



FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

Vinicius Oliveira Ceribelli

Estudo de um ataque de negação (DDoS)

Americana - SP

2020

FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

Vinicius Oliveira Ceribelli

Estudo de um ataque de negação (DDoS)

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação da Profa. MARIA CRISTINA ARANDA.

Área de concentração: Segurança da Informação.

Americana - SP

2020

**FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte**

C392e CERIBELLI, Vinícius Oliveira

Estudo de um ataque de negação (DDoS). / Vinícius Oliveira Ceribelli. –
Americana, 2020.

34f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação)
- - Faculdade de Tecnologia de Americana – Centro Estadual de Educação
Tecnológica Paula Souza

Orientador: Profa. Dra. Maria Cristina Aranda

1 Segurança em sistemas de informação I. ARANDA, Maria Cristina II.
Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de
Tecnologia de Americana

CDU

Vinicius Oliveira Ceribelli

Estudo de um ataque de negação (DDoS)

Americana, de mês de defesa de 9999.

BANCA EXAMINADORA

Orientador: Maria Cristina Aranda

Doutora

Fatec Americana Ministro Ralph Biasi

Banca 1: João Emmanuel D'Alkmin Neves

Mestre

Fatec Americana Ministro Ralph Biasi

Banca 2: Daniela Dal Fabbro Amorim

Mestre

Fatec Americana Ministro Ralph Biasi

Resumo:

Nos últimos anos houve um gradativo aumento na quantidade e qualidade dos ataques distribuídos de negação de serviço (DDoS). Além dos alvos tradicionais como portais de bancos e e-commerce, existe hoje uma grande quantidade de ataques direcionados a órgãos governamentais. Tal fato aumenta ainda mais a importância na pesquisa nesta área. Uma ferramenta importante para apoiar os pesquisadores é a simulação destes ataques. Apesar disso, as ferramentas tradicionalmente disponíveis não apresentam facilidades necessárias para a modelagem das características deste tipo de ataque. Neste trabalho de pesquisa é proposto um ambiente de simulação de ataques DDoS utilizando como base o simulador de redes ns-3. A plataforma permite que o pesquisador realize experimentos com flexibilidade e escalabilidade.

Palavras Chave: Segurança da informação; Ataque DDoS; Segurança de redes.

Abstract:

In recent years there has been a gradual increase in the quantity and quality of distributed denial of service (DDoS) attacks. In addition to traditional targets such as bank portals and e-commerce, there are now a large number of attacks directed at government agencies. This fact further increases the importance of research in this area. An important tool to support researchers is the simulation of these attacks. However, the traditionally available tools do not present the necessary facilities for modeling the characteristics of this type of attack. In this research work it is proposed a DDoS attack simulation environment using the ns-3 network simulator as a basis. The platform allows the researcher to perform experiments with flexibility and scalability

Keywords: Information Security; DDoS Attack; Network Security.

SUMÁRIO

1.	INTRODUÇÃO	9
1.1	Motivação.....	9
1.2	Definição do problemas	10
1.3	Obejativo	10
2.	Política de segurança.....	10
2.1	Spam e Engenharia Social.....	15
2.2	Malwares	17
2.3	Ataques físicos	21
2.4	Ataques de negação de serviço (DoS e DDoS).....	21
2.5	Packet Sniffing	22
3.	Funcionamento do DDoS.....	22
4.	Classificação do Ataques DDoS	27
5.	Simulação de Ataque DDoS em servidores	30
5.1	Resumo técnico do ataque DDOS.....	30
5.2	Simulação de Ataque DDoS em servidores	30
5.3	Resultado.....	31
6.	Conclusão	32
6.1	Projetos Futuros.....	33
	REFERÊNCIAS.....	34

LISTA DE ABREVIATURAS E SIMBOLOS

AS	- <i>Autonomous System</i>
BGP	- <i>Border Gateway Protocol</i>
BRITE	- <i>Boston university Representative Internet Topology gEnerator</i>
CPU	- <i>Unidade Central de Processamento</i>
DDoS	- <i>Distributed Denial of Service</i>
DNS	- <i>Domain Name System</i>
DoS	- <i>Denial of Service FC - Flash Crowd</i>
HTTP	- <i>Hypertext Transfer Protocol</i>
ICMP	- <i>Internet Control Message Protocol</i>
IGP	- <i>Interior Gateway Protocol</i>
IP	- <i>Internet Protocol</i>
IRC	- <i>Internet Relay Chat</i>
I/O	- <i>Entrada e Saída</i>
IME	- <i>Instituto Militar de Engenharia</i>
PoP	- <i>Ponto de presença</i>
OSI	- <i>Open Systems Interconnection</i>
RAM	- <i>Random Access Memory</i>
SIP	- <i>Session Initiation Protocol</i>
Tcl	- <i>Tool Command Language</i>
TCP	- <i>Transmission Control Protocol</i>
TTL	- <i>Time to Live UDP - User Datagram Protocol</i>
DMZ	- <i>Demilitarized Zone</i>

1. INTRODUÇÃO

1.1 Motivação

O uso da Internet tornou-se parte essencial da vida moderna. As empresas e agências governamentais estão cada vez mais buscando fornecer seus serviços e informações em uma rede global para aumentar a cobertura e a eficiência para atender às necessidades de seus clientes e usuários. Uma das maiores ameaças à disponibilidade desses serviços são os ataques DDoS. DoS (*Denial of Service*) é definido como um ataque que reduz ou elimina ilegalmente a disponibilidade de serviços para usuários legítimos (NOURELDIEN, 2002). Quando vem de várias fontes, é chamado de DDoS (*Distributed Denial of Service*). A defesa contra esses ataques é um grande desafio. Inclui métodos para prevenir, detectar, identificar perpetradores e mitigar ataques. Uma das principais formas de defesa Ele detecta ataques e pode distinguir o tráfego malicioso do tráfego legítimo.

Ataques reais são difíceis de obter, não só porque a rede nem sempre é monitorada para gerar rastros, mas também porque são dados estratégicos de pesquisadores e segurança de empresas e governos. Um ambiente controlado pode ser usado para realizar ataques sintéticos, nos quais existem pessoas responsáveis pelo tráfego legítimo e malicioso e direcionam seus fluxos para hosts específicos. No entanto, essa conquista é quase não escalável porque existem milhares de ataques a nós e é difícil ter tantos hosts. Em um ambiente de laboratório.

A maior vantagem da simulação é a escalabilidade e o custo. Em comparação com outros métodos, as desvantagens são o distanciamento da realidade e a dificuldade de implementação. Vale lembrar que o ambiente a ser simulado é uma rede particularmente complexa: a Internet. Os principais alvos dos ataques DDoS são os serviços disponíveis na Internet. A dificuldade de obtenção dos vestígios é o principal obstáculo nos campos de pesquisa citados. O objetivo deste trabalho é começar a desenvolver uma plataforma que possa simular ataques DDoS e todo o tráfego existente em situações reais.

