, devido as similaridades entre todos os ataques.

Michael Calce é conhecido como um dos hackers mais famosos da história da Internet. Trabalha atualmente no ramo de segurança e escreveu um livro chamado “*Mafiaboy: How I Cracked the Internet and Why It's Still Broken*” (Mafiaboy: Como eu quebrei a Internet e por que ela ainda está quebrada*).*

4.3 2002 - 13 ROOT SERVER

Umas das funções mais importantes na Internet, a tradução de nomes em endereços (*domain name system* ou DNS), é executada por 13 servidores espalhados pelo mundo. Alguns deles são formados por um conjunto de outros servidores, para garantir a redundância geográfica. Os Root Servers, como são conhecidos, centralizam as informações de tradução dos endereços do mundo inteiro e alimentam outros *root server*s secundários. Na noite de 21 de outubro de 2002, os 13 Root Servers sofreram um ataque DDoS. Foi um ataque muito bem organizado que afetou principalmente 7 dos 13 servidores. Na tabela a seguir, são listados o nome, endereço IP e a empresa responsável por cada *root server.*

a.root-servers.net	198.41.0.4	VeriSign, Inc.
b.root-servers.net	192.228.79.201	University of Southern California (ISI)
c.root-servers.net	192.33.4.12	Cogent Communications
d.root-servers.net	199.7.91.13	University of Maryland
e.root-servers.net	192.203.230.10	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4	US Department of Defence (NIC)
h.root-servers.net	128.63.2.53	US Army (Research Lab)
i.root-servers.net	192.36.148.17	Netnod
j.root-servers.net	192.58.128.30	VeriSign, Inc.
k.root-servers.net	193.0.14.129	RIPE NCC
l.root-servers.net	199.7.83.42	ICANN
m.root-servers.net	202.12.27.33	WIDE Project

Tabela 2 – Utilização de portas nas ferramentas DDoS

Fonte: Kessler, Gary C. Defenses Against Distributed Denial of Service Attacks.

Sete servidores ficaram indisponíveis de várias partes da Internet, devido ao congestionamento de seus links causado pelo ataque. Este foi executado utilizando uma rede de computadores Agentes e uma combinação de ataques inundação ICMP (*Smurf*), inundação SYN, fragmentação e inundação UDP, utilizando endereço de origem forjado (IP spoofing). O volume de dados recebido por cada servidor foi de 50 à 100 Mbits/sec, totalizando 900Mbits/sec. Porém os efeitos não foram grandes. Poucos usuários sentiram dificuldade ou lentidão durante a navegação. O impacto maior foi na rede entre os Root Serves. Este ataque foi considerado o maior e o mais complexo ataque ao sistema DNS da Internet. Felizmente o objetivo dos atacantes, uma paralisação total da Internet, nunca foi atingido e nenhum culpado foi apontado.

4.4 2007 - ATAQUES A ESTÔNIA

Em 2007, a Estônia sofreu uma série de ataques DDoS que duraram 2 semanas, de 7 de abril até 11 de maio. Este é considerado o primeiro ataque de grandes proporções. Vários servidores e sites do governo foram atingidos, ficando indisponíveis. Na Estônia, muitos serviços públicos são disponibilizados através da Internet, o que torna esse país muito vulnerável a problemas e ataques à rede. A repercussão dos ataques foi muito grande, pois atingiu diretamente a população. A motivação desses ataques foi claramente política. Um dia antes do feriado nacional que comemora a vitória contra a Alemanha nazista, um memorial russo, o Soldado de Bronze de Tallinn, foi removido do centro da capital para um cemitério militar. Este ato não foi bem visto pela Rússia e pela população russa residente na Estônia desde a Guerra Fria. Os ataques começaram nesse mesmo dia. Inicialmente, o governo russo foi apontado com o responsável pelos ataques. Porém negaram qualquer envolvimento. Logo depois, um membro do movimento democrático e antifascista da Rússia, Konstantin Goloskokov, admitiu ter organizados os ataques.

De acordo com um relatório disponibilizado pelo CERT (Computer Emergency Reponse Team) da Hungria, com dados coletados pela empresa

Atlas System, a Estonia sofreu 128 ataques nas duas semanas. Desse total, 115 foram ataques de inundação ICMP (*Smurf*), 4 de inundação SYN e 9 ataques de tráfego genérico. Não foi uma distribuição uniforme. Alguns sites foram mais atacados que outros.

N° de ataques	IP de destino	Domínio
35	195.80.105.107/32	pol.ee
7	195.80.106.72/32	www.riigikogu.ee
36	195.80.109.158/32	www.riik.ee
2	195.80.124.53/32	m53.envir.ee
2	213.184.49.171/32	www.sm.ee
6	213.184.49.194/32	www.agri.ee
35	213.184.50.69/32	www.fin.ee

Tabela 3 – Utilização de portas nas ferramentas DDoS

Fonte: Kessler, Gary C. Defenses Against Distributed Denial of Service Attacks.

Alguns ataques duraram poucos muitos, porém outros duraram várias horas. Todos os domínios .ru foram bloqueados pelo governo estoniano, na tentativa de parar os ataques. Mas esta ação não teve efeito, pois a rede DDoS era formado por *hosts* Agentes nos Estados Unidos, China, Vietnã, Egito e Peru. O governo solicitou ajuda da OTAN (Organização do Tratado do Atlântico Norte) e das Nações Unidades. Pouco tempo depois do final dos ataques, *hackers* estonianos invadiram sites russos, deixando mensagens como “Estônia para sempre”.

4.5 2008 - ATAQUES A IGREJA DE CIENTOLOGIA

No começo de 2008, os hackers ativistas do grupo *Anonymous*, iniciaram um projeto chamado “*Project Chanology*” com uma série de protestos contra a Igreja de Cientologia. O projeto foi criado em resposta a tentativa da Igreja de retirar na Internet um vídeo do ator Tom Cruise. No vídeo, o ator defende as ideias da cientologia, sua importância e superioridade. Segundo a Igreja, o vídeo era material privado que foi publicado na Internet sem

autorização. No dia 21 de janeiro, um vídeo foi postado no YouTube, de autoria do grupo *Anonymous* e dirigido a Igreja de Cientologia, acusando-a de censurar conteúdo na grande rede. O protesto em vídeo foi seguido de uma série de ataques ao site da Igreja, com motivações claramente ideológicas.

De acordo com dados coletados pelo Dr. Jose Nazario da empresa Arbor Networks, foram executados um total de 448 ataques DDoS, todos com o mesmo endereço IP de origem. Isso indica que não foi um ataque de grandes proporções, sendo uma pequena rede DDoS responsável. Dr. Nazario considerou os ataques comuns, porém com grande consumo de banda (em torno de 200Mbps) e duração máxima de 1,8 horas. Para parar o ataque e evitar outros, a Igreja de Cientologia mudou seu site para os servidores de outra empresa que oferecem maior segurança e proteção contra ataques de negação de serviço.

4.6 2009 - ATAQUES AOS ESTADOS UNIDOS E COREIA DO SUL

Em julho de 2009, uma série de ataques DDoS foram coordenados contra sites do governo, agências de notícias e bancos dos Estados Unidos e Coreia do Sul. Esses ataques foram precedidos por uma ação massiva que consistiu em invadir e comprometer computadores com um *malware* específico para executar ataques DDoS. Estima-se que 78 mil computadores foram comprometidos e utilizados no ataque na Coreia do Sul. O número total de computadores espalhados pelo mundo é desconhecido.

Segundo um relatório publicado pela empresa de telecomunicações japonesa Internet Initiave Japan, os ataques começaram nos dias 6 e 7 de julho, contra sites do governo dos Estados Unidos. No dia 7, os alvos passaram a ser sites da Coreia do Sul, mas não apenas do governo, mas também de bancos, serviços de *e-mail* e outros serviços populares no país. Os ataques pararam apenas no dia 10, depois que o *malware* foi removido de praticamente 95% dos computadores infectados, depois de um grande esforço dos provedores de acesso da Coreia do Sul, organizações de segurança e da mídia. Um estudo feito posteriormente com o código do *malware* descobriu que

os ataques gerados foram do tipo inundação de SYN, ACK, UDP e ICMP, além de HTTP GET e HTTP POST.

Os responsáveis por esses ataques nunca foram descobertos. Alguns especialistas afirmar que foram originados de dentro da Inglaterra, outros indicam a Coreia do Norte como culpado. Em março de 2011, um ataque muito parecido foi executado novamente, durante 10 dias consecutivos. No décimo dia o *malware* se autodestruiu, inutilizando o computador hospedeiro. Esses ataques ficaram conhecidos como “Os dez dias de chuva” (*Ten Days of Rain)*.

