MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE WANDENKOLK

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
SEGURANÇA DAS INFORMAÇÕES E COMUNICAÇÕES

CAPITÃO-TENENTE BRUNO FIGUEIRA GAIGNOUX

ANÁLISE SOBRE AS TÉCNICAS DE ATAQUE DE NEGAÇÃO DE SERVIÇO (DoS) E SEUS IMPACTOS NA GUERRA CIBERNÉTICA

Rio de Janeiro
2020

CT BRUNO FIGUEIRA GAIGNOUX

ANÁLISE SOBRE AS TÉCNICAS DE ATAQUE DE NEGAÇÃO DE SERVIÇO (DoS) E SEUS IMPACTOS NA GUERRA CIBERNÉTICA

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança das Informações e Comunicações.

Orientadores:
CT André Luiz Brabo Monte
Prof. Dr. Anderson Oliveira da Silva

CIAW
Rio de Janeiro
2020

Gaignoux, Bruno Figueira.
Análise sobre as técnicas de Ataque de Negação de Serviço (DoS) e seus impactos na Guerra Cibernética / Bruno Figueira Gaignoux. — Rio de Janeiro, 2020.
74f.: il.

Orientador: CT André Luiz Brabo Monte;
Prof. Dr. Anderson Oliveira da Silva.

Monografia (Curso de Aperfeiçoamento Avançado de Segurança da Informação e Comunicações) — Centro de Instrução Almirante Wandenkolk, Rio de Janeiro, 2020.

1. Guerra Cibernética. 2. Negação de Serviço. 3. Ataque de DoS. I. Centro de Instrução Almirante Wandenkolk. II. Título.

CT BRUNO FIGUEIRA GAIGNOUX

ANÁLISE SOBRE AS TÉCNICAS DE ATAQUE DE NEGAÇÃO DE SERVIÇO (DoS) E SEUS IMPACTOS NA GUERRA CIBERNÉTICA

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

Aprovada em _____/_____/ 2020

Banca Examinadora:

_____

CMG (RM1-EN) Gian K. Huback Macedo de Almeida - CIAW

_____

CT André Luiz Brabo Monte – CAAML

_____

Anderson Oliveira da Silva, D. Sc. – PUC Rio

CIAW
Rio de Janeiro
2020

Dedico esse trabalho a minha filha Thayná, que com toda sua inocência e pureza me faz entender o sentido da vida.

AGRADECIMENTOS

Primeiramente gostaria de agradecer a Deus, por toda força e coragem que me deu para enfrentar os inúmeros momentos de dificuldade do curso.

Aos meus queridos pais, Márcia e Eduardo, obrigado por todo esforço e sacrifício em prol da minha educação escolar e, acima de tudo, da minha educação ética e moral.

À minha amada esposa Greicy Gaignoux, obrigado por ter aceitado navegar comigo pelos rumos desconhecidos dessa vida e por toda compreensão com minha ausência ao longo da minha carreira. Seu apoio foi, é e sempre será fundamental!

À minha pequena Thayná, agradeço por toda luz e amor que trouxe a minha vida! Saiba que você é minha fonte de motivação diária para seguir em frente!

Ao CMG Huback, Coordenador do Curso de Segurança da Informação e Comunicações, agradeço por todo tratamento dispensado ao longo do curso, sempre cortês e compreensivo! Levarei o senhor como exemplo de liderança a me guiar na carreira naval.

Ao CT Brabo, meu orientador técnico, agradeço por todas orientações transmitidas. Suas palavras de confiança nos momentos de dificuldade foram fundamentais para a conclusão deste trabalho!

Aos Docentes da PUC-RJ, em especial os Professores Anderson Oliveira, Sérgio Colcher e Carlos Rodriguez, agradeço pelas excelentes aulas ministradas. Saibam que os senhores serão referência de profissionalismo e conhecimento técnico para uma geração de Oficiais!

Por fim, agradeço aos amigos do quarto de Segurança da Informação e Comunicações pelo convívio harmonioso ao longo desses últimos meses! Espero que breve voltemos a nos encontrar nas Praças D'Armas dos Navios da nossa gloriosa Marinha!

“Isso também vai passar!” Chico Xavier

ANÁLISE SOBRE AS TÉCNICAS DE ATAQUE DE NEGAÇÃO DE SERVIÇO (DoS) E SEUS IMPACTOS NA GUERRA CIBERNÉTICA

Resumo

Os avanços da informática e dos sistemas automatizados alteraram ao longo dos anos a forma de se relacionar dos indivíduos. Cada vez mais serviços essenciais e rotineiros são fornecidos a partir de sistemas de Tecnologia da Informação, tornando as sociedades dependentes deles. Porém, esses sistemas possuem vulnerabilidades que podem ser exploradas em conflitos bélicos através de ataques cibernéticos. Observando casos recentes de Guerra Cibernética, percebe-se o uso maciço de ataques de Negação de Serviço (DoS) nestes conflitos, com a finalidade de tornar indisponível serviços importantes a sociedade civil e causar sérios danos morais e psicológicos a população atingida. Com isso, este trabalho tem como objetivo analisar as técnicas de ataque de DoS e compreender os impactos que o ataque de negação de serviço causa no contexto de uma Guerra Cibernética. Para esse fim, ao longo do trabalho, serão abordados casos de Guerra Cibernética de grande repercussão mundial, bem como serão expostas algumas técnicas importantes utilizadas para efetuar um ataque de Negação de Serviço. Ao final, será realizada uma simulação de ataque de DoS em ambiente de máquinas virtuais, com o intuito de observar na prática as consequências deste ataque.

Palavras- chave: Guerra Cibernética. Negação de Serviço. Ataque de DoS.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTAS DE SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
ACK	*Acknowledgement*
ARP	*Address Resolution Protocol*
BOTNET	*Robot Network*
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CETIC	Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação
DARPA	*Defense Advanced Research Projects Agency*
DDoS	*Distributed Denial of Service*
DGDNTM	Diretoria-Geral de Desenvolvimento Nuclear e Tecnológico da Marinha
DGMM	Diretoria-Geral de Material da Marinha
DNS	*Domain Name System*
DoD	*U.S. Department of Defense*
DoS	*Denial of Service*
DRDoS	*Distributed Reflection Denial of Service*
EB	Exército Brasileiro
FIN	*Finite*
FTP	*File Transfer Protocol*
FSB	Serviço Federal de Segurança da Rússia
HD	*Hard Disk*
HTTP	*Hypertext Transfer Protocol*
ICMP	*Internet Control Message Protocol*

IP	*Internet Protocol*
ISO	*International Organization for Standardization*
MB	Marinha do Brasil
MD	Ministério da Defesa
MTU	*Maximum Transmission Unit*
OSI	*Open Systems Interconnection*
PSH	*Push*
RAM	*Random Access Memory*
RST	*Reset*
SIC	Segurança da Informação e Comunicações
SMTP	*Simple Mail Transfer Protocol*
SO	Sistema Operacional
STIC2	Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle
SYN	*Synchronize*
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicações
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
UE	União Europeia
UIT	União Internacional de Telecomunicações
URG	*Urgent*

SUMÁRIO

1 INTRODUÇÃO

Inicia-se a terceira década do Século XXI e o Mundo vive intensamente a Era da Informação ou a Era Digital. Cada vez mais, serviços essenciais à população são operados e fornecidos a partir de infraestruturas informatizadas. Este cenário tem reflexos diretos nas sociedades, pois gera um aumento crescente na dependência da internet (LOUREIRO, 2016).

Com a sociedade brasileira não tem sido diferente. De acordo com a União Internacional de Telecomunicações (UIT, 2017), o Brasil é o quarto país no mundo em número de usuários absolutos da internet, ficando atrás apenas dos Estados Unidos, Índia e China. Porém, percebe-se claramente que esta posição está intimamente relacionada ao ranking de países mais populoso do mundo. Analisando apenas os dados nacionais, o número de brasileiros que utilizavam a internet em 2018 representava 70% do total da população, segundo a pesquisa TIC Domicílios divulgada pela CETIC (2019). Este dado representa um aumento de dez milhões de usuários em dois anos (de 2016 até 2018) e leva o Brasil a se aproximar dos índices de países desenvolvidos (CETIC, 2019).

No contexto dessa conectividade global, surgiu um novo conceito de ambiente, um ambiente virtual onde os indivíduos passaram a se relacionar, que é o espaço cibernético. Porém, ele trouxe consigo vulnerabilidades que expõem os seus usuários a riscos antes inexistentes. A exploração desses riscos pode ser feita através de diferentes técnicas de ataques cibernéticos e tem o poder de causar grandes impactos em uma Nação (LOUREIRO, 2016).

Cientes desse potencial bélico, diferentes Nações já usaram esses ataques cibernéticos em campanhas militares com o intuito de desestabilizar seus oponentes e obter vantagem estratégicas, o que gerou uma nova modalidade de guerra, chamada de Guerra Cibernética (AVELAR, 2018).

Atento ao cenário mundial e a nova tendência tecnológica, em 2008, o Brasil aprovou a Estratégia Nacional de Defesa. Nela foram estabelecidos três setores estratégicos para a Defesa Nacional: o setor nuclear, o setor espacial e o setor cibernético. Coube ao Exército Brasileiro (EB) ficar responsável pela desenvolvimento do setor cibernético, enquanto a Marinha ficou com a parte nuclear e a Força Área com o setor espacial (BRASIL, 2012)

Seguindo o planejamento de desenvolver uma mentalidade de segurança cibernética no âmbito das Forças Armadas, em 2012 foi inaugurado o Centro de Defesa Cibernética, subordinado ao EB. Dois anos mais tarde, em 2014, o Ministério da Defesa (MD) aprovou a Doutrina Militar de Defesa Cibernética com a finalidade de estabelecer os fundamentos da Doutrina Militar de Defesa Cibernética, proporcionando unidade de pensamento sobre o

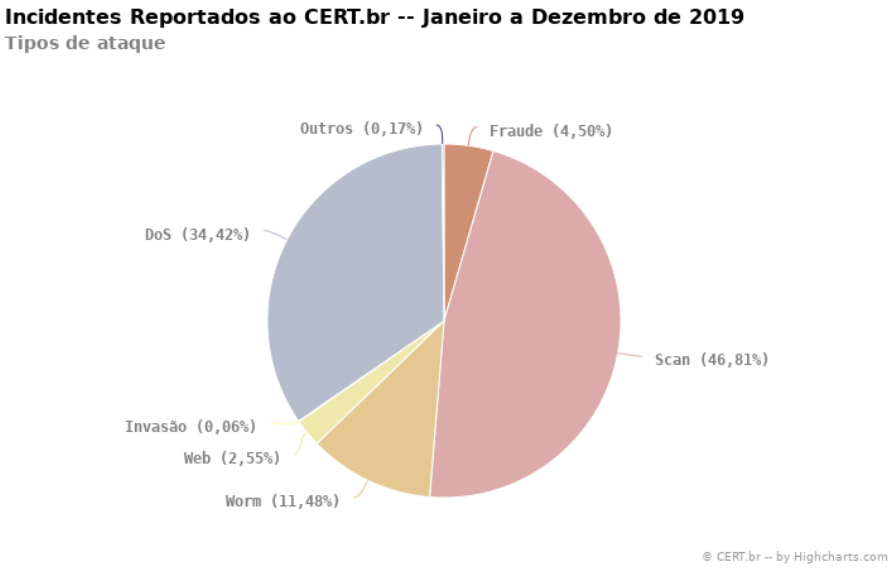
assunto, no âmbito do Ministério da Defesa (MD), e contribuindo para a atuação conjunta das Forças Armadas (FA) na defesa do Brasil no espaço cibernético (BRASIL, 2014)

Assim, a partir desta contextualização, este trabalho tem como finalidade apresentar uma análise sobre um tipo de ataque muito utilizado na Guerra Cibernética, que é o ataque negação de serviço (Denial of Service, DoS). A análise será feita através de estudo de casos, revisão bibliográfica e abordagem prática.

1.1 Apresentação do Problema

Com base nos dados divulgados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), em 2019, os ataques de negação de serviço (DoS) foram responsáveis por quase 35% dos ataques cibernéticos realizados no Brasil, ficando atrás apenas do ataque de *scan* (figura 1).

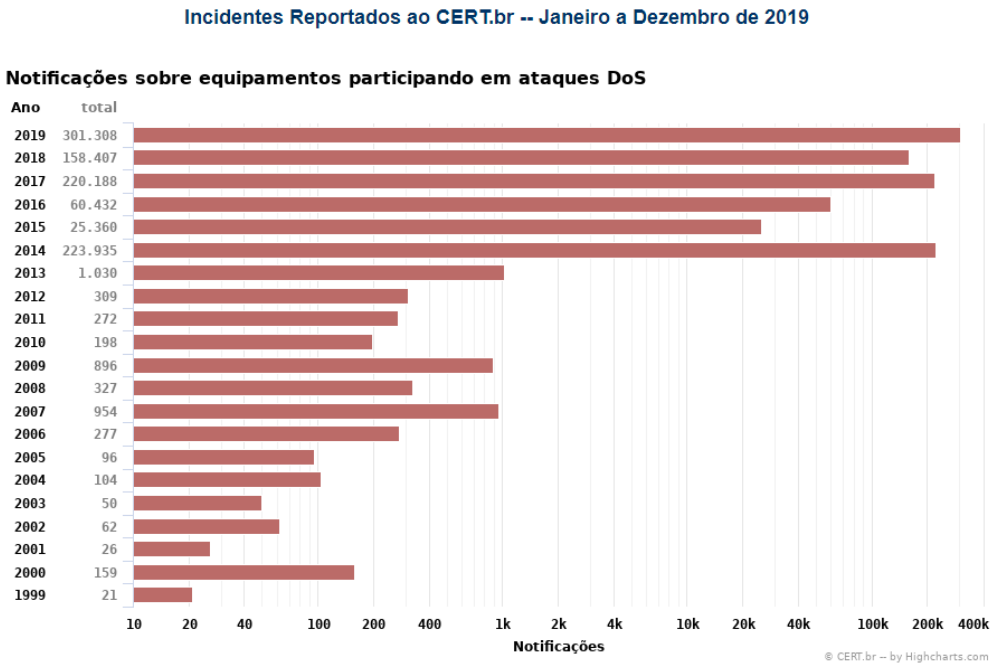
Figura 1 - Tipos de incidentes cibernéticos reportados no ano de 2019



Fonte: CERT.br, 2020

Estima-se que mais de trezentas mil máquinas participaram dos ataques no país, o que representa um aumento de quase 100% no número de máquinas em relação ao ano de 2018 (figura 2).

Figura 2 - Total de máquinas participantes de ataques de DoS



Fonte: CERT.br, 2020

Observando o contexto global e analisando os casos mais recentes de Guerra Cibernética, percebe-se que a negação de serviço é uma arma maciçamente usada nesta modalidade de conflito. Exemplos como os ataques à Estônia e à Geórgia, serviram de alerta para o mundo e mostraram os impactos devastadores que esta técnica de ataque cibernético pode causar em países dependentes de Tecnologias de Informação (MENDONÇA, 2014).

Portanto, considerando o cenário da crescente utilização de ataques de DoS no Brasil e o emprego de ataques de negação de serviço na Guerra Cibernética, este trabalho analisará as técnicas e consequências de um ataque de negação de serviço.

1.2 Justificativa e Relevância

No início de 2007, a Estônia foi atingida por um grande Ataque Distribuído de Negação de Serviço (DDoS). Diversos serviços do país foram atingidos nesse ataque. A infraestrutura dos serviços essenciais à população estoniana era em grande parte informatizada, o que contribuiu para o ataque causar um grande impacto no país (CLARKE, 2010).

Esse foi o primeiro exemplo de Guerra Cibernética onde ataques de negação de serviço foram amplamente utilizados. Nos anos seguintes, outros países enfrentaram situações semelhantes. Geórgia, Coreia do Sul, Estados Unidos e Ucrânia também tiveram sites e serviços

afetados por ataques de DoS. Nessas situações, percebeu-se que quanto maior a dependência de infraestruturas de Tecnologia da Informação, maior eram os impactos causados. Alguns destes países sofreram o ataque cibernético em paralelo a operações militares tradicionais. Nestes casos, observou-se uma importante vantagem estratégica do inimigo (MEDVEDEV, 2015).

No Brasil, conforme já apresentado, cresce o número de usuários da internet e, consequentemente, de serviços informatizados. Com isso, os sistemas passam a depender mais de conexões a redes de computadores e se expõem mais as vulnerabilidade do espaço cibernético. Com as Forças Armadas e, particularmente, com a Marinha do Brasil não é diferente. A tendência é cada vez mais os sistemas, tanto administrativos quanto operativos, serem conectados, o que representa uma vulnerabilidade em caso de conflito.

Portanto, a relevância do trabalho está em entender que a Marinha está sujeita a este tipo de ataque e identificar os impactos que a indisponibilidade de um destes sistemas pode causar a Força Naval.

1.3 Objetivos

1.3.1 Objetivo Geral

Este trabalho tem como objetivo principal analisar as técnicas de ataque de DoS e compreender os impactos que o ataque de negação de serviço causa no contexto de uma Guerra Cibernética. Para esse fim, será realizada análise sobre casos de Guerra Cibernética onde foram utilizados ataques maciços de DoS e que tiveram repercussão mundial, além de realizar uma simulação de ataque de DoS utilizando máquinas virtuais.

1.3.2 Objetivos Específicos

Este trabalho tem como objetivo específico revisar e analisar bibliografias sobre Guerra Cibernética e Ataques de Negação de Serviço.

1.4 Metodologia

Este trabalho tem como objetivo principal compreender os impactos que o ataque de negação de serviço causa no contexto de uma Guerra Cibernética e entender as técnicas empregadas nesse ataque.

1.4.1 Classificação quanto aos fins

Este trabalho quanto aos fins é classificado como descritivo e explicativo. Descritivo, pois mostra casos de Guerra Cibernética com utilização intensa de ataques de DoS. Explicativo, pois mostra as técnicas usadas para executar um ataque de DoS.

1.4.2 Classificação quanto aos meios

Este trabalho quanto aos meios é classificado como documental, bibliográfico e experimental. Documental, pois foram utilizados documentos da Administração Pública Federal que não são de amplo acesso. Bibliográfico, pois foram utilizadas teses, livros, sites e revistas para a confecção da revisão bibliográfica. Experimental em laboratório, pois foi realizada uma simulação em ambiente controlado através de máquinas virtuais.

1.4.3 Limitações da metodologia

Em decorrência da utilização de simulação em ambiente controlado, os resultados não são influenciados por todas as variáveis possíveis em um ambiente real. Dentre essas variáveis ausentes destacam-se: tráfego de pacotes oriundo de hosts fora da rede local e hosts com elevada capacidade de processamento.

1.4.4 Coleta e tratamento de dados

Os dados foram coletados através de simulações em ambiente controlado utilizando máquinas virtuais com Sistema Operacional Kali Linux para o atacante e Ubuntu para a vítima. O software de virtualização usado foi o Oracle VM VirtualBox.

1.5 Etapas do Trabalho

O presente trabalho encontra-se organizado em sete capítulos, descritos a seguir:

O capítulo 1, INTRODUÇÃO, contextualiza o trabalho e apresenta o problema e os objetivos pretendidos.