1.2 Definição do problemas

Os ataques DDoS são muito complexos e novas formas de ataque aparecem todos os dias. (MIRKOVIC, 2004b) propôs um método de classificação de ataques, que representa os vários ataques que estão ocorrendo hoje. O objetivo não é esgotar todas as formas de ataques existentes. Porém, é proposta uma plataforma que busca ser independente da tecnologia de ataque utilizada.

1.3 Obejativo

Este Artigo tem como objetivo desmitificar e simular um ataque DDOS (ataque de negação de serviço) e suas consequências, demonstrar e encontrar técnicas de solução para os ataques DDoS, configurando ferramentas de monitoramento. Ambiente de teste: um computador com Windows 10, processador i7, 8 gb de ram ddr3 com disco rígido de 120gb SSD. Foram utilizadas uma máquinas virtuais através do *software* VitruaBox, em uma distribuição Debian (Kali Linux), utilizando as ferramentas Slowloris.pl para simular os ataques virtualmente. O teste foi realizado em ambiente físico com máquinas virtualizadas, apontando e testando todas as vulnerabilidades encontradas nos servidores e em sistemas operacionais, não importando sua politica de segurança, demonstrando assim que todos os sistemas estão vulneráveis a um ataque.

2. POLÍTICA DE SEGURANÇA

Conhecida como PSI, a Política de Segurança da Informação é um documento que contém normas, procedimentos e métodos, os quais devem ser comunicados a todos os colaboradores, assim como devem ser revistas e analisadas suas criticidades em intervalos regulares ou quando for necessário realizar uma mudança. Assim o sistema de Gestão da segurança da informação irá garantir a viabilidade e o uso dos dados e ativos somente por pessoas autorizadas e cuja utilização se faça necessário para suas funções dentro da empresa.

Na abertura dos trabalhos das Políticas de segurança da Informação deve-se levar em consideração a NBR ISO/IEC 27001, que visa as normas de código e práticas para uma gestão de segurança da informação, levando às melhores práticas para

iniciar, implantar e manter a melhor usabilidade da gestão de segurança da informação dentro de uma empresa ou organização segura. A importância da Política de Segurança da informação na organização se dá pelo fato de a informação ser um dos seus ativos mais valioso e intangível, não bastando ter apenas meios tecnológicos ou informatizados para assegurar sua confidencialidade, integridade, disponibilidade, não repúdio e autenticidade.

Consequências de Políticas da informação bem aplicadas, implementadas corretamente seguidas podendo ser resumidas segundo (Dhillon, 2004) em aspectos: redução da probabilidade de incidentes, redução de danos causados, aplicando correções e criando processos para recuperação de eventuais danos. Com a implantação de segurança da informação a: Gestão a informação, classificação das informações, impressão da informação, eliminação da informação, acesso físico, equipamentos, *hardware* e *softwares*, acesso a redes, acesso à Internet, uso do correio eletrônico e monitoramento dos *logs* e eventos.

A elaboração de uma política da informação bem definida e devidamente implantada protege a informação e ajuda na diminuição dos possíveis problemas de acessos indevidos internos, vírus, pirataria, falta de cultura dos colaboradores quanto a segurança e possíveis fraudes. A aplicação dessa metodologia, não assegura que será suficiente caso não se tenha um mecanismo de controle. Sendo necessário auditoria efetiva periodicamente, que verifique não apenas a existência de uma polícia de segurança da informação, mas as normas que estão sendo efetivamente cumpridas. O auditor deverá elaborar relatórios para evidenciar falhas encontradas.

De acordo com *site AllEasy* (2018) com o aumento significativo do volume de dados e informações que circulam na *web*, se tornaram mais frequentes os ataques distribuídos de negação (DDoS), sobrecarregando diversos *sites* e aplicações, afetando e comprometendo suas ações legítimas, afetando não apenas o alvo como usuários legítimos desses serviços.

Sendo a segurança da informação um dos problemas mais importantes a serem resolvidos em redes de computadores, é um dos maiores problemas para lidar com

ataques no ambiente virtual e por meios físicos, portanto, quando uma vulnerabilidade é descoberta e resolvida, outra vulnerabilidade será utilizada.

Diante de um mercado competitivo e concorrido, as empresas por sua vez vêm buscando tecnologias mais eficazes para executar seus processos, facilitando e flexibilizando suas ações no mercado, gerando mais produtividade e em consequência lucros maiores. Exigindo que ele tenha confiabilidade, integridade e disponibilidade estando protegidos e que chegue aos seus usuários íntegros sem qualquer alteração e de maneira confiável, tornando a segurança da rede e dos dados fundamentais para sua legitimidade.

Ameaça é uma causa potencial de acidentes e pode causar danos ao sistema ou à organização. Pode ser descrita como ameaça natural, caso em que as condições climáticas, como incêndios e inundações, podem causar danos aos ativos. Por outro lado, ameaças deliberadas são causadas deliberadamente, ou seja, com a intenção de causar danos, como fraude e destruição eletrônica. Finalmente, as ameaças involuntárias podem ser causadas por comportamentos inconscientes ou ingênuos dos usuários, como engenharia social. (CERT.br, 2016),

O Centro Brasileiro de Pesquisa, Resposta e Processamento de Incidentes de Segurança (CERT.br, 2016) é o grupo de resposta a incidentes de segurança da Internet brasileira, responsável por receber, analisar e responder a incidentes de segurança envolvendo redes conectadas à Internet. Esse grupo é mantido pelo NIC.br (Centro de Informação e Coordenação), que faz parte do Comitê Gestor da Internet (CGI) e tem como objetivo aumentar a conscientização sobre questões de segurança (CERT.br, 2016), conforme mostrado na Tabela 1.

Tabela 1: Pessoas que podem causar problemas de segurança e os motivos para fazê-lo

Inimigo	Objetivo
---------	----------

Estudante	Divertir-se bisbilhotando as mensagens de correio eletrônico de outras pessoas
Cracker	Testar o sistema de segurança de alguém; roubar dados
Representante de vendas	Tentar representar toda a Europa e não apenas Andorra
Executivo	Descobrir a estratégia de marketing do concorrente
Ex-funcionário	Vingar-se por ter sido demitido
Contador	Desviar dinheiro de uma empresa
Corretor de valores	Negar uma promessa feita a um cliente através de uma mensagem de correio eletrônico
Vigarista	Roubar números de cartão de crédito e vendê-los
Espião	Descobrir segredos militares ou industriais de um inimigo
Terrorista	Roubar segredos de armas bacteriológicas

Fonte : Tanenbaum, 2010.

Uma das principais ameaças à segurança da informação são os usuários mal treinados ou sem treinamento nenhum. Iniciando processos ou procedimentos, portanto, obtendo o poder de clicar, aceitar, autenticar, executar ou ignorar o que em uma fração de segundo pode representar uma ameaça ou risco.

