MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA
INSTITUTO MILITAR DE ENGENHARIA
CURSO DE GRADUAÇÃO EM ENGENHARIA DA COMPUTAÇÃO

CÉSAR MORAES CONTERNO
NATAN SHALOM FRUTUOSO DE OLIVEIRA

FUNÇÕES DE PROTEÇÃO CONTROLADAS POR UMA CENTRAL DE DETECÇÃO DE PADRÕES MALICIOSOS

RIO DE JANEIRO
2020

CÉSAR MORAES CONTERNO
NATAN SHALOM FRUTUOSO DE OLIVEIRA

FUNÇÕES DE PROTEÇÃO CONTROLADAS POR UMA CENTRAL DE DETECÇÃO DE PADRÕES MALICIOSOS

Projeto de Final de Curso apresentado ao Curso de Graduação em Engenharia da Computação do Instituto Militar de Engenharia, como requisito parcial para a obtenção do título de Bacharel em Engenharia da Computação.

Orientador(es): Sérgio dos Santos Cardoso Silva, M.Sc.
Ronaldo Ribeiro Goldschmidt, D.Sc.

Rio de Janeiro
2020

Conterno, César Moraes; Oliveira, Natan Shalom Frutuoso de.
Funções de proteção controladas por uma central de detecção de padrões maliciosos / César Moraes Conterno e Natan Shalom Frutuoso de Oliveira. – Rio de Janeiro, 2020.
62 f.

Orientador(es): Sérgio dos Santos Cardoso Silva e Ronaldo Ribeiro Goldschmidt.

Projeto de Final de Curso (graduação) – Instituto Militar de Engenharia, Engenharia da Computação, 2020.

1. defesa cibernética. 2. ataque cibernético. 3. malware. i. Silva, Sérgio dos Santos Cardoso (orient.) ii. Goldschmidt, Ronaldo Ribeiro (orient.) iii. Título

CÉSAR MORAES CONTERNO
NATAN SHALOM FRUTUOSO DE OLIVEIRA

Funções de proteção controladas por uma central de detecção de padrões maliciosos

Projeto de Final de Curso apresentado ao Curso de Graduação em Engenharia da Computação do Instituto Militar de Engenharia, como requisito parcial para a obtenção do título de Bacharel em Engenharia da Computação.

Orientador(es): Sérgio dos Santos Cardoso Silva e Ronaldo Ribeiro Goldschmidt.

Aprovado em Rio de Janeiro, 26 de Outubro de 2020, pela seguinte banca examinadora:

Prof. **Sérgio dos Santos Cardoso Silva** - M.Sc. do IME - Presidente

---

Prof. **Ronaldo Ribeiro Goldschmidt** - D.Sc. do IME

Prof. **Paulo Cesar Salgado Vidal** - D.Sc. do IME

Prof. **Luiz Carlos Castro Guedes** - D.Sc. do IME

Rio de Janeiro
2020

Ao Instituto Militar de Engenharia, alicerce de nossa formação e aperfeiçoamento.

AGRADECIMENTOS

Agradecemos a todas as pessoas que nos incentivaram, apoiaram e possibilitaram esta oportunidade de ampliar nossos horizontes. Nossos familiares, amigos e mestres. Em especial aos Professores Orientadores M.Sc. Sérgio dos Santos Cardoso Silva e D.Sc. Ronaldo Ribeiro Goldschmidt, por suas disponibilidade e atenção irrestritas.

Sem publicação, a ciência é morta.
(Gerard Piel)

RESUMO

Em virtude do aumento do uso da rede mundial de computadores, a Internet, e do número de serviços disponibilizados através dela para a sociedade e as entidades públicas e privadas, o ser humano tornou-se mais do que nunca dependente e conectado à rede. Seguindo este fluxo, os criminosos também passaram a atuar no meio virtual, que por ser recente, apresenta muitas fragilidades exploráveis e lucrativas, demandando o desenvolvimento de soluções de proteção e combate ao crime cibernético: a defesa cibernética. Neste contexto, o Exército Brasileiro identificou uma oportunidade e necessidade de desenvolver uma solução própria de defesa cibernética, visando à manutenção da soberania nacional, o que culminou no projeto EB-CyberDef, capitaneado pelo Instituto Militar de Engenharia. O presente projeto final de curso tem por missão desenvolver um dos módulos componentes do EB-CyberDef, que é responsável por receber as informações de ataques cibernéticos contra uma rede identificados por outros módulos e tomar as ações defensivas previstas para mitigar ou anular o efeito do ataque. Para cumprir essa missão foi desenvolvido um protótipo de defesa que, automaticamente, ao receber informações de um ataque, invoca funções de defesa pré-programadas a fim de neutralizar o ataque cibernético. Além da implementação do protótipo automatizado, foi desenvolvida uma ferramenta de interface gráfica com usuário para que o administrador do sistema de defesa possa consultar os tipos de ataques presentes no módulo e adicionar um novo mecanismo de defesa utilizando as funções pré-programadas no módulo sem a necessidade de programar.

Palavras-chave: defesa cibernética. ataque cibernético. malware.

ABSTRACT

Due to the increasing use of the world wide web, the Internet, and the rising number of services made available through it for society and public and private organisations, human beings have become more than ever dependant and connected to the web. Following this flow, criminals have also begun acting in the virtual world, which by being recent, shows many frailties both exploitable and lucrative, demanding the development of solutions to protect from and fight cyber crimes: cyber defense. In this context, the Brazilian Army identified the opportunity and need for the development of its own cyber defense solution, aiming to the preserve the national sovereignty, which culminated in the EB-CyberDef project, led by the Military Institute of Engineering. The present end-of-course project has the mission of developing one of the composing modules of EB-CyberDef, responsible for receiving the information of cyber attacks against a network identified by other modules and take the defensive actions pre-programmed to mitigate or negate the effects of the attack. In order to do so, a defense prototype was developed, capable of, upon receiving information of an attack, automatically invoking pre-programmed defense functions that seek to neutralize the cyber attack. Aside from the implementation of the automated prototype, a graphics user interface was developed for the defense system administrator to be able to consult the attack types present at the module and to add a new defense mechanism using the pre-programmed functions already in the module without the need of programming.

Keywords: cyber defense. malware. cyber attack.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ARP	Address Resolution Protocol
AS	Autonomous System
ASN	Autonomous System Number
DHCP	Dynamic Host Configuration Protocol
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IP	Internet Protocol
MAC	Media Access Control
POP3	Post Office Protocol 3
SFTP	Simple File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TELNET	Teletype Network
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network

SUMÁRIO

1 INTRODUÇÃO

O termo *cibernética* surgiu com o objetivo de resumir a sistematização da comunicação e controle entre animal e máquina. Já a cibernética como ciência surgiu na década de 40, focando no desenvolvimento de técnicas que permitiram resolver o problema de controle e comunicação e acabou por criar profundas mudanças na sociedade, nas relações entre as pessoas e na relação entre humanos e máquinas. No contexto das organizações, fossem públicas ou privadas, se iniciou uma busca pela segurança das informações e novas tecnologias detidas por elas, o que foi intitulado de segurança cibernética (1).

1.1 Motivação

As questões de segurança cibernética estão se tornando uma luta cotidiana por todas as organizações pelo mundo afora, seja por empresas privadas e públicas ou instituições governamentais, militares e acadêmicas. Num mundo onde todos estão conectados e com os dados se tornando o novo petróleo graças ao valor deles, é inquestionável a preocupação de todos pela segurança da informação na internet (2).

É crescente o risco de ameaças direcionadas que focam em espionar ou destruir sistemas de infraestruturas críticas, como bancos de dados do governo (3). Nesse ambiente de fragilidade cibernética surge também a necessidade de soluções na área (3).

Com isso surgiu a necessidade do Governo Brasileiro, por intermédio do Exército Brasileiro, criar um sistema integrado de defesa cibernética próprio, para apoio à detecção e à proteção e defesa de comportamentos maliciosos no tráfego de redes de computadores. O projeto ficou conhecido como EB-CyberDef (4).

Em linhas gerais, o projeto EB-CyberDef consiste em diversos módulos de identificação e detecção de fluxos de dados maliciosos, um módulo de defesa e proteção (que atua sobre os fluxos detectados), um banco de dados que contém, entre outras informações, o histórico de ocorrências e é alimentado e atualizado por todos os módulos do projeto, e um módulo de consultas gerenciais a esse banco de dados.

1.2 Objetivo

Para construir um ambiente de defesa e proteção dos ativos de rede, é preciso entender como são essas ameaças cibernéticas para poder criar procedimentos de neutralização adequados.

O presente projeto tem por finalidade elaborar um módulo de defesa e proteção que será incorporada ao projeto EB-CyberDef. O módulo de Defesa/Proteção irá receber informações de outros módulos e coordenar uma decisão a fim de minimizar ou impedir o ataque sofrido por algum ativo de rede previamente designado. O Módulo de Defesa/Proteção deve procurar evitar que o fluxo normal dos dados na rede seja afetado, mesmo depois das intervenções realizadas com o objetivo de minimizar os ataques sofridos, garantindo a disponibilidade do serviço, a confidencialidade e a integridade dos dados.

1.3 Metodologia

Na fase 1 foi realizado o levantamento dos tipos de ataques cibernéticos e suas características. Para tanto, foi necessário o estudos de taxonomia de ataques a fim de distinguir os diferentes ataques cibernéticos.

Na fase 2 foi definida a arquitetura do módulo de defesa e proteção. Para resolver o problema proposto, foi analisado o sistema em que o módulo foi acoplado e os requisitos do projeto.

Na fase 3 foi construído o módulo de defesa e proteção para os tipos de ataque cibernético escolhidos.

Na fase 4 foi implementada uma estrutura de comunicação de um usuário com o módulo de defesa a fim de verificar seu funcionamento a nível de administrador.