O capítulo 2, REFERENCIAL TEÓRICO, apresenta conceitos e definições relacionados com os temas Segurança da Informação e Comunicações e Guerra Cibernética, a partir de definições encontradas em diferentes fontes bibliográficas. Nele também serão abordados os conceitos de espaço cibernético e ataque cibernético.

O capítulo 3, GUERRA CIBERNÉTICA: CASOS DE ATAQUES DE NEGAÇÃO DE SERVIÇO, contextualiza o leitor no assunto negação de serviço e apresenta casos de Guerra Cibernética onde ataques de DoS foram maciçamente utilizados.

O capítulo 4, PROTOCOLOS IP E TCP, tem como objetivo apresentar ao leitor noções básicas sobre arquitetura de redes de computadores e sobre protocolos da internet, visando o melhor entendimento da técnica TCP SYN flood, que será realizada na simulação de ataque de DoS.

O capítulo 5, TÉCNICAS EMPREGADAS EM ATAQUES DE NEGAÇÃO DE SERVIÇO, tem como objetivo descrever as principais técnicas de DoS utilizadas.

O capítulo 6, ANÁLISE PRÁTICA, contém a análise de simulação de ataque de DoS realizada em máquinas virtuais.

Finalmente, o capítulo 7, CONCLUSÃO, encerra este trabalho, expondo as conclusões do autor referentes a pesquisa realizada, assim como apresenta sugestões de trabalhos futuros.

2 REFERENCIAL TEÓRICO

Visando auxiliar no melhor entendimento do tema abordado, este capítulo tem como propósito apresentar a conceituação dos dois temas centrais deste trabalho, que são: Segurança da Informação e Comunicações (SIC) e a Guerra Cibernética. Para isso, foram consultadas diversas fontes bibliográficas que versam sobre o assunto. As definições de espaço cibernético e ataques cibernéticos também serão expostas, tendo em vista que os dois conceitos são complementares ao assunto Guerra Cibernética.

2.1 Segurança da Informação e Comunicações

É notório, observando o panorama global de hoje, que nas sociedades modernas há um crescimento cada vez mais do uso da internet e um aumento da dependência de serviços baseados em infraestruturas de Tecnologia da Informação e Comunicações (TIC). Em 2010, o Livro Verde Segurança Cibernética no Brasil enumerou alguns acontecimentos determinantes para a maturação deste cenário. Esses acontecimentos foram chamados de *Fenômenos da Sociedade da Informação*, que são descritos a seguir:

> "a) Elevada convergência tecnológica; b) Aumento significativo de sistemas e redes de informação, bem como da interconexão e interdependência dos mesmos; c) Aumento crescente e bastante substantivo de acesso à Internet e das redes sociais; d) Avanços das tecnologias de informação e comunicação (TIC); e) Aumento das ameaças e das vulnerabilidades de segurança cibernética; e, f) Ambientes complexos, com múltiplos atores, diversidade de interesses, e em constantes e rápidas mudanças" (BRASIL, 2010).

Acompanhando esse fluxo de crescimento tecnológico, ataques contra redes de computadores e contra infraestruturas críticas de informação passaram a ser mais comuns. Portanto, as ameaças relacionadas à interconectividade global tornaram-se um dos grandes desafios da atualidade (BRASIL, 2015).

Neste contexto o conceito de Segurança da Informação e Comunicações ganha evidência. Hoje, SIC é essencial para os negócios e serviços de uma organização, seja ela pública ou privada, e diversos são os documentos e as normas que tratam sobre o assunto.

De acordo com a ABNT NBR ISO/IEC 27002: 2005 (2005), norma que versa sobre a prática da gestão de SIC dentro das empresas, Segurança da Informação "é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".

Percebe-se que esta definição é totalmente direcionada para o mundo corporativo e se adequa mais as instituições privadas.

Entretanto, conforme já foi dito, a Segurança das Informações e Comunicações também é uma preocupação para a Administração Pública Federal e, particularmente, para as Forças Armadas.

Em 2014, o Ministério da Defesa, através da publicação MD31-M-07, elaborou a Doutrina Militar de Defesa Cibernética, com o objetivo de estabelecer uma doutrina cibernética no âmbito das Forças Armadas. Esta publicação define a SIC, de forma bem resumida, como "ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações" (BRASIL, 2014).

A Marinha do Brasil (MB), em seu documento que normatiza a utilização da infraestrutura de Tecnologia da Informação dentro da Força Naval, apresenta uma definição mais completa. Segunda a publicação DGMM 0540, em sua mais recente revisão (2019), SIC é definida como:

> A proteção resultante de todas as medidas postas em execução visando negar, impedir ou minimizar a possibilidade de obtenção do conhecimento de dados que trafeguem ou sejam armazenados digitalmente nos sistemas de redes locais, compreendendo, segundo definição estabelecida pelo Governo Federal, ações voltadas às Seguranças física, lógica, de tráfego e criptológica das Informações Digitais. Portanto, a SIC corresponde não só ao conjunto de procedimentos, como também aos recursos (programas e equipamentos específicos de segurança) e às normas aplicáveis que irão garantir os seus requisitos básicos. (BRASIL, 2019).

Além disso, a DGMM 0540, em conformidade com a MD31-M-07, também relaciona à Segurança da Informação e Comunicações às ações que visam garantir aos dados e as informações propriedades como disponibilidade, integridade, confidencialidade e autenticidade, podendo também em alguns casos mais específicos ser necessário assegurar propriedades como não-repúdio, confiabilidade e responsabilidade (BRASIL, 2019).

Observando as definições dos dois documentos militares, percebe-se que os termos disponibilidade, integridade, confidencialidade e autenticidade se repetem. Essas propriedades são consideradas os pilares da SIC e são definidas da seguinte forma pela publicação DGMM 0540:

> a) Disponibilidade - capacidade da informação digital estar disponível para alguém autorizado a acessá-la no momento próprio.
> b) Integridade - capacidade da informação digital somente ser modificada por alguém autorizado;
> c) Confidencialidade - capacidade da informação digital somente ser acessada por alguém autorizado;

> d) Autenticidade - capacidade da origem da informação digital ser aquela identificada (BRASIL, 2019).

2.2 Espaço Cibernético

Para entender o que é Guerra Cibernética, é importante entender dentro de que ambiente ela está inserida.

A guerra convencional a que a maioria dos indivíduos está acostumada tem seus ambientes de confronto bem definidos. São eles: espaço aéreo, terrestre e marítimo. Porém, com a evolução da Tecnologia da Informação (TI), cada vez mais as ações cinéticas empregadas na guerra tradicional têm sido substituídas ou complementadas por ações cibernéticas. Essas ações ocorrem no espaço cibernético ou ciberespaço, cuja definição é encontrada em diversas fontes de informação.

Uma definição é apresentada pelo Departamento de Defesa (DoD) dos Estados Unidos, que considera o ciberespaço o quinto domínio da guerra (o domínio espacial é o quarto domínio) e o define como:

> Um domínio global dentro do ambiente de informação, que consiste em uma rede interdependente de infraestruturas de tecnologia da informação (TI), que inclui a Internet, redes de telecomunicações, sistemas computacionais dotados de processadores e controladores embutidos. Neste ambiente, a eletrônica e o espectro eletromagnético são empregados para armazenar, modificar e trocar dados através de sistemas interligados em rede (STEVE, WINTERFELD, 2011, APUD MOURÃO, 2014).

Para o Ministério da Defesa (MD) do Brasil, conforme consta na Doutrina Militar de Defesa Cibernética (2014), o espaço cibernético é o "espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas".

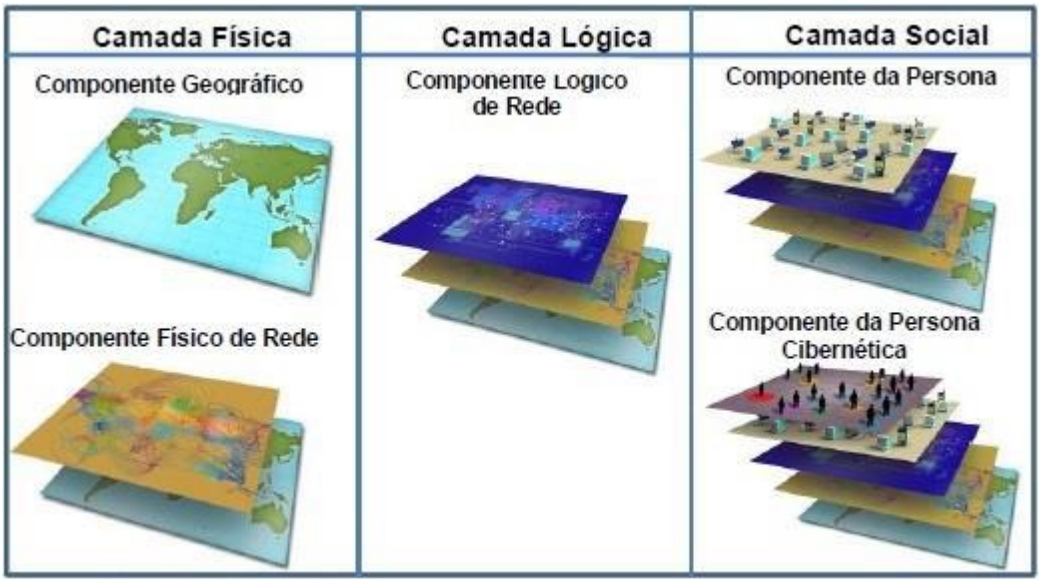
Pelas duas definições, infere-se que ambiente de informação e espaço virtual são semanticamente iguais. Ambos são considerados uma nova dimensão, que não se restringe a uma estrutura física, embora necessite dela (AVELAR, 2018).

De acordo com Carneiro (2012, apud AVELAR, 2018), o espaço virtual (e consequentemente o espaço cibernético) é global e costuma ser dividido em três camadas, que são as camadas física, lógica e social. Carneiro (2012, apud AVELAR, 2018) as define da seguinte forma:

- Camada física: Abrange todos os componentes físicos que dão suporte a rede, como hardware, cabos, conectores, roteadores etc.;

- Camada lógica: Abrange as conexões lógicas existentes entre os componentes físicos principais, que são chamados de nós da rede;
- Camada social: Composta pelas pessoas que interagem com o espaço virtual.

Figura 3 - Camadas do espaço cibernético



Fonte: Carneiro (2012, apud AVELAR, 2018)

A partir das considerações acima, um aspecto importante do espaço cibernético deve ser destacado. Por ser um domínio global, onde vários sistemas estão interligados em rede, pode-se dizer que não há fronteiras e nem distâncias no ciberespaço. As informações que por ele transitam podem ser acessadas de qualquer ponto (AVELAR, 2018).

Na guerra cinética, quando uma Força Naval executa uma ação ofensiva, é necessário que ela se desloque para o mais próximo possível do alvo, de forma que este fique dentro do alcance dos seus armamentos. Para uma ação cibernética essa aproximação não é necessária, tendo em vista que um ataque cibernético pode ser executado a partir de qualquer lugar do globo.

2.3 Guerra Cibernética

A expressão Guerra Cibernética é muito utilizada atualmente, embora muitas vezes ela seja empregada de maneira equivocada. Não há um consenso quanto a melhor definição para o

termo. Porém, a maioria dos autores sobre Guerra Cibernética converge quanto à uma característica que a difere de um ataque cibernético comum: a motivação política e estratégica.

Um ataque cibernético para ser enquadrado dentro de um contexto de Guerra Cibernética precisa ter sido motivado por razões estratégicas ou políticas e contar com a participação de alguma Nação (MENDONÇA, 2014). Ataques cibernéticos contra instituições privadas motivados por razões pessoais não podem ser considerados como ações de Guerra Cibernética, e sim, como incidentes cibernéticos (NUNES, 2010).

Com o objetivo de sedimentar o entendimento sobre o assunto, este trabalho apresentará algumas definições de Guerra Cibernética encontradas em publicações relacionadas ao tema.

Segundo Mendonça (2014), pode-se dizer que Guerra Cibernética é um termo empregado para se referir a modalidade de guerra que utiliza o espaço cibernético e a infraestrutura de informação como campo de batalha. Nessa modalidade armas físicas são substituídas por artifícios virtuais, que muitas vezes tem o potencial de causar danos materiais.

Já Nunes (2010), apresenta uma definição mais completa, a partir de definições encontradas em publicações militares. Para ele, Guerra Cibernética pode ser definida como:

> Ações ofensivas, defensivas e de exploração realizadas por meio de sistemas de informação e de redes de computadores, destinadas a interromper, negar, corromper, destruir ou acessar as informações contidas nos sistemas de TI inimigos e, ao mesmo tempo, garantir o uso continuado e a inviolabilidade dos nossos sistemas de TI (NUNES, 2010).

Para o Ministério da Defesa, conforme consta na publicação MD31-M-07, que trata sobre a Doutrina Militar de Guerra Cibernética, a Guerra Cibernética se caracteriza pelo:

> Uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC (BRASIL, 2014).

Nota-se que a definição acima delimita a Guerra Cibernética dentro de um contexto militar. Porém, ao analisar todos os conceitos expostos, entende-se que para caracterizar uma Guerra Cibernética não é necessário o envolvimento das Forças Armadas, embora a palavra "guerra" possa assim sugerir, e sim, a participação de Estados como um dos atores do conflito.

Os alvos da Guerra Cibernética muitas vezes são infraestruturas críticas eminentemente civis. Ataques contra essas instalações podem acarretar impactos na área econômica, política, militar, psicossocial ou científico, o que os tornam extremamente perigosos para a sociedade moderna (AVELAR, 2018).

Estas infraestruturas são uma grande vulnerabilidade para as Nações devido a sua importância estratégica e porque, praticamente no mundo todo, elas estão conectadas a rede de dados que facilitam o gerenciamento e a operação dos seus serviços (AVELAR, 2018).

Por esses motivos, ataques cibernéticos contra instalações de valor estratégico, como setores de energia, financeiro, telecomunicações, transporte e saúde, que venham a comprometer o funcionamento e a soberania de uma Nação, são considerados como ações de Guerra Cibernética.

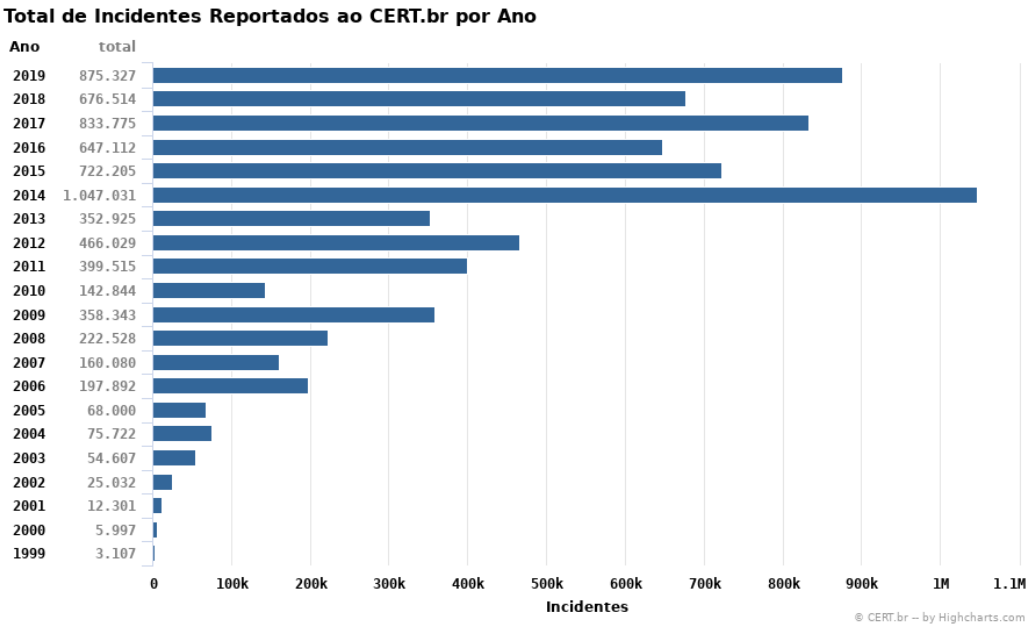
2.4 Ataques Cibernéticos

Segundo Lewis (2010, apud MENDONÇA, 2014), o limiar entre ataque cibernético e Guerra Cibernética é muito tênue. Para se determinar se um ataque cibernético está inserido dentro de um contexto mais amplo, caracterizando uma guerra cibernética, deve-se analisar o propósito do ataque. Como já foi abordado na seção sobre Guerra Cibernética, um ataque cibernético para ser considerado uma ação de guerra cibernética precisa ter motivações políticas ou estratégicas, com a participação de Estados como agentes da ação. (MENDONÇA, 2014).

Os ataques na internet podem ter outras motivações, como demonstrações de poder, prestígio, motivações financeiras, ideológicas e comerciais, dentre outros (CERT.br, 2016). Porém, nesses casos não será considerado a ocorrência de guerra cibernética. Esses ataques serão tratados como incidentes cibernéticos (NUNES, 2010).

No Brasil, o número de incidentes cibernéticos teve um aumento significativo a partir do 2014, ano em que o país foi sede da Copa de Mundo de futebol e recebeu diversas autoridades e delegações estrangeiras. Naturalmente o país, naquele momento, se tornou um potencial alvo para ataques cibernéticos. O gráfico que mostra o total de incidentes reportados por ano a partir de 1999 pode ser visto na figura 4.

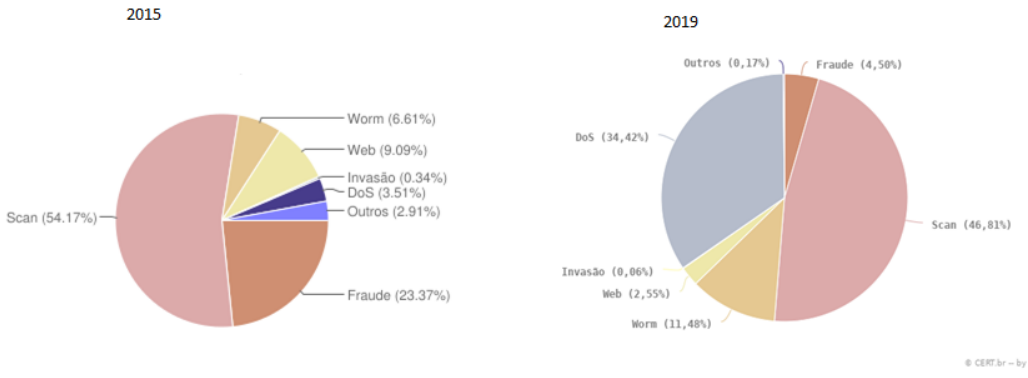
Figura 4 - Total de incidentes cibernéticos reportados ao CERT.br nos últimos vinte anos



Fonte: CERT.br, 2020

Dentre os ataques reportados se destacam as técnicas de varredura de rede, utilizadas para identificar potenciais alvos, com mais de 46% do total de incidentes reportados em 2019, e os ataques de negação de serviço (Denial of Service- DoS), que foram os ataques que proporcionalmente mais cresceram comparando-se os dados dos incidentes reportados nos últimos cinco anos, passando de 3,51% em 2015 para 34,42% em 2019, conforme consta na figura 5. As definições de cada um dos tipos de ataques presentes no gráfico encontram-se no quadro 1 e foram extraídas do site do CERT.br.