Com um programa de conscientização treinamento de todos os colaboradores/usuários o recurso humano deve cuidar da organização, considerando o usuário um grande fator de risco a proteção das informações em seus processos. É de extrema importância que o novo usuário seja orientado pelos seus superiores como chefia e principalmente a diretoria da organização quanto a comportamento as regras nos processos de segurança da informação.

Todo o acesso a informações deve ser devidamente restringido a usuários que tenha a real necessidade à mesma, não valendo de nada a organização obter a resolução de controle de acesso lógico se os usuários repassarem a senha para outro usuário que não tinha acesso à devida informação. Deve-se levar em consideração os processos para facilitar e não engessar os processos de negócio.

Usuários devem se manter atentos para não deixar desprotegidos *notebooks*, *tablets*, celulares ou qualquer recurso que obtenha informação da organização, levando em consideração papéis impressos que também contém informações confidenciais em locais de acesso a outros usuários. Tendo como objetivo para a organização a realização do negócio sendo necessário o entendimento do usuário para o bem mais importante, a informação, estando protegida adequadamente.

As mensagens mais enviadas por fraudadores, referem-se aos chamados problemas no serviço de Internet Banking, e exigem que os usuários visitem *links* contendo aplicativos que irão corrigir os problemas. Esse método é chamado de *phishing scam*, no qual muitos *e-mails* (semelhantes a *spam*) são enviado para roubar senhas para acessar a conta bancária de um usuário e enviá-la ao invasor (CERT.br, 2016).

Outro modelo de ataque pode ocorrer por telefone, em que o atacante telefona para a vítima informando ser do suporte técnico do provedor. O invasor relatou um problema com a conexão à Internet e pediu à vítima uma senha para resolver o problema. A senha é usada para atividades maliciosas e, portanto, está relacionada ao nome de *login* do usuário atacado.

Uma das principais ameaças são os intrusos, tanto dentro da corporação quanto fora dela com a intenção de promover ataques aos sistemas, com finalidade de explorar a rede e ver o que encontra dentro dela ou de forma maligna-realizar alterações não autorizadas nas informações ou interromper algum sistema.

Pode-se classificar os intrusos em três tipos (CERT.br, 2016):

Infrator: Usuário de dentro da organização, com acesso a dados, recursos ou

sistemas no quais tenha ou não autorização, realizando mal o uso de seus acessos.

Usuário clandestino: Usuário que obtém controle administrativo de sistemas e o utiliza para se esconder de auditoria e controles de acessos podendo ser de dentro da organização ou não.

Mascarado: Usuários que por algum meio obteve acesso de usuários legítimos ou administradores sem a autorização, explorando os recursos obtidos.

2.1 Spam e Engenharia Social

Spam são mensagens indesejadas que geralmente são enviadas a um grande número de pessoas sem sua solicitação ou autorização. São também chamadas de UCE (*Unsolicited Commercial E-mail*) quando o conteúdo é exclusivamente comercial.

Historicamente, o primeiro e-mail de spam foi enviado por dois advogados, Canter e Siegel. O e-mail era sobre *green cards* dos EUA e foi enviado para o grupo de discussão Unix *User Network* (USENET). Posteriormente, a mesma mensagem foi enviada a vários grupos de discussão da USENET, o que despertou a surpresa e o desgosto de muitos membros do grupo (CERT.br, 2016).

Os usuários são afetados de diversas formas, tais como (CERT.br, 2016):

Incapaz de receber e-mail - No caso do provedor de Internet limitar o tamanho da caixa de correio do usuário, se o usuário receber um grande número de *spam* pode exceder o limite de armazenamento, resultando em *e-mails* descartados, uma solução é usar regras *anti-spam*.

Gasto desnecessário de tempo - Os usuários devem reservar um tempo para ler e identificar os *e-mails* como *spam*.

Aumento de custos - A pessoa que paga pelo *spam* é a pessoa que recebe o *spam*. Ao baixar o *spam*, ele vai consumir a franquia mensal.

Prejuízos financeiros causados por fraude - O *spam* tem sido usado para induzir os usuários a visitar páginas clonadas de instituições financeiras ou instalar programas maliciosos para roubar dados pessoais e financeiros.

Provedores de acesso, redes de *backbone* e organizações são afetados por razões, tais como (CERT.br, 2016):

Impacto na banda - O tráfego gerado pelo *spam* forçou organizações e provedores a aumentar seus *links* de conexão.

Má utilização dos servidores - O servidor de *e-mail* leva tempo e espaço em disco para processar mensagens indesejadas.

Inclusão em listas de bloqueio - O provedor ou servidor de *e-mail* da organização pode ser incluído em uma lista negra chamada *Black-List*. Que impedirá o recebimento de *e-mails* legítimos e autorizados.

Investimento em pessoal e equipamentos - Provedores e organizações precisam contratar profissionais, comprar mais equipamentos e sistemas de filtragem de *spam*.

Engenharia social é um termo usado para descrever um método de ataque no qual alguém usa a persuasão (geralmente um abuso do intelecto ou da confiança do usuário) para obter informações que podem ser usadas para obter acesso não autorizado a computadores ou informações (CERT.br, 2016).

As mensagens mais enviadas referem-se aos chamados problemas no serviço de Internet Banking e exigem que os usuários visitem *links* contendo aplicativos que irão corrigir os problemas. Este método é chamado de verificação de *phishing*. Neste método, semelhante ao *spam*, muitos *e-mails* são enviados para roubar a senha para acessar a conta bancária do usuário e enviá-la ao invasor (CERT.br, 2016).

Sempre que se duvidar da verdadeira identidade do autor de uma mensagem ou chamada, necessita-se entrar em contato com a agência, provedor ou empresa

para verificar a verdade (CERT.br, 2016).

2.2 Malwares

Código malicioso ou *malware* (*Software* Malicioso) é um termo usado para caracterizar programas desenvolvidos para realizar ações maliciosas para destruir ou roubar informações em um computador. O *software* legítimo que contém erros de programação (intencionalmente ou não) e executa operações ilegais também é considerado *malware*. A seguir são apresentados diferentes tipos de *malware*.

O vírus é um programa de computador que contém comandos maliciosos, que são usados simplesmente para perturbar o usuário, causar danos sérios, alterar ou destruir o programa ou arquivo no disco. O vírus se espalha inserindo uma cópia de si mesmo enquanto se move. Isso depende da operação do usuário, ou seja, a execução do programa ou arquivo hospedeiro durante a transmissão do vírus é executada pelo usuário. Alguns tipos de vírus são: vírus de inicialização, vírus executáveis, vírus de macro, vírus de e-mail e vírus de telefone celular propagados por meio da tecnologia Bluetooth (TANEMBAUM, 2010; CERT.br, 2016).