4.7 2009 - ATAQUE CONTRA O BLOGUEIRO CYXYMU

Cyxymu é um blogueiro da Geórgia que fez a cobertura da Guerra da Abecásia em 1992, os protestos na Georgia em 2007 e os conflitos entre a Geórgia e Rússia em 2008. No dia 6 de agosto de 2009, ele foi alvo de um grande ataque de negação de serviço. Com claras motivações políticas, o ataque tinha o objetivo de censurar o blogueiro. Porém os efeitos do ataque foram muito maiores. Vários serviços utilizados por Cyxymu, ficaram indisponíveis ou tiveram seu tráfego reduzido por várias horas, entre eles as grandes empresas da Internet como Facebook, Youtube, Twitter (figura 16) e Livejournal.

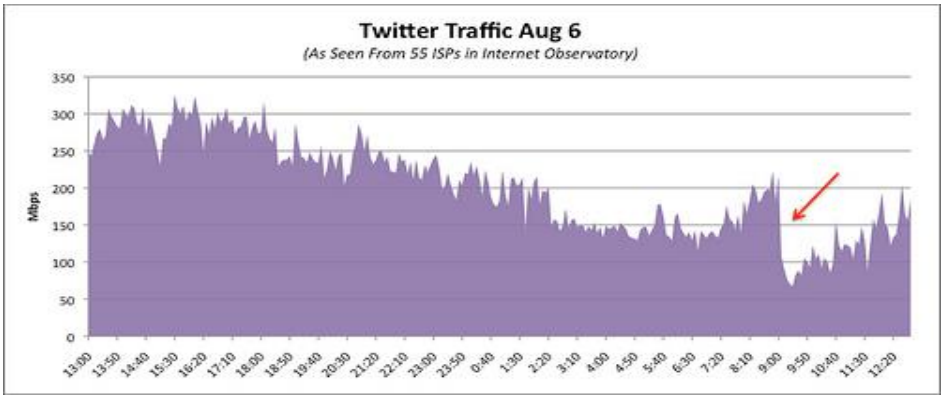

Figura 16 – Tráfego do microblog Twitter no dia do ataque

Fonte: Finin, Tim. Apparent DDoS Attacks on Twitter, Facebook and Livejournal

O ataque foi executado através de uma grande rede DDoS, com computadores Agentes espalhados pelo mundo. Porém outro artifício foi utilizado. Um *e-mail* spam, enviado em nome do blogueiro, com um link para seu blog (figura 17). O efeito desse *e-mail* foi um tráfego enorme para o principal alvo do ataque, o blog de Cyxymu.

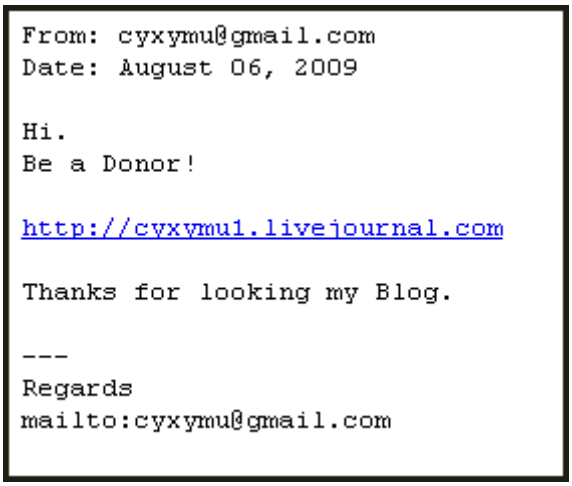

Figura 17 – E-mail spam enviado em nome de Cyxymu.

Fonte: F-Secure. Silence Cyxymu.

Este ataque, apesar de simples execução, teve grande repercussão, pois acabou atingindo sites e serviços utilizados por milhões de usuários. E o resultado acabou sendo o contrário do esperado: em vez de censurar o blogueiro, o ataque acabou chamando mais atenção ainda para sua causa.

4.8 2012 - ANONYMOUS CONTRA ISRAEL

Um outro ataque com motivações políticas foi coordenado pelo grupo *hacker Anonymous* contra o país de Israel. Mais de 700 sites de Israel foram afetados, incluindo o site oficial do presidente, de ministros e outras áreas do governo. Para este ataque foi utilizado um *software* chamado LOIC, executado nos computadores invadidos que formavam a rede DDoS. Esse episódio ficou

conhecido com o Operação #OpIsrael e mostra como cada vez mais os ataques na Internet têm sido usados como uma arma de guerra.

4.9 2013 - ATAQUE CONTRA SPAMHAUS

Spamhaus é uma organização anti-spam. Mantém uma lista negra (*blacklist*) dos *e-mails* utilizados por *spammers* que é utilizada por provedores de acesso, instituições educacionais, militares, centros de pesquisa e várias empresas. No dia 18 de março de 2013, o site da Spamhaus sofreu um ataque de negação de serviço que ocupou toda sua conexão com a Internet, tornando o site indisponível. O tráfego chegou a crescer 75Gbps (figura 18). Nos dois dias que se seguiram, o site continuou sob ataques e a variação do tráfego foi de 30Gbps a 100Gbps. No quarto dia de ataque, o tráfego atingiu 120Gbps.

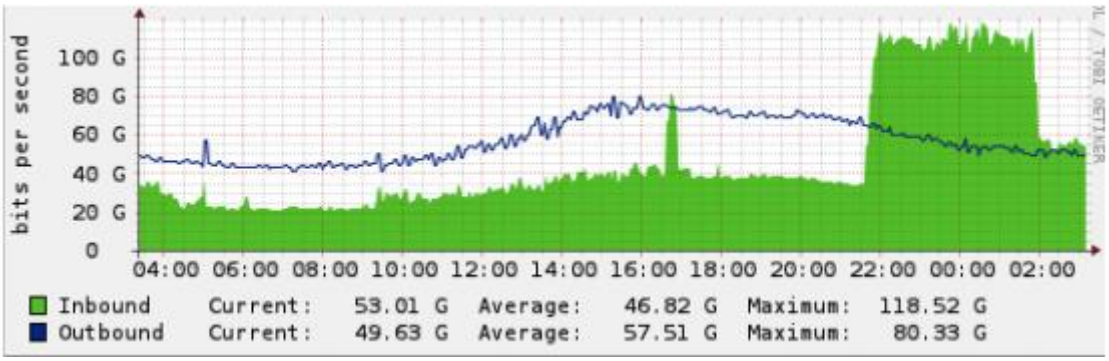

Figura 18 – Aumento do tráfego no site da Spamhaus

Fonte: NSFOCUS Technical Report. Analysis of DDoS Attacks on Spamhaus and recommended solution.

Após resistir por vários dias, devido ao serviço de proteção da empresa CloudFlare, os atacantes mudaram de alvo e passaram a atacar o provedor de acesso da empresa e a infra-estrutura da Internet ligada a rede vítima. Nos últimos dias no mês de março, os ataques atingiram 300Gbps, causando um congestionamento em várias redes da Europa, atingindo 10 milhões de usuários. Estou foi considerado na época o maior ataque na história. O motivo para ter atingido proporções tão grandes, foi o uso de da técnica reflexão ou

amplificação de DNS. Nesse tipo de ataque, os Agentes a rede DDoS fazem requisições a servidores DNS abertos e mal configurados disponíveis na Internet. O pacote enviado aos servidores é pequeno, com tamanho de 36bytes, enquanto a resposta, destinada à vítima, devido ao endereço IP forjado (IP *spoofing*) é muito maior, com tamanho de 3kbytes. Como foram utilizados cerca de 30 mil servidores de DNS, o fator de amplificação foi enorme.

Este foi um ataque de motivações ideológicas, pois teve início quando a Spamhaus adicionou à sua lista negra o domínio da empresa Cyberbunker. Esta empresa havia sido acusada de enviar *spams* e participar de redes DDoS. O alemão Sven Olaf Kamphuis, defensor do Cyberbunker, assumiu a responsabilidade do ataque e acusou a Spamhaus de abusar de sua influência e que ninguém tem o direito de dizer o que deve ou não transitar na Internet.