Figura 5 - Comparativo entre incidentes cibernéticos reportados em 2015 e 2019



Fonte: CERT.br, 2020

Quadro 1 - Definição dos tipos de ataque cibernético

Tipo de ataque	Definição
Worm	Atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
DoS	Ataque cibernético onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
Invasão	Ataque cibernético bem sucedido que resulte no acesso não autorizado a um computador ou rede.
Web	Caso particular de ataque cibernético visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
Scan	Ataque cibernético utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
Fraude	Categoria de ataque cibernético que engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

Fonte: Autoria própria

Para o Ministério da Defesa, em caráter doutrinário, ataques cibernéticos "compreendem ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente" (BRASIL, 2014).

De acordo com a Marinha do Brasil, em sua publicação usada como referência para questões relacionadas a TI, os ataques cibernéticos podem ser classificados quanto a intenção, quanto a origem e quanto a forma de atuar.

Quanto à intenção, os ataques podem ser intencionais ou acidentais. A DGMM 0540 aborda está classificação de ataque de maneira bastante superficial. De acordo com ela, o que diferencia um do outro é identificar se o ataque acorreu de forma premeditada ou não (BRASIL, 2019).

Em relação à classificação quanto à origem, o ataque pode ser de origem interna ou externa. O ataque interno se caracteriza quando o atacante o realiza de dentro da rede local, com ou sem autorização de acesso, ou então, quando o ataque é realizado de fora da rede local, porém por um usuário com autorização de acesso. O ataque é considerado externo quando o atacante realiza o ataque fora da rede local, não possui autorização de acesso e mesmo assim consegue burlar todo o perímetro de segurança da rede (BRASIL, 2019).

Por último, quanto à forma de atuar, o ataque cibernético pode ser ativo ou passivo. São considerados passivos os ataques que não resultam na modificação das informações contidas no sistema. Nesses casos, na maioria das vezes as vítimas não sabem que estão sendo atacadas. Já os ataques ativos se caracterizam por haver modificação, interrupção ou fabricação de novas informações, ou ainda alteração do estado ou operação do sistema (BRASIL, 2019).

3 GUERRA CIBERNÉTICA: CASOS DE ATAQUES DE NEGAÇÃO DE SERVIÇO

Este capítulo tem como finalidade apresentar casos de Guerra Cibernética que tiveram repercussão mundial, com foco nos acontecimentos onde os ataques de negação de serviço foram amplamente utilizados. Para isso, o capítulo se iniciará com um abordagem teórica sobre o ataque de DoS e posteriormente serão apresentados os estudos de caso.

3.1 Negação de Serviço (DoS)

Negação de Serviço (DoS, do inglês Denial of Service) é um ataque cibernético praticado por uma entidade hostil através de um computador conectado à internet e tem como objetivo tirar de operação um serviço, um computador ou uma rede de computadores (CERT.br, 2016).

O DoS não é um ataque de invasão de computadores utilizada por hackers para roubar informações e fazer espionagem, ele é um tipo de ataque cibernético que sobrecarrega o sistema alvo de forma que um usuário legítimo não consiga acessar os serviços ou recursos computacionais oferecidos por este sistema (CERT.br, 2016). Como ataques de invasão e ganho de acesso requerem um esforço maior do atacante, muitas vezes estes optam por executar um ataque de negação de serviço por este ser de menor complexidade (BARDAL, 2014).

Também é comum que hackers utilizem ataques de negação de serviço como despistamento e não como ataque principal. Nesses casos, o objetivo é fazer com que equipes de resposta a incidentes cibernéticos concentrem seus esforços na mitigação dos ataques de DoS e, assim, outros ataques cibernéticos aconteçam e não sejam notados, como, por exemplo, a invasão a sistemas e roubo de informações (CERT.br, 2016).

A DoS pode causar diversos prejuízos aos negócios do alvo, como danos à imagem, perda financeira e de credibilidade. As motivações para o ataque são variadas, podendo ser de caráter estratégico, econômico, político, ideológico ou até mesmo individuais (CERT.br, 2016).

De acordo com Piedrahita (2014) e o CERT.br (2016), as principais motivações para se utilizar um ataque de DoS são:

- Crenças ideológicas: Associados à prática do hacktivismo. Os ataques têm como alvo serviços e sites relacionados a questões ideológicas e são usados como forma de protesto para atrair a atenção do público geral.
- Questões financeiras: Ataques realizados contra empresas concorrentes, com a finalidade de obter alguma vantagem no mercado.

- Motivos pessoais e fúteis: Ataques realizados por grupos pequenos de pessoas, muitas vezes iniciantes e que, geralmente, não causam grandes impactos as vítimas.
- Questões políticas e estratégicas: Ataques geralmente praticados por militares ou terroristas, que dispõem de amplos recursos para realizar o ataque. Os alvos na maioria das vezes são setores estratégicos de um país e tem o objetivo de afetar a moral de uma Nação inimiga.

Nas próximas seções serão mostrados casos de ataques de negação de serviço que tiveram repercussão a nível mundial e, por terem sidos motivados por uma aparente causa política e estratégica, são categorizados como exemplos de Guerra Cibernética.

3.2 Ataques contra a Estônia

No início de 2007, a Estônia foi atingida por um grande Ataque Distribuído de Negação de Serviço (DDoS), culminando com a paralisação de diversos serviços do país. Este país do norte europeu é conhecido por ser um dos países mais conectados do mundo, competindo com a Coreia do Sul, e bem à frente dos Estados Unidos. A infraestrutura dos serviços essenciais à população estoniana é toda informatizada, o que contribuiu para o ataque causar um grande impacto no país (CLARKE, 2010).

A principal razão para o ataque foi um desentendimento diplomático com a Rússia, motivado pela troca de posição de uma estátua soviética, conhecida como Soldado de Bronze e que fazia alusão aos soldados soviéticos que combateram o nazismo na Segunda Guerra Mundial. Com a independência da Estônia em relação a União Soviética, após o fim da Guerra Fria, o povo estoniano via a estátua como símbolo que representava as décadas de opressão pelos quais eles foram submetidos à URSS e pressionaram o governo para derrubá-la. Porém, os russos pressionaram e alegaram que mover a estátua seria uma afronta ao governo de Moscou, acirrando as tensões entre os dois países. Houve protestos e tumultos pelas ruas da capital Tallinn entre um grupo nacionalista estoniano e uma minoria russa que ainda morava na Estônia, na revolta que ficou conhecida como Noite de Bronze. Pressionados, as autoridades estonianas retiraram o Soldado de Bronze de sua localização e a colocaram em um cemitério militar próximo. No entanto, esta atitude não agradou os radicais russos, que começaram um conflito online contra a Estônia (MALONE, 2012).

A batalha no espaço cibernético foi realizada principalmente através de ataques de DDoS direcionados a servidores de serviços essenciais do país, como servidores da rede bancária, de empresas de comércio eletrônico e de provedores de serviço de internet, usando inundações de ping e inundações de pacotes TCP SYN. Além dos ataques de negação de

serviço, outras alterações na Web foram realizadas, usando várias ferramentas como Injeções de SQL e inundação de e-mail. Os ataques afetaram fortemente a infraestrutura de comunicações da Estônia, alteraram as tabelas de roteamento, sobrecarregaram os servidores DNS e fizeram com que os mainframes dos servidores de e-mail sobrecarregassem. Além disso, sites do governo, como o da presidência e do parlamento por exemplo, também foram atacados, ficando semanas incapazes de voltar a operar, causando um dano psicológico significativo ao povo estoniano (MALONE, 2012).

No início, os estonianos pensaram que as quedas nos serviços online seriam passageiras e logo os serviços seriam restabelecidos. Porém, esse ataque não durou um dia, mas durou semanas, com sites subindo e descendo durante todo esse tempo. Os ataques mais pesados ocorreram entre 9 de maio e 11 de maio de 2007. No entanto, o período todo dos ataques durou quase um mês, sendo realizado de 26 de abril a 23 de maio. O ataque só teve fim após o governo estoniano isolar digitalmente seus servidores, bloqueando todo o tráfego de origem internacional (MALONE, 2012).

Até hoje não há uma confirmação efetiva que os ataques tenham sidos praticados pelo governo de Moscou. Os russos sempre negaram ser os autores dos ataques e nunca colaboraram com as investigações. Porém, as evidências são fortes. A maioria dos sites invadidos foi desfigurado com propaganda nacionalista russa e as ferramentas de ataque cibernético empregadas pelos autores também foram escritas em russo, o que corrobora com a teoria de que, no mínimo, os ataques tiveram a conivência de Moscou (GHAVAM, 2016).

3.3 Ataques contra a Geórgia

A guerra entre a Rússia e a Geórgia, em 2008, foi um marco importante na história da guerra moderna, pois foi a primeira vez que ataques cibernéticos foram utilizados junto a campanhas militares. O conflito foi motivado devido as ambições nacionalistas de duas regiões na época controladas pela Geórgia, que eram os territórios de Abkházia e Ossétia do Sul. Após a dissolução da URSS, esses dois territórios, apoiados por Moscou, conseguiram derrotar o exército georgiano e estabeleceram governos independentes. Desde então, forças de paz georgianas e russas mantiveram a estabilidade na Ossétia do Sul. Porém, em agosto de 2008, após uma série de provocações por parte de rebeldes da Ossétia do Sul, o exército georgiano invadiu este território e conquistou sua capital. As forças russas responderam prontamente e, em cinco dias, forçaram um cessar-fogo após expulsarem o exército georgiano. Durante este breve engajamento militar russo, uma campanha cibernética, formalmente não reconhecida,

mostrou as habilidades de Moscou em usar meios cibernéticos para atingir seus objetivos. (MEDVEDEV, 2015).

As milícias cibernéticas russas atacaram a Geórgia com ataques de DDoS semelhantes aos orquestrados contra a Estônia. O objetivo inicial era impedir que os georgianos percebessem o que estava acontecendo através da negação de sites de mídias de comunicação. Os ataques interromperam as comunicações da Geórgia, sites do governo foram invadidos e desfigurados com propaganda russa e informações militares e políticas dos sistemas estratégicos da Geórgia também foram extraídas. No total, cinquenta e quatro sites da Geórgia de setores políticos, financeiros e telecomunicações foram atacados durante o conflito (GHAVAM, 2016.)

Com o maciço ataque de DDoS, a Geórgia perdeu o controle sobre o domínio ".ge" e teve que mudar os servidores dos sites do governo para outros países. Na tentativa de interromper o ataque, a Geórgia bloqueou todo o tráfego vindo da Rússia, porém os russos redirecionaram seus ataques para parecerem que os pacotes vinham da China. O sistema bancário georgiano ficou totalmente paralisado, pois os russos ordenaram que suas *botnets* atacassem a comunidade bancária internacional como se fossem ataques oriundos da Geórgia. Com isso, os principais bancos internacionais encerraram as conexões com os bancos georgianos (CLARKE, 2010).

Segundo Clarke (2010), no auge do ataque cibernético, os russos utilizaram até seis *botnets* para realizar os ataques de DDoS, usando tanto máquinas invadidas e controladas sem a permissão do usuário, quanto máquinas de pessoas pró Rússia e com vontade de participar do ataque. As máquinas controladoras desses exércitos de *zumbis,* chamadas de mestre, estavam espalhadas por diversos países, como Rússia, Canadá, Turquia e Estônia.

Assim como no ataque à Estônia, os russos não assumiram a autoria do ataque. Apenas alegaram que os ataques eram uma resposta popular e que em nada tinham a ver com o governo russo. Porém, a organização e coordenação mostradas nos ataques somadas a não contribuição de Moscou em solucionar o conflito cibernético, sugerem mais uma vez que as autoridades russas tiveram participação ativa no conflito cibernético com a Geórgia (CLARKE, 2010).

3.4 Ataques contra a Coreia do Sul

De 2009 até 2011, a Coreia do Sul foi alvo de recorrentes ataques de negação de serviço. O principal país suspeito de ter efetuado os ataques foi o seu vizinho homônimo do norte. Os ataques não foram motivados por nenhum acontecimento geopolítico específico. Especialistas afirmam que o principal objetivo dos norte-coreanos com os ataques foi testar a resiliência

cibernética da Coreia do Sul e verificar o poder das armas cibernéticas da Coreia do Norte (CLARKE, 2010).

O primeiro ataque de DDoS ocorreu entre os dias 7 e 9 de julho de 2009. Os alvos foram vinte e um sites de setores políticos (incluindo o site da presidência) e estratégicos da Coreia do Sul, como sites de notícias e institutos financeiros. Para tentar ocultar a origem do ataque, os hackers norte-coreanos usaram algumas técnicas de computação para apagar os rastros na rede, como exclusão automática de arquivos de origem e destruição de discos rígidos dos computadores zumbis. Além disso, o ataque distribuído utilizou mais de quatrocentos servidores mestres espalhados pelo mundo. No total foram usados vinte mil bots, dentre os quais doze mil estavam localizados dentro da própria Coreia do Sul (PARK, 2015).

Antes dos ataques a Coreia do Sul, os Estados Unidos, país aliado dos sul-coreanos, também foram alvo de ataques de DDoS. O início dos ataques ocorreu justamente no dia 4 de julho, dia em que os norte-americanos comemoram a sua independência. De acordo com Clarke (2010), sites ligados ao governo foram atingidos por quase um milhão de requisições por segundo, ficando indisponíveis em vários determinados momentos. O site da Casa Branca só não saiu do ar pois ele é sustentado por vinte mil servidores espalhados pelo mundo. Com isso, durante o ataque todo o tráfego que buscava o site oficial do governo americano foi roteado para os servidores localizados mais próximo dos atacantes, o que deixou inoperante apenas os servidores hospedados em países asiáticos (CLARKE, 2010).

Durante o ataque simultâneo aos dois países, autoridades sul-coreanas identificaram que alguns servidores de comando e controle desse ataque estavam localizados no Reino Unido. Porém, o ataque pode ser atribuído à Coreia do Norte porque os códigos de ataque estavam no idioma coreano e alguns endereços IP que foram usados pelos atacantes foram identificados como sendo do Ministério dos Correios e Telecomunicações da Coreia do Norte. Além disso, um mês antes do ataque, o governo de Pyongyang anunciou oficialmente que estava totalmente pronto para qualquer forma de guerra de alta tecnologia, o que reforça a teoria de que o ataque foi orquestrado para testar o poderio cibernético norte-coreano (PARK, 2015).

Como esse ataque de negação de serviço trouxe um grande impacto a Coreia do Sul, prejudicando a disponibilidade de serviços públicos essenciais a população, o governo sul-coreano percebeu a importância de se ter um órgão central, forte e preparado para detecção precoce e resposta adequada a esses tipos de ataque. Assim, a Coreia do Sul estabeleceu a criação de um Comando de Guerra Cibernética (PARK, 2015).

Em julho de 2010, novos ataques de DDoS atingiram a Coreia do Sul, tendo como alvo novamente sites do governo e de setores estratégicos, como o site da Casa Azul (sede do

governo), do Ministério de Relações Exteriores e Comércio, do Korean Exchange Bank (importante banco coreano) e o Naver.com (site de pesquisa, semelhante ao google). Embora o ataque não tenha sido em larga escala, como no ano anterior, a Coreia do Norte utilizou métodos de ataque semelhantes. De acordo com a Agência Nacional de Polícia da Coreia do Sul (apud PARK, 2015), esse ataque de DDoS foi conduzido pelas mesmas redes de bots usadas para o ataque maciço de DDoS em 2009 (PARK, 2015).

Em março de 2011, um novo ataque de DDoS foi realizado contra o governo de Seul e serviços privados, desta vez mais intenso do que o de 2009. Mais de setecentos servidores foram usados como hosts mestres e cem mil computadores zumbis foram mobilizados para este ataque. A forma como o ataque ocorreu foi semelhante ao ataques anteriores já identificados como sendo da Coreia do Norte. Desta vez, as autoridades sul-coreanas identificaram que os norte-coreanos usaram sites de jogos ilegais para espalhar o malware que infectou as máquinas e configurou as botnets (PARK, 2015).

3.5 Ataques contra a Ucrânia

Em fevereiro de 2014, tropas russas invadiram a península da Crimeia, região ao sul da Ucrânia. O conflito foi causado a partir de uma disputa política entre a Rússia e a Ucrânia sobre um acordo comercial fracassado com a União Europeia (UE). Com a não firmação deste acordo, conflitos internos na Ucrânia culminaram na queda do presidente Viktor Yanukovich, que tinha origens russas. Aproveitando a instabilidade do país vizinho e almejando conquistar a região da Crimeia por questões estratégicas, em poucas semanas, a Rússia realizou um referendo local, anexou com sucesso a Península da Crimeia e iniciou uma guerra na região de Donbass, na Ucrânia (GHAVAM, 2016.)

Em paralelo a anexação da Criméia por meios militares tradicionais, o governo russo também iniciou uma campanha de desestabilização na Ucrânia usando métodos de guerra assimétrica, que consistia em desinformação, operações psicológicas e de fraude e invasões cibernéticas. De acordo com a empresa de segurança cibernética LookingGlass Cyber Solutions (apud GHAVAM, 2016), desde 2013, a Rússia havia iniciado uma campanha de espionagem cibernética contra instituições do governo ucraniano. Usando técnicas de spear phishing, hackers russos ocultaram malwares nos anexos de e-mails spam e enviaram para servidores do governo ucraniano. Uma vez abertos, os anexos infectaram as redes ucranianas e extraíram informações altamente valiosas para a estratégia russa. As informações confidenciais coletadas pelos hackers incluíam dados sobre equipamentos militares ucranianos, números de soldados,

ações de combate e posições estratégicas das forças ucranianas, além de localização de alvos estratégicos. Consequentemente, o governo ucraniano já iniciou o conflito em desvantagem. Como na tática usada pela Rússia durante a guerra contra a Geórgia, os hackers russos usaram técnicas de guerra cibernética e espionagem eficazes em conjunto com ataques militares tradicionais (GHAVAM, 2016.)

As operações cibernéticas da Rússia na Ucrânia foram uma mistura dos métodos e técnicas observadas nos casos da Estônia e da Geórgia. As atividades cibernéticas do Kremlin na Ucrânia se concentraram na coleta de informações para melhorar a eficácia de sua campanha terrestre. No entanto, as atividades russas na Ucrânia também envolveram ataques de negação de serviço comparáveis aos observados na Geórgia e na Estônia. O Kremlin empregou ataques de DDoS em sites políticos e de mídia ucranianos, desfigurando vários sites da OTAN com a propaganda russa, vazou informações confidenciais do governo ucraniano e interrompeu as telecomunicações e as redes ucranianas. Quanto à atribuição, aliados do governo ucraniano afirmam que o todo aparato tecnológico do Serviço Federal de Segurança da Rússia (FSB) foi amplamente usado na coordenação dos ataques cibernéticos (GHAVAM, 2016.)

4 PROTOCOLOS TCP/IP

Este capítulo tem como propósito apresentar conceitos fundamentais para o entendimento das técnicas de Ataques de Negação de Serviço que serão apresentadas no capítulo cinco e para o entendimento da simulação de ataque demonstrada no capítulo seis. Nas primeiras seções serão apresentados o conceito de arquitetura de rede de computadores, onde serão descritos ao leitor o modelo de arquitetura OSI e o modelo de arquitetura Internet TCP/IP. Na seção 4.2 serão expostas características importantes do protocolo TCP. Ressalta-se que este capítulo não tem a intenção de esgotar os assuntos que serão apresentados, mas sim dar ao leitor um entendimento básico sobre o tema.