WORM - programa ou fragmento de programa que pode espalhar uma cópia de si mesmo para outros computadores por meio de uma conexão de rede e não requer nenhuma ação do usuário. O *worm* procurará outros *sites* para infectar e, cada computador infectado atuará como uma plataforma de lançamento para atacar automaticamente outros computadores. Na replicação, o *worm* usa, por exemplo, recursos de e-mail para enviar cópias de si mesmo a outros usuários ou sistemas. Ele também tem a capacidade de realizar *login* remoto e remotamente, pode realizar acesso a sistemas e, em seguida, executar comandos para espalhar-se (STALLINGS, 2020).

BOT - programa que pode se espalhar automaticamente na rede e explorar brechas ou falhas de configuração do sistema. Ao contrário de um *worm*, ele pode se comunicar com atacantes remotamente. O *bot* e o invasor se conectam ao servidor Internet Relay Chat (IRC) e entram em uma “sala”, onde enviam mensagens contendo

sequências de caracteres especiais, que são interpretadas por *bots* residentes no computador comprometido. Um grupo de computadores infectados com *bots* cria uma rede chamada *botnet*, que é usada para enviar milhares de golpes de *phishing* e desencadear ataques de negação de serviço (TORRES, 2013; CERT.br, 2016).

CAVALO DE TRÓIA - programa ou processo de comando muito útil que pode executar as funções que cria, mas o código oculto nele contido pode executar funções maliciosas e prejudiciais sem o consentimento do usuário. Eles são usados, por exemplo, para distribuição *backdoor*, instalação de keyloggers ou gravadores de tela e destruição de dados (CERT.br, 2016).

BACKDOORS (porta dos fundos) ou **TRAPDOORS** (alçapão) - programas instalados incorretamente, que farão com que a porta se abra para acesso remoto futuro para um invasor. Os programadores usam *backdoors* para iniciar e testar seus programas, mas quando os *hackers* começam a usar *backdoors* para invadir o sistema, isso se torna uma ameaça. Normalmente, o computador recebe a porta dos fundos por meio de um programa cavalo de Tróia e é acionado quando reconhece uma sequência de entrada especial ou é executado por um ID de usuário específico (CERT.br, 2016).

KEYLOGGERS - programa que captura e armazena a chave inserida pelo usuário no sistema. Na maioria dos casos, a ativação do *keylogger* ocorre ao mesmo tempo que a ativação do usuário, e esse tipo de malware possui um mecanismo para enviar automaticamente as informações coletadas ao invasor. Com o aprimoramento desse *malware*, surgiu um programa de gravação de tela, que pode capturar e armazenar a posição do cursor e a área ao redor da tela exibida no monitor e onde o *mouse* é clicado (CERT.br, 2016).

ADWARE - (*Advertising software*) é um *software* com características exclusivas que pode exibir anúncios através do navegador do usuário ou outro *software* como o *MSN Messenger*. Muitas organizações têm legalmente usado *adware* para patrocínio, especialmente em projetos ou serviços gratuitos. Quando o *adware* tem a função de monitorar os hábitos de navegação dos usuários para enviar anúncios mais específicos, o uso ilegal ocorrerá (ZARGAR, 2016).

SPYWARE - programa que monitora as atividades realizadas pelo sistema e envia as informações coletadas ao atacante. Como o adware, alguns *spywares* são usados legalmente, por exemplo, para monitorar as atividades dos usuários em uma determinada organização. Por outro lado, o *spyware* é amplamente utilizado para ativar um *keylogger* ou gravador de tela quando reconhece que um usuário está visitando o *site* de um banco por exemplo. Os *rootkits* são programas instalados no computador da vítima e projetados para se esconder no sistema para ocultar as atividades e informações do invasor. Os *rootkits* podem ter as mais diversas funções, tais como: programas *backdoor*, *sniffers* que são programas que capturam informações que trafegam pela rede, *keyloggers* entre outros.

KEYLOGGER - Os *keyloggers* são *softwares* de computador que visam monitorar, armazenar e enviar tudo o que foi digitado pela vítima para um terceiro. Os *keyloggers* podem ser inseridos em outros códigos prejudiciais como os *trojans*.

ADWARE - O *adware* é um programa cuja função é executar automaticamente e exibir um grande volume de anúncios, sem que o usuário tenha dado a devida permissão.

BACKDOOR - É um mecanismo usado por vários *malwares* para promover acesso remoto a *softwares* ou à rede infectada. Esse programa busca explorar falhas problemáticas não documentadas em aplicações instaladas, desatualizadas e do *firewall* para ter acesso às portas do roteador.

BROWSER HIJACKER - Trata-se de um tipo de vírus de computador que tem por meta a mudança das principais configurações do navegador. Quando instalado, modifica a *homepage* e as formas de busca. Demonstrem anúncios em páginas legítimas e redirecionam o usuário para *sites* maliciosos que podem apresentar *exploits* ou outras pragas digitais.

TROJAN HORSES - Os Cavalos de Troia mantêm-se ocultos enquanto baixam e instalam ameaças em computadores e *laptops*. São conhecidos por fazerem parte dos primeiros estágios de infecção de dispositivos digitais. Eles aparecem em mensagens de *e-mail*, arquivos de música, *sites* maliciosos, entre outros. Além disso,

esse tipo de vírus pode se aproveitar de vulnerabilidades presentes no navegador para instalar *softwares* maliciosos no computador.

ROOTKIT - *Rootkit* são trojans que usam mecanismos avançados de programação para serem instalados em classes documentadas ou não documentadas do sistema operacional. As suas funções mais devastadoras são: a sua capacidade de recuperação, reinstalando-se mesmo depois da limpeza do computador; e sua disseminação em alta velocidade.

SPYWARE - Esse tipo de *software* apresenta a característica de espionagem e visa captar dados sobre os costumes dos usuários na Internet, com o objetivo de distribuir propaganda “customizada”.

TIME BOMB - O *Time Bomb* é um tipo de *malware* que apresenta contagem regressiva. Ele é uma ameaça pré-ordenada para ser executada em uma ocasião específica no sistema operacional, provocando sérios danos.

GREYWARE - É um *malware* que se encontra na chamada zona cinzenta, entre o *software* normal e um vírus, provocando mais irritação do que problemas, como programas de piada e adware. Assim, o *Greyware* refere-se a *softwares* que são instalados sem a permissão do usuário.

JOKE PROGRAM - Trata-se de mecanismos ou códigos criados para provocar danos temporários ao sistema operacional, como travamentos e alterações inesperadas de comportamento. Os códigos dessa natureza não causam nenhum dano real ao computador.

RANSOMWARE - São códigos maliciosos que retêm arquivos ou todo o sistema do usuário por meio de técnicas de criptografia. Após o “sequestro”, o *malware* apresenta mensagens exigindo o depósito de uma certa quantia ou a compra de alguma mercadoria, informando que em seguida fará o envio da senha para liberar os arquivos. Contudo, mesmo depois do pagamento, a maioria dos usuários não recebe senha alguma.

TROJAN BANKING - É o trojan caracterizado pelo acesso a dados bancários, redes sociais, *sites* de compras e servidores de *e-mail*. As formas utilizadas são as mesmas de um *trojan*, sendo partilhado como um *software* ou arquivo legítimo, em *sites* infectados ou *e-mails*.