1.4 Estrutura

O capítulo 2 apresenta a fundamentação teórica acerca dos princípios de segurança da informação e os tipos de ataques com exemplos para que se possa classificar os ataques e criar mecanismos de defesa nos ativos a serem protegidos. Já o capítulo 3 descreve o projeto EB-CyberDef, seu objetivo e suas características. O capítulo 4 aborda as características do Módulo de Proteção/Defesa, considerando as tecnologias a serem utilizadas, a arquitetura e sua estrutura de funcionamento. O capitulo 5 apresenta os Estudos de Caso realizados para atestar a usabilidade do protótipo desenvolvido neste projeto. Finalmente, o capítulo 6 apresenta a conclusão do projeto, incluindo os aprendizados adquiridos no desenvolvimento deste projeto.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Princípios da Segurança da Informação

A seguir são apresentados os três princípios da Segurança da Informação, também chamados de tríade CIA (do inglês *Confidentiality*, *Integrity* e *Availability*) (5).

A Confidencialidade trata do acesso à informação, de forma que este princípio é preservado quando somente pessoas autorizadas têm acesso aos dados. Já a Integridade é preservada quando é garantido que a informação não seja modificada de forma ilegítima, isto é, adulterada (5). Por fim, a Disponibilidade deve ser um dos pontos de extrema importância nos mecanismos de defesa e proteção dos ativos de rede, já que sua ausência gera falta de acessibilidade aos dados, que na Internet são extremamente preciosos e custosos (6).

2.2 Taxonomias de Ataques Cibernéticos

Há na literatura diversas abordagens quando o assunto é classificação de ataques cibernéticos (7). Foram exploradas algumas formas de classificação a fim de identificar o ataque cibernético. O objetivo de classificar o ataque cibernético está em facilitar a criação de mecanismos de defesa e analisar suas diversas vertentes. As classificações seguem linhas diversas, algumas com fins acadêmicos e outras com ênfase em aplicações diversas. Serão listadas as taxonomias e abordados alguns ataques e seus exemplos.

2.2.1 Taxonomia Geral de Ataques Cibernéticos

Os ataques podem ser classificadas em 7 tipos distintos (8):

- Externo, geralmente sem envolver tecnologia de acesso às máquinas, fisicamente separado dos computadores, como espionagem visual;
- Uso indevido de hardware, que pode ser passivo, sem dano colateral (imediato), ou ativo, com dano colateral;
- Mascaramento, ao assumir uma identidade legítima indevidamente (como em ataques de playback e spoofing, etc.);

- Programas de Vírus, ao instalar num sistema computacional um software malicioso embutido num arquivo aparentemente inofensivo, que tem a habilidade ainda de se auto-multiplicar na máquina infectada;
- Uso indevido ativo de recursos, que é um mal uso de autoridade concedida (incorretamente) pelo sistema, a alguém que na verdade não deveria ter tal autoridade, e que permite a este usuário alterar o sistema ou seus dados;
- Uso indevido passivo de recursos, que é um mal uso de autoridade concedida (incorretamente) pelo sistema, a alguém que na verdade não deveria ter tal autoridade, e que permite a este usuário apenas realizar a leitura de dados do sistema;
- Uso indevido, que é um mal uso de autoridade concedida legitimamente pelo sistema, a alguém deveria ter tal autoridade, e que permite a este usuário alterar o sistema ou seus dados.

Por outro lado, (9) classifica os incidentes conforme a Figura 1 abaixo.

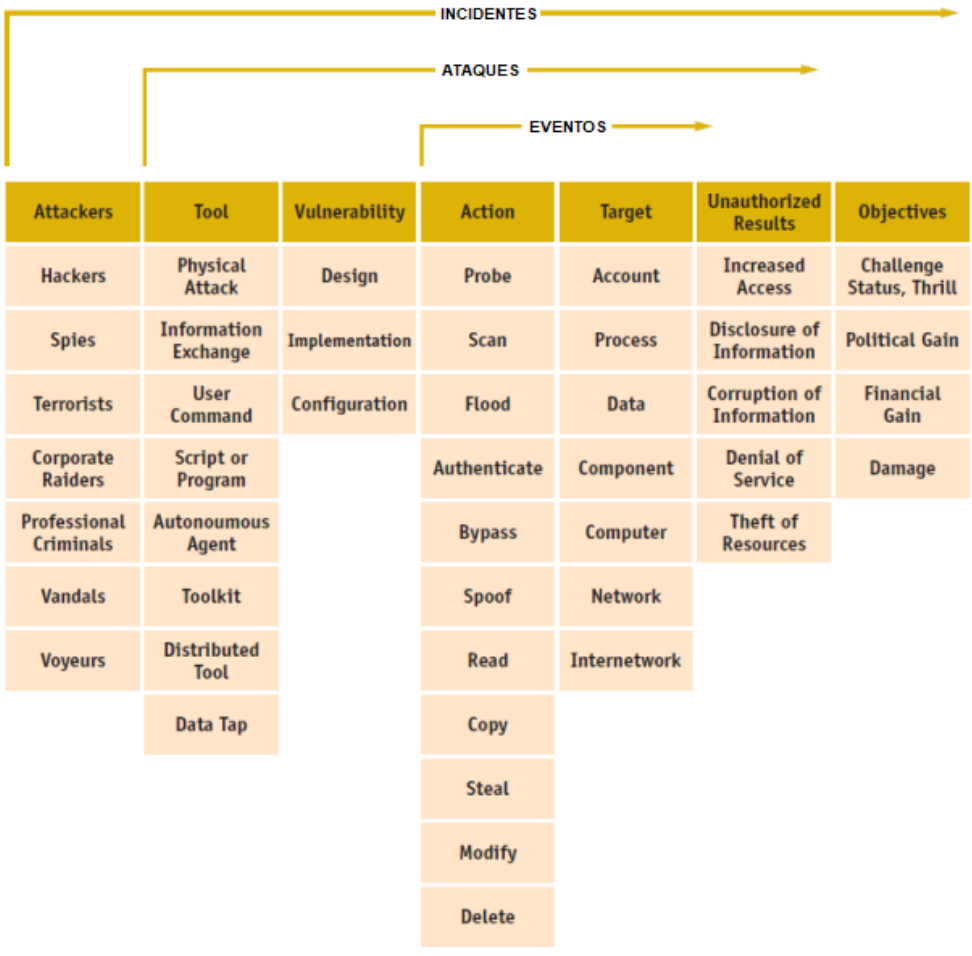

Figura 1 – Taxonomia de Incidentes de Segurança em Linguagem Comum (9)

Com base nas técnicas iniciais do ataque conforme proposto por (10), a taxonomia pode ser dividida em 3 categorias distintas:

- Passar por cima (*bypass*) dos controles projetados, dividindo-se em ataques de senhas, *spoofing* de programas privilegiados ou utilização de autenticação fraca;
- Uso indevido ativo de recursos, que se divide em exploração inadvertida de permissão de escrita ou exaustão de recursos;
- Uso indevido passivo de recursos, que aborda a possibilidade de leitura dos dados e se divide em exploração manual ou busca automática.

2.2.2 Taxonomia por Tipo de Atacante

Uma opção de divisão dos ataques cibernéticos é baseada no acesso inicial do atacante (11).

Um exemplo disso é a matriz de tipos de invasores segundo (12), representada na Tabela 1 a seguir. Nela é classificado o atacante, caso ele tenha direito a iniciar ou usar o programa/informação e se ele tem acesso à máquina/computador.

Tabela 1 – Matriz de Tipos de Invasores

	NÃO tem autorização de uso do recurso de dados ou programa	tem autorização de uso do recurso de dados ou programa
NÃO tem autorização de uso do computador	A - Invasão Externa	
tem autorização de uso do computador	B - Invasão Interna	C - Abuso de autoridade

Na Intrusão/Invasão Externa (caso de interesse deste trabalho), o sujeito tem acesso a alguma máquina ou sistema mas não tem autorização de usar um recurso ou programa nessa máquina. Esse sujeito pode ser dividido em 3 classes: usuário falso, usuário legítimo ou usuário clandestino (11). Um exemplo de ataque de Intrusão e suas consequências na vítima é apresentado a seguir.

Caso de Intrusão - Maroochy Water System (2000)

Em Maroochy Shire, Queensland, Austrália, em 2000, um grupo descontente de ex-funcionários invadiu um sistema de controle de água e inundou os jardins de um hotel e um rio próximo com um milhão de litros de esgoto (3).

2.2.3 Taxonomia por Tipo de Alvo

Diversos ataques têm por alvo uma variedade de tipos de hosts. O alvo visado pelos

atacantes pode ser o sistema operacional, rede, um computador local, informação pessoal de usuário ou uma aplicação (13).

Ataques que alvejam o Sistema Operacional (Kernel/Usuário/Driver) buscam acessar um conjunto de programas com a função de gerenciar os recursos do sistema. Um ataque pode ser feito para atingir vulnerabilidades dentro de um sistema operacional (13).

Um ataque à Rede, que é um grupo de nós interconectados por links que são usados para trocar mensagens entre si, pode obter acesso ao sistema através de uma vulnerabilidade dentro de uma rede ou protocolo de rede (13).

Um ataque Local é focado a um computador ou máquina local de um usuário. Já um ataque contra um Usuário é um ataque para roubar dados pessoais do usuário (13).

Um ataque à Aplicação pode explorar um software específico, um programa de computador, normalmente instalado pelo usuário, com intenção de ajudá-lo a executar uma tarefa específica. A aplicação pode ser do tipo cliente ou do tipo servidor, e esses 2 tipos são alvos dos atacantes cibernéticos (13).

2.2.4 Taxonomia por Tipo de Meio de Ataque

Há diversos meios utilizados pelos atacantes cibernéticos para realizar um ataque. Em geral, diferentes meios buscam explorar fragilidades distintas no alvo. A seguir estão descritos alguns meios de ataques, dentre os quais selecionaram-se 4 a serem tratados pelo módulo de proteção desenvolvido neste trabalho.