4.1 Arquiteturas de Redes de Computadores

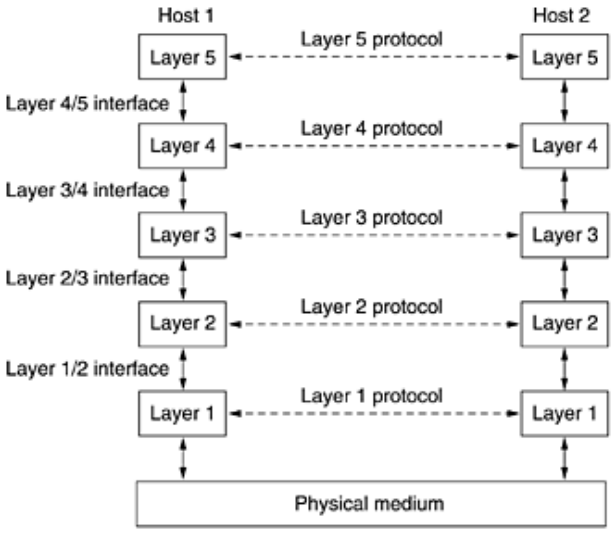
As arquiteturas de redes de computadores são estruturadas em camadas ou níveis hierárquicos, onde cada uma dessas camadas possui regras específicas para se comunicar com a camada equivalente de outra máquina ou host (COLCHER et al, 1995).

Essas regras específicas são chamadas de protocolos, cuja implementação permitiu gerir a estrutura de redes de maneira mais eficiente. A utilização de protocolos específicos para cada camada permite que se faça alterações em um nível da estrutura sem causar impacto na estrutura global (COLCHER et al, 1995).

Nessas estruturas, cada nível presta um conjunto de serviços para o nível imediatamente superior, da mesma forma que usufrui dos serviços oferecidos pelo nível inferior. O limite entre as camadas adjacentes é chamado de interface (COLCHER et al, 1995).

A seguir é apresentada uma estrutura que exemplifica um modelo em camadas genérico.

Figura 6 -Camadas, protocolos e interfaces



Fonte: TANENBAUM, 2003.

É importante ressaltar que a transferência de dados entre duas camadas correspondentes, ou seja, a comunicação entre a mesma camada de hosts diferentes, não ocorre diretamente (horizontalmente). Na realidade, o dado transferido “desce” verticalmente até a camada mais baixa, passando por todos os outros níveis inferiores ao seu nível de origem. Na camada mais baixa, chamada de camada 1 ou camada física, é que ocorre a comunicação propriamente dita entre as máquinas e o dado é fisicamente transferido. Ao chegar no nível 1 da estação de destino, o dado “sobe” verticalmente até o nível correspondente ao nível de origem na máquina transmissora (COLCHER et al, 1995).

Existem diversos modelos de arquitetura de rede. Inicialmente, cada fabricante de computador desenvolveu seu próprio modelo para que suas máquinas pudessem trocar informações entre si. Porém, logo se percebeu que essa não era a melhor solução, pois dessa forma os usuários eram sempre obrigados a usar equipamentos do mesmo fornecedor, já que máquinas de fabricantes diferentes não conseguiam se comunicar (COLCHER et al, 1995).

Como solução para esse problema, foi proposto pela *International Organization Standardization* (ISO) a adoção de uma arquitetura base padrão, aberta e pública com o objetivo de fornecer um modelo de referência que permitisse o desenvolvimento coordenado de padrões para a interconexão de sistemas. Esse modelo foi denominado de modelo de referência OSI, do inglês *Open Systems Interconnection* (OSI), e estrutura a arquitetura de redes em sete camadas de referência. (COLCHER et al, 1995).

O modelo OSI é basicamente um esquema geral e possui aplicação mais conceitual. As características descritas para cada uma de suas camadas são muito importantes, porém, os seus protocolos raramente são utilizados hoje em dia (TANENBAUM, 2003).

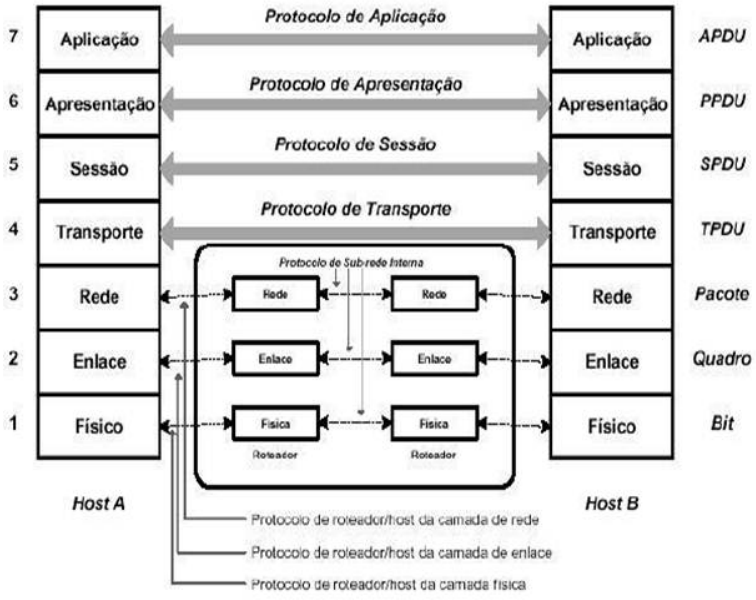
A Arquitetura Internet é outro modelo importante de arquitetura de redes. Sua estrutura é dividida em quatro camadas e ela surgiu a partir da necessidade de se ligar redes heterogêneas, ou seja, interligar de maneira uniforme diferentes tecnologias de rede, formando assim uma inter-rede. Seu sucesso é devido a implementação dos seus dois protocolos principais, que são o *Internet Protocol* (IP) e o *Transmission Control Protocol* (TCP) (COLCHER et al, 1995).

Nas seções a seguir serão analisados esses dois modelos de arquiteturas de rede, o modelo de referência OSI e o modelo de referência Internet TCP/IP.

4.1.1 Modelo de Referência OSI

Conforme dito no início do capítulo quatro, o modelo OSI é um modelo de arquitetura proposto pela ISO como primeiro passo na busca da padronização dos protocolos de comunicação entre redes de computadores. Este modelo é estruturado em sete camadas, que são: a física, a de enlace, a de rede, a de transporte, a de sessão, a de apresentação e, por fim, a de aplicação (TANENBAUM, 2003).

Figura 7 - Modelo OSI



Fonte: COLCHER, et al, 1995

De acordo com Tanenbaum (2003), a ISO se baseou em cinco princípios para definir a divisão da estrutura nessas sete camadas. São eles:

> 1. Uma camada deve ser criada onde houver necessidade de outro grau de abstração.
> 2. Cada camada deve executar uma função bem definida.
> 3. A função de cada camada deve ser escolhida tendo em vista a definição de protocolos padronizados internacionalmente.
> 4. Os limites de camadas devem ser escolhidos para minimizar o fluxo de informações pelas interfaces.
> 5. O número de camadas deve ser grande o bastante para que funções distintas não precisem ser desnecessariamente colocadas na mesma camada e pequeno o suficiente para que a arquitetura não se torne difícil de controlar (TANENBAUM, 2003).

A tabela abaixo apresenta um resumo identificando as principais funções das camadas que serão abordadas nas próximas seções.

Quadro 2 - Resumo das camadas Modelo OSI

Camada	Função
Camada 7 - Aplicação	Possibilitar acesso aos recursos de rede.
Camada 6 - Apresentação	Traduzir códigos; comprimir dados; criptografar.
Camada 5 - Sessão	Controle de diálogo e controle de sincronização.
Camada 4 - Transporte	Comunicação fim-a-fim; segmentação e remontagem de mensagens.
Camada 3 - Rede	Roteamento e encaminhamento de pacotes.
Camada 2 - Enlace de dados	Detectar erros; delimitar os quadros; controle de fluxo.
Camada 1 - Física	Transmitir bits através de um canal de comunicação; prover especificações físicas e de sinais.

Fonte: Autoria própria

4.1.1.1 Nível Físico

É o nível mais inferior do modelo OSI. Essa camada se preocupa com as características físicas e de transmissão do sinal, que vão tornar possível a transferência do bit através de um canal de comunicação. Portanto, questões como tipo de conectores, tipos de codificação do sinal, voltagem a ser usada para representar cada bit, se a transmissão será full-duplex ou half-duplex e formas de se estabelecer a conexão, devem ser definidas nessa camada. O nível físico não se preocupa com o conteúdo da mensagem transmitida, assim como também não tem a obrigação de corrigir erros de transmissão (COLCHER et al, 1995).

4.1.1.2 Nível de Enlace de Dados

A segunda camada do modelo de referência OSI é a de enlace de dados. Esta camada possui como objetivo principal detectar possíveis erros que tenham ocorrido no nível físico. Porém, caso algum erro seja detectado, o nível de enlace não tem a obrigatoriedade de corrigi-lo, deixando essa tarefa para as camadas superiores (COLCHER et al, 1995).

Para tornar possível a detecção dos erros a camada de rede do transmissor, através dos protocolos nela implementados, divide os bits que serão enviados ao nível físico em quadros de bits e os envia em sequência. Cada um desses quadros possui alguma forma de redundância, permitindo assim que o nível de enlace do receptor detecte se houve algum erro na transmissão (COLCHER et al, 1995).

Outra função importante desta camada é implementar mecanismos de controle de fluxo para não sobrecarregar o receptor. Esta sobrecarga pode ocorrer quando a velocidade na qual os dados são enviados pelo transmissor for maior que a velocidade na qual os dados são recebidos pelo receptor. A camada de enlace regula esse tráfego de dados e reporta ao transmissor quanto de espaço o buffer do receptor tem em um dado momento (TANENBAUM, 2003).

4.1.1.3 Nível de Rede

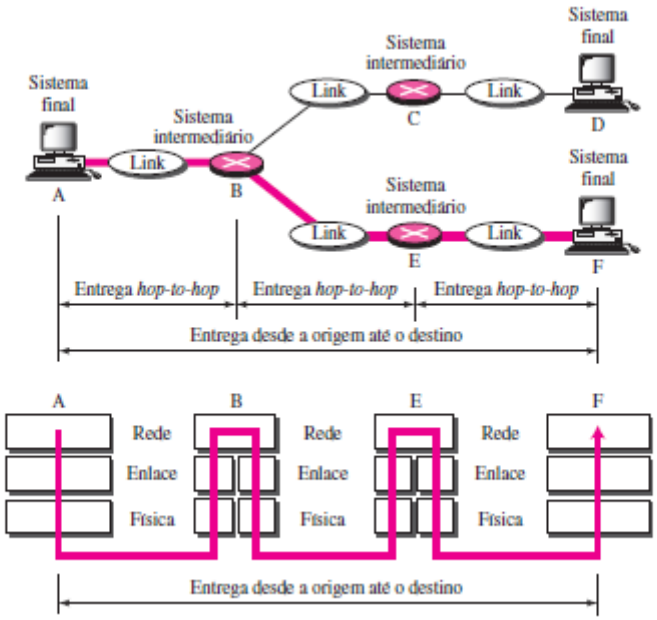
A camada de rede é responsável pelo roteamento e pelo encaminhamento dos pacotes que nela chegam, garantindo a entrega destes desde a estação de origem até a estação de destino, provavelmente passando por diversas redes ao longo do caminho (FOROUZAN, 2010).

Se dois sistemas estiverem conectados na mesma rede, teoricamente, a camada de rede seria irrelevante, pois a camada de enlace cumpriria essa função. Entretanto, no caso desses sistemas estarem conectados a redes diferentes por meio de dispositivos intermediários de

conexão, como roteadores e comutadores, é necessário um mecanismo que faça o endereçamento lógico e o roteamento dos pacotes. Nesses casos, a camada de rede acrescenta um cabeçalho em cada pacote proveniente da camada de transporte contendo os endereços lógicos das estações de origem e destino (FOROUZAN, 2010).

A figura abaixo demonstra como ocorre a entrega de pacotes entre as estações transmissora e receptora pertencentes a redes diferentes, ou seja, quando há a presença de sistemas intermediários.

Figura 8 - Entrega de pacotes desde a origem até o destino



Fonte: FOROUZAN, 2010

No exemplo acima um pacote tem como origem a estação A e como destino a estação F. A camada de rede de A encaminha o pacote a camada de rede de B. Esta consulta sua tabela de rotas e verifica que o próximo sistema intermediário até o destino F é o terminal E. Então, B encaminha o pacote para a camada de rede de E, que por sua vez encaminha para a camada de rede de F. Note que nos sistemas intermediários, os dados transmitidos só chegam no máximo até o nível de rede, não passando para os níveis superiores.

4.1.1.4 Nível de Transporte

A camada de transporte é responsável por garantir a comunicação fim-a-fim entre as aplicações da máquina transmissora e da máquina receptora, diferente do que ocorre nos níveis inferiores, onde a comunicação se dá entre máquinas adjacentes na rede. Esse controle de entrega é feito utilizando os cabeçalhos das mensagens e mensagens de controle (COLCHER et al, 1995).

Segundo Tanenbaum (2003), a função básica da camada de transporte é receber os dados oriundos da camada de sessão, fragmentar esses dados em unidades menores e repassá-los para a camada de rede, assegurando que todos esses fragmentos cheguem à aplicação na máquina de destino. Esses fragmentos contêm números de sequências, permitindo assim que a camada de transporte da máquina receptora consiga remontar a mensagem original ou até mesmo identificar e substituir pacotes perdidos na transmissão.

Assim como a camada de enlace de dados, a camada de transporte também realiza o controle de fluxo. Porém, diferente do nível mais inferior, o nível de transporte é responsável por controlar o fluxo de todo o caminho percorrido pelos dados, desde a origem até o destino. Na camada de enlace, o controle de fluxo é realizado apenas entre as máquinas imediatamente vizinhas (adjacentes) (FOROUZAN, 2010).

O mesmo ocorre com o controle de erros, que também é fim-a-fim. A camada de transporte da estação transmissora certifica-se que a mensagem chegou sem erros à camada de transporte da estação receptora. Normalmente, o erro detectado é corrigido por retransmissão (FOROUZAN, 2010).

4.1.1.5 Nível de Sessão

O nível de sessão é responsável pelo controle de diálogo e pela sincronização.

O controle de diálogo é o mecanismo que controla a vez em que cada estação deve transmitir, tornando possível assim que a comunicação entre dois processos ocorra em modo half-duplex ou full-duplex (FOROUZAN, 2010).

O controle de sincronização é o mecanismo que, em caso de falha na conexão, permite que a comunicação seja restabelecida a partir do último ponto de sincronização, não sendo necessário que todos os dados sejam retransmitidos. O ponto de sincronização funciona como um ponto de verificação e é uma marca lógica acrescentada ao diálogo entre dois usuários pela camada de sessão. Cada vez que um usuário receber este ponto, ele deve responder ao usuário com quem está mantendo a comunicação com um aviso de recebimento (COLCHER et al, 1995).

4.1.1.6 Nível de Apresentação

A camada de apresentação é a responsável por realizar algumas transformações específicas nos dados antes de enviá-los para a camada de sessão, como criptografia, compressão de dados e tradução de códigos. Para oferecer esses serviços, o nível de apresentação deve se preocupar com a sintaxe e a semântica das informações transmitidas, conhecendo assim a sintaxe tanto do sistema local como do sistema de transferência. Portanto, possui função diferente dos seus níveis inferiores, que se preocupam mais com a movimentação dos bits (COLCHER et al, 1995).

4.1.1.7 Nível de Aplicação

A camada de aplicação é a sétima e última camada do modelo de referência OSI. Ela é responsável por prover serviços ao usuário, seja ele humano ou um software, permitindo que o mesmo acesse a rede. Dentre os serviços oferecidos por esta camada, destacam-se a transferência de arquivos, e-mail, serviços de diretório, entre outros (FOROUZAN, 2010).

4.1.2 Arquitetura Internet TCP/IP

Será abordado nesta seção a Arquitetura de Rede Internet, também conhecida como Modelo de Referência TCP/IP, devido aos seus dois principais protocolos.

A Internet hoje conhecida mundialmente teve origem nos Estados Unidos, em 1969, a partir de um projeto desenvolvido pela Agência de Projetos de Pesquisa Avançada de Defesa (DARPA – *Defense Advanced Research Projects Agency*). Este projeto foi batizado de ARPANET e tinha como objetivo desenvolver um método rápido de comunicação em rede entre os computadores das bases militares e os departamentos de pesquisa do governo americano (SANZ, 2017).

Ao longo dos anos novas tecnologias de rede foram surgindo, o que provocou a necessidade de desenvolvimento de uma nova arquitetura de referência, capaz de interligar essas redes heterogêneas. O sucesso desta arquitetura está na sua habilidade em conectar redes diferentes de maneira uniforme, o que se deve principalmente a dois de seus protocolos: o TCP, que oferece um serviço de transporte orientado à conexão, e o IP, que oferece um serviço de rede não-orientado à conexão (COLCHER et al, 1995).

Uma das diferenças do modelo TCP/IP para o modelo OSI é a quantidade de camadas. Na Arquitetura Internet TCP/IP os serviços oferecidos pelas três camadas superiores do modelo OSI (aplicação, apresentação e sessão) foram em sua maioria concentrados em apenas uma camada, denominada de camada de aplicação. Também há diferença na divisão dos níveis mais inferiores. As funções exercidas pelas camadas físicas e de enlace no modelo OSI são exercidas por um único nível no modelo TCP/IP, que funciona como uma camada de interface física da rede, chamada em algumas literaturas de camada de sub-rede ou host-rede (SANZ, 2017).

Portanto, a arquitetura Internet TCP/IP é estruturada em quatro camadas conceituais, que serão abordadas nas próximas seções.

4.1.2.1 Camada de interface física da rede

Não existe um protocolo específico para esta camada, pois na arquitetura TCP/IP não há restrições quanto as redes que serão interligadas para formar a inter-rede. A única exigência para os protocolos dessa camada é que eles sejam compatíveis com o protocolo IP, pois este nível recebe datagramas IP do nível superior e os transmite através de uma rede específica (COLCHER et al, 1995).

4.1.2.2 Camada Inter-rede

A camada inter-redes da arquitetura TCP/IP possui função equivalente à da camada de rede do modelo de referência OSI. É de sua responsabilidade transferir os dados através das diversas redes heterogêneas conectadas, desde a estação de origem até a estação de destino, realizar o roteamento dos pacotes e é nela que está implementado o protocolo IP e seus protocolos auxiliares, como o ARP (*Adress Resolution Protocol*) e o ICMP (*Internet Control Message Protocol*) (TANENBAUM, 2003).

Na transmissão, a camada inter-rede recebe da camada de transporte o pacote a ser transmitido com o seu respectivo endereço de destino. Então, o pacote é encapsulado em um datagrama IP e a camada inter-rede verifica, através de um algoritmo de roteamento, se o datagrama deve ser entregue dentro da mesma rede ou se há a necessidade de enviá-lo para um equipamento gateway de forma a dar continuidade ao processo de transmissão. Na recepção, ao receber o pacote da camada de interface, o nível inter-rede executa o algoritmo de roteamento para definir se encaminha o pacote para o nível de transporte, no caso de ser a máquina de

destino, ou repassa o pacote para o próximo gateway, no caso de não ser a máquina de destino (COLCHER et al, 1995).