2.3 Ataques físicos

O furto de informação importante de uma organização pode ocorrer a partir de um ataque físico buscando qualquer periférico que possa ser usado para posteriores ataques. Tratando da segurança física e do ambiente a norma ISO/IEC 27002 tem o objetivo de proporcionar diretrizes e prevenções do acesso indevido a periféricos não autorizados, danos e interferência nas instalações.

Com as medidas adequadas pode-se impedir danos, furtos, perdas ou comprometimentos de ativos e interrupção das atividades na organização.

O acesso físico deve ser protegido com a criação de um perímetro de segurança física, incluindo controles de entrada física, segurança nos escritórios, salas e instalações, proteção contra ameaças externas e do meio ambiente e acesso do público, área de entrega e carregamento (ISO/IEC 27002, 2005).

2.4 Ataques de negação de serviço (DoS e DDoS)

Um ataque de negação de serviço ou DoS (Denial of Service) consiste na ação em um *host* ou nó de rede enviar um número arbitrário de solicitações ao *host* por meio de um programa malicioso chamado *flooding*. Como resultado, o *host* estará sob a maior pressão e o sistema ou serviço se tornará indisponível, tornando impossível acessar o *host*. Ataque de estouro de *buffer* (estouro de memória), em que o tamanho do *buffer* excede a capacidade máxima de armazenamento, destruindo ou travando o sistema, levando a um ataque de negação de serviço.

O ataque denominado SYN *Flooding*, visa esgotar o *link* de dados no qual vários

pacotes SYN são enviados para preencher a fila de conexão do servidor e causar uma negação de serviço. Em um ataque de *spoofing* de IP, o programa forja o endereço IP de origem. Essa é também uma técnica usada em um ataque DoS. Nessa técnica, vários *hosts* podem enviar pacotes de dados como se fossem um determinado endereço de origem, fechando assim o endereço IP, o endereço do servidor que executa a autenticação.

Em um ataque DDoS (negação de serviço distribuído), milhares de computadores são usados para realizar um ataque de negação de serviço. O invasor consegue instalar *software* malicioso em estações comuns e depois de infectadas passam a ser chamadas de zumbi, assim, realizam requisições ao *host* alvo. Tornando o *host* de destino indisponível (TREVENZOLI, 2006; STALLINGS, 2008).

2.5 Packet Sniffing

O ataque de *packet sniffing* realiza monitoramento passivo do tráfego da rede e captura pacotes de dados que podem conter informações importantes (como senhas) e copiam arquivos que estão espalhados na rede. Ele monitora passivamente o tráfego de rede (CARVALHO, 2005).

3. FUNCIONAMENTO DO DDOS.

As vítimas do DDoS podem ser os próprios *hosts* como uma infraestrutura da Internet que presta serviço a estes *hosts*.

O flooding citado anteriormente, se refere a dois casos segundo Zargar (2013):

- Dificultar/Impedir que qualquer usuário consiga se conectar/acessar recurso do servidor como CPU, memória, banco de dados, *sockets* ou largura de banda do disco. Sendo assim inundando a camada de aplicação no modelo OSI.

- Dificultar/Impedir que qualquer usuário consiga se conectar/acessar devido ao esgotamento do tráfego/capacidade de banda larga, congestionar os recursos de rede ou a capacidade de processamento do roteador. Sendo assim o principal ataque realizado na camada de rede no modelo OSI.

Para poder gerar um tráfego que consiga sobrecarregar os recursos da vítima, o atacante necessita de um computador com alta capacidade de processamento e banda larga suficiente para obter o efeito necessário e efetivo. Como a vítima pode possuir recursos abundantes, o ataque vindo apenas de um único computador se torna ineficaz. Assim, supondo que o atacante possua milhares de computadores sobre seu controle, mesmo com baixos processamentos e largura de banda, em conjunto formam uma grande rede, assim sobrecarregando os recursos da vítima.

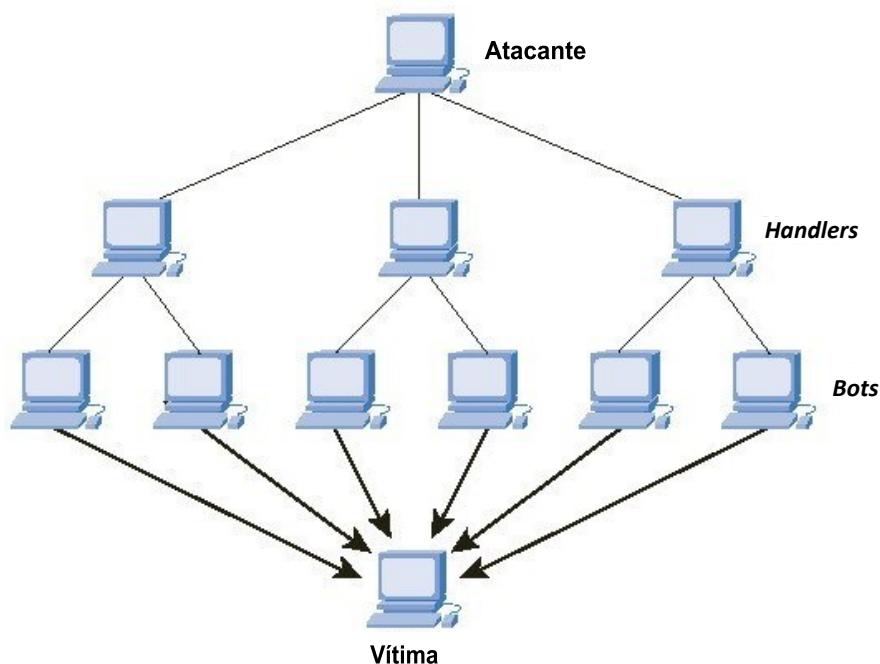
Com o alvo predeterminado e um ataque coordenado para esse alvo, definindo e realizando vários ataques de negação de serviço, sendo ambos os ataques DoS e DDoS grandes ameaças, sendo o mais complexo e de difícil solução o ataque DDoS. Utilizando muitos computadores na realização dos ataques, até mesmo as vítimas receberam recursos abundantes, e os recursos foram prejudicados.

Uma das dificuldades para se identificar um ataque DDoS é porque o tráfego é similar a um usuário legítimo, dificultando a comparação das mensagens dos usuários lícitos por não existirem características relevantes, desta forma responder a um ataque, pode-se estar atingindo a um usuário legítimo.

Para a realização de um ataque DDoS se faz necessária a formação de uma rede que é definida como *Botnet*, formando uma rede de *hosts* infectados por malware comandado pelo atacante, denominado como *botmaster*. Os *hosts* infectados são comandados pelo *botmaster* através de comandos remotos assim como exemplo básico de arquitetura na Figura 1.

Figura 1. Hosts infectados sendo comandado pelo *botmaster*

Fonte : Tanenbaum, 2010.