2.2.4.1 Denial of Service (DoS)

Esse tipo de ataque cibernético (de Negação de Serviço, em tradução livre) utiliza como princípio a quebra de disponibilidade de um sistema de computação. Ele pode ser utilizado como uma forma de distração para o atacante explorar outras vulnerabilidades do sistema. Em geral, o ataque de DoS parte de diferentes máquinas atacantes, constituindo-se num DoS distribuído ou, em inglês, DDoS (14).

As diferentes seções em que um ataque DDoS pode ser dividido a fim de classificar os tipos de ataque são: a preparação (que consiste nas fases de *recrutamento*, *exploração* e *infecção*), a duração de fato do ataque (fase de *uso*) e o efeito na vítima (15).

Grau de Automação

As 4 primeiras fases podem sem realizadas manualmente, semi-automaticamente ou automaticamente. Ataques manuais só foram realizados nos tempos iniciais do DDoS e, portanto, não serão mais investigados (16).

Ataques totalmente automatizados consistem geralmente em programas de propósito

único, porque o atacante necessita acionar a botnet[1] *somente* durante a primeira fase do ataque, no *recrutamento*. Terminada essa fase, o código original contido nas máquinas infectadas da botnet já tem armazenado o momento de início, o tipo, a duração e o alvo do ataque, possuindo autonomia para completar o ataque DDoS. Ainda assim, é comum para o atacante deixar um *backdoor* aberto para adaptação dos parâmetros do ataque automatizado, caso surja essa necessidade (16).

Ataques semi-automáticos são a vasta maioria atualmente, posto que conjugam a automação em fases mais iterativas (como o *recrutamento*, *exploração* e *infecção*) à liberdade do atacante interferir em quaisquer fases do ataque, adaptando as características do ataque aos problemas encontrados durante a preparação e execução do ataque.

Durante a preparação, seção que engloba as 3 primeiras fases do ataque DDoS, o objetivo do atacante é conseguir gerar uma botnet maior possível, infectando máquinas iniciais, que buscarão elas mesmas infectar outras máquinas, processo que é muito repetitivo.

O atacante utiliza ferramentas automatizadas para essa seção, alterando apenas parâmetros nessas ferramentas quando considerar necessário (alteração manual). Além disso, ao deflagrar o ataque, ele também utiliza ferramentas que automatizam a ativação das máquinas da botnet, mas ele ainda tem a possibilidade de interferir manualmente nas propriedades do ataque.

Dessa forma, o ataque é caracterizado como semi-automático por utilizar os pontos fortes de controlar e executar o ataque ora de forma automatizada e ora de forma manual (16).

Fraqueza Explorada para Negação de Serviço

Primeiramente, serão abordados os ataques *semânticos* (também chamados de ataques *a vulnerabilidade*) os quais exploram um recurso ou uma funcionalidade específica da vítima, ao forçar a vítima a processar cargas excessivas de dados dentro do escopo desse recurso, dessa forma tornando a vítima incapaz de receber novas e (possivelmente) legítimas requisições, esgotando esse recurso (16).

Há também os ataques de *força-bruta* (também chamados de *enchente*) que consistem em esgotar os recursos da vítima ao enviar uma quantidade de pacotes que é maior do que a vítima pode processar. É importante notar que os pacotes enviados para a vítima nesse caso são geralmente disfarçados de pacotes oriundos de usuários legítimos, o que torna a defesa muito mais difícil, porque meramente filtrar pacotes maliciosos bloqueará usuários de fato ao mesmo tempo em que bloqueará o atacante de acessar a rede da vítima (16).

[1] botnet é uma rede de dispositivos conectados à Internet, sejam computadores, smartphones ou dispositivos eletrônicos inteligentes, cada um rodando um bot. A botnet é usada para realizar ataques cibernéticos como DDoS, roubo de dados e envio de spam.

Validade do Endereço de Origem

Em primeiro lugar, considera-se o tipo mais comum: o ataque com *endereço de origem mascarado*, em que o atacante mascara o endereço de origem com um diferente do seu próprio, a fim de evitar responsabilização e detecção. Isso pode ser feito utilizando um IP Gerado aleatoriamente, um IP de sub-rede não-utilizado de uma rede pré-existente ou um IP de usuário legítimo de uma lista previamente (geralmente ilegalmente) coletada (16).

Existem ainda ataques que utilizam o IP da máquina real do *agente* (máquina infectada utilizada pelo atacante para enviar fluxo de dados para o alvo), explorando as vulnerabilidades de máquinas previamente infectadas que somente são acionadas para enviar pacotes pelo mestre (atacante) no momento do ataque. Nesse cenário, a fase de *recrutamento* das máquinas *agentes/escravas* é geralmente realizada muito antes do ataque propriamente dito (16).

Dinâmica de Taxa de Ataque

A maioria dos ataques é de natureza de *taxa constante*, isto é, as máquinas infectadas, ao ser lançado o ataque, enviam fluxos contínuos de pacotes para a vítima, geralmente à maior taxa que seus recursos lhes permitem (16).

Por outro lado, ataques de *taxa variável* buscam esgotar os recursos da vítima ao mesmo tempo em que atrasam ou evitam detecção e resposta. Mecanismos de *taxa crescente* paulatinamente degradam os recursos da vítima, tornando o ataque muito mais difícil de detectar. Por fim, mecanismos de *taxa flutuante* geralmente exploram temporizações de defesa pré-programadas, a fim de evitar e contornar mecanismos de defesa para um ataque de sucesso (16).

Possibilidade de Caracterização

Ao analisar o conteúdo e o cabeçalho dos pacotes de ataque, é possível identificar características compartilhadas ou comuns, tornando o ataque identificável. Ataques caracterizáveis alvejam protocolos ou aplicações específicas na rede da vítima e podem ser divididos em *filtráveis* e *não-filtráveis*.

Ataques *filtráveis* utilizam pacotes mal formados ou pacotes para serviços não-críticos da vítima (que podem ser resolvidos por um firewall) e exemplos são o ataque de inundação UDP e o ataque de inundação de eco de ICMP.

Ataques *não-filtráveis* utilizam pacotes bem formados e alvejam serviços legítimos e críticos da vítima, então realizar filtro irá negar imediatamente serviço tanto para atacantes quanto para clientes legítimos. Ex.: requisições HTTP fazendo enchente num servidor Web ou uma enchente de requisições DNS alvejando um servidor de nomes (16).

Ataques *não-caracterizáveis* almejam consumir os recursos da vítima ao aplicar

vários protocolos e diferentes aplicações simultaneamente, tornando mecanismos de defesa sem ferramentas sofisticadas de caracterização (geralmente custosos e demorados para desenvolver) inúteis. A linha entre ser capaz de caracterizar ou não um ataque é bastante tênue e depende muito da capacidade da vítima de diferenciar e analisar pacotes a fim de identificar com sucesso um ataque (16).

Persistência do Conjunto de Agentes/Máquinas Zumbis

Ataques podem variar na maneira em que máquinas infectadas são acionadas no ataque através do tempo, podendo ser um ataque de *conjunto constante de agentes* ou um ataque de *conjunto variável de agentes*. O primeiro consiste de todas as máquinas sendo acionadas (e possivelmente desacionadas) ao mesmo tempo, mesmo em ataques de pulso, por exemplo. No segundo caso, o atacante divide as máquinas infectadas em diversos grupos, acionando estes grupos em tempos diferentes, tornando rastreamento e detecção mais difíceis, enquanto permite uma taxa razoavelmente constante de ataque à vítima (16).

Tipo de Componente Alvejado na Vítima

É possível diferenciar ataques pelo tipo de componente alvejado na vítima. Ataques a *aplicação* alvejam aplicação(ões) específica(s) na vítima e são razoavelmente difíceis de identificar porque geralmente consistem de um baixo volume de ataque e também permitem que outras aplicações da vítima continuem entregando serviço normal aos clientes (16).

Ataques a *hospedeiro* alvejam a máquina da vítima para desabilitar seu mecanismo de comunicação e buscam derrubar, congelar ou reiniciar o hospedeiro. Um exemplo desse ataque é um ataque TCP SYN. Como o volume de ataque é alto, a detecção é facilitada, porém a defesa sem ajuda externa não é possível. A vítima geralmente pede ajuda de uma máquina de nível mais alto no fluxo da rede, como um firewall de nível mais alto no fluxo da rede (16).

Ataques a *recurso* alvejam recursos críticos específicos para a rede da vítima, geralmente "gargalos". Os pacotes de ataque convergem no "gargalo" e podem divergir após isso. Esse tipo de ataque pode ser evitado ao se replicar serviços críticos e desenhar topologias robustas de rede (16).

Ataques a *rede* procuram consumir completamente a banda da rede do alvo. Esses ataques são facilmente detectados por seu alto volume de pacotes e só podem ser tratados por redes de nível mais alto no fluxo de rede, dado que a rede da vítima não consegue atuar sozinha sobre o ataque (16).

Ataques a *infraestrutura* alvejam serviços críticos para toda a Internet, como o dos servidores de nome de domínio (DNS). Eles podem alvejar máquinas específicas nesses serviços, que os classificariam como ataque a hospedeiro, por exemplo, mas a ideia chave é que o ataque irá desabilitar um serviço que afeta toda a rede mundial de

computadores, demandando esforço coordenado de múltiplos participantes da internet para contra-atacá-los (16).

Impacto na Vítima

Ataques podem, por fim, ser divididos em *disruptivos* e *degradantes*, considerando o impacto na vítima. Ataques *disruptivos* buscam negar completamente o serviço da vítima a seus clientes e podem ser: *auto-recuperáveis*, se a vítima pode recuperar-se automaticamente depois de terminado o ataque; *humanamente-recuperáveis*, se com a intervenção necessária de um humano (para uma reinicialização ou reconfiguração, por exemplo) a vítima é recuperada; e *não-recuperáveis* se o ataque inflige dano permanente ao hardware da vítima (16).