5 CENÁRIO ATUAL

Nos últimos anos, os ataques de negação de serviço tiveram uma grande evolução, virando uma verdadeira arma de guerra. Novas técnicas e estratégias surgem a cada dia. Novos *softwares* são desenvolvidos e aprimorados. De acordo com um relatório escrito pela empresa Neustar (provedora de serviços na Internet e análise de dados em tempo real) em 2014, os ataques DDoS aumentam em número, ano após ano, porém o perfil está mudando. Uma nova tática dos criminosos, chamada *smokescreening*, está se tornando muito comum. Os ataques deixaram de ter como o objetivo principal indisponibilizar um serviço, site ou servidor. A real intenção dos hackers é distrair os responsáveis pela segurança da rede atacada para poder invadi-la e roubar dados e informações importantes, assim como introduzir *malwares*. O número de empresas atacadas está aumentando, mas a duração destes está se tornando menor. Ataques demorados ainda são comuns, mas a maioria acaba ocupando menos de 1Gbps da banda disponível da vítima. De 2013 para 2014 o número de empresas atacadas duplicou, enquanto o número de ataques onde a banda consumida nos ataques entre 500Mbps e 1Gbps triplicou. Muitas dessas empresas estimam que o prejuízo causado pelos ataques atinge valores na faixa de 50 mil a 100 mil dólares por hora de indisponibilidade. Outro dado importante é o número de pessoas necessárias na defesa de um ataque que também está aumentando, de uma média de 6 pessoas em 2013 para 10 em 2014. Um grande problema entre essas empresas é que elas estão usando ferramentas tradicionais para proteção como *Firewalls* e lista de acessos (acl) em vez de tecnologias próprias contra ataques DDoS, como os chamados Sistemas de Prevenção à Intrusão (IPS).

Segundo dados apresentados pelo site Digital Attack Map, levantados e organizados pelas empresas Arbor Networks, Google Ideas e Big Picture Group, mais de 2000 ataques DDoS são observador na Internet a cada dia. Um terço dos problemas que indisponibilizam sites e servidores são causados por ataques. Um mapa em tempo real foi desenvolvido pelas empresas e mostra o número e o fluxo dos ataques no mundo (Figura 19).

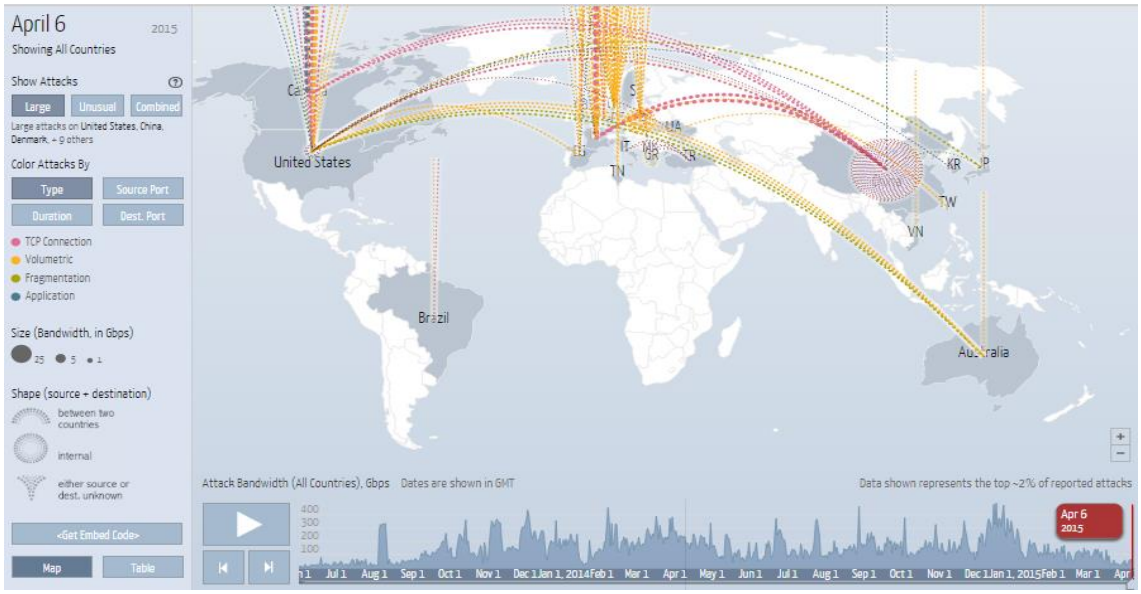

Figura 19 – Mapa de ataques

Fonte: Digital Attack Map. http://www.digitalattackmap.com.

De acordo com uma pesquisa realizado pela empresa Trend Micro Incorporated em 2012, o serviço de um hacker ou grupo pode ser “comprado” no mercado negro por um preço de 30 a 70 dólares por dia de ataque. Quando maior o ataque, maior o preço cobrado.

Em 2014 uma nova técnica de ataque DDoS surgiu. Em vez de utilizar servidores DNS abertos e mal configurados, os atacantes passaram a usar servidores NTP (Network Time Protocol) como rede amplificadora, atingindo tráfego que pode chegar a mais de 300Gbps.

A empresa Nurse Corporation oferece serviços para combate e defesa dos ataques, auxiliando grandes empresas, governos e centros tecnológicos. Desenvolveram também um mapa com dados detalhados, mostrando origem e destino dos ataques (Figura 20).

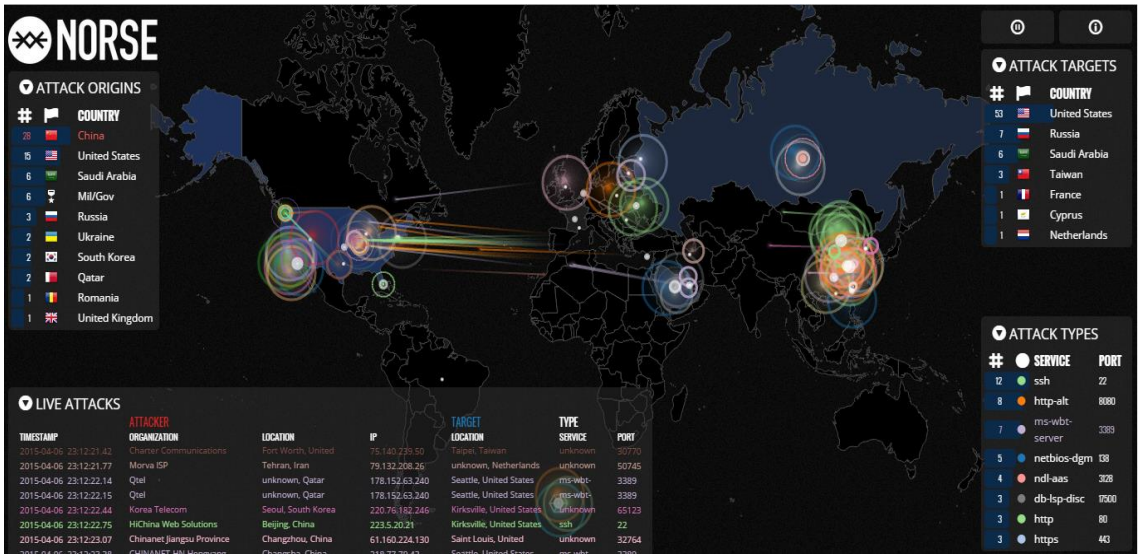

Figura 20 – Mapa de ataques

Fonte: Norse. http://map.ipviking.com.

6 PROPOSTA PRÁTICA

A seguir serão propostas algumas simulações de ataques de negação de serviço possíveis de se executar em laboratório. São práticas para serem realizas em um ambiente controlado, em uma rede isolada, onde nenhum risco possa ser infligido a serviços essenciais ou equipamentos utilizados em ambientes de produção. Pode ser utilizado um laboratório com computadores com sistema operacional Windows e Linux, conectados em uma rede através de *switchs* e roteadores. Como alternativa, pode-se usar um ambiente baseado em máquinas virtuais, como o software Oracle VM Virtual Box. Serão utilizados *softwares* desenvolvidos para Linux que farão o papel do atacante. Outro host será a vítima, utilizando outro sistema operacional e um software monitor de rede, que irá medir e mostrar o tráfego que recebe, como o Wireshark.

Nas simulações descritas a seguir, são utilizadas duas máquinas virtuais, uma com o sistema operacional Kali Linux e outra com Microsoft Windows XP, configuradas em uma mesma rede local com ip 192.168.0.1/24 (figura 21). O mesmo cenário pode ser reproduzido em uma rede física local.