As fases de preparação e condução a um ataque DDoS apresentadas por MIRKOVIC (2003):

Recrutamento: O atacante seleciona, dentre *hosts* localizados na Internet, aqueles que realizarão o ataque. Estes equipamentos, usualmente são chamados de *boots*, e normalmente são: (a) externas à rede da vítima, visando evitar uma resposta eficiente da vítima, e (b) externas à rede do atacante, com o objetivo de evitar a responsabilização caso seja identificada a fonte do ataque. Para que os *hosts* se transformem em *boots* é necessário que existam falhas de segurança para que códigos maliciosos possam ser instalados. Também é desejável que os *boots* possuam recursos abundantes para serem capazes de realizar ataques poderosos. Este processo pode ser realizado manualmente, entretanto, é comum que seja feito de forma automática com a utilização de ferramentas que produzem listas de *hosts* que sejam potencialmente vulneráveis.

Comprometimento: O atacante ganha acesso (normalmente *root*) nos *hosts* através de brechas na segurança e implanta o código de ataque. Ele adota medidas para impedir que o código seja descoberto (renomeando arquivos, tornando-os ocultos ou colocando-os no diretório do sistema) e

desativado (fazendo com que a agenda do sistema, como o *cron* do Linux, o reinicie periodicamente). Esta fase também pode ser automática. As mesmas ferramentas utilizadas para escanear a Internet podem obter acesso, inserir o código de ataque e enviar ao atacante a lista de *hosts* comprometidos.

Comunicação: *bots* reportam sua prontidão para o ataque através de *handlers-hosts* comprometidos que serão usados para controlar o ataque. Nos primeiros ataques DDoS, os endereços IP dos *handlers* encontravam-se diretamente no código do ataque e os *handlers* guardam os *bots* disponíveis para o ataque em um arquivo encriptado. Logo a descoberta de um simples *bot* participante do ataque revelava todos os outros participantes. Com a utilização de outros canais de comunicação como o Internet Relay Chat (IRC), o servidor IRC rastreia o endereço dos *bots* conectados e dos *handlers* e facilita a comunicação entre eles. A descoberta de um participante do ataque leva à descoberta do canal de comunicação, mas a identidade dos outros participantes permanece protegida.

Ataque: Os atacantes normalmente comandam o ataque através dos *handlers* e dos canais de comunicação para os *bots*. O alvo, duração e características dos pacotes como tipo, tamanho, TTL1, número das portas, dentre outros, podem ser customizados. Atualmente as ferramentas de ataque DDoS utilizam-se de várias técnicas para evitar sua detecção, sendo elas:

* IP *spoofing*: ocorre quando um código malicioso cria seu próprio pacote, não seta o endereço IP real no cabeçalho do pacote (MIRKOVIC, 2004a).

* Tamanho variável de pacotes: a utilização de variados tamanhos de pacotes pelos *bots* dificulta a criação de uma assinatura para o ataque.

* Diferentes canais de comunicação: os *bots* podem comunicar-se entre si e com o *botmaster* utilizando vários canais e protocolos como IRC, HTTP, e-mail, redes P2P, dentre outros.

As organizações precisam implementar vários mecanismos para prevenir ameaças e mitigar riscos que podem afetar a continuidade dos negócios. A seguir estão os principais mecanismos, segundo STALLINGS, 2008 de proteção de ativos:

Educar o usuário: Esta organização é a principal responsável pela manutenção da segurança da informação e deve zelar por seus recursos humanos, conscientização e treinamento dos usuários, fator importante na difusão da cultura de proteção da informação.

Quando for necessário realizar o uso e definição de senhas, necessita-se de algumas medidas preventivas (STALLINGS, 2008): Trocar imediatamente a senha padrão fornecida pelo administrador na criação do *login* de acesso; Não usar senhas curtas, sendo recomendável usar pelo menos oito caracteres, incluindo letras, números e caracteres especiais; Não usar senhas com palavras do dicionário; Não usar a data de nascimento, o nome da pessoa, o nome da equipe ou outras informações vinculadas a você ou à organização; Não usar números de telefone, números de documentos ou letras e números de placas de veículos.

Autenticação: O objetivo da verificação de identidade, é verificar a identidade do usuário no sistema ou recurso, para garantir que a comunicação seja autêntica e que o solicitante da comunicação seja realmente o que se afirma. Os métodos de autenticação podem ser divididos em três tipos: “usar coisas que você é, coisas que você conhece e coisas que você possui” (CARVALHO, 2005).

A autenticação utilizando algo que você “É”, usando informações sobre as características físicas e comportamentais do usuário para realizar a verificação de identidade, que é chamada de biometria. Exemplos de biometria são impressão digital, leitura de retina e íris, formato da mão e reconhecimento de voz. A implementação de controle de acesso e autenticação por meio de tecnologia biométrica é considerada cara para a organização. Nesse tipo de tecnologia também pode acontecer falsos

positivos ou falsos alarmes advindos de acidentes ou doenças que afetam de alguma forma as características físicas de seu proprietário, bem como problemas nos leitores.

A autenticação utilizando tecnologias mais populares e de menor custo financeiro são as mais utilizadas pelas organizações. Uma senha é uma *string* de *strings* usada para verificar a identidade do usuário com base no sistema que o usuário deseja acessar. Esta é considerada a forma mais comum de autenticação e a menos segura, porque a segurança do sistema depende da confidencialidade da senha. Outra forma de autenticação é o uso de um PIN (número de identificação pessoal). Um PIN é uma série de números e/ou letras usadas para autorizar o acesso a chaves privadas ou outros dados armazenados na mídia e é aplicável apenas a pessoal autorizado (ICP BRASIL, 2006).

Ainda a autenticação utilizando alguma tecnologia que a empresa já domina são cada vez mais usado em organizações e dispositivos físicos são frequentemente usados para realizar a identificação do usuário. Os certificados digitais são arquivos eletrônicos que contêm dados do usuário ou da organização e são armazenados em um cartão inteligente (*smart card*). O *microchip* inserido no cartão plástico armazena e processa os dados. Eles são amplamente utilizados para armazenar certificados digitais (ICP BRASIL, 2006).

A técnica de autenticação conhecida como OTP (*One-Time Password*), geralmente é implementado na forma de um *token*, um dispositivo de *hardware* que armazena um programa que gera uma nova senha periodicamente ou toda vez que o usuário se autentica. Uma vantagem na utilização da OTP é a proteção contra *phishing* de senha.(ICP BRASIL, 2006).