Ataques *degradantes*, por outro lado, procuram consumir os recursos da vítima apenas parcialmente, tornando a detecção virtualmente impossível. Eles também forçam a vítima a gastar seus recursos de forma crescente, possivelmente negando serviço durante horários de pico para clientes legítimos, fazendo que estes fujam para um competidor ou forçando a vítima a aumentar custos para fornecer seu serviço de maneira aceitável (16).

2.2.4.2 Trojan

É um tipo de código ou software malicioso que parece legítimo, mas pode assumir um caráter indesejado no computador. Um Trojan é projetado para causar alguma ação prejudicial aos seus dados ou rede. A seguir são apresentados 2 casos de ataques reais deste tipo, visando ressaltar a relevância atual de proteger-se contra ele.

Caso Real 1 - Explosão de Gasoduto Siberiano (1982)

É o primeiro incidente conhecido de segurança cibernética, ocorrido em 1982 (3). Os Estados Unidos adicionaram um Trojan ao software de controle de gasoduto da União Soviética (17).

O software infectado da tubulação funcionava com as bombas, turbinas e válvulas e foi programado para funcionar mal, redefinindo as velocidades da bomba e as configurações das válvulas para produzir pressões muito além daquelas aceitáveis pelas juntas e soldas da tubulação (17). O resultado foi a explosão não nuclear e o fogo mais monumentais já vistos do espaço (17).

Caso Real 2 - Aeroporto de Worcester, Massachusetts (1997)

Em 1997, um hacker não identificado invadiu um sistema de controle das comunicações de tráfego aéreo no aeroporto de Worcester, Massachusetts, causando um congelamento no sistema e desativando o sistema telefônico no aeroporto por seis horas (3).

2.2.4.3 Vírus

Um vírus é um tipo de malware de computador que, quando executado, se replica modificando outros programas de computador. A seguir é apresentado um caso real deste tipo de ataque, ressaltando a importância de proteger-se contra ele e seus possíveis danos.

Caso Real - CSX Corporation (2003)

Um vírus chamado Sobig, que era enviado através de anexo de e-mail, foi identificado por ter desligado o sistema de sinalização dos trens na Flórida, EUA, prejudicando o sistema de transporte do país (3).

2.2.4.4 Worm

Um worm é um malware de computador que se auto-replica, a fim de se espalhar para outros computadores. Geralmente, usa uma rede de computadores para se espalhar. O objetivo do golpe, em geral, é roubar dados do usuário ou de empresas. A seguir é apresentado um caso real deste tipo de ataque, destacando seus efeitos sobre a vítima e a importância de desenvolver medidas defensivas contra ele.

Caso Real - Flame (2012)

Pesquisadores descobriram à época um malware, chamado *Flame* operando no Irã, Líbano, Síria, Sudão, Cisjordânia e outros lugares no Oriente Médio e Norte da África por pelo menos dois anos.

A análise inicial indicou que esse software foi projetado principalmente para espionar os usuários de computadores infectados e roubar dados, incluindo documentos, conversas gravadas e pressionamentos de teclas.

Ele também abriu um *backdoor* para sistemas infectados para permitir que os atacantes ajustassem o kit de ferramentas e adicionassem novas funcionalidades.

2.2.4.5 Intrusão

Uma intrusão de rede é qualquer atividade não-autorizada a uma rede de computadores. Para se detectar uma Intrusão, é necessário que o time de segurança da rede compreenda bem o regime do fluxo de dados normal da rede e do comportamento do ataque do tipo Intrusão. Este tipo de ataque em geral causa: consumo de recursos da rede que deveriam ser empregados para outros fins, o que pode gerar uma falta de recursos para o desempenho adequado do sistema para clientes ou usuários legítimos, ou ainda onerar a instituição responsável pela manutenção do sistema, pois ela terá que elevar sua capacidade de recursos para manter o nível de serviço ao cliente adequado, gerando um custo adicional desnecessário; ameaça à segurança da rede e de seus dados.

2.2.4.6 Eavesdropping

É uma técnica de violação de confidencialidade sem interferência no conteúdo da informação, em que a interceptação é feita em tempo real de forma não autorizada em uma comunicação privada. Pode ser em uma ligação telefônica, e-mail ou videoconferência. Ao contrário do ataque Man-in-Middle, Eavesdropping somente monitora a informação sendo transmitida (14).

2.2.5 Taxonomia de Ataques Web

Com o objetivo de extrair informações para construir sistemas Web mais seguros, a taxonomia de ataques Web pode ser dimensionada de forma que cada aspecto pode ser representado como uma característica particular do ataque. É uma classificação de natureza horizontal, dividindo-se nos seguintes eixos (18) :

- Ponto de entrada - Por onde o ataque penetra
- Vulnerabilidade - Tipo de fraqueza que pode ser explorada num sistema permitindo ação não-autorizada
- Escopo - Impacto do ataque no servidor Web
- Alvos - O objetivo do ataque

2.2.6 Taxonomia por Método de Disseminação

Podemos classificar os ataques cibernéticos quanto ao método de disseminação em maciço ou direcionado (19).

Ataque Maciço

É um tipo de ataque sem uma vítima específica, sua propagação é de forma difusa e sem foco, buscando causar dano sem discriminar tipo ou localização do alvo. Seu objetivo pode ser o de danificar o funcionamento de computadores, excluindo arquivos importantes ou apenas corrompê-los, aparentando um caso de mero erro humano (19).

Um exemplo é o vírus Melissa, um tipo de vírus que se dissemina através dos serviços de email. O usuário recebe um email com arquivo anexo .doc. Quando o usuário abre o anexo, o vírus executa e procura pela lista de emails dos contatos do usuário e envia emails maliciosos para essa lista de forma automática. Além disso, ele modifica arquivos com extensão .doc com frases soltas (20).

Ataque Direcionado

Os ataques direcionados são projetados para ações específicas para invadir um sistema de informação de uma organização específica. Seus alvos geralmente são grandes empresas, indústrias ou organizações governamentais (19).

Um exemplo de ataque direcionado foi o Spyware Flame, que tinha por objetivo infectar os sistemas operacionais de controle da indústria de petróleo com objetivo de espionagem, coletando informações do computador, gravando áudios, capturando telas, detectando atividades do teclado e o tráfego de rede. Ele também podia gravar conversas por videoconferência e controlar o bluetooth de aparelhos infectados para obter informações a respeito de outros aparelhos que também tivessem conexão via bluetooth (3).

O Stuxnet é um worm implementado para controlar as centrífugas de enriquecimento de urânio iranianas e danificá-las. Em sistemas operacionais Windows e MAC OS ele se mostrava totalmente inofensivo, já no sistema operacional SCADA da Siemens, utilizado nas usinas, ele se desenvolvia. O worm tinha duas funções, sendo a primeira delas fazer com que as centrífugas iranianas girassem 40% mais rapidamente por quinze minutos, o que causava danos nas centrífugas. A segunda função inicialmente gravava dados telemétricos de uma típica operação normal das centrífugas nucleares, assim os operadores não desconfiavam do evento por ver os dados em condições normais, e as centrífugas se danificavam com o tempo (3).

2.2.7 Taxonomia por Forma de Ataque

Observando as formas de ataques cibernéticos, podemos subdividi-los em 5 diferentes grupos, sendo: ataque remoto, ataque do lado do cliente, método da força bruta, sequestro de IP e vírus/ bugs de software (21).

Ataque Remoto

Trata-se de dados sendo capturados da rede da vítima, por meio de redes infectadas que estão conectadas à rede-alvo, causando grandes danos à rede e aos hosts da vítima (21).

Ataque no Lado do cliente

Através de uma interação direta do atacante com o usuário, o atacante força o usuário a inserir dados pessoais através de recurso falso, que pode ser uma página ou programa falso. Também podem ser utilizados mensagens de email ou formulários (21).

Método da Força Bruta

Usar todos os métodos de penetração ao mesmo tempo, esperando que um deles permita acesso privilegiado à vítima (21).

Sequestro de IP

Uma forma de ataque na qual um usuário autorizado consegue acesso a uma conexão legítima de outro cliente na rede. Após obter a sessão, o invasor pode ler e editar pacotes de dados transmitidos, além de enviar suas próprias mensagens para o destinatário (21).

Vírus e Bugs de software

Através do vírus, o atacante pode obter não só informações da vítima, mas exercer controle total sobre o dispositivo dela. Os programas de vírus podem entrar através de vulnerabilidades na rede, erros de software, entre outras formas (21).

2.3 Técnicas de Defesa

Apresentam-se a seguir os mecanismos de defesa que podem ser aplicados aos tipos de ataque que foram desenvolvidos no presente trabalho: DDoS, Trojan, Worm e Intrusão.

2.3.1 Mecanismo de Defesa Contra Ataque Distribuído de Negação de Serviço (DDoS)

Existem muitos fatores a serem considerados quando se analisam mecanismos de defesa contra DDoS e o desafio que eles buscam superar. Primeiro e mais importante, é o fato de a internet ser distribuída, então um esforço coordenado para proteger uma vítima de ataque DDoS geralmente necessitará da intervenção de vários atores que podem não estar interessados em ajudar ou não têm os meios para fazê-lo. Então, esses atores, enquanto não diretamente afetados, ainda têm que gastar recursos (econômicos, sociais) mas não se beneficiam do investimento.

Ademais, há a falta de informação detalhada sobre ataques, em grande parte porque não existem agentes capazes de fazê-lo e aqueles que têm a capacidade podem manter os dados privativos para fins econômicos.

Existe a dificuldade de comparar desempenhos para diferentes mecanismos, pois não existem critérios bem estabelecidos para avaliação e comparação. Finalmente, testes em larga escala são de difícil realização, dado que simulações de "problema real" requereriam um grande esforço de toda a internet (16).