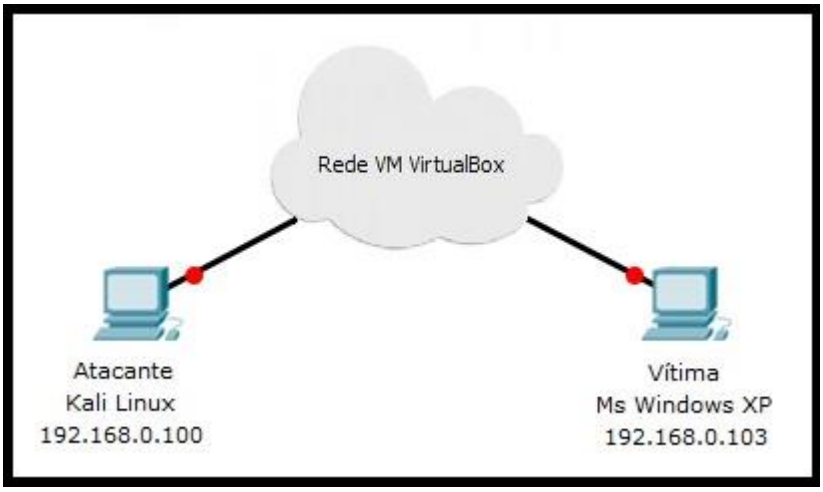

Figura 21 - explicar

Fonte: google images

Para execução das simulações serão necessários os seguintes sistemas operacionais e softwares. OS Kali Linux, disponível em https://www.kali.org/downloads/.

a. OS Microsoft Windows XP, necessária licença de uso.

b. Analisador de protocolo Wireshark, disponível em https://www.wireshark.org/download.html

c. Software Scapy para Linux, disponível em http://www.secdev.org/projects/scapy/. Pode ser instalado via comando apt-get nas distribuições baseadas no Debian Linux.

d. Software DDoSim, disponível em http://sourceforge.net/projects/ddosim/

e. Servidor HTTP XAMP para Windows, disponível em https://www.apachefriends.org/pt_br/download.html

As sugestões de OS podem ser substituídas por outras. Em vez do Kali Linux, qualquer outra distribuição pode ser usada. No lugar do OS Windows XP, outra versão do próprio Windows ou uma distribuição Linux pode ser usada.

6.1 SIMULAÇÃO DE ATAQUE DOS SMURF

Nesta simulação é utilizado o software Scapy para Linux. O comando “scapy”, irá gerar uma sequência de pacotes ICMP direcionados à máquina vítima. Os comandos usados são:

$scapy

>>>send(IP(dst="192.168.0.103",src="192.168.0.100")/ICMP(),count=100,verbose=1)

O parâmetro dst é o endereço IP da vítima, src o IP do atacante e count é o número de pacotes enviados (Figura 23). Nessa simulação não é usada a técnica de IP *Spoofing*.

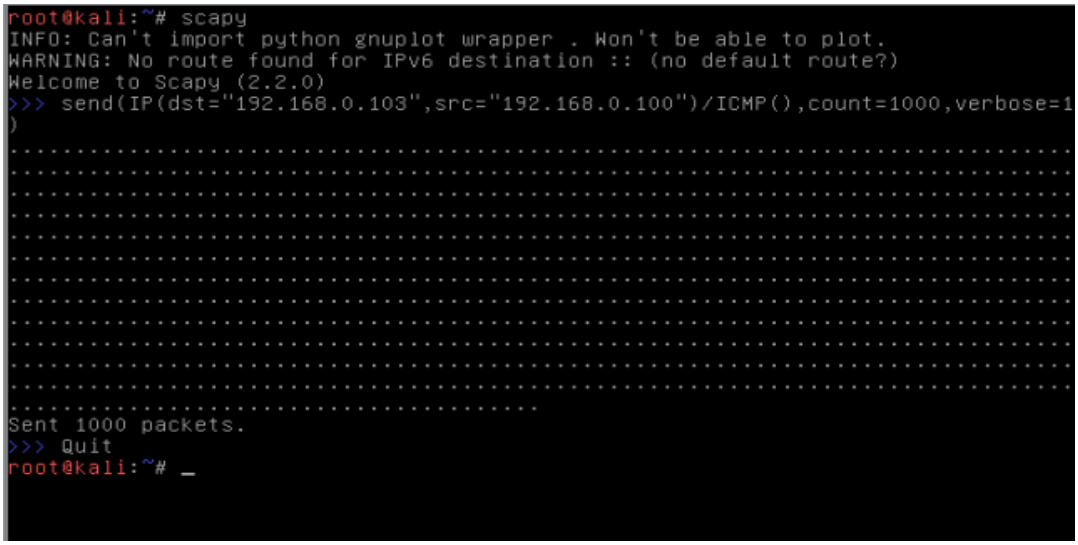

Figura 23 – Software Scapy send executado em um ataque smurf simulado

Fonte: Autoria Própria

Utilizando o software Wireshark na máquina vítima (Figura 24), é possível observar os pacotes ICMP *Request* sendo enviados ao alvo e os pacotes ICMP *Reply* sendo respondidos ao atacante.

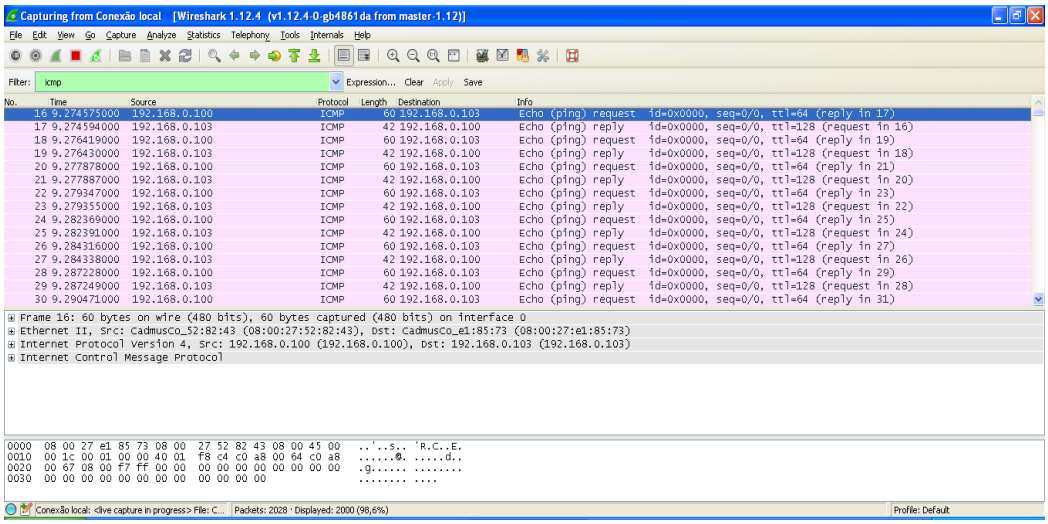

Figura 24 – Tela do software Wireshark durante um ataque Smurf simulado

Fonte: Autoria Própria

Através do Gerenciador de tarefas do Windows (Figura 25) é possível observar o aumento da ocupação na interface de rede da máquina atacada. Como uma simulação está sendo executada em uma rede virtual, a alta ocupação da rede não é alcançada.

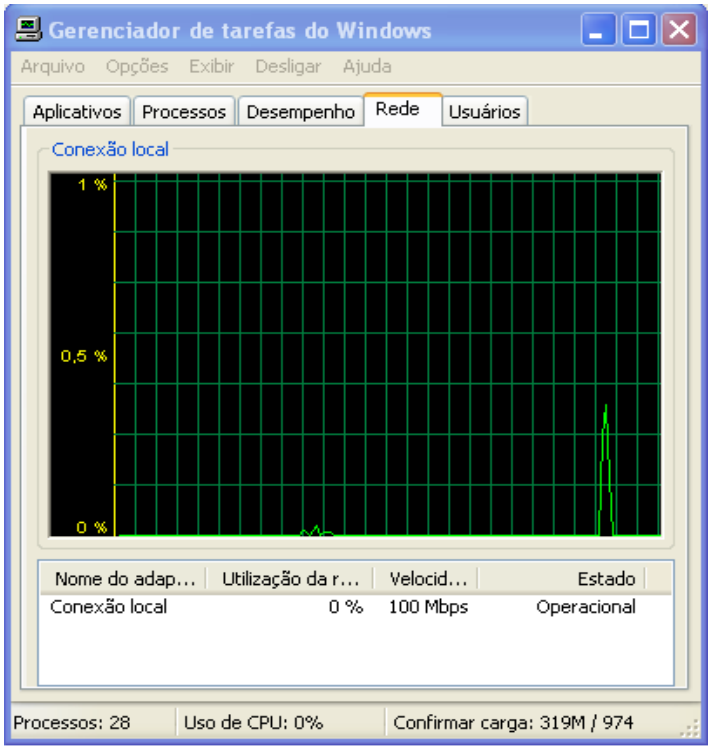

Figura 25 – Monitor da interface de rede do Ms Windows

Fonte: Autoria Própria

6.2 OUTRA SIMULAÇÃO DE ATAQUE DOS SMURF

Uma alternativa para um ataque DoS Smurf é a utilização do comando “smurf6” (Figura 26), disponível do Kali Linux. Este comando irá gerar uma sequência de pacotes ICMP utilizando endereçamento IPv6 direcionados à máquina vítima. O comando usado é:

$smurf eth0 192.168.0.103

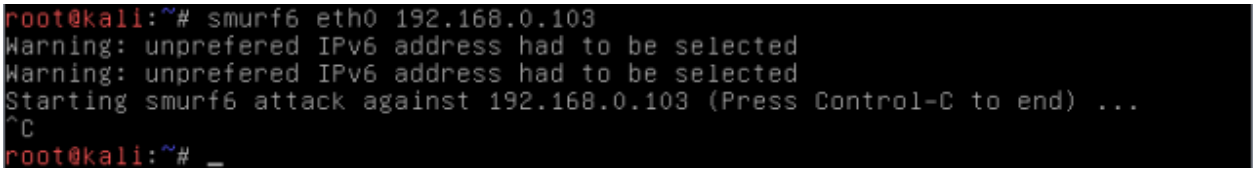

Figura 26 – Software Smurf6 realizando um ataque Smurf simulado

Fonte: Autoria Própria

Utilizando o o software Wireshark na máquina vítima (Figura 27), é possível observar os pacotes ICMPv6 *Request* sendo enviados ao alvo.

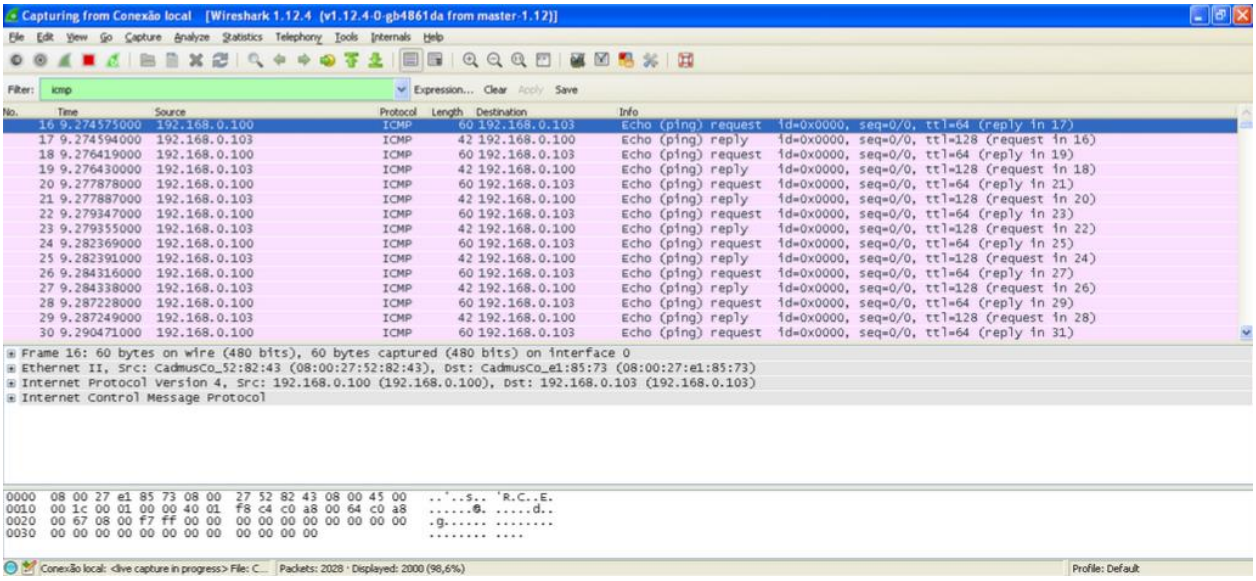

Figura 27 - Tela do software Wireshark durante um ataque Smurf simulado

Fonte: Autoria Própria

Através do Gerenciados de tarefas do Windows (Figura 28) é possível observar o aumento no uso da CPU na máquina alvo. Durante o ataque DoS Smurf o processamento do atingiu 100%, tornando o computador praticamente inutilizável.

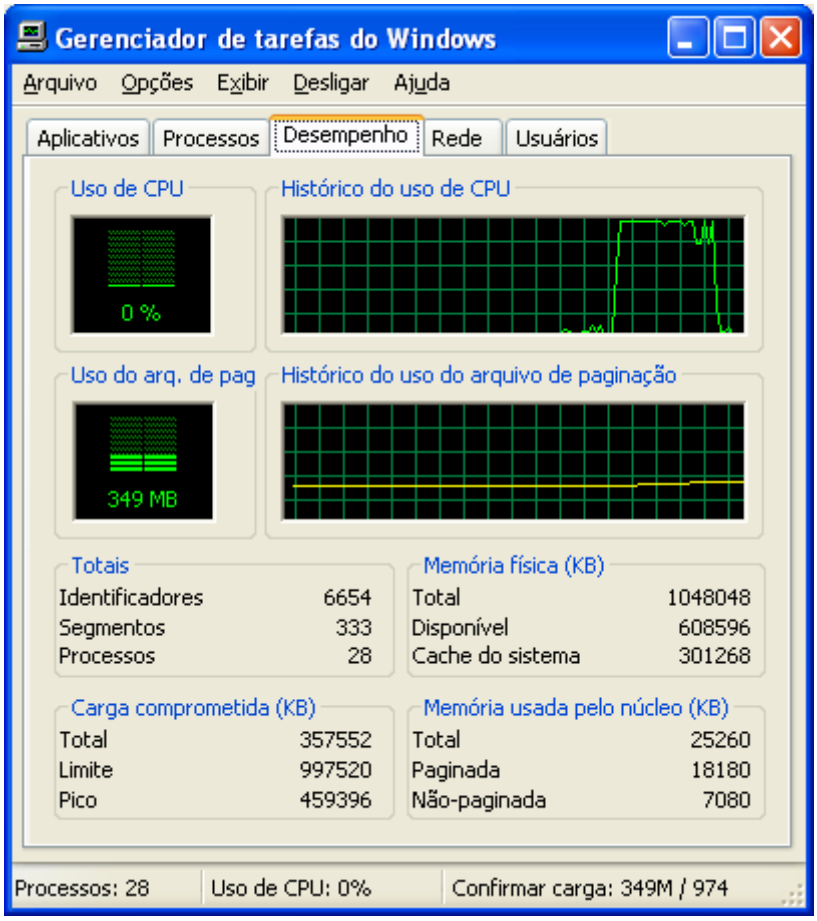

Figura 28 - Monitor da CPU do Ms Windows

Fonte: Autoria Própria

6.3 SIMULAÇÃO DE ATAQUE DE INUNDAÇÃO SYN

Nesta simulação é utilizado o comando “hping3”, disponível do Kali Linux. Este comando irá gerar uma sequência de requisições TCP SYN à máquina vítima (Figura 28). O comando usado é:

$hping3 -i u1 -S -p 80 192.168.1.1

Onde o parâmetro -i u1 indica intervalo de 1ms entre as mensagens, -S indica o uso do TCP SYN e -p 80 o uso da porta 80 (HTTP).

```
root@kali:~# hping3  -i u1 -S -p 80 192.168.0.103
HPING 192.168.0.103 (eth0 192.168.0.103): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.103 ttl=128 id=763 sport=80 flags=RA seq=0 win=0 rtt=0.0 ms
len=46 ip=192.168.0.103 ttl=128 id=764 sport=80 flags=RA seq=0 win=0 rtt=0.0 ms
len=46 ip=192.168.0.103 ttl=128 id=765 sport=80 flags=RA seq=0 win=0 rtt=0.0 ms
len=46 ip=192.168.0.103 ttl=128 id=766 sport=80 flags=RA seq=0 win=0 rtt=0.0 ms
len=46 ip=192.168.0.103 ttl=128 id=767 sport=80 flags=RA seq=0 win=0 rtt=0.0 ms
len=46 ip=192.168.0.103 ttl=128 id=768 sport=80 flags=RA seq=0 win=0 rtt=0.0 ms
len=46 ip=192.168.0.103 ttl=128 id=769 sport=80 flags=RA seq=0 win=0 rtt=0.0 ms
^C
--- 192.168.0.103 hping statistic ---
70935 packets transmitted, 6 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
len=46 ip=192.168.0.103 ttl=128 id=769 sport=80 flags=RA seq=0 win=0 rtt=0.0 ms
root@kali:~# _
```

Figura 28 - Software Hping3 realizando um ataque Inundação SYN simulado

Fonte: Autoria Própria

Utilizando o o software Wireshark na máquina vítima (Figura 29), é possível observar os pacotes TCP SYN enviados ao alvo. O grande número de pacotes enviados é suficiente para gerar arquivos com os dados capturados tão grandes que o espaço em disco na máquina virtual se esgota em poucos minutos.