4. CLASSIFICAÇÃO DO ATAQUES DDOS

Em relação a fases de um ataque, pode-se classificar os ataques que atuam na camada de aplicação e os que atuam na camada de rede e transporte. (NSFOCUS, 2013)

Ataque em camada de aplicação, o ataque *flooding*: ataque que tem o foco de atuação sobre recursos do servidor (CPU, memória e etc), impedindo que usuários legítimos utilizem serviços. Este tipo de ataque DDoS costuma consumir menos banda larga e acaba sendo difícil sua detecção quando comparado aos ataques na camada de transporte e rede. Usualmente os ataques *flooding* tem o mesmo impacto aos serviços pela sua atuação em características específicas de aplicações como DNS, HTTP ou SIP 2. (NSFOCUS, 2013)

- Ataques de *flooding* com amplificadores/refletores: com as mesmas características dos ataques das camadas de transporte e rede, enviando a muitos refletores requisições da camada de aplicação forjadas. O ataque de amplificação de DNS emprega características tanto de amplificação quanto de reflexão. Gerando pequenas consultas DNS pelos *bots* com um endereço de IP forjado, ocorrendo um grande volume de tráfego de rede, pois o retorno do DNS pode ser substancialmente maior que as mensagens de consulta no DNS.
- Ataques de *flooding* HTTP, são classificados em 3 tipos:
 - Ataques de *flooding* de sessão: A quantidade de sessões feitas é maior que a de um usuário legítimo.
 - Ataques de *flooding* de requisição: A quantidade de requisições por sessão é maior que a de um usuário legítimo.
 - Ataques assimétricos: As sessões exigem do servidor uma alta carga de trabalho.
- Flooding de múltiplos HTTP: são enviados pacotes que contêm múltiplas requisições sem possuírem uma única sessão HTTP.
- Slowloris: são enviadas diversas sessões HTTP incompletas que crescem rapidamente, realizando autenticação lenta e nunca são

fechadas, ocupando todos os sockets disponíveis até que o servidor se torna inacessível.

- Fragmentação de HTTP: é realizada uma conexão HTTP legítima enviando pequenos pacotes de fragmentos mais lentos que o time out do servidor permite.
- Slowpost: são enviados um cabeçalho HTTP definindo o campo “content-length” iniciando o tráfego, com uma taxa de dois minutos por byte, assim o servidor aguarda ser completado o corpo da mensagem.
- Slowreading: é enviado requisição de abertura de sessão TCP com um valor pequeno, forçando o servidor a estabelecer muitas sessões/conexões abertas.
- Ataques de flooding dentro da camada de rede e transporte: Na maior parte os ataques em redes e transporte são executados nos protocolos TCP, UDP, ICMP e DNS. Existindo quatro tipos de ataques:
 - Ataques de *flooding*: com o foco de impedir usuários legítimos de se conectar devido a exaustão da rede de banda larga da vítima (ICMP *flood*, DNS *flood*, UDP *flood*);
 - Ataques de *flooding* de *exploit* de protocolo: Explorando erros de implementação ou características específicas dos protocolos da vítima consumindo em quantidades excessivas os recursos da vítima (TCP SYN *flood*, TCP SYN-ACK *flood*, ACK & PUSH ACK *flood*, RST/FIN *flood*);
 - Ataques de *flooding* com refletores: enviando requisições (ICMP *echo request*) com o endereço da vítima pelos refletores forjadas. Assim refletores enviam suas respostas para a vítima e esgotando seus recursos (Ataques *Fraggle* e *Smurf*);

- Ataques de *flooding* com amplificadores: Explorando serviços que geram várias respostas para cada requisição ou respostas maiores que as requisições realizadas.

Existem uma predominância dos ataques na utilização dos protocolos na camada de aplicação como DNS e HTTP, os quais foram reportados no relatório DDoS Threat Report 2013 (NSFOCUS, 2013) do NSFOCUS.

5. SIMULAÇÃO DE ATAQUE DDoS EM SERVIDORES

5.1 Resumo técnico do ataque DDoS

Cenário: 5 máquinas virtuais, sendo 4 atacantes e 1 como alvo. A rede utilizada é 10.0.1.0/24, e os IPs utilizados foram: 10.0.1.30, 10.0.1.50, 10.0.1.52, 10.0.1.53, 10.0.1.54.

A vítima tem o IP 10.0.1.30, composta pelos serviços de apache (HTTP, porta 80) e também do Zabbix (porta 10050 – não explorada). O ataque foi realizado com o *software* Slowloris. Em cada servidor atacante, já com o Slowloris instalado, iremos executando o comando “perl slowloris.py 10.0.1.30 -p 80 -s 500”, sendo: (10.0.1.30 = Alvo | -p = Porta | -s = Sockets)

O *Slowloris* é um tipo de ataque de negação de serviço HTTP. Ele envia muitas solicitações HTTP, como cabeçalhos, periodicamente a cada 15 segundos para manter as conexões abertas. Sua conexão nunca é fechada, a menos que o servidor o faça. Se o servidor fechar uma conexão, ele cria uma nova que continuará fazendo o ataque.

5.2 Simulação de Ataque DDoS em servidores

O *download* do *Slowloris* foi pelo *git* clone “<https://github.com/gkbrk/slowloris.git>” e após finalizado nos direcionamos até o diretório criado (*slowloris* – cd *slowloris*).

Dentro do diretório foi executado o ataque com o script “slowloris.py”. Para iniciar o ataque foi executado o *script* slowloris.py através do comando:

```
perl slowloris.py [website url] -p [port] -s [number of sockets]
```

Por padrão, ele envia 150 *sockets*. Para efeito em testes são utilizados 500 *sockets*.

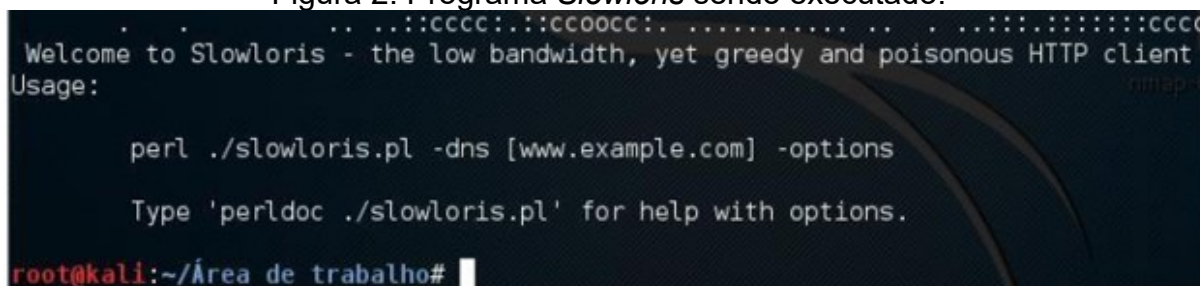
São necessários o Python 3.x e o Perl instalado no SO. Não exigindo que seja uma distribuição voltada para *pentest*, como o Kali ou Parrot, mas neste estudo foi utilizado o Kali Linux.

5.3 Resultado

Verifica-se que foi enviado mais de 4500 *packets* em 1 segundo enviadas ao *site*, causando uma lentidão na aplicação e até uma rápida indisponibilidade. Nos *logs*, pode-se observar os IPs que atacaram fazendo as requisições (*get*) no endereço.