Para caracterizar mecanismos de defesa contra DDoS, serão analisados Nível de Atividade, Grau de Cooperação e Localidade de Emprego (16).

Nível de Atividade

Aqui, dividem-se os mecanismos existentes em *preventivos* e *responsivos*. Mecanis-

mos *preventivos* buscam tornar ataques DDoS virtualmente impossíveis ou permitir que serviços continuem a ser entregues a clientes legítimos mesmo que um ataque contra a rede da vítima esteja ocorrendo. Por outro lado, mecanismos *responsivos* procuram aliviar o dano de um ataque na vítima depois que o ataque é lançado e faz isso identificando, caracterizando e empregando ações para minimizar ou acabar com os efeitos do ataque nos serviços da vítima (16).

Grau de Cooperação

Mecanismos *autônomos* atuam somente internamente às redes em que se situam, então mesmo que o Sistema de defesa realize ações de maneira distribuída, ele terá cobertura apenas na rede em que os serviços são processados; exemplos são *firewalls* e sistemas de detecção de intrusos.

Mecanismos *cooperativos* podem detectar e responder a ataques autonomamente ao mesmo tempo em que podem recorrer a entidades fora da rede da vítima a fim de empregar suas medidas de defesa; um exemplo é o controle de congestionamento agregado (ACC), que é capaz de limitar a taxa de tráfego não somente nos roteadores da vítima como também em roteadores de fora da rede da vítima.

Mecanismos *independentes* não podem identificar e responder a ataques localmente, necessitando do uso de dispositivos de rede para coletar dados de múltiplas redes, localidades ou entidades para poder agir sobre ataques em curso, muitas vezes requerendo modificação em software de clientes; exemplos são mecanismos de rastreamento e serviços de sobrescrita segura (16).

Localidade de Emprego

Mecanismos de *Rede de Vítima* atuam somente no alcance interno da rede da vítima e são os mais comumente aplicados, pois a vítima é a parte mais interessada na solução. Geralmente, esses apenas aliviam os ataques, mas não os superam completamente; exemplos são mecanismos de contabilidade de recursos e de segurança de protocolos.

Mecanismos de *Rede Intermediária* fazem uso do poder dos hospedeiros da internet, ao contatar provedores de internet e agir na infraestrutura *deles* para defender-se de ataques DDoS; exemplos são técnicas de rastrear e repelir o atacante.

Mecanismos de *Rede Fonte* procuram fazer máquinas inutilizáveis por atacantes potenciais atuando, por exemplo, em máquinas pessoais, através de software ou hardware que impeça a máquina de se tornar máquina-zumbi numa botnet, etc.

Embora o conceito para esses mecanismos de rede de vítima, intermediária e fonte seja válido, isto é, ser capaz de garantir que clientes da rede não serão parte de um ataque DDoS, não fica claro quem deveria arcar com os custos de tal implementação (usuário final, provedores de serviço de internet ou possíveis vítimas, como empresas e organizações) e

por isso a aderência a esse tipo de mecanismo é escarça (16).

2.3.2 Mecanismo de Defesa Contra Ataque Trojan

Devido aos ataques do tipo Trojan terem propósitos razoavelmente diversos, como controle da máquina infectada (backdoor), aproveitar-se da fraqueza de um software específico (exploit) ou impedir o descobrimento de outros malwares já presentes na máquina (rootkit), a principal técnica para impedir danos colaterais a máquinas conectadas à mesma rede da máquina infectada é desconectar da rede esta máquina afetada, isolando-a das suas vizinhas para evitar uma contaminação maior.

Após o isolamento, é necessário informar o administrador da rede e realizar uma varredura local no HD da máquina infectada para identificar e neutralizar o Trojan presente.

Apesar de ataques Trojan geralmente não tentarem se injetar em outros arquivos da máquina infectada ou propagar-se, alguns Trojan apresentam essa característica; além disso, comumente o Trojan está combinado com outros tipos de malwares que buscaram se auto-replicar (como Worms) dentro da máquina e para outras máquinas da mesma rede.

Ademais, vários Trojans utilizam-se de interações externas por um controlador para atuar na máquina infectada, tornando o corte do acesso à rede imprescindível do ponto de vista da segurança da rede atacada.

2.3.3 Mecanismo de Defesa Contra Ataque Worm

A principal característica do Worm enquanto malware é sua auto-replicação, o que torna o corte da máquina afetada de sua rede o principal mecanismo de defesa.

A forma dos Worms causarem danos pode ser avaliada pela presença ou não de "carga"(do inglês *payload*) que este malware carrega. Mesmo sem carga, Worms causam problemas de tráfego de rede, ocupando consideravelmente a banda e impedindo uma comunicação e uso eficiente da rede para seus fins originais; por outro lado, com carga, eles carregam outros malwares como vírus ou Trojans, estes sim, capazes de alterar o funcionamento normal das máquinas infectadas, roubar ou apagar dados, instalar um *backdoor*, etc.

Dada a natureza dual dos Worms de causarem dano tanto à máquina infectada, quanto à rede a que a máquina está conectada, faz-se necessário primariamente isolar a(s) máquina(s) infectada(s) para evitar a propagação do Worm e depois informar ao administrador da rede para que se realize a varredura local em cada máquina para remover o Worm e quaisquer outros malwares embutidos nele.

Outras medidas de segurança contra Worms, porém preventivas são:

- listas de controle de acesso em roteadores e switches, limitando o tráfego de entrada e saída de uma rede a endereços conhecidos, semelhante a um firewall;
- filtros de pacotes (uma forma de firewall de rede), que inspeciona pacotes trocados entre máquinas, checando se o pacote está de acordo com um conjunto de regras pré-estabelecidas para permitir ou não sua transmissão;
- daemons empacotadores de TCP, softwares de sistema que funcionam sem a interação de um usuário, disponíveis em máquinas que utilizam sistemas operacionais baseados em Unix e permitem que respostas de *queries* de endereços de sub-redes IP e nomes sejam tokenizadas para controle de acesso; e
- rotas nulas (ou buracos negros), que são rotas de rede na tabela de roteamento que levam a lugar nenhum, descartando pacotes e tráfego malicioso sem avisar ao remetente que o pacote foi rejeitado, o que é especialmente útil contra Worms e ataques DDoS em massa.

2.3.4 Mecanismo de Defesa Contra Ataque de Intrusão

Para defender-se de ataques de Intrusão, existem 2 tipos de sistema: de Detecção, que é reativo perante ataques em tempo real; e de Prevenção, preventivos contra ataques futuros.

Sistemas de Prevenção atuam na tentativa de impedir que ataques sequer passem da camada de proteção da rede ou da máquina através de:

- bloqueio de roteamento assimétrico, que permite que uma máquina seja acessada dentro de uma rede por caminhos diversos e não um único;
- controle do buffer, reduzindo seu limite máximo e instalando uma checagem de lógica de borda, identificando código executável e strings de URL longas antes de serem escritas no buffer;
- verificação de entrada (*input*) e checagem de caracteres de *backtracking* em CGIs (Common Gateway Interfaces), evitando a modificação de caminhos de arquivos, tornando arquivos que deveriam ser inacessíveis externamente, acessíveis; etc.

Já os Sistemas de Detecção podem ser classificados em modelos baseados em assinatura e baseados em anomalia de comportamento. Os primeiros herdam essa nomenclatura de softwares anti-vírus, que estudam malwares ou comportamentos já conhecidos e geram padrões previsíveis que conseguem eficientemente detectar e neutralizar os malwares antigos, mas não malwares novos.

Já os últimos, que geralmente se utilizam de aprendizado de máquina, têm como principal foco identificar novos ataques ao monitorar o tráfego da rede ou máquina usual e ser capaz de perceber perturbações no funcionamento nesse funcionamento normal, identificando uma Intrusão, ataques DDoS em masa, etc.

Após identificar uma Intrusão, é necessário bloquear o acesso à máquina infectada, o acesso do usuário que está acessando a máquina e do IP usado para acessar a máquina externamente. Então é necessário notificar o dono da conta de usuário que foi utilizada e o administrador da rede, para que seja realizada uma varredura na máquina afetada e exclusão de quaisquer malwares que facilitaram ou permitiram o acesso do Intruso à máquina e à rede administradas.

3 CONTEXTUALIZAÇÃO: PROJETO EB-CYBERDEF

A fim de se fazer frente à crescente demanda de segurança no ambiente cibernético, e à singularidade desse setor, o Exército adotou estratégias para estruturar a cibernética nas Forças Armadas. Com base nessa estratégia, o Instituto Militar de Engenharia iniciou o projeto EB-CyberDef.

3.1 Introdução ao EB-CyberDef

O EB-CyberDef é um projeto da seção de Engenharia de Computação do Instituto Militar de Engenharia e que tem como objetivo geral desenvolver um protótipo de um ambiente computacional para apoio à detecção e ao combate de comportamentos maliciosos no tráfego de redes de computadores.

O projeto se justifica por conta da Estratégia Nacional de Defesa, no qual incumbiu ao Exército Brasileiro (EB) de liderar o processo de estruturação do setor cibernético. O projeto se apresenta como uma solução própria a ameaças que podem comprometer de forma significativa o funcionamento do ambiente cibernético do Estado brasileiro e suas instituições.

Com os dados coletados de diversas fontes, informações obtidas e resultados gerados, o sistema permitirá uma resposta a altura de seus desafios de forma remota e automatizada, o que é fundamental nesse ambiente, já que muitos dados são de caráter sensível e com alta criticidade. Outro ponto a levantar, é que o produto proporcionará um acompanhamento de desempenho das soluções implementadas, possibilitando análises e estudos futuros do ambiente monitorado.