4.1.2.3 Camada de Transporte

É a camada localizada acima da camada de inter-rede e que dá suporte a dois protocolos importantes na arquitetura internet, o TCP e o UDP (*User Datagram Protocol*). Sua função é a mesma que a camada de transporte do modelo OSI, permitir comunicação fim-a-fim entre aplicações (COLCHER et al, 1995).

O protocolo TCP fornece à camada serviços mais completos, como controle de erro, controle de fluxo, sequenciação e reordenamento dos segmentos de dados e multiplexação de acesso ao nível inter-rede. O UDP é um protocolo mais simples e não oferece um serviço confiável, acrescentando ao seu cabeçalho apenas os endereços das portas de origem e destino, mecanismo para controle de erro (*checksum*) e informações do comprimento do campo de dados (FOROUZAN, 2010).

4.1.2.4 Camada de Aplicação

Esta camada oferece suporte aos protocolos de nível mais alto que permitem a interação dos usuários com os programas de aplicação. Podem usar tanto os serviços oferecidos pelo TCP (confiável e orientado à conexão) quanto os serviços oferecidos pelo UDP (não confiável e não orientado à conexão). São alguns exemplos de protocolos de aplicação: o SMTP, protocolo utilizado em correio eletrônico; o FTP, utilizado para transferência de arquivos; e o HTTP, usado para buscar páginas na World Wide Web (TANENBAUM, 2003).

4.2 Funcionamento dos Protocolos TCP/IP

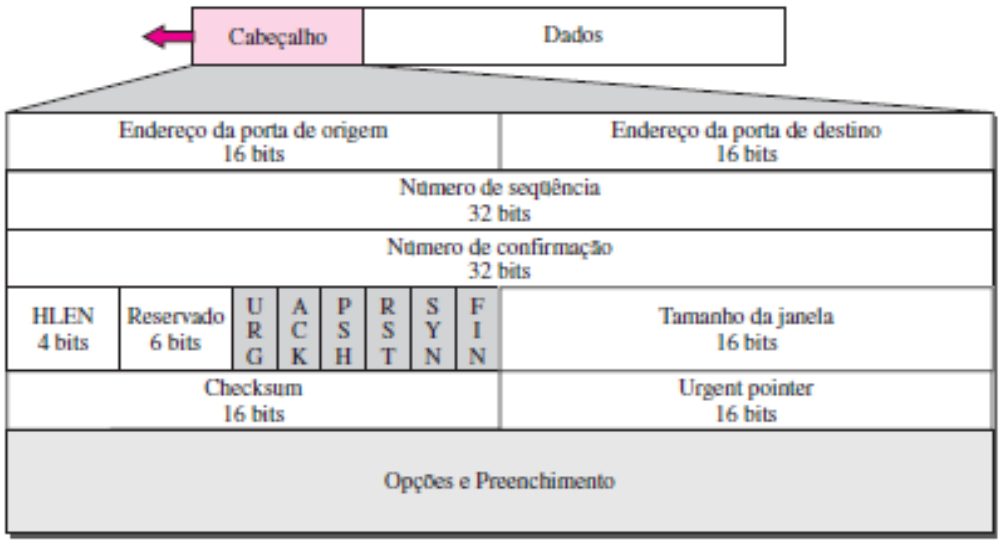
A comunicação entre as aplicações mais utilizadas na internet tem como suporte esses dois protocolos. O IP é responsável por adicionar o endereço virtual aos pacotes oriundos da camada de transporte. Porém, ele não oferece um serviço confiável, pois não verifica se a entrega foi realizada e não corrige os erros. Sua vantagem é flexibilidade que ele permite ao usuário em acrescentar funcionalidades necessárias para cada aplicação. Já o TCP oferece um serviço confiável e antes de iniciar a transmissão dos dados estabelece uma conexão com a

camada de transporte da máquina de destino, de forma a garantir que ela está apta para receber a mensagem. (FOROUZAN, 2010).

4.2.1 Estrutura do Segmento TCP

Para entender o funcionamento do protocolo TCP é importante saber como é a sua estrutura. O pacote TCP é divido em duas partes, o cabeçalho e o corpo. O cabeçalho é a parte onde são acrescentadas informações de controle importantes e o corpo contém os dados da mensagem recebida da camada de aplicação (SANZ, 2017).

Figura 9 - Estrutura do segmento TCP



Fonte: FOROUZAN, 2010

A figura acima representa o cabeçalho do pacote TCP. Os primeiros campos são destinados as identificações das portas de origem e de destino, que é por onde a camada de aplicação comunica-se com a camada de transporte. Cada porta recebe um número de identificação e as aplicações padrões são identificadas sempre pelo mesmo número. Por exemplo, um servidor de e-mail que utilize o protocolo SMTP para envio de e-mail criptografados sempre se conectará com um cliente através da porta 587, da mesma forma que uma aplicação web que utiliza o protocolo HTTPS sempre usará a porta 443 (IBRAHIM, 2011).

O próximo campo do cabeçalho é destinado ao número de sequência, que consiste em um número de 32 bits que indica a posição dos dados carregados pelo segmento TCP

transmitido, em relação ao fluxo de bits da origem dele. É usado para o reordenar os segmentos que chegarem fora de ordem. O campo número de confirmação também é um número de 32 bits e corresponde sempre ao número do próximo segmento esperado, e não o número do recebido. O campo comprimento do cabeçalho (HLEN, do inglês *header length*) é usado para indicar a posição do início dos dados do pacote e o campo Reservado é um espaço vazio destinado para uso futuro (FOROUZAN, 2010).

O próximo campo é destinado as flags do segmento TCP que possibilitam o controle de fluxo, estabelecimento e encerramento de conexão e a configuração do modo de transferência de dados. Existem seis flags principais, cujas funções estão descritas na tabela abaixo:

Quadro 3 - Funções das flags do cabeçalho TCP

Flags	Função
URG (*Urgent*)	Se ativo, o pacote é tratado com urgência.
ACK (*Acknowledgement*)	Se ativo, o valor do campo de confirmação é válido.
PSH (*Push*)	Se ativo, o pacote vai ser tratado pelo método Push, forçando seu envio imediatamente.
RST (*Reset*)	Se ativo, a conexão é reiniciada.
SYN (*Synchronize*)	Pedido de estabelecimento de conexão.
FIN (*Finite*)	Se ativo, a conexão é finalizada.

Fonte: Autoria própria

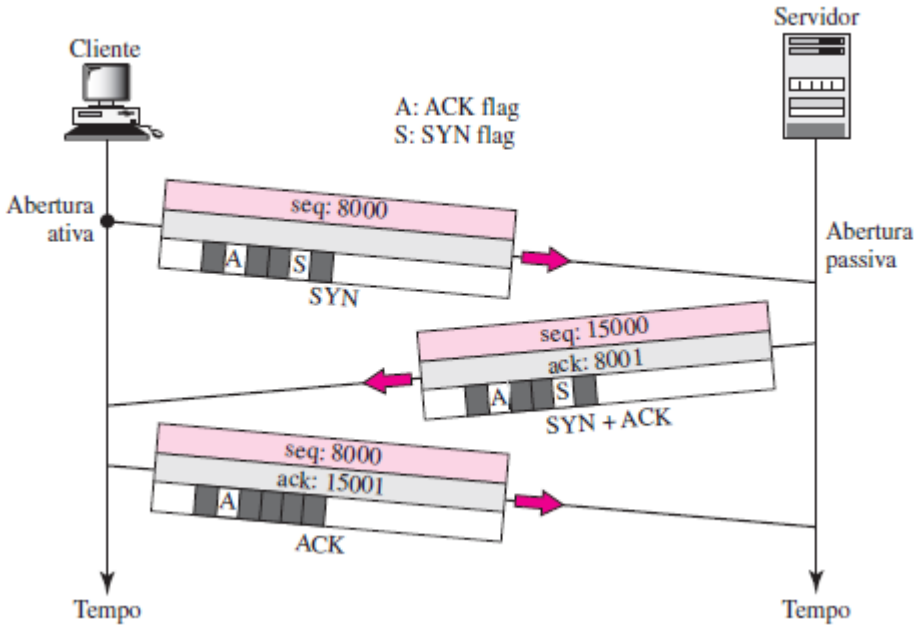
O campo que se segue é o campo Tamanho da janela que informa a quem está transmitindo o segmento TCP a quantidade máxima de octetos que o receptor do segmento pode aceitar no momento. Na prática serve para o receptor controlar o fluxo de dados enviado pelo transmissor. Os bits do campo Checksum são responsáveis pela verificação de erros no pacote. O campo Urgent Pointer só é válido se a flag URG estiver ativada e é usada quando o segmento contém dados urgentes. E, por último, o campo opções é um campo variável para incluir opções diversas (FOROUZAN, 2010).

4.2.2 Conexão TCP

Por ser um protocolo orientado a conexão, antes de iniciar a transferência de dados, o protocolo TCP estabelece conexão virtual entre as máquinas de origem e de destino (FOROUZAN, 2010).

Tipicamente em uma comunicação TCP existe uma extremidade denominada de servidor e outra denominada de cliente. A etapa inicial do estabelecimento da conexão virtual TCP entre esses dois é conhecida com *handshake* de três vias. Inicialmente, o cliente solicita ao servidor estabelecer uma conexão enviando um segmento TCP com a flag SYN ativa. Ao aceitar a solicitação, o servidor responde ao cliente enviando um segmento TCP com as flags SYN e ACK e aloca buffer para atender a futura conexão. Após receber a confirmação, o cliente retorna para o servidor outro segmento TCP, mas apenas com a flag ACK ativa, completando assim a terceira e última via do processo de estabelecimento de conexão. O processo é exemplificado na figura abaixo. (IBRAHIM, 2011).

Figura 10 - Handshake de três vias



Fonte: FOROUZAN, 2010

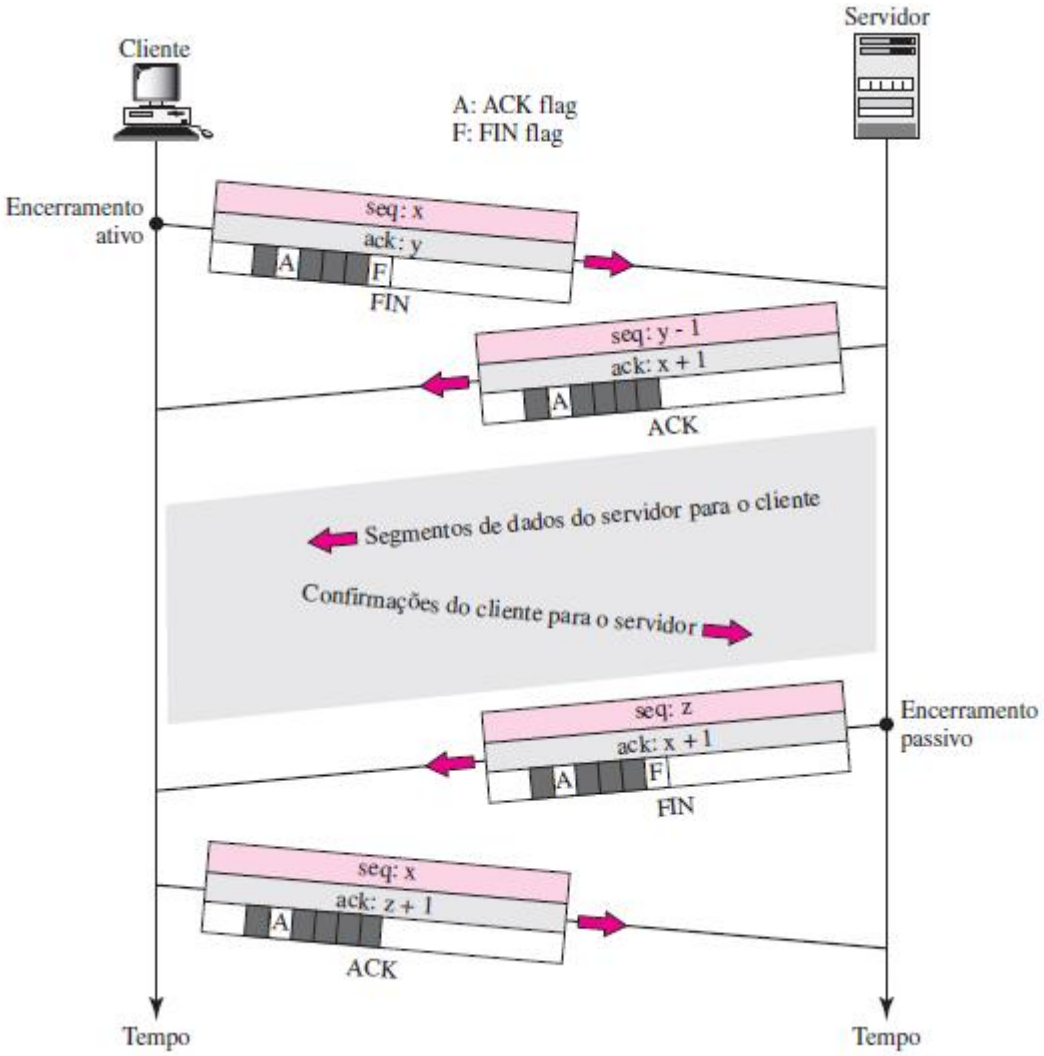
Terminada essa fase, o servidor adiciona o cliente a uma tabela própria onde estão discriminadas todas as conexões estabelecidas. Esta tabela possui um limite de conexões, e no

caso dela ser totalmente preenchida, nenhuma outra conexão com o servidor poderá ser estabelecida e todos os segmentos TCP SYN subsequentes serão rejeitados (IBRAHIM, 2011).

Com a conexão estabelecida, cliente e servidor estão prontos para iniciar a transferência de dados. Nessa fase podem ser transferidos tanto dados quanto confirmações, ou os dois ao mesmo tempo, no mesmo segmento, quando estiverem trafegando no mesmo sentido. Quando isso acontece, diz que se ocorreu um *piggybacking*. Durante esta fase, diversos mecanismos garantem ao TCP confiabilidade e robustez: números de sequência que garantem a entrega ordenada, código detector de erros (*checksum*) para detecção de falhas em segmentos específicos, confirmação de recepção e temporizadores que permitem o ajuste e contorno de eventuais atrasos e perdas de segmentos (IBRAHIM, 2011).

O processo de encerramento de conexão é semelhante ao processo de estabelecimento. Entretanto, ao invés de três fases, ele ocorre em quatro. A extremidade que resolve finalizar a sessão, envia para a outra um segmento com a flag FIN ativa e espera receber o segmento de resposta com a flag ACK ativa. O outro interlocutor, após enviar o segmento ACK, executa o mesmo procedimento, envia um segmento com a flag FIN e espera ser respondido com um segmento ACK (IBRAHIM, 2011).

Figura 11 - Encerramento de conexão TCP



Fonte: FOROUZAN, 2010

5 TÉCNICAS EMPREGADAS EM ATAQUES DE NEGAÇÃO DE SERVIÇO

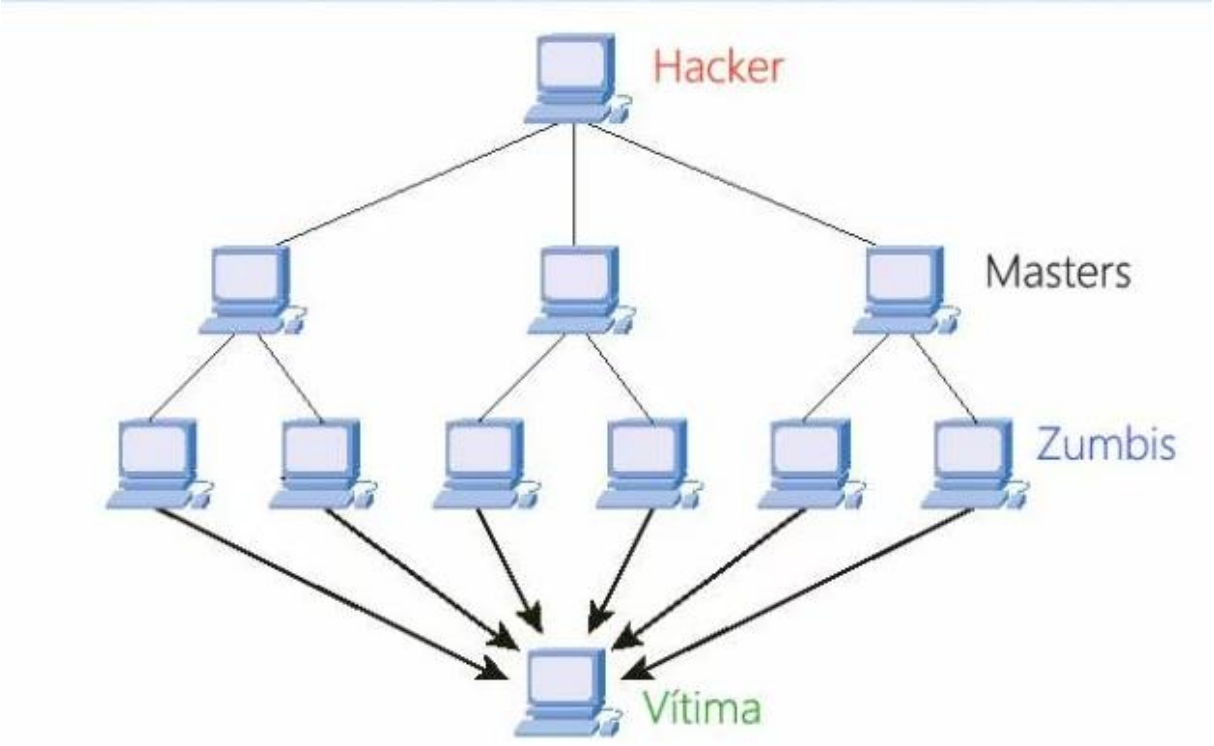
Este capítulo tem como objetivo principal apresentar as principais técnicas empregadas em um Ataque de DoS ou DDoS. Primeiramente será descrito como funciona um Ataque Distribuído de Negação de Serviço, depois serão apresentadas as categorias que classificam as técnicas de ataques e, então, serão abordadas as técnicas propriamente ditas.

5.1 Distributed Denial of Service (DDoS)

O Ataque Distribuído de Negação de Serviço (DDoS) é uma evolução do Ataque de Negação de Serviço, cuja principal diferença está na quantidade de computadores empregados pelo atacante para realizar o ataque. Por utilizar diversos computadores para atacar a vítima de forma coordenada, a execução do ataque de DDoS é muito mais complexa que o DoS e o seu efeito é muito mais devastador, uma vez que a capacidade do ataque é proporcional ao número de máquinas utilizadas. (PIEDRAHITA, 2014).

A arquitetura do ataque de DDoS pode ser vista na figura abaixo:

Figura 12 - Arquitetura do Ataque de DDoS



Fonte: GOOGLE IMAGENS

Para sua execução é necessária a realização de algumas etapas anteriores ao ataque propriamente dito. O primeiro passo é obter o controle das máquinas que serão utilizadas no ataque. Esse hosts são vítimas secundárias, que podem ser usadas como máquinas mestra ou *master*, que são as máquinas que vão controlar toda a rede de *botnets*, ou podem ser os hosts chamados de *zumbis* ou *bots*, que são as máquinas que efetuam o ataque. Segundo Piedrahita (2014), as formas mais comuns de conseguir o acesso a essas máquinas são as seguintes: por engenharia social, fazendo com a vítima acesse um site ou um link que execute um script malicioso e a infecte; explorando vulnerabilidades encontradas nos hosts das vítimas e abrindo um *backdoor* que possibilite o envio de comandos remotos para esses hosts; ou através de um código malicioso (*malware*) que infecte a máquina da vítima com ferramentas de ataque de DDoS.