A figura 2 mostra a execução do programa *Slowloris* e o ataque sendo realizado.:

Figura 2. Programa *Slowloris* sendo executado.



```
.. ..:cccc:::ccoooc:. .. . .:cccco
Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client
Usage:
    perl ./slowloris.pl -dns [www.example.com] -options
    Type 'perldoc ./slowloris.pl' for help with options.
root@kali:~/Área de trabalho#
```

Fonte: Elaborado pelo Autor, 2020

Ao lançar um ataque, vários pacotes de dados serão enviados ao servidor de destino, fazendo com que o usuário, o servidor caia ou diminua a velocidade da conexão. A Figura 3 mostra o pacote sendo enviado ao destinatário.

Figura 3. Programa *Slowloris* realizando o ataque.

```
Current stats: Slowloris has now sent 40750 packets successfully.  
This thread now sleeping for 1 seconds...  
Building sockets.  
Sending data.  
Current stats: Slowloris has now sent 40800 packets successfully.  
This thread now sleeping for 1 seconds...  
Building sockets.  
Sending data.  
Current stats: Slowloris has now sent 40850 packets successfully.  
This thread now sleeping for 1 seconds...  
Building sockets.  
Sending data.  
Building sockets.  
Sending data.  
Current stats: Slowloris has now sent 40924 packets successfully.  
This thread now sleeping for 1 seconds...  
Current stats: Slowloris has now sent 40950 packets successfully.  
This thread now sleeping for 1 seconds...
```

Fonte: Elaborado pelo Autor, 2020

6. CONCLUSÃO

Ao iniciar um ataque DDoS, tem-se que ter em mente um objetivo. O DDoS demanda tempo, preparo e recurso. Da mesma forma que o ataque foi executado, necessita-se, ter em mente que o atacante também pode ser atacado ou até mesmo identificado.

Em nosso laboratório, utilizou-se 4 máquinas virtuais compartilhando a mesma *interface* de rede. Em um ataque real necessita-se dispor de computadores e Internet para que seja enviado uma alta quantidade de pacotes ao mesmo tempo. O método utilizado é o sequestro de computadores na Internet e fazendo-os de zumbis. Esses computadores irão efetuar o ataque sem que os donos saibam, utilizando a banda de Internet. Um usuário comum de computador não percebe e não tem ideia de como mitigar ou evitar essa situação.

O sucesso do ataque ocorre assim que se consegue derrubar um serviço ou um *site*. Quanto mais *bits* enviados em menor tempo, mais rápido se chegará ao objetivo. O orquestralmente deve ser bem conduzido, pontual e certo. Cada

computador zumbi deve efetuar o ataque ao mesmo tempo, podendo chegar a mais de 50 computadores. Controlar 50 computadores simultaneamente, monitorar a efetividade de cada um, é um trabalho que deve ter um objetivo claro, e não apenas por esporte.

Essa prática é crime, e o que foi demonstrado, foi em um ambiente controlado e um *site* simples. Ambientes produtivos de empresas, em sua menor parte, conta com sistemas de detecção de intrusão ou sistema de proteção (IDS ou IPS).

A lei nº 12.737 de 2012 diz claramente que a interrupção ou perturbação de serviços telegráficos, telefônicos, informático, telemático ou de informação de utilidade pública, pode resultar em uma pena de detenção de um a três anos, fora a multa. E se for caso de calamidade pública, a pena dobra. Baseado nestas informações, necessita-se implantar esse tema nos currículos escolares, bem como oferecer cursos às diferentes comunidades.

Tudo o que se faz na Internet há registro, seja um acesso a site ou uma conversa no chat por aplicativo.

6.1 Projetos Futuros

Atualmente, este trabalho não inclui alguns recursos relevantes que podem existir em futuras implementações e pesquisas. A distribuição do *bots* é de responsabilidade do usuário. O *Botmaster* não é mostrado na simulação, portanto, não há mensagem entre ele e o *bots*. Não existe mecanismo para troca de mensagens entre *bots*. Tmix se aplica apenas ao protocolo TCP. Como resultado, o procedimento para converter o traço do formato em um vetor de conexão só é aplicável a pacotes TCP. É necessário estudar o funcionamento do Tmix no protocolo UDP e os procedimentos de acompanhamento usados com este protocolo. Comparar a plataforma proposta com os trabalhos citados também é desejável em pesquisas futuras.

REFERÊNCIAS

ALLEASY. **Aumento significativo do volume do mundo web**. AllEasy, 2018. Disponível em: <https://www.alleasy.com.br/>. Acesso em: 8 jun. 2020.

ABNT- Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27002 Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro, ABNT, 2005.

BSIGROUP. **ISO/IEC 27001**: gestão de segurança da informação, 2018. Disponível em: <https://www.bsigroup.com/pt-BR/ISO-IEC-27001-Seguranca-da-Informacao/>. Acesso em: 30 jan. 2020.

CARVALHO, L. G. **Segurança de redes**. São Paulo: Ciência Moderna, 2005.

CERT.BR. **Cartilha de segurança para Internet**, 2013. Disponível em: [https:// https://cartilha.cert.br/malware/](https://cartilha.cert.br/malware/). Acesso em: 08 jun. 2020.

CERT.BR. **Recomendações para melhorar o cenário de ataques distribuídos de negação de serviço (DDoS)**, 2016. Disponível em: <https://www.cert.br/docs/whitepapers/ddos/>. Acesso em: 08 jun. 2020.

DHILLON, G. Realizing benefits on an information security program. **Business Process Management Journal**, 10 (3), 260-261, 2004.

OURCODEWORLD. Executando um ataque slowloris genuíno (SlowHTTP) de duração indefinida no Kali Linux, 2018. Disponível em: <https://ourcodeworld.com/articles/read/962/performing-a-genuine-slowloris-attack-slowhttp-of-indefinite-length-in-kali-linux>. Acesso em: 20 jun. 2020.

MIRKOVIC, J. A taxonomy of DDoS attack and DDoS defense mechanisms. **ACM SIGCOMM Computer Communication Review**, 34(2):39–53, 2004.

NSFOCUS. **NSFOCUS Information Technology**, 2013. Disponível em: <https://www.nsfocus.com>. Acesso em: 30 jan. 2020.

STALLINGS, W. **Criptografia e segurança de redes: princípios e práticas**. 4. ed. São Paulo: Prentice-Hall. 2008.

TANENBAUM, A. S. **Sistemas operacionais modernos: segurança**. São Paulo, Pearson Prentice Hall, 3ª edição, 2010.

TORRES, G. **Redes de computadores: segurança**. Rio de Janeiro, Nova Terra, 2013.

TREVENZOLI, A. C. **Perícia forense computacional: ataques, identificação da autoria, leis e medidas preventivas das ameaças sobre o ambiente operacional**. Sorocaba: Faculdades SENAC, 2006.

ZARGAR, S. T. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. **IEEE communications surveys & tutorials**. 15(4):2046–2069, 2013.