Por conta de suas características, este sistema está alinhado com os objetivos traçados pelo Livro Branco de Defesa Nacional, o mais completo e acabado documento acerca das atividades de defesa do Brasil. Nele é mencionado a preocupação da Defesa Nacional com as áreas de infraestrutura sensíveis e os ativos de rede por conta de ameaças cibernéticas (22).

3.2 Arquitetura do Ambiente

A arquitetura do EB-CyberDef é dividida em módulos, cada qual com sua função perante o funcionamento integral do sistema, conforme ilustrado na Figura 2 e descritos a seguir:

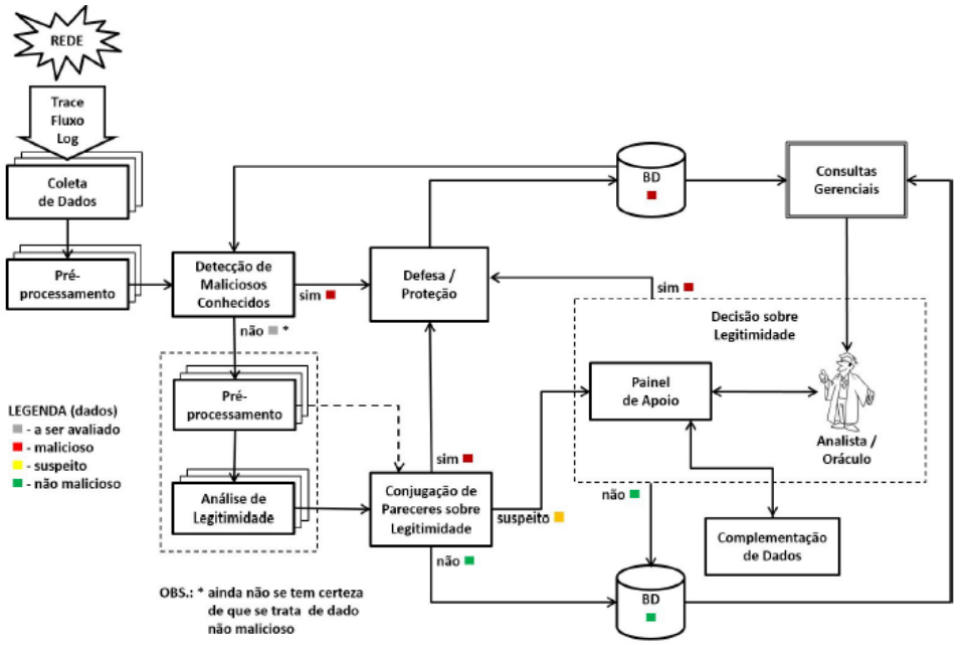

Figura 2 – Visão Macro-Funcional da Arquitetura da Fase de Produção/Operação do EB-CyberDef.

3.2.1 Coleta de Dados

O módulo Coleta de Dados tem a função de realizar a coleta dos dados de rede de fontes variadas e em formatos também variados.

3.2.2 Pré-processamento

Este módulo compreende operações de tratamento e padronização dos dados de redes coletados, a fim de serem processados pelo sistema.

3.2.3 Detecção de Dados Maliciosos Conhecidos

Módulo com a finalidade de identificação dos dados maliciosos conhecidos com base no banco de dados do sistema (marcados como vermelhos, conforme figura 2) através de sua assinatura, isto é, características do código malicioso que podem ser percebidas sem a necessidade de mecanismos baseados em Inteligência Artificial e Aprendizado de Máquina.

Este módulo, portanto, utiliza a técnica de detecção baseada em assinatura para realizar uma primeira filtragem dos logs coletados e pré-processados.

3.2.4 Defesa/Proteção

Assim que determinado fluxo de dados é classificado como malicioso, este módulo deve acionar medidas de defesa e/ou proteção para minimizar o problema. Tais medidas são denominadas Funções de Proteção. Estas funções podem ser especializadas para diversos ativos de rede.

Um exemplo de medida preventiva que pode ser tomada é a adição de uma regra de tráfego de rede com o objetivo de impedir um fluxo malicioso. Conforme Visão Macro-Funcional da arquitetura, exposta na figura 2, verifica-se que os logs de entrada para este módulo podem ser direcionados a ele em três momentos distintos do processo, após cada uma das etapas responsáveis por decidir se o fluxo é malicioso ou não.

Após as medidas de proteção e defesa feitas por esse módulo, ele enviará um relatório padronizado informando as medidas tomadas e dados do ataque a fim de registrar esse evento no banco de dados para futuras análises por esse sistema.

Este módulo é o foco do presente trabalho, que será detalhado no próximo capítulo e tem como objetivo o desenvolvimento de:

- Funções de Proteção contra ataques cibernéticos;
- Uma interface gráfica para usuários poderem adicionar novos tipos de mecanismo de defesa contra ataques cibernéticos, através da seleção de quais das Funções de Proteção já existentes no módulo ele deseja que sejam invocadas quando um ataque do tipo que está sendo cadastrado no sistema for deflagrado e
- Envio de logs de ataques tratados pelo módulo para o Banco de Dados do sistema.

3.2.5 Pré-processamento e Análise de Legitimidade

Este módulo compreende a execução de algoritmos inteligentes de análise de legitimidade dos dados, responsáveis por avaliar os padrões de dados, procurando classificá-los quanto ao seu potencial em se constituir um padrão malicioso. Ou seja, ele utiliza a técnica de detecção baseada no comportamento da aplicação, tendo como entrada os logs marcados como a ser avaliados (cinzas, aqueles que em um primeiro momento não foram identificados como maliciosos, de acordo com a Figura 2) pelo módulo Detecção de Maliciosos Conhecidos (23).

Vale lembrar que a execução dos algoritmos de análise de legitimidade pode ser precedida de diferentes processamentos que irão adequar (pré-processar) os dados conforme a necessidade de cada algoritmo (23).

3.2.6 Conjugação de Pareceres sobre Legitimidade

Este módulo tem como propósito integrar os pareceres emitidos pelos algoritmos de legitimidade executados pelo módulo anterior, sobre os fluxos que ainda não se tem certeza de que se trata de dado não malicioso, a fim de obter um parecer único que reflita a impressão do sistema quanto à classificação do padrão analisado.

Com base na classificação dos dados eles poderão ser enviados para o módulo Defesa/Proteção a fim de se mitigar uma ameaça.

3.2.7 Painel de Apoio

O módulo de Painel de Apoio tem como objetivo apresentar a um analista humano (oráculo) os resultados da conjugação de pareceres de legitimidade dos fluxos marcados como suspeitos (24).

Com os dados apresentados, o oráculo deverá opinar sobre a situação do padrão apresentado e indicar como tal padrão deverá ser tratado pelo sistema. É requisito da interface a ser desenvolvida apresentar também características (destes tráfegos suspeitos) consideradas relevantes ao processo decisório do analista, servindo como um auxílio à sua tomada de decisão. Além disso, caso o oráculo deseje, o painel de apoio poderá apresentar, com o mesmo intuito de ajudar no julgamento, dados externos ao sistema (24).

3.2.8 Complementação de Dados

Módulo com a finalidade de coletar dados externos ao sistema para serem apresentados pelo Painel de Apoio. Esse dados externos servirão para subsidiar decisões do oráculo de forma complementar.

O módulo deve realizar buscas inteligentes para que o resultado possa ser útil para futuras decisões do oráculo.

3.2.9 Consultas Gerenciais

Este módulo compreende a exibição de relatórios e consultas gerenciais sobre o comportamento do sistema, permitindo monitorar a qualidade dos resultados encontrados e assim facilitar um eventual ajuste dos parâmetros do sistema a ser realizado na fase de experimentação/configuração.

4 MÓDULO DEFESA/PROTEÇÃO

Nesta seção serão descritas a modelagem e a implementação do módulo desenvolvidas no presente trabalho. Inicialmente serão apresentados os objetivos do módulo, posteriormente as arquiteturas e tecnologias empregadas, e por fim, o protótipo construído.

4.1 Objetivo

O objetivo do módulo de defesa e proteção é dar uma resposta aos relatos de ameaças que o EB-CyberDef irá receber, seja através de alertas, de notificações ou mesmo com bloqueios de tráfego.

As atividades e eventos do módulo são as seguintes, conforme apresentadas na figura 3:

1. Receber parâmetros de um ataque identificado por qualquer um dos 3 módulos de alimentação do módulo de Defesa/Proteção;
2. Acionar funções de contra-ataque do módulo de Defesa/Proteção, que serão empregadas de acordo com o tipo de ataque identificado pelo módulo de Defesa/Proteção;
3. Enviar um registro das medidas tomadas, identificando o tipo de tráfego malicioso e ações tomadas, ao banco de dados do sistema;

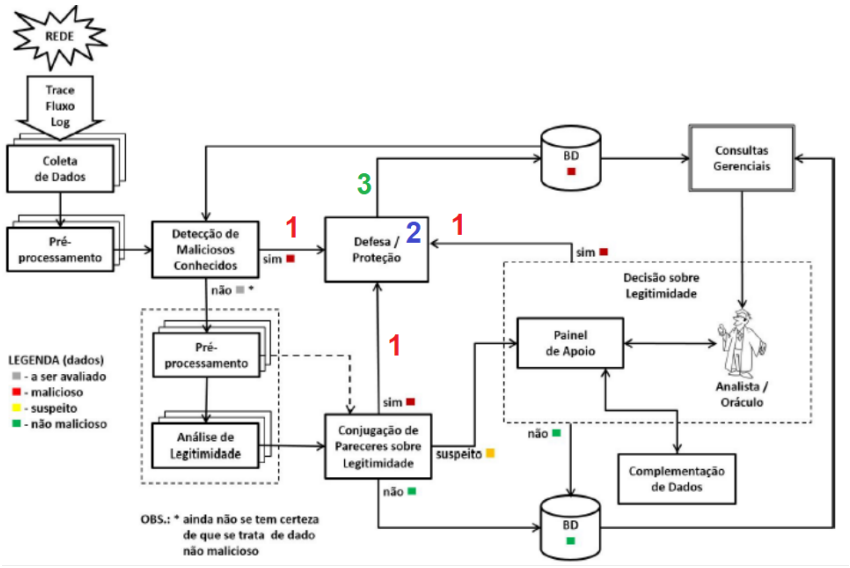

Figura 3 – Visão do Fluxo do Módulo de Defesa/Proteção do EB-CyberDef.