A tabela abaixo sintetiza as etapas utilizadas para o recrutamento do exército de *zumbis*, de acordo com Piedrahita (2014):

Quadro 4 - Etapas do recrutamento de bots

Etapas	Como ocorre
1ª) Varredura	Utilizando ferramentas de varredura, como o *netcat*, realiza-se uma varredura de máquinas em diferentes redes para encontrar portas abertas ou serviços que tenham alguma vulnerabilidade para contaminarem as máquinas. Ou seja, identifica máquinas com vulnerabilidades.
2ª) Exploração de Vulnerabilidades	Utilizando ferramentas de exploração de vulnerabilidades, como o *metasploit*, as máquinas selecionadas na varredura são exploradas através do envio de comandos ou requisições que gerem uma condição inesperada e que permita a execução do código malicioso na vítima.
3ª) Propagação	Consiste em instalar o código malicioso para realizar o ataque, abrir algum canal de comunicação para coordenar o ataque e possivelmente o código da ferramenta de varredura para continuar infectando outras vítimas.

Fonte: Autoria própria

Após o recrutamento, o segundo passo consiste no ataque ao alvo, chamado de vítima primária. Nesta etapa, o atacante utiliza as máquinas mestras para ordenar ao exército de *bots* que execute o ataque. As vítimas secundárias estão distribuídas pela Internet, portanto, o ataque provém de endereços IP de diferentes regiões, o que torna o ataque de DDoS quase impossível de ter sua origem identificada (PIEDRAHITA, 2014).

5.2 Categorias de Ataques de DoS/DDoS

Existem várias técnicas ou métodos de se executar um ataque de DoS/DDoS. As Diversas literaturas consultadas para este trabalho dividem estas técnicas dentro de categorias, cuja nomenclatura e critério de classificação variam de autor para autor.

O CERT.br divide os tipos de ataque em ataques à camada de aplicação, ataques de exaustão de recursos de hardware e ataques volumétricos.

Bardal (2014), em sua dissertação, classifica os ataques de DoS/DDoS em quatro categorias, que são: consumo de largura de banda, consumo de recursos, falhas de programação e ataques de roteamento ou DNS.

Já Vordos (2009), utiliza em geral quatro categorias principais, que são: ataques de inundação, ataques de amplificação, ataques de exploração de protocolo e ataques de pacotes malformados.

Porém, este trabalho classificará as técnicas de ataques de DoS de acordo com a classificação apresentada por Piedrahita (2014) em sua dissertação de Mestrado. Nela Piedrahita classifica as técnicas de ataques em dois grandes grupos, que são: os ataques por inundação e os ataques por vulnerabilidade.

5.2.1 Ataques por Inundação

Os ataques de inundação têm como objetivo consumir os recursos da vítima para impedir que atenda requisições de usuários legítimos. Nestes ataques é necessário gerar grandes cargas no servidor ou no enlace. Para isso o atacante usa a *botnet* para aumentar sua capacidade de enviar grandes quantidades de tráfego para o sistema da vítima, a fim de consumir a largura de banda disponível com tráfego IP ou provocar operações no servidor que consumam processamento ou memória. O sistema sob ataque diminui a velocidade ou trava, dificultando seu acesso por usuários legítimos. Ataques de inundação podem ser executados explorando os protocolos UDP, TCP ou ICMP (PIEDRAHITA, 2014).

A inundação pode ser direta, quando o atacante direciona as altas taxas de tráfego IP diretamente para a máquina da vítima, ou pode ser por amplificação e reflexão. Nos ataques de amplificação e reflexão, o atacante falsifica o endereço IP do alvo e envia ou ordena que as máquinas *bots* enviem mensagens para um endereço IP broadcast, com o intuito de fazer com que todos os hosts alcançados pelo endereço de broadcast enviem uma resposta ao sistema da

vítima. O endereço IP de broadcast é usado para amplificar e refletir o tráfego de ataque e, assim, reduzir a largura de banda do sistema da vítima. As vantagens de este tipo de ataque são: um atacante pode aproveitar outra infraestrutura para amplificar sua capacidade gerar tráfego; é mais difícil rastrear este tipo de ataques; e, em muitos casos este tipo de ataques geram efeitos colaterais nas entidades que são usadas como refletores (PIEDRAHITA, 2014).

5.2.2 Ataques por Vulnerabilidade

Os ataques por vulnerabilidade têm como objetivo indisponibilizar o servidor ou a rede da vítima através da exploração de características específicas de um protocolo ou de uma aplicação. Geralmente, as vulnerabilidades exploradas desencadeiam nas máquinas das vítimas um estado de bloqueio ou um estado de looping. Sua execução é mais simples que os ataques de inundação, pois não necessitam de muitas máquinas e nem de muito tráfego para atingirem seus objetivos, requerendo, na maioria das vezes, de apenas um pacote para conseguir a negação de serviço. Esses ataques são de difícil detecção, pois muitas vezes eles são confundidos com falhas de programação da aplicação (PIEDRAHITA, 2014).

5.3 Técnicas de Ataques de DoS/DDoS

5.3.1 TCP SYN Flood

Esta é uma técnica de inundação que explora o processo de estabelecimento de conexão do protocolo TCP, chamado de handshake de três vias e visto na seção 4.2.2. deste trabalho.

No início do ataque, o atacante envia para o servidor uma solicitação de estabelecimento de conexão utilizando um IP de origem falso, através de uma técnica chamada de IP *spoofing*. Seguindo o processo padrão, o servidor encaminha para o IP de origem o segmento TCP SYN+ACK, altera seu estado de conexão e aloca recursos para a conexão que está sendo estabelecida. Existe um limite de recursos que o servidor pode alocar para as conexões. É justamente esse limite que é explorado nesta técnica. Após o envio do pacote SYN+ACK, o servidor aguarda receber a resposta ACK do cliente, conforme já foi visto. Porém, por ser um IP forjado, esta resposta não chega e o servidor mantém os recursos alocados durante um intervalo de espera, mesmo sem estabelecer a conexão. Esse tempo varia de sistema para sistema, podendo ser segundos ou minutos. O atacante, então, faz várias requisições SYN em

um intervalo de tempo menor que o intervalo de espera, de forma a esgotar rapidamente os recursos do servidor, impedindo o mesmo de estabelecer novas conexões (BARDAL, 2014).

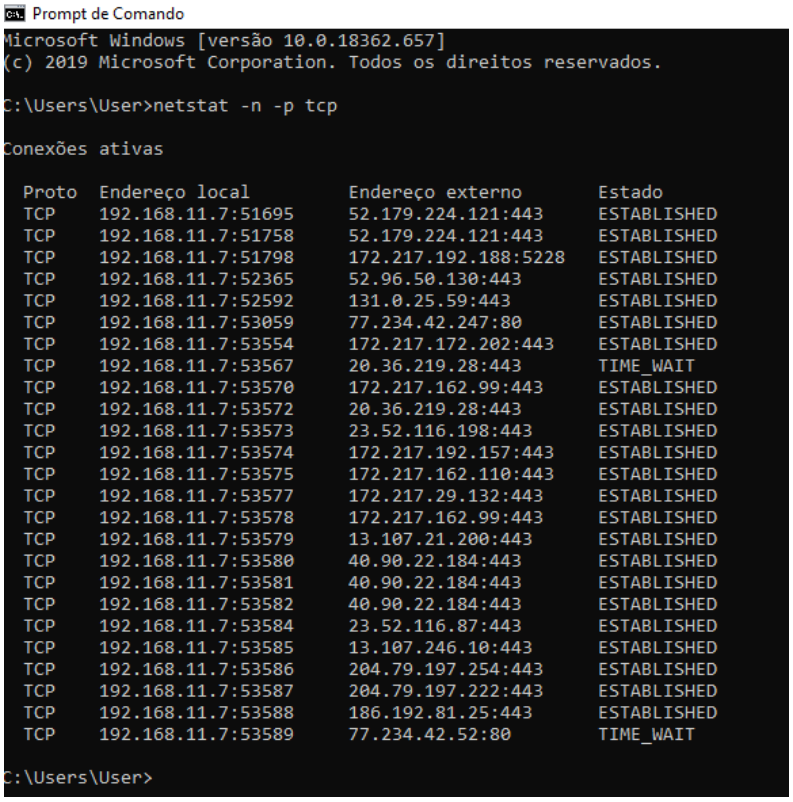
É importante ressaltar que além do IP de origem ser falso, ele precisa ser inalcançável ao servidor. Pois, se o IP forjado existir e receber o segmento TCP SYN+ACK, ele responderá ao servidor com uma mensagem RST, indicando que ele não foi o origem da solicitação. Após isto, então, o servidor cancelará o processo de handshake e disponibilizará novamente os recursos alocados. Outro aspecto importante da associação da técnica de IP spoofing com a SYN flood é o fato de tornar a origem desse ataque de difícil identificação. (BARDAL, 2014).

Apesar de ser difícil se defender de um ataque de SYN flood, algumas ações como aumentar o tempo de espera para o estabelecimento da conexão e aumentar o número de conexões possíveis são ações que podem ser tomadas pelo administrador do servidor para mitigar ou evitar possíveis ataques. Porém, essa medidas tem um custo operacional, tendo em vista que elas podem diminuir o desempenho do sistema (BARDAL, 2014).

Existe um comando, que pode ser utilizado em diversos sistemas operacionais, que mostra o estado das conexões ativas do endereço local e pode ser utilizado para determinar se um ataque de inundação SYN está ocorrendo. Trata-se do comando “netstat”.

A figura abaixo mostra o print do *promp* de comando de uma máquina que não está sendo atacada:

Figura 13 - Conexões ativas de uma máquina sem ataque

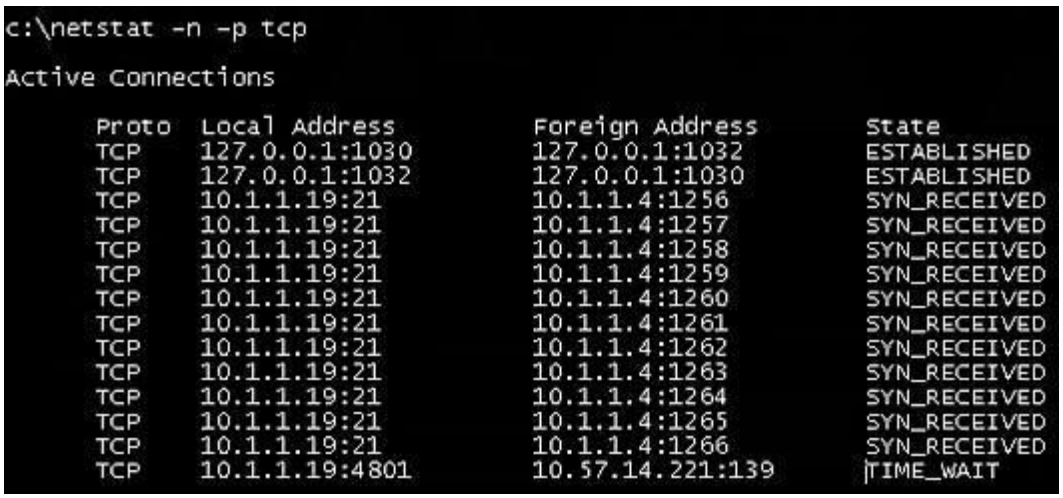


Fonte: Autoria própria

Após a execução do comando “netstat -n -p tcp”, lista-se o estado de todas as conexões ativas do endereço local. A máquina da figura acima apresenta dois estados de conexão, o “ESTABLISHED”, que indica que há uma conexão estabelecida entre os dois endereços IP apresentados, e o estado “TIME_WAIT”, que indica que a conexão está em fase de encerramento e o host local está esperando um intervalo de tempo para encerrar a sessão.

Caso houvesse várias conexões com o estado “SYN_RECEIVED” (figura 14), a probabilidade de haver um ataque de inundação SYN em execução seria grande.

Figura 14 - Conexões ativas de uma máquina sendo atacada



Fonte: BARDAL, 2014

5.3.2 UDP Flood

Em um ataque por inundação UDP, o atacante envia muitos pacotes UDP através das máquinas *zumbis* para portas aleatórias ou específicas do sistema da vítima. Então, sistema atacado tenta processar os dados recebidos para determinar quais aplicações solicitaram os dados. Se o sistema da vítima não estiver executando nenhum aplicativo na porta de destino, ele enviará um pacote ICMP ao sistema de envio, indicando uma mensagem de "porta inalcançável". Assim, para um grande número de pacotes UDP, o sistema alvo será forçado a gerar e enviar muitos pacotes ICMP, ocorrendo sobrecarga e, consequentemente, levando-o a ficar inacessível a outros clientes (VORDOS, 2009).

A grande quantidade de pacotes UDP direcionados a um único servidor, por si só também pode provocar a indisponibilidade do sistema alvo. Um tráfego muito grande chegando à vítima termina por ocupar toda a largura de banda disponível e impede o acesso a usuários legítimos. A largura de banda das redes vizinhas ao sistema atacado também pode ser afetada e estes terem seus serviços prejudicados (PIEDRAHITA, 2014).

Geralmente, em um ataque de DDoS por inundação UDP o atacante também falsifica o endereço IP de origem. Isso ajuda a esconder a identidade das máquinas *zumbis*, já que os pacotes de retorno do sistema da vítima não são enviados de volta a eles, mas sim aos endereços falsificados (VORDOS, 2009).

Muitas vezes o sistema atacado demora a identificar que um ataque de DDoS está em curso, pois, tirando seu grande volume, o tráfego de UDP não apresenta nenhuma característica que o diferencie do tráfego legítimo (PIEDRAHITA, 2014).

5.3.3 ICMP Flood

A cinemática dos ataques de inundação ICMP é semelhante ao que acontece na inundação UDP. O atacante, através das máquinas *zumbis*, envia um grande número de pacotes ICMP *echo request* (ping) direcionados ao sistema da vítima, com o intuito de obter a resposta desses pacotes. A combinação de tráfego de entrada e saída satura a largura de banda da conexão de rede da vítima. Assim como na inundação UDP, nesta técnica de ataque de DDoS o atacante também falsifica o endereço IP de origem (VORDOS, 2009).

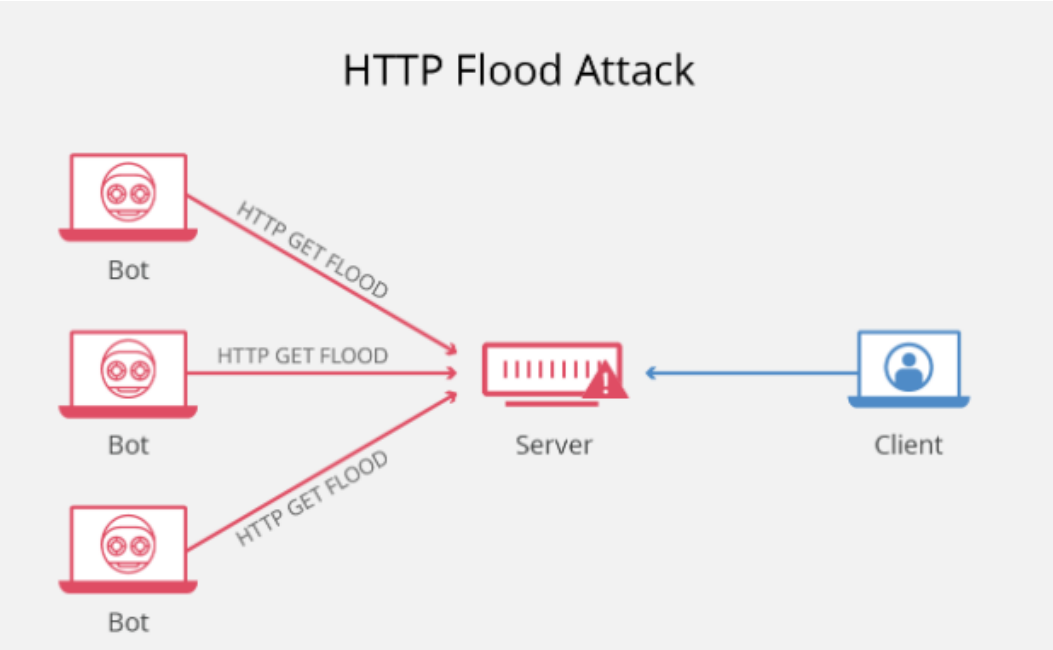
5.3.4 HTTP Flood

Esta é mais uma técnica de ataque por inundação, desta vez dirigida a camada de aplicação.

O HTTP (*Hypertext Transfer Protocol*) é um protocolo da camada de aplicação, que é comumente utilizado para carregar páginas web (método GET) ou para enviar conteúdo de formulários pela internet (método POST). Com a técnica de inundação HTTP, o atacante pretende gerar uma carga de processamento muito grande no servidor web, impedindo o servidor de atender as requisições de usuários legítimos (PIEDRAHITA, 2014).

Em uma inundação HTTP simples, o atacante utiliza a botnet para gerar uma grande quantidade de requisições GET ou POST a um servidor web que, para responder a todas as solicitações, aloca o máximo de recursos possível para cada solicitação, sobrecarregando assim o servidor. Por característica intrínseca, as requisições POST exigem um processamento mais complexo do servidor web, o que torna os ataques de inundação HTTP POST mais comuns. (PIEDRAHITA, 2014).

Figura 15 - Ataque de Inundação HTTP



Fonte: WebSite CLOUDFLARE, 2020

5.3.5 Ataques Smurf

O smurf é uma técnica simples de ataque de Negação de Serviço, que envolve três elementos: o atacante ou seu exército de *botnet*, uma rede amplificadora e a vítima. Ela combina a técnica de IP spoofing com o comando “ping” direcionado ao endereço de difusão da rede. Esta rede funcionará como fator amplificador visando consumir toda a largura de banda da vítima. Quantos mais hosts estiveram conectados a essa rede, mais rápida a largura de banda da vítima será consumida (BARDAL, 2014).

Para entender esta técnica, é importante saber como funciona o comando “ping”. Este comando está presente em quase todos os sistemas operacionais e tem como função testar a conectividade entre equipamentos. Ao executá-lo, o equipamento de origem envia um pacote ICMP Echo Request para o endereço de destino que deve responder o comando com um pacote ICMP Echo Reply para confirmar que há conectividade entre eles.

O ataque funciona da seguinte forma: o atacante envia um comando “ping” direcionado ao endereço de broadcast (difusão) da rede amplificadora. Como o ataque é destinado ao endereço de difusão da rede, todos os host da mesma respondem ao comando “ping” com o pacote ICMP Echo Reply. Porém, o atacante faz o spoofing do IP de origem e camufla o seu IP

com o IP da vítima, fazendo com que todos os pacotes ICMP Echo Reply se direcionem para a máquina alvo, consumindo assim a largura de banda disponível. (BARDAL, 2014).

Assim como no ataque TCP SYN flood, a origem do smurf também é de difícil identificação devido ao uso da técnica de IP spoofing. Para se prevenir deste ataque, os administradores das redes devem desabilitar no roteador de borda a funcionalidade direct broadcast, através do comando: "*no ip directed-broadcast*". (BARDAL, 2014).