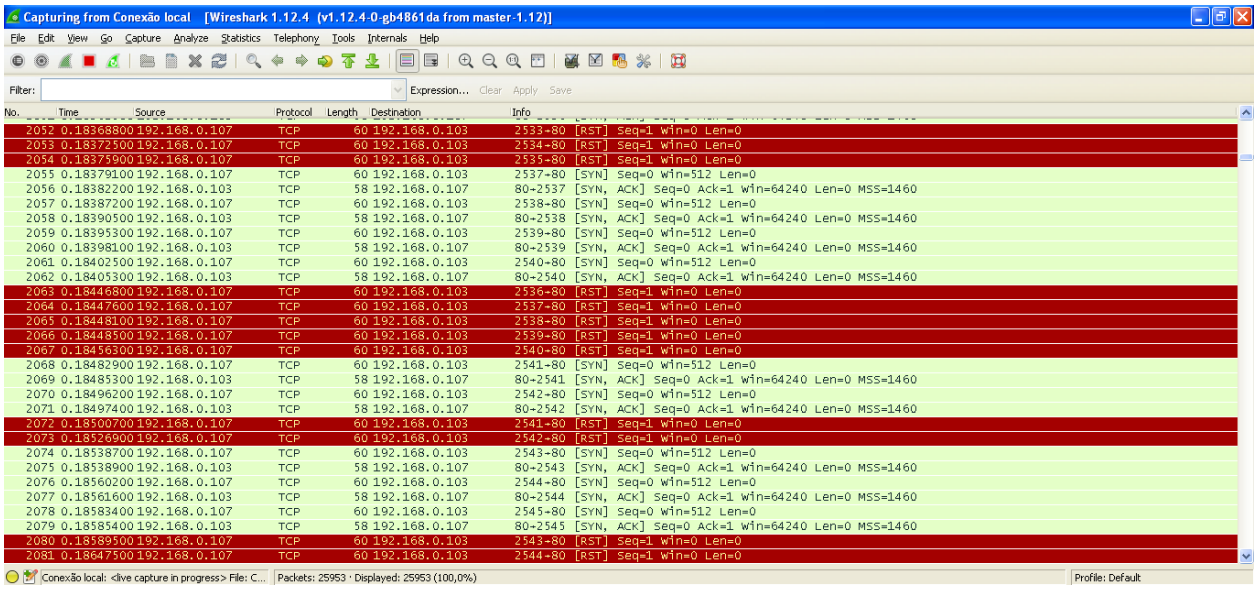

Figura 29 - Tela do software Wireshark durante um ataque Inundação SYN simulado

Fonte: Autoria Própria

Através do Gerenciados de tarefas do Windows é possível observar o aumento no uso da CPU na máquina alvo e da ocupação da interface de rede

(Figura 30). Durante o ataque DoS o processamento da máquina atingiu 100%, tornando o computador praticamente inutilizável. Em alguns momentos, o endereço IP do alvo ficou indisponível para a máquina atacante, sendo necessário interromper a simulação para o host ficar acessível novamente.

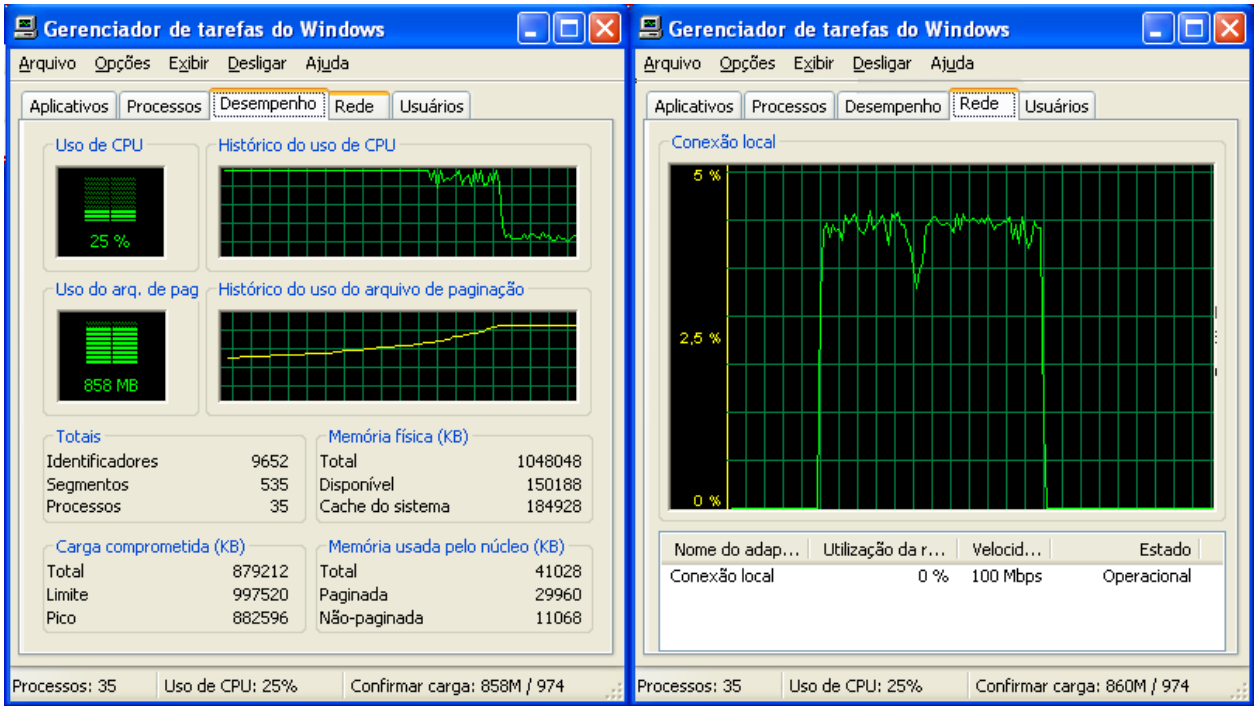

Figura 30 – Monitor do uso da CPU e da interface de rede durante um ataque Inundação SYN

Fonte: Autoria Própria

6.4 SIMULAÇÃO ATAQUE DDoS

Nesta simulação é utilizado o software DDoSIM, que deve ser compilado antes de ser executado. O comando “ddosim” gera uma sequência de requisições HTTP inválidas que são enviadas ao alvo (Figura 31). Porém, o endereço IP de origem é forjado (IP *Spoofing*), simulando um ataque distribuído, onde a origem são muitos *hosts* diferentes.

$./ddosim -d 192.168.0.103 -p 80 -c 10 -r HTTP_INVALID -i eth0

Onde o parâmetro -d indica o endereço IP do alvo, -p 80 indica o uso da porta 80 (HTTP), -r HTTP_INVALID indica que são enviadas requisições HTTP inválidas e -i eth0 indica a interface de saída utilizado na máquina de origem.