A estrutura interna do módulo pode ser resumida na figura 4, em que há diversas funções de proteção, e a combinação deles gera o mecanismo de defesa para cada tipo de ataque.

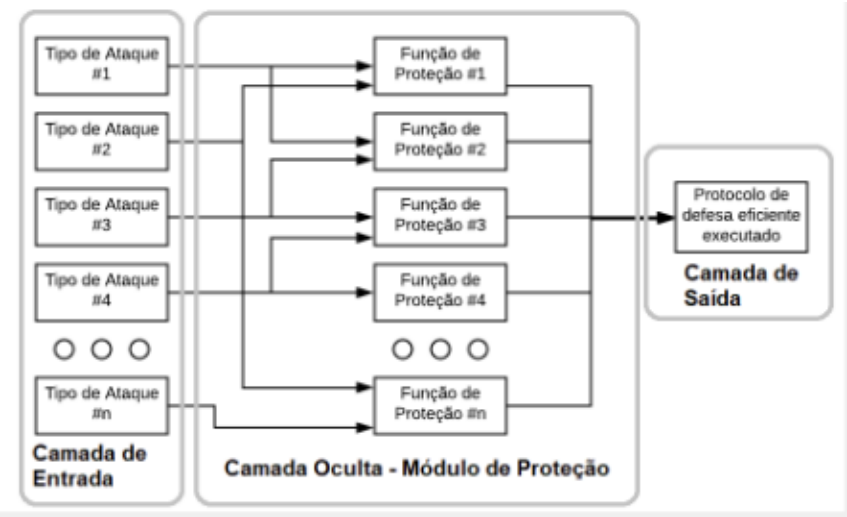

Figura 4 – Funções de Proteção

4.1.1 Esquema de Funcionamento

O funcionamento do módulo se baseia em receber uma requisição dos outros módulos, enviar comandos necessários para máquinas espalhadas na rede afetada e máquinas no domínio de ação do Sistema (como roteadores e switches externos à rede afetada), emitir notificações diversas aos devidos stakeholders do ataque e por fim retornar para o Sistema um relatório padronizado das ações realizadas.

Por enquanto não foi definida a interface de comunicação dos módulos, logo foi padronizada uma interface do módulo interna ao Sistema da seguinte forma para fins de implementação, apresentada na Figura 5:

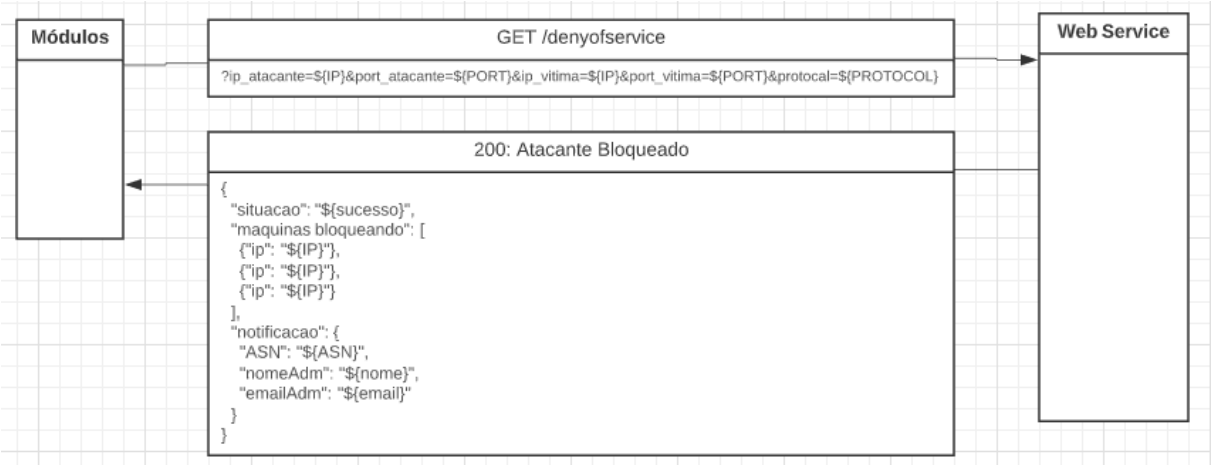

Figura 5 – Interface Interna ao Sistema do Módulo de Defesa/Proteção

Os módulos responsáveis por decidir quando um fluxo é malicioso enviam uma requisição /GET para a API Web Service do módulo de Defesa e Proteção, especificando o tipo de ataque que foi identificado e os dados do ataque, conforme apresentado no bloco *GET /denyofservice* na Figura 5. A API irá processar os dados, podendo ter que consultar ou não APIs externas, e retornará um resposta com o corpo da mensagem no formato JSON contendo dados especificando quais máquinas receberam comandos para bloquear o ataque e dados das notificações realizadas pelo Módulo Defesa/Proteção conforme bloco *200: Atacante Bloqueado* na Figura 5 acima.

4.2 Características

Como o Módulo de Defesa/Proteção está inserido no Sistema EBCyberDef, ele deverá se comunicar com outros módulos do sistema.

Para isso verificou-se a arquitetura utilizada no Sistema para que seu acoplamento dentro dele fosse feito da forma mais ajustada possível.

Além disso, o módulo foi dividido em duas partes, o back-end, com a estrutura da API que se comunicará com os outros módulos e o Banco de Dados e o front-end, com uma interface para o administrador do Sistema poder interagir com o módulo Defesa/Proteção de forma independente dos outros módulos.

4.2.1 Arquitetura

O projeto EB-CyberDef utiliza o modelo de arquitetura de microsserviços com interface RESTFUL. O modelo da arquitetura de microsserviços se baseia em dividir um único software em partes pequenas independentes que se conectam de acordo com o projeto do software (25).

Internamente, a fim de padronizar o fluxo de dados no Web Service, o módulo foi construído de acordo com a arquitetura MVC (26), a fim de separar a interface de comunicação das regras de negócio. Dessa forma, o módulo pode reutilizar funções em mais de um tipo de requisição.

4.3 Tecnologias Empregadas

Com base nos requisitos do projeto, foram definidas tecnologias a serem empregadas na construção do sistema visando ao seu adequado funcionamento.

4.3.1 Linguagem de Programação

Por não ter um conjunto de requisitos pré-definidos em seu início, variando com o transcorrer de seu desenvolvimento, foi necessário escolher uma linguagem que pudesse se adequar com os diversos cenários que os desenvolvedores fossem enfrentar. Assim, foi escolhida a linguagem Javascript (JS), que é de tipo multiparadigma, facilitando o desenvolvimento do projeto de acordo com as demandas que surgiram.

Dessa forma, o código tem características de natureza procedural, orientada a objeto e funcional, senda este última a mais utilizada. As razões de se escolher JS foi por esta ser uma linguagem de programação robusta de alto nível, dinâmica, interpretada e não tipada, adequada para programação funcional (27).

4.3.2 Node.js

NodeJs é um ambiente Javascript no lado do servidor (28). Ele é implementado em C e C++, com foco no desempenho, sendo baseado no modelo de eventos de I/O assíncrono (29).

Com este ambiente, é possível criar aplicações com a linguagem Javascript no lado do servidor, que é muito útil para o presente projeto.

4.3.3 RDAP

O Protocolo de Acesso a Dados de Registro (RDAP na sigla em inglês) é um protocolo de redes desenvolvido pela IETF em 2015 e é utilizado para investigar dados de registro relevantes de recursos da Internet como nomes de domínio, endereços de IP e Números de Sistemas Autônomos (ASN). Apresenta-se como sucessor do WHOIS, que meramente recupera texto bruto, enquanto o RDAP entrega os dados num formato JSON legível (para máquinas) e padronizado (30).

No presente projeto, utilizou-se a API fornecida pelo site https://registro.br/rdap/ (31). Com ele, foram coletadas informações a respeito do IP úteis para o projeto, como o ASN, o email do administrador e seu nome, além de outras informações de rede relevantes.

4.3.4 Traceroute

O comando traceroute tenta rastrear a rota da origem até o destino especificado (referência). Essa função é de extrema importância para o módulo, já que ele e a vítima estão geograficamente separados e as informações que são recebidas do atacante se resumem a IP, PORT e protocolo utilizado, que não são suficientes para saber qual máquina deverá executar uma ação de defesa contra o ataque.

Há a necessidade de se descobrir por onde os pacotes de ataque transitaram para minimizar o número de máquinas a serem designadas para bloquear possíveis tráfegos. A fim de suprir essa necessidade o comando traceroute é utilizado no módulo, facilitando a designação das máquinas gerenciáveis para possíveis bloqueios.

4.3.5 SSH

O protocolo SSH é um protocolo de rede que permite acessar e enviar comandos para máquinas remotas pela internet. Para o Módulo de Defesa/Proteção essa função é fundamental, já que a defesa efetiva se resume a enviar comandos de bloqueio de tráfego de pacote para máquinas remotas.

O módulo utiliza um pacote para utilizar o protocolo SSH para comunicação entre as máquinas gerenciáveis, chamado *simple-ssh*.

4.3.6 IPTABLES

A fim de criar regras de tráfego de rede, utilizou-se o Iptables, por conter um conjunto de características que facilitam futuras adequações para outros tipos de programas de bloqueio de rede.