5.3.6 Ataque de Fragmentação IP

O ataque de fragmentação é uma técnica que explora uma característica do protocolo IP, que é a fragmentação, e visa gerar um bloqueio no sistema vítima.

A estrutura do datagrama IP consiste em um cabeçalho e uma carga útil. O cabeçalho contém informações de controle, inclusive os endereços IP de origem e destino, enquanto a carga útil contém os dados que estão sendo transmitidos. A fragmentação IP é o processo de dividir o datagrama em pequenos pedaços, para depois enviá-los a camada física. É a fragmentação que torna possível a passagem do datagrama pelas diversas redes físicas, visto que cada rede física suporta um tamanho máximo de datagrama, chamado de MTU (*Maximum Transmission Unit*). Um datagrama já fragmentado pode ser fragmentado outra vez, caso ele trafegue por uma rede de MTU menor. Todos esses pacotes são remontados ao chegar no host de destino, para que o datagrama original seja reconstituído (FOROUZAN, 2010).

A técnica mais comum de ataque de fragmentação envolve o envio de datagramas que serão impossíveis de remontar na entrega. O objetivo é abusar dos recursos dos servidores e impedi-los de executar as operações que deveriam. Nessa técnica, dois campos do cabeçalho IP são alterados, o *Header Length,* que indica o tamanho do cabeçalho, e o offset de fragmentação, que mostra a posição do fragmento em relação ao datagrama inteiro (original). Na prática, os bits do *offset* mostram a posição inicial dos dados e os bits do *Header Length* são utilizados para calcular o final do pacote. No pacote seguinte, o campo *offset* será igual a soma do *offset* e tamanho do pacote anterior (BARDAL, 2014).

No destino, o host receptor alocará recursos de processamento e memória para reordenar os fragmentos IP que chegarem. Porém, como o atacante enviou os pacotes com os campos *Header Length* e *offset* com valores inconsistentes, a máquina de destino tentará reordená-los, não irá conseguir e fará o processo novamente, acabando por ficar instável por ficar sem recursos para processar outras requisições (BARDAL, 2014).

5.3.7 Ping of Death

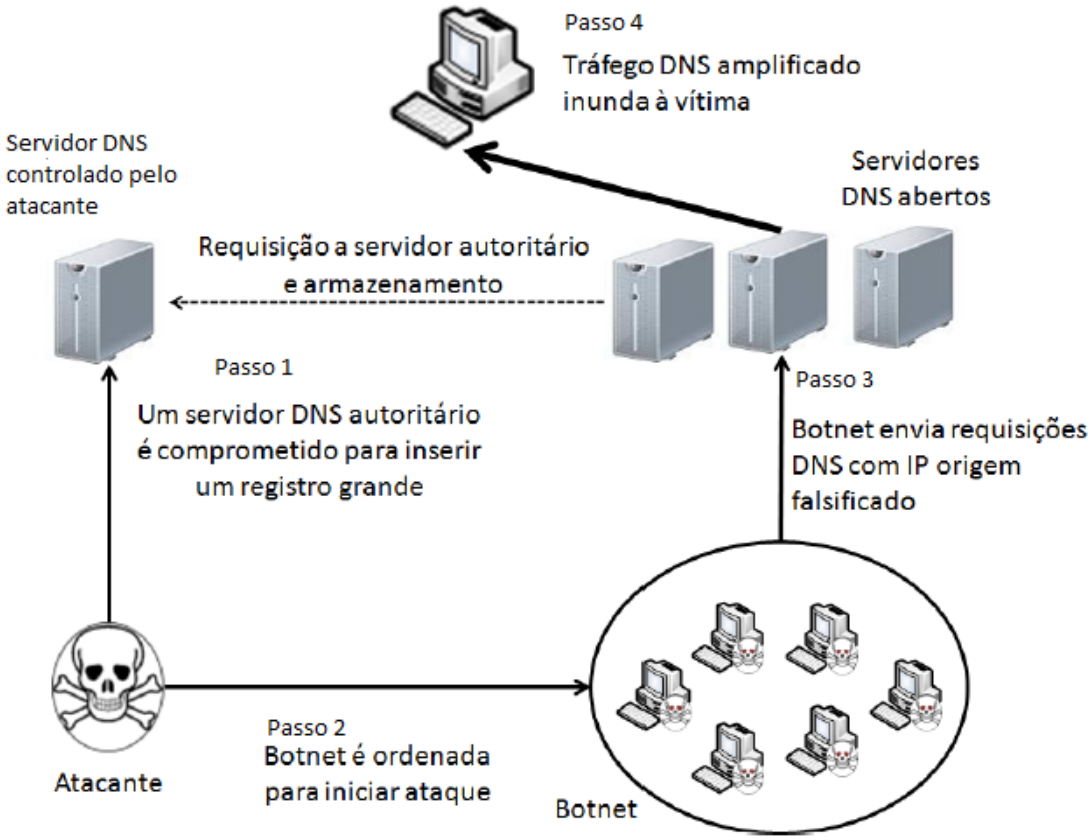
Esta é mais uma técnica de ataque por vulnerabilidade. O *Ping of Death* é uma técnica de execução de DoS simples e que não exige muitos conhecimentos computacionais do atacante, além de saber a linha de comando "*ping -i 1 -l 65500 ip_do_destino –t*" (comando "ping" com alguns parâmetros adicionais) e o endereço IP da vítima. Ela foi muito utilizada durante os anos 1990, justamente no período onde se tem as primeiras notícias de ataques de Negação de serviço, e é uma técnica que hoje não é mais efetiva, pois as vulnerabilidades exploradas por ela foram corrigidas (BARDAL, 2014)

O ataque consiste em enviar um comando "ping" para o endereço IP da vítima com o tamanho de pacote IP maior que o suportado, que é 64k bytes ou 65635 bytes. Durante o envio, esse datagrama será fragmentado em pacotes menores, sendo remontado no destino. Porém, ao ver que o datagrama possuía um tamanho maior que o suportado, o Sistema Operacional que recebia o datagrama não sabia como tratar esse pacote e acabava travando ou reiniciando, causando uma instabilidade nos seus serviços (SEARCHSECURITY, 2006).

5.3.8 Ataque de Reflexão/Amplificação DNS

Esse tipo de ataque utiliza os servidores DNS como entidades refletoras e amplificadoras. Primeiramente, o atacante publica um registro muito grande em um servidor DNS sob o seu controle (possivelmente comprometido). Posteriormente, ele ordena que o seu exército de botnet façam centenas ou milhares de consultas aos servidores DNS recursivos abertos sobre os registros publicados no servidor DNS comprometido. Porém, nestas consultas é utilizado o IP forjado (IP spoofing) da vítima, de forma que as respostas são direcionadas para ela, e não para as máquinas que realmente fizeram as requisições. A amplificação é obtida porque as respostas DNS têm um tamanho maior às requisições e costumam gerar um tráfego de 28 a 54 vezes maior que o tráfego da consulta. Adicionalmente, o tráfego dos servidores DNS normalmente não é bloqueado como malicioso, pois se um firewall bloqueia a porta 53 do serviço DNS, o servidor não poderá resolver nomes (CERT.br, 2016).

Figura 16 - Visão geral do Ataque de Reflexão/Amplificação DNS



Fonte: PIEDRAHITA, 2014

5.3.9 Ataque Memcached

Memcached é sistema distribuído de cache em memória, utilizado para acelerar aplicações web e redes, reduzindo o número de chamadas a banco de dados pelos servidores (MEMCACHED.ORG, 2018)

O ataque de Memcached é um ataque de inundação com amplificação, que opera de forma semelhante ao ataque de DDoS de amplificação DNS, visto na seção 5.3.8. Nesta técnica o atacante envia solicitações com o IP forjado da vítima (IP spoofing) para um servidor vulnerável e que utiliza memcached. Este servidor responde com uma quantidade maior de dados que a solicitação inicial, aumentando o volume de tráfego e causando a negação de serviço. Este método de ataque de amplificação é possível porque os servidores memcached têm a opção de operar usando o protocolo UDP. O UDP é um protocolo de transporte que permite o envio de dados sem estabelecer primeiro uma conexão. Desta forma, o host de destino

não é consultado se deseja ou não receber os dados, permitindo que uma grande quantidade de dados seja enviada ao destino sem o seu consentimento prévio (CLOUDFLARE, 2020).

Basicamente, o ataque do memcached ocorre em 4 etapas: primeiro o atacante implanta uma grande quantidade de dados em um servidor memcached vulnerável. Em seguida, o atacante faz o spoofing do IP do servidor da vítima e faz uma solicitação HTTP GET dos dados implantados para o servidor Memcached. Este recebe a solicitação e envia a resposta para o IP da vítima, sem estabelecer a conexão previamente, pois ele utiliza o UDP. A vítima não consegue processar a grande quantidade de dados enviados do servidor Memcached e acaba sobrecarregando e não conseguindo atender as solicitações legítimas (CLOUDFLARE, 2020).

O fator de ampliação desse tipo de ataque é significativo. Há casos onde o tráfego para a vítima foi amplificado 52 mil vezes em relação ao tráfego inicial. Isso significa que, para uma solicitação de 15 bytes, uma resposta de 750 kB pode ser enviada, o que representa um enorme fator de amplificação e risco de segurança para propriedades da Web que não conseguem suportar o peso desse volume de tráfego. Ter um fator de amplificação tão grande associado a servidores vulneráveis torna o memcached uma excelente técnica de DDoS (CLOUDFLARE, 2020).

6 ANÁLISE PRÁTICA

Neste capítulo será apresentada uma análise sobre uma simulação de Ataque de Negação de Serviço realizada em um ambiente baseado em máquinas virtuais, através do software Oracle VM VirtualBox. Nas duas máquinas virtuais foram utilizados Sistemas Operacionais (SO) Linux.

Para desempenhar o papel do atacante foram utilizadas as ferramentas presentes no SO Kali Linux versão 2020.1, que é baseado no sistema Debian. E, para representar o papel da vítima, foi escolhido uma máquina virtual com o Sistema Operacional Ubuntu, que é o SO utilizado pela Marinha do Brasil atualmente, além de ser um software livre e que não requer licença para utilização. As duas máquinas foram configuradas na mesma rede local como o IP 192.168.56.1/24.

Na máquina da vítima também foi utilizado o software Wireshark, que é um programa utilizado para analisar os protocolos e capturar o tráfego de rede.

Os Sistemas Operacionais e softwares utilizados na simulação podem ser encontrados e baixados nos seguintes endereços:

- Oracle VM VirtualBox, disponível em https://www.virtualbox.org/wiki/Downloads
- SO Kali Linux, disponível em https://www.kali.org/downloads/
- SO Ubuntu, disponível em https://ubuntu.com/download/desktop
- Software Wireshark, disponível em https://www.wireshark.org/download.html

6.1 Simulação do Ataque SYN flood

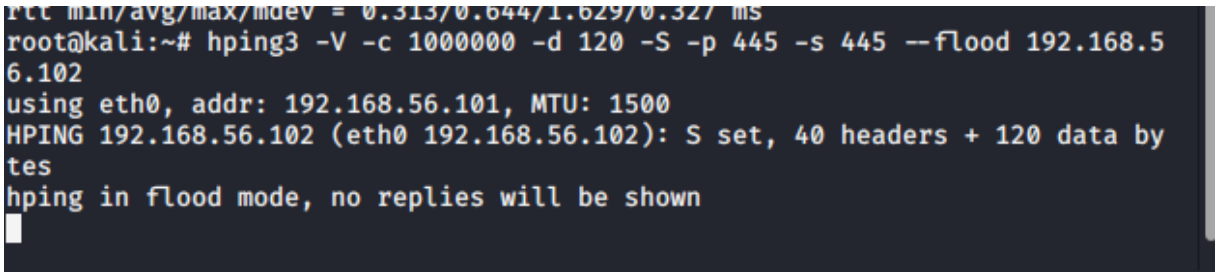
Para a simulação foi escolhida a técnica de ataque por inundação SYN e foi utilizado o comando “hping3”, disponível no Kali Linux. Hping3 é a terceira versão da ferramenta hping, que é uma ferramenta orientada a linha de comando que permite ao usuário montar e analisar pacotes TCP/IP, além de manipular todos os campos, atributos e tipos de protocolo existentes na conjunto de protocolos baseados em TCP/IP. É muito utilizada para gerar tráfego anormal de rede.

Com a intenção de gerar uma inundação de requisições TCP SYN à máquina da vítima, foi utilizado o comando “hping3 -V -c 1000000 -d 120 -S -p 445 -s 445 --flood 192.168.56.102” (figura 17), onde os significados de cada parâmetro são descritos a seguir:

- -V: ativa o modo verbose, que mostra informações mais detalhadas do comando;
- -c 1000000: indica que serão enviados um milhão de segmentos TCP;
- -d 120: indica que o tamanho de cada segmento é de 120 bytes;

- -S: indica que serão enviados segmentos TCP SYN;
- -p 445: indica que a porta de destino é a 445;
- -s 445: indica que a porta de origem é a 445; e
- --flood: envia o máximo de pacotes por segundo possível;

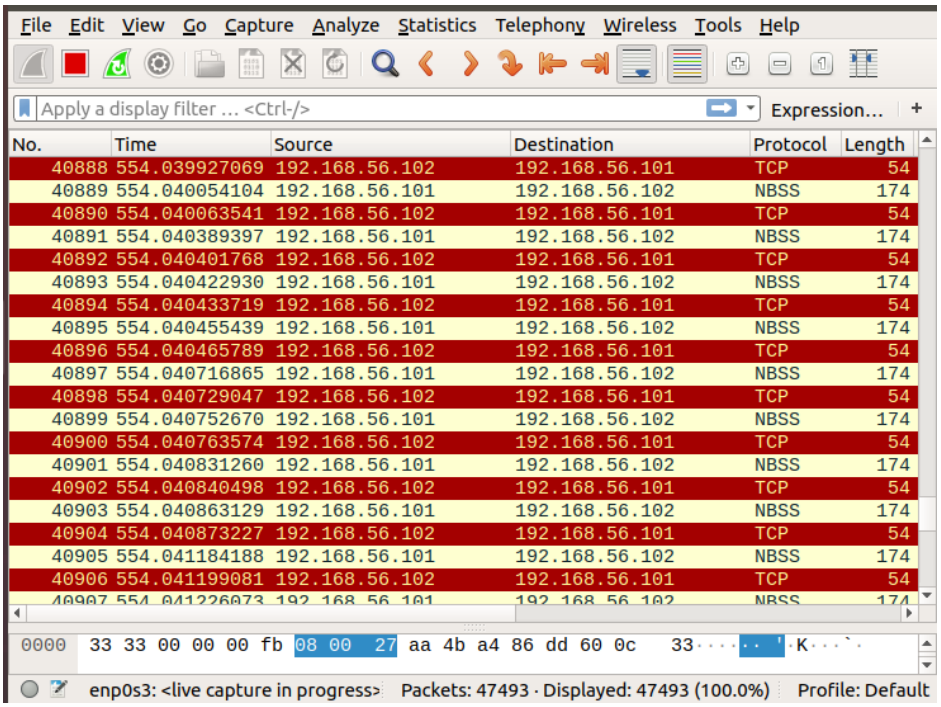
Figura 17 - Comando hping3 utilizado para fazer o ataque de inundação SYN simulado



Fonte: Autoria própria

Utilizando o software Wireshark na máquina vítima (Figura 18), é possível observar o tráfego de pacotes TCP SYN e NBSS enviados ao alvo. A cada pacote TCP SYN recebido a máquina virtual vítima entende que será estabelecida uma conexão e aloca buffer para as futuras requisições.

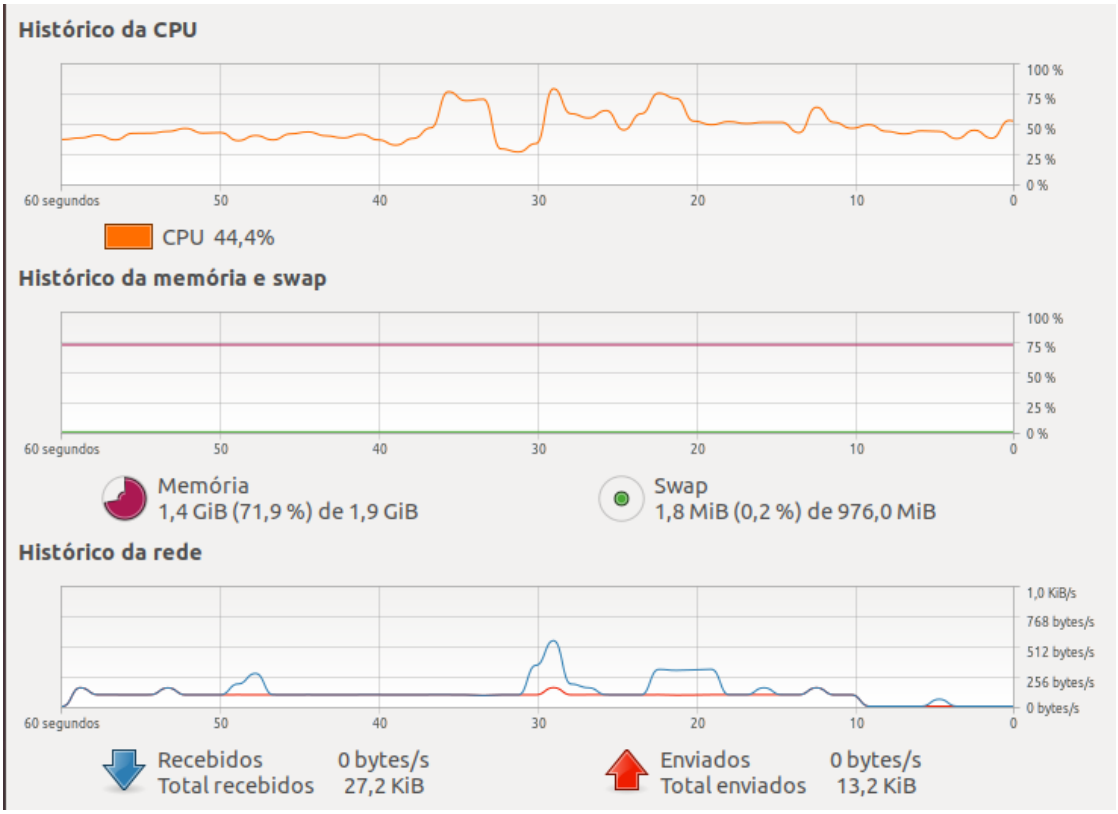
Figura 18 - Wireshark capturando o tráfego de pacotes TCP na máquina da vítima



Fonte: Autoria própria

Na figura a seguir (figura 19) é apresentada a situação operacional dos recursos computacionais da vítima antes do ataque ser efetuado. Percebe-se que em uma situação de operação normal o percentual de memória RAM utilizada estava próximo a 70%, a memória virtual (*swap*) praticamente não era utilizada (0,2%) e o tráfego de rede era baixo.