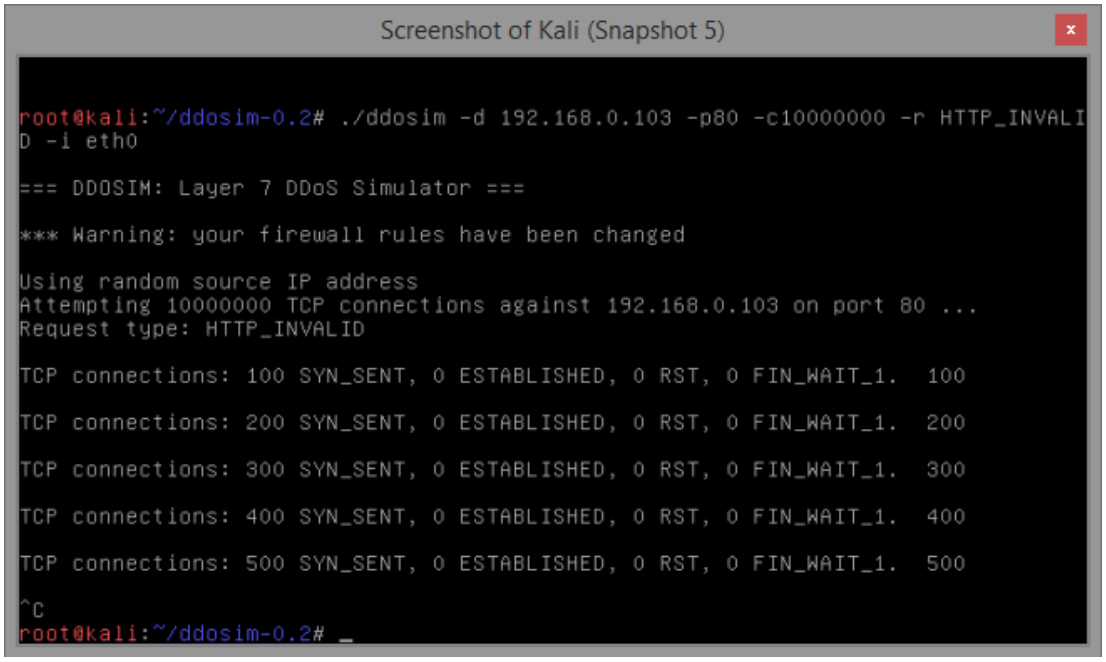

Figura 31 - Software DDoSim realizando um ataque DDoS simulado

Fonte: Autoria Própria

Utilizando o software Wireshark na máquina vítima (Figura 32), é possível observar os pacotes HTTP recebidos e os diferentes endereços IP de origem.

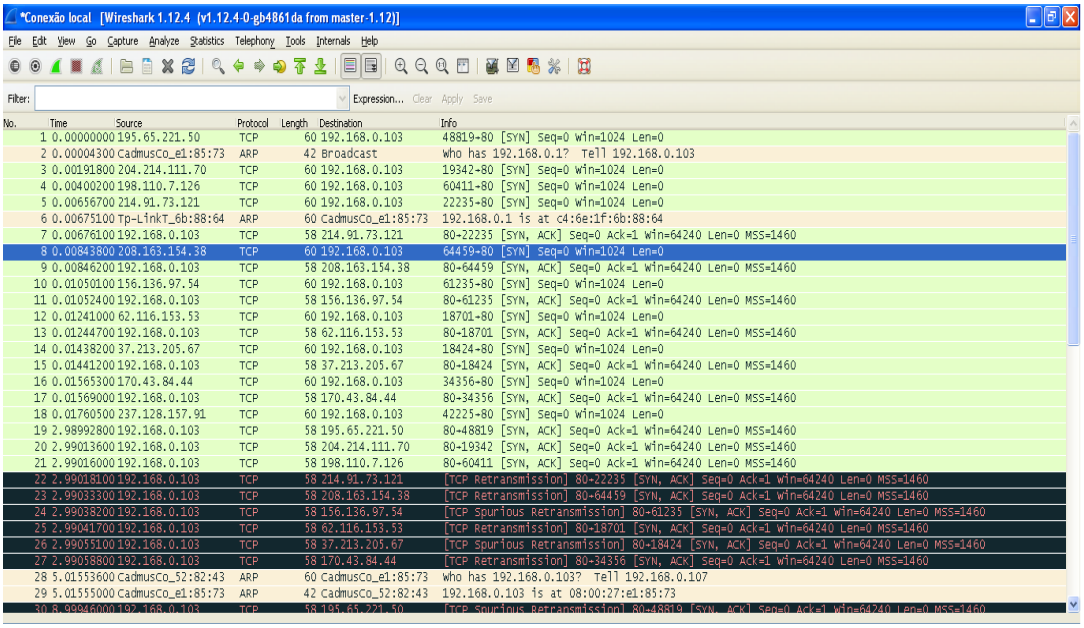

Figura 32 - Tela do software Wireshark durante um ataque DDoS simulado

Fonte: Autoria Própria

Como ocorre em ataques DDoS reais, os endereços IP de origem são forjados, evitando assim que a máquina alvo responda as soliticações. Os endereços de origem são redes de redes totalmente inalcançáveis, como 208.163.154.38, 156.136.97.54, 62.116.153.53 (Figura 33).

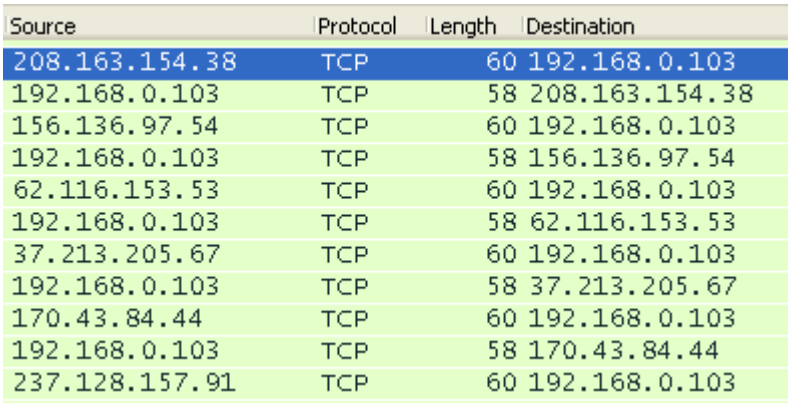

Figura 33 – Detalhe da tela do software Wireshark mostrando endereços IP forjados

Fonte: Autoria Própria

Durante o ataque, uma terceira máquina, que acessava normalmente o servidor HTTP da máquina alvo, passa a ter problemas na navegação das páginas hospedadas no servidor atacado (Figura 35).

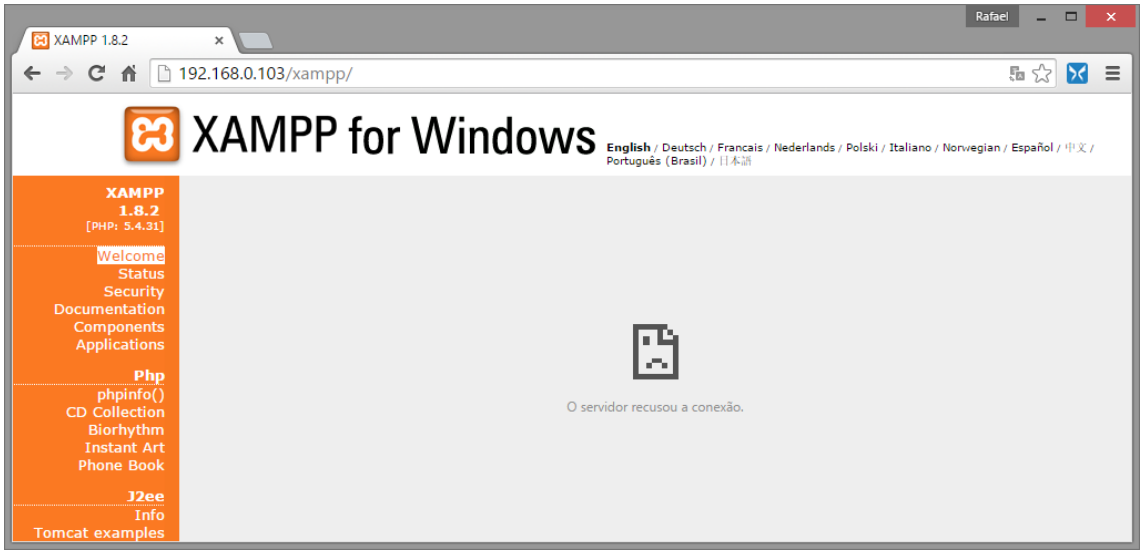

Figura 34 – Navegador acessando servidor HTTP da máquina vítima durante o ataque DDoS simulado

Fonte: Autoria Própria

7 CONSIDERAÇÕES FINAIS

A evolução em todos os setores ligados às comunicações digitais foi enorme desde o surgimento da Internet. Muitas tecnologias surgiram para resolver problemas e se desenvolveram em função da grande rede. A Internet tornou-se uma entidade autônoma na vida das pessoas e da qual todos são dependentes. Mas em vez de se tornar uma estrutura única que beneficia todos, a rede se tornou um verdadeiro campo de batalha. Dividida em nações, grupos religiosos, ideologias contrárias, comunidades rebeldes, a Internet é o palco da maior guerra que a humanidade já viu.

Para todos que trabalham ou tem alguma ligação com tecnologia e a Internet, é muito importante saber o que acontece na rede e o que pode afetar todos os usuários. O ataque de negação de serviço é a maior ameaça que um computador ou rede pode sofrer. O estudo dos DoS e DDoS são ainda mais importantes para os profissionais de segurança e administradores de redes. Recomenda-se assim que todos do ramo tenham conhecimento suficiente para poder reconhecer e defender sua rede no caso de um ataque. Este trabalho é um ponto de partida pois reúne informações suficientes para entender o que são e como acontecem os ataques de negação de serviço.

Trabalhos futuros podem ainda dar continuidade a esse estudo, seja aprofundando o entendimento dos ataques ou mesmo trazendo à tona as novas estratégias de defesa. As simulações aqui apresentadas podem também ser desenvolvidas e uma análise dos resultados pode ser realizado de forma mais profunda. Outras abordagens podem ser estudadas, sempre com o objetivo de tornar a Internet mais segura e livre de ameaças.

8 REFERÊNCIAS

ARBOR NETWORKS. **Digital Attack Map: A Global Threat Visualization**. Disponível em < http://www.arbornetworks.com/threats/> Acesso em 6 de abril de 2015, 21:23.

CENTRO DE ESTUDOS, RESPOSTA e TRATAMENTO de INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet**. Disponível em <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf> Acesso em 18 de setembro de 2014, 22:40.

CNET - SECURITY. **Technical aspects of the DDoS attacks upon the Churck of Scientology.** Disponível em <http://www.cnet.com/news/technical-aspects-of-the-ddos-attacks-upon-the-church-of-scientology/> Acesso em 03 de abril de 2015, 21:33.

COGENT COMMUNICATIONS. **Events of 21-Oct-**2002. Disponível em <http://c.root-servers.org/october21.txt> Acesso em 02 de abril de 2015, 21:12.

COMPUTER HISTORY MUSEUM. **Internet Hostory**. Disponível em <http://www.computerhistory.org/internet_history/> Acesso em 18 de setembro de 2014, 22:12.

COMPUTERWORLD. **Mafiaboy grows up: A hacker seeks redemption**. Disponível em <http://www.computerworld.com/article/2533517/networking/mafiaboy-grows-up--a-hacker-seeks-redemption.html> Acesso em 31 de maio de 2015, 22:54.

DARKREADING. **Anonymous Launches OpIsrael DDoS Attacks After Internet Threat**. Disponível em <http://www.darkreading.com/attacks-and-breaches/anonymous-launches-opisrael-ddos-attacks-after-Internet-threat/d/d-id/1107409?page_number=2> Acesso em 4 de abril de 2015, 19:58.

DEFIGO ORBIS TERRARUM. **Let the Hacking Begin**. Disponível em <http://www.exunclan.com/tqfinal/tq/history/let-the-hacking-begin/> Acesso em 06 de novembro de 2014, 20:35.

DIGITAL ATTACK MAP. **What is DDoS Attack?**. Disponível em <http://www.digitalattackmap.com/understanding-ddos> Acesso em 6 de abril de 2015, 19:11.

F-SECURE. **Silence Cyxymy**. Disponível em < https://www.f-secure.com/weblog/archives/00001746.html> Acesso em 4 de abril de 2015, 19:02.

GREENHAW ANDY. **Who is Cyxymy?**. Disponível em <https://andygreenhaw.wordpress.com/tag/ddos-attack/> Acesso em 4 de abril de 2015, 19:33.

HUNGARIAN COMPUTER EMERGENCY RESPONSE TEAM FOR COUNCIL OF INTERNET SERVICE PROVEIDERS (HUN CERT). **Estonia under cyber attack**. Disponível em <http://cert.hu/sites/default/files/Estonia_attack2.pdf> Acesso em 03 de abril de 2015, 20:02.

INFOSEC INSTITUTE. **DOS Attacks and Free DOS Attacking Tools**. Disponível em <http://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/> Acesso em 22 de maio de 2015, 20:17.

INTERNET ENGINEERING TASK FORCE (IETF). **RCF 2828 – Internet Security Glossary**. Disponível em <https://www.ietf.org/rfc/rfc2828.txt> Acesso em 9 de dezembro de 2014, 18:35.

INTERNET INITIATIVE JAPAN. **Large-Scale DDoS Attacks in the United States and South** Korea. Disponível em < http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol05_infra_EN.pdf> Acesso em 03 de abril de 2015, 22:23.

IT WORLD CANADA. **Mafiaboy´s story points to Net weaknesses**. Disponível em <http://www.itworldcanada.com/article/mafiaboys-story-points-to-net-weaknesses/29212> Acesso em 31 de maio de 2015, 23:15.

JUNIPER NETWORKS. **Understanding Teardrop Attacks**. Disponível em <https://www.juniper.net/techpubs/software/junos-es/junos-es92/junos-es-swconfig-security/understanding-teardrop-attacks.html> Acesso em 16 de maio de 2015, 21:50.

KESSLER, Gary C. **Defenses Against Distributed Denial of Service Attacks**. Disponível em <http://www.garykessler.net/library/ddos.html> Acesso em 20 de maio de 2015, 21:22.

MARKS, Paul. **The gentleman hacker´s 1903**. Disponível em <http://www.newscientist.com/article/mg21228440.700-dotdashdiss-the-gentleman-hackers-1903-lulz.html?full=true#.VSsaFfnF9JN> Acesso em 6 de novembro de 2014, 21:10.

MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. **Hacking Exposed: Network Security Secrets & Solutions**. Estados Unidos da América: McGrawHill, 1999.

NEUSTAR. **2014 The Danger Deepens – Neustar Annual DDoS Attacks and Impact Report**. Disponível em <https://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf> Acesso em 6 de abril de 2015, 18:07.

NORSE. **Watch Live Attacks**. Disponível em < http://map.ipviking.com/> Acesso em 6 de abril de 2015, 22:10.

NSFOCUS. **Analysis of DDoS Attacks on Spamhaus and recommended solution**. Disponível em <http://www.nsfocus.com/SecurityView/Analysis%20of%20DDoS%20Attacks%20on%20Spamhaus%20and%20recommended%20solution-EN-20130510.pdf> Acesso em 04 de abril de 2015, 21:43.

REDOND, Jacques. **The Morris Worm – 25 Years later**. Disponível em <http://drtech.bangordailynews.com/2013/11/10/reviews/the-morris-worm-25-years-later/> Acesso em 8 de dezembro de 2014, 20:33.

REVOLUÇÃO DIGITAL. **Morris Worm, o primeiro worm do mundo fez 25 anos**. Disponível em <http://www.revolucaodigital.net/2013/11/06/morris-worm-25-anos-65790/> Acesso em 8 de dezembro de 2014, 19:55.

THE ARBOR NETWORKS IT SECURITY BLOG. **Estonian DDoS Attacks – A summary to date**. Disponível em <http://www.arbornetworks.com/asert/2007/05/estonian-ddos-attacks-a-summary-to-date/> Acesso em 03 de abril de 2015, 20:43.

TODD, Bennet. **Distributed Denial of Service Attacks**. Disponível em <http://www.linuxsecurity.com/resource_files/intrusion_detection/ddos-whitepaper.html>. Acesso em 18 de setembro de 2014, 21:32.

TONY SALE´S CODES AND CIPHERS. **The Enigma Cipher Machine**. Disponível em <http://www.codesandciphers.org.uk/enigma/> Acesso em 06 de novembro de 2014, 20:23.

TREND MICRO INCORPORATED. **Russian Underground 101**. Disponível em <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf> Acesso em 6 de abril de 2015, 19:45.

SECURITY AFFAIRS. **All about offensive of anomymous against Israel**. Disponível em <http://securityaffairs.co/wordpress/10428/intelligence/opisrael-all-about-offensive-of-anonymous-against-israel.html> Acesso em 04 de abril de 2015, 20:24.

SLATER, WIllian F. **The Internet Outage and Attacks of October** 2002. Disponível em <http://www.isoc-chicago.org/internetoutage.pdf> Acesso em 02 de abril de 2015, 21:35.

SPAFFORF, Eugene H. **The Internet Worm Program: An Analysis**. Department of Computer Sciences - Purdue University - West Lafayette. Disponível em <http://spaf.cerias.purdue.edu/tech-reps/823.pdf> Acesso em 8 de dezembro de 2014, 19:30.

SUNGOOK, Hong. **Wireless From Marconi Black Box to the Audion**. Massachusetts Institute of Technology. 2011

UMBC EBIQUITY. **Apparental DDOS attacks on twitter, facebbok and livejournal**. Disponível em <http://ebiquity.umbc.edu/blogger/2009/08/06/apparent-ddos-attacks-on-twitter-facebook-and-livejournal/> Acesso em 4 de abril de 2015, 19:15.

ZDNET. **McAfee: South Korea botnet self-destructed after DDoS**. Disponível em <http://www.zdnet.com/article/mcafee-south-korea-botnet-self-destructed-after-ddos/> Acesso em 03 de abril de 2015, 22:01.