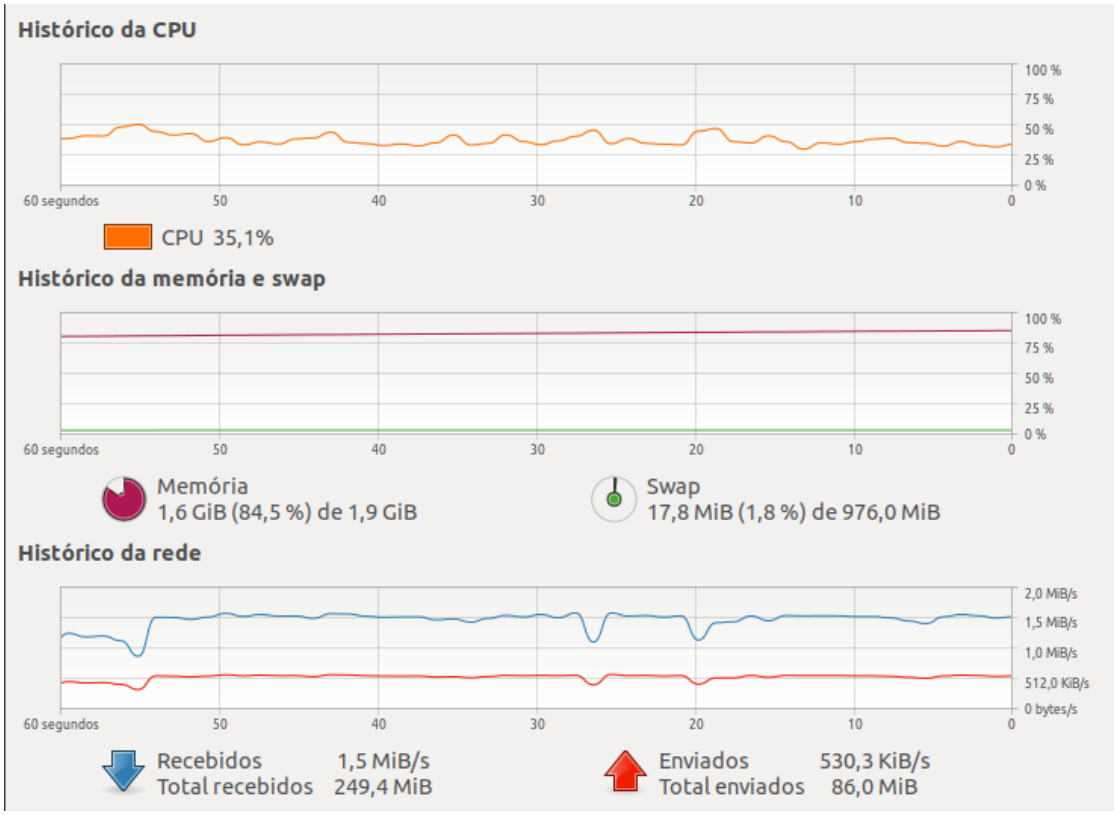
Figura 19 - Monitor do sistema vítima antes do ataque



Fonte: Autoria própria

Logo após o início do ataque, o monitor do sistema (figura 20) registrou um aumento gradual da memória alocada, passando de 70% para 85%, e um aumento significativo no tráfego de rede, onde percebe-se que o tráfego recebido (na ordem de megabytes) é muito maior que o enviado (na ordem de kilobytes), constatando que a máquina vítima não consegue responder na mesma velocidade a todas as solicitações recebidas, devido a inundação de pacotes TCP SYN.

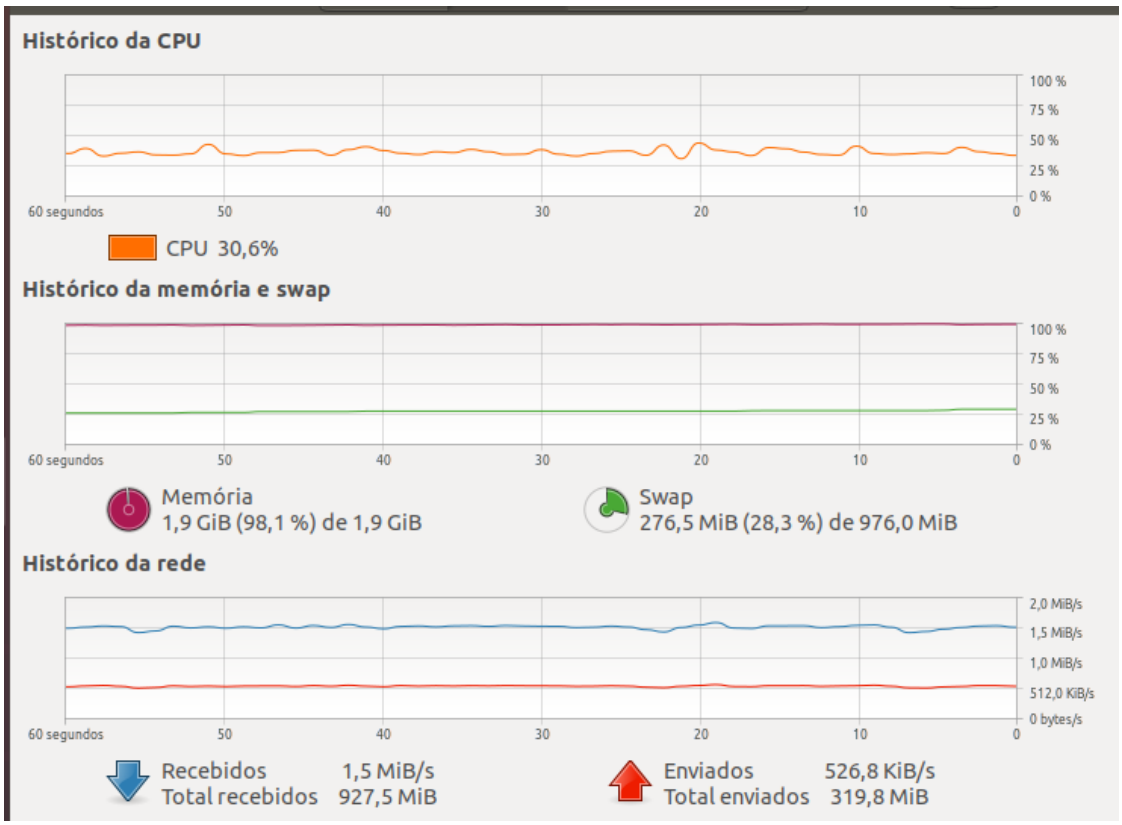
Figura 20 - Monitor do sistema logo após o início do ataque



Fonte: Autoria própria

Outro aspecto importante que pode ser percebido, é que após utilizar praticamente toda a memória RAM (98,1%) a máquina atacada começou a alocar a memória virtual, conforme pode ser visto na próxima figura 21.

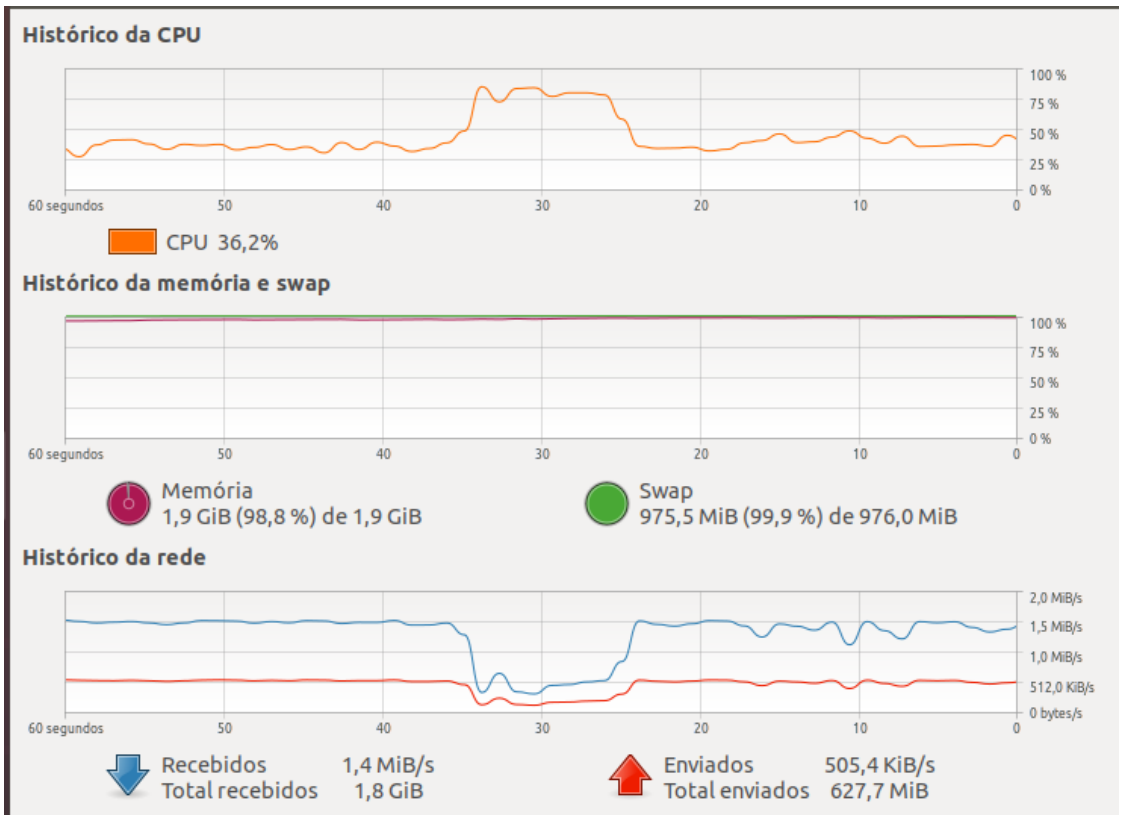
Figura 21 - Monitor do sistema: memória virtual começa a ser alocada



Fonte: Autoria própria

Durante o ataque foi notado uma queda acentuada no rendimento do sistema atacado. As respostas as solicitações feitas a máquina eram lentas, o que dificultou a utilização de outras aplicações pelo usuário. Quando toda memória RAM e toda memória virtual foram alocadas (figura 20) a máquina virtual atacada travou completamente, ficando indisponível. Nesse momento foi encerrado o ataque e a máquina alvo permaneceu congelada, necessitando ser reiniciada para ter seu funcionamento restabelecido.

Figura 22 - Parâmetros no monitor do sistema no momento em a máquina fica indisponível



Fonte: Autoria própria

7 CONCLUSÃO

Considerando o conceito e os casos de Guerra Cibernética apresentados é possível compreender que as Nações estão diante de uma nova forma de se fazer guerra, onde as fronteiras não são estabelecidas e o inimigo muitas vezes é desconhecido. A nova tendência mundial é que cada vez mais ações ofensivas tradicionais com movimentação de Esquadras e desembarque de tropas sejam acompanhadas de ações cibernéticas, capazes de desestabilizar o inimigo e extrair informações estratégicas. Este fato é corroborado pela crescente dependência das sociedades em relação as infraestruturas de Tecnologia da Informação, o que torna as armas cibernéticas bastante efetivas.

Dentre os ataques cibernéticos empregados em conflitos, o ataque de negação de serviço destacou-se como exemplo de ferramenta com potencial de causar grandes danos ao oponente. Nesses casos os danos não são físicos, pois o ataque em si não tem a capacidade de destruir fisicamente nenhuma instalação militar ou um veículo blindado. As suas principais consequências são estratégicas, pois tem capacidade de paralisar o fornecimento de serviços essenciais de qualquer país, além de interromper o fluxo e o acesso a informações fundamentais no processo decisório do conflito.

A análise feita no capítulo 6 demonstrou que é muito fácil obter ferramentas para executar um ataque de negação de serviço. A partir da simulação executada no ambiente controlado com máquinas virtuais, observou-se algumas das consequências desse tipo de ataque cibernético. Utilizando um comando simples foi possível tornar a máquina atacada indisponível em poucos minutos, através da saturação dos seus principais recursos computacionais.

Analisando em conjunto os casos de Guerra Cibernética apresentados neste trabalho e extrapolando o ambiente controlado onde a simulação foi realizada, conclui-se que um ataque de DoS é um ataque cibernético bastante efetivo e de fácil execução quando comparado a outros tipos de ataques. Além disso, pode ter seus efeitos potencializados quando executado a partir de uma estrutura hierarquizada e já estabelecida, como no caso das Forças Armadas.

7.1 Considerações Finais

A Marinha do Brasil acompanha a evolução do cenário global e sabe da importância em investir em Tecnologia da Informação para manter seu poder de combate frente as novas ameaças. Como prova disso, nos últimos anos tomou algumas medidas com o objetivo de

adequar sua estrutura a essa tendência tecnológica. Para coordenar esses desenvolvimentos, criou a Diretoria-Geral de Desenvolvimento Nuclear e Tecnológico da Marinha (DGDNTM), que tem como um de seus propósitos aplicar o Poder Naval em atividades relacionadas à ciência, tecnologia e inovação. Além disso, investe na modernização de seus meios navais, através do programa dos Navios "Classe Tamandaré", cujo projeto prevê sistemas de alta complexidade tecnológica. Do mesmo modo, tem aumentado a qualificação técnica de seu pessoal, para que estes consigam extrair o melhor na operação e manutenção dos seus futuros equipamentos.

Nessa conjuntura, cabe destacar que um fator importante quando se trabalha com sistemas altamente informatizados é o desenvolvimento da mentalidade de segurança cibernética e esta é uma das principais bandeiras deste estudo: gerar conhecimento dentro da Marinha sobre o tema Guerra Cibernética.

Sendo assim, conclui-se que a Marinha do Brasil, como parte integrante de um sistema de defesa, tem que estar pronta para responder em casos de conflito de qualquer natureza. Ainda que não haja casos de ataques de DoS contra sistemas exclusivamente navais, esta hipótese não pode ser negligenciada, pois suas consequências podem ser desastrosas.

7.2 Sugestões para Futuros Trabalhos

Para dar continuidade a este trabalho e fomentar a mentalidade de segurança cibernética na Marinha do Brasil, sugerem-se as seguintes abordagens para trabalhos futuros:

- Técnicas de Defesa Cibernética contra ataques de DoS/DDoS; e
- Análise de ataques cibernéticos empregados em sistemas exclusivamente navais.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 27002: Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação**. 1ª ed. Rio de Janeiro, RJ, 31 ago. 2005.

AVELAR, J. R. C. A Guerra Cibernética e seus desafios para o Brasil. **Escola de Comando e Estado-Maior do Exército.** Rio de Janeiro, 2018.

BARDAL, R. M. Estudo sobre ataques de negação de serviço e uma abordagem prática. **Universidade Tecnológica Federal do Paraná**, Curitiba, PR, 2014.

BRASIL. Gabinete de Segurança Institucional. **Livro Verde Segurança Cibernética no Brasil**. Brasília, DF, 2010.

BRASIL. Gabinete de Segurança Institucional. **Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal**. v 1. Brasília, DF 2015.

BRASIL. Marinha do Brasil. **DGMM-0540 Normas de Tecnologia da Informação da Marinha**. 3ª rev. Rio de Janeiro, RJ, 2019.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa: paz e segurança para o Brasil.** Brasília, DF, 2012.

BRASIL. Ministério da Defesa. **MD31-M-07 Doutrina Militar de Defesa Cibernética**. Brasília, DF, 2014.

CLARK, R. A.; KNAKE, R. **Guerra Cibernética: A próxima ameaça à segurança e o que fazer a respeito**. Rio de Janeiro: Brasport, 2015.

CERT**. Estatísticas mantidas pelo CERT.br**. 2020. Disponível em: <https://www.cert.br/stats/>. Acesso em: 21 fev. 2020

CETIC. **TIC Domicílios 2018**, 28 ago. 2019. Disponível em: < https://www.cetic.br/pesquisa/domicilios/analises> Acesso em: 01 mar. 2020.

CLOUDFLARE. **Ataque de inundação HTTP**. Disponível em: < https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/> Acesso em: 24 fev. 2020.

COLCHER, S.; LEMOS, G.; SOARES, L. F. G**. Redes de Computadores: das LANs, MANs e WANs às redes ATM**. 2ª ed. Rio de Janeiro: Campus, 1995.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores.** 4ª ed. Porto Alegre: AMGH, 2010.

GHAVAM, Z. M. NATO's preparedness for cyberwar. **Naval Postgraduate School**, Monterey, California, EUA, 2016. Disponível em: <https://calhoun.nps.edu/handle/10945/50552>. Acesso em: 28 fev. 2020.

IBRAHIM, I. Conjunto de protocolos TCP/IP e suas falhas. **Universidade Tecnológica Federal do Paraná**, Curitiba, PR, 2011.

LOUREIRO, M. V. C. Ataques Cibernéticos: Ameaças reais ao Poder Naval. **Revista Passadiço**, Niterói, RJ, ano 29, p. 08 – 14, 2016.

MALONE, P. J. Offense-defense balance in cyberspace: a proposed model. **Naval Postgraduate School**, Monterey, California, EUA, 2012. Disponível em: <https://calhoun.nps.edu/handle/10945/27863>. Acesso em: 28 fev. 2020.

MEDVEDEV, S. A. Offense-defense theory analysis of russian cyber capability. **Naval Postgraduate School**, Monterey, California, EUA, 2015. Disponível em: <https://calhoun.nps.edu/handle/10945/45225>. Acesso em: 28 fev. 2020.

MEMCACHED. **O que é o Memcached?** 2020. Disponível em: < https://memcached.org/> Acesso em: 24 fev. 2020.

MENDONÇA, C. S. Guerra Cibernética: Desafios de uma nova Fronteira**. Universidade Federal do Rio de Janeiro.** Rio de Janeiro, 2014.

MOURÃO, A. M. Guerra Cibernética e o DICA: a tecnologia desafia a Lei da Guerra**. Escola de Guerra Naval.** Rio de janeiro, 2014.

NUNES, L.A. R. Guerra Cibernética: Está a MB preparada para enfrentá-la? **Escola de Guerra Naval**. Rio de Janeiro, 2010.

PARK, J. M. Finding effective responses against cyber attacks for divided nations. **Naval Postgraduate School**, Monterey, California, EUA, 2015. Disponível em: <https://calhoun.nps.edu/handle/10945/47841>. Acesso em: 28 fev. 2020.

PIEDRAHITA, A. F. M. Ferramenta de Avaliação de Ataques de Negação de Serviço em uma Plataforma de Testes. **Universidade Federal do Rio de Janeiro,** Rio de Janeiro, 2014.

SANZ, I. J. Uma função de rede virtual para detecção de varredura lenta de portas na nuvem. **Universidade Federal do Rio de Janeiro,** Rio de Janeiro, RJ, 2017.

SEARCHSECURITY. **Pind of death**. 2020. Disponível em: < https://searchsecurity.techtarget.com/definition/ping-of-death/> Acesso em: 24 fev. 2020.

TANENBAUM, A. S. **Redes de Computadores.** 4. ed. Tradução. Rio de Janeiro: Campus, 2003.

UIT. **Brasil é o quarto país com mais usuários de Internet do mundo, diz relatório da ONU**. União Internacional de Telecomunicações. 04 out. 2017. Disponível em: < https://nacoesunidas.org/brasil-e-o-quarto-pais-com-mais-usuarios-de-internet-do-mundo-diz-relatorio-da-onu/> Acesso em: 01 mar. 2020

VORDOS, I. Mitigating distributed denial of service attacks with Multiprotocol Label Switching—Traffic Engineering (MPLS-TE). **Naval Postgraduate School,** Monterey,

California, EUA, 2009. Disponível em: <https://calhoun.nps.edu/handle/10945/4817>. Acesso em: 21 fev. 2020.