O Iptables será usado para configurar as tabelas de regras de filtro de pacotes IP no kernel do Linux. Para a criação das tabelas, seguiu-se o seguinte padrão, apresentado na Figura 6:

```
var SSH = require('simple-ssh');
const bloqueioTrafego = (host, user, pass, ip_atacante, ip_vitima,
    port_atacante=3000, port_vitima=3000, protocolo=icmp) => {
    var ssh = new SSH({
        host: host,
        user: user,
        pass: pass
    });
    ssh.exec(`sudo iptables -A FORWARD -s ${ip_atacante} --sport ${
        port_atacante} --dport ${port_vitima} -d ${ip_vitima} -j -p ${
        protocolo} DROP`, {
        pty: true,
        out: console.log.bind(console)
    }).start();
}
```

Figura 6 – Padrão para criação de Tabelas

4.4 Protótipo

O protótipo do módulo se divide em duas partes, o back-end, contendo a API que irá se comunicar com os outros módulos do EB-CyberDef e executará as funções principais, e o Front-end, contendo a interface gráfica com o administrador do módulo, através de um chatbot em uma plataforma de bate-papo.

4.4.1 Back-end

A estrutura do back-end é definida por uma API Web Service responsável por estabelecer a comunicação do Módulo de Defesa/Proteção e os outros módulos do sistema EB-CyberDef, utilizando o protocolo HTTP.

O módulo recebe requisições /GET para cada tipo de ataque, com seus devidos parâmetros e a resposta é enviada no formato JSON, padronizada, independente do tipo

de ataque, informando quais providências foram tomadas, assim como o status indicando se o ataque foi ou não neutralizado.

Para que a defesa seja realizada, essa parte do módulo realiza consulta na API do https://registro.br/rdap/ (31) a fim de coletar informações dos IPs fornecidos, como o ASN deles, para que seja resgatado outros dados como nome e e-mail do administrador do AS. Tudo isso é feito de acordo com o tipo de ataque.

No back-end há também disponível uma lista de máquinas gerenciáveis para que o módulo possa enviar comandos de inclusão de regras de firewall para essas máquinas. Esse envio é feito através de comandos SSH para cada máquina que esteja em uma área que possa surtir algum efeito na defesa do ataque, como estar no mesmo AS que a vítima, ou próximo do atacante, e as regras de bloqueio são feitas de acordo com cada tipo de ataque.

De acordo com o tipo de ataque, se faz necessário informar por e-mail o administrador do AS ou a própria vítima sobre o ocorrido para que se tome alguma providência, assim, o back-end do módulo também envia e-mails padronizados por tipo de ataque para o devido destinatário.

Após a realização de todas essas etapas, há também um envio de um relatório padronizado para o administrador do EB-CyberDef do ocorrido e de todas as ações realizadas por este módulo, para que o mesmo tenha ciência dos fatos ocorridos em tempo real e tomar alguma providência.

Por fim, o módulo envia um resposta com as ações tomadas para que o EB-CyberDef prossiga nas suas ações de encerramento da neutralização do ataque.

4.4.1.1 Interfaces de Entrada e Saída do Sistema

Por conta da estruturação do Sistema EB-CyberDef, as interfaces de entrada e saída precisam ter uma estrutura padronizada para que haja uma comunicação eficaz entre o módulo de Defesa/Proteção e os outros módulos do sistema, de forma que o módulo de Defesa/Proteção funcione de forma independente deles.

A fim de facilitar a modularidade da interface de entrada e saída, possibilitando futuras especializações para cada tipo de ataque, o protótipo terá quatro interfaces distintas de acesso para ativar cada um de seus mecanismos de defesa. São estas:

- /api/denyofservice
- /api/intrusao
- /api/worm
- /api/trojan

4.4.2 Front-end

No front-end do módulo foi construído um chatbot de comunicação através do Telegram. Com ele, o usuário tem a possibilidade de realizar interações com o back-end do módulo, a fim de criar novas defesas e ver seu funcionamento.

Primeiramente, o usuário irá se deparar com o login, o qual solicita a senha de acesso, para que apenas usuários possuidores da senha possam interagir com o Bot.

Após ter a senha validada, o usuário irá receber um menu com diversas opções no formato de botões.

No botão "Voltar", o usuário retorna no login inicial, solicitando novamente a senha de acesso.

No botão "Nova Defesa", o usuário irá responder um questionário a fim de criar uma nova defesa para o Módulo de Defesa/Proteção. Se o nome da defesa for de alguma defesa já criada anteriormente, a última defesa sobrescreverá a anterior.

No botão "Testar Defesa", o usuário escolherá qual tipo de defesa irá usar e colocará os parâmetros necessários para a realização da defesa. Com isso o Bot irá enviar ao back-end uma solicitação /GET e receberá a resposta no chat com o relatório da defesa. As verificações de validação dos dados não serão feitas pelo Bot, e sim pelo back-end do módulo.

No botão "Mostrar Defesas", o usuário receberá uma lista das defesas criadas através do Bot e as que o módulo já tinha.

No botão de "Status", o usuário poderá verificar se o back-end da aplicação está online ou offline.

4.4.3 Tipos de ataque tratados

Visando à facilitação do desenvolvimento completo do presente trabalho, que teve por objetivo apresentar um protótipo do Módulo de Defesa/Proteção do Projeto EB-CyberDef, foram selecionados 4 tipos de ataque com implementação de defesa mais simples dentre os pesquisados, contemplando o tratamento de requisições dos seguintes tipos: DoS - ICMP Flood, Intrusão, Trojan e Worm.

DoS - ICMP flood

Como explicado na fundamentação teórica, esse ataque se baseia em um volume muito grande de pacotes ICMP com destino à vítima.

Implementação

O protótipo se resumiu a identificar o Sistema Autônomo (AS, na sigla em inglês)

do atacante, para bloquear o ataque ICMP o mais próximo possível do atacante. Para isso, o protótipo segue o fluxo de ações ilustrado na Figura 7 e descrito a seguir.

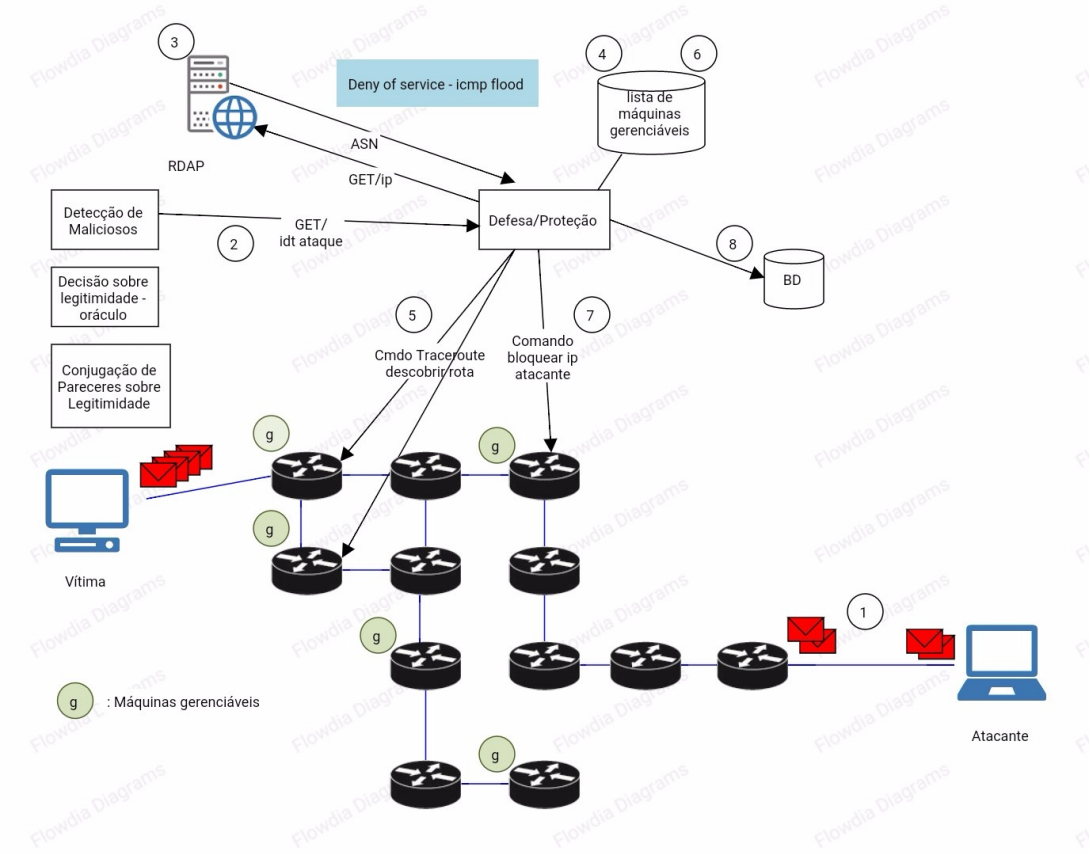

Figura 7 – Ataque DoS - ICMP flood

1. Deflagração do ataque DoS;
2. Máquina sendo afetada pelo DoS e módulo de defesa recebendo o aviso de ataque;
3. API envia uma requisição /Get para a API RDAP do registro.br (31) com IP do atacante para obter informações de redes próximas;
4. API busca no banco quais máquinas dessas redes próximas da vítima nas quais ela tem acesso como administrador para enviar comandos remotos;
5. API envia comando remoto para essas máquinas, a fim de descobrir a rota do atacante;
6. API busca no banco uma máquina que esteja na rota mais próxima do atacante;
7. Enviar comando de bloqueio do IP do atacante;
8. Enviar uma resposta à central do EBCyberDef com o detalhamento da defesa;

Intrusão

Com base na fundamentação teórica, existem duas formas de se defender de um ataque de intrusão, através da detecção ou da prevenção. Após a identificação do ataque, é necessário realizar os seguintes passos:

- bloquear o acesso à máquina infectada;
- bloquear o acesso do usuário que está acessando a máquina;
- bloquear o IP do Atacante;
- notificar o dono da conta de acesso;
- notificar o administrador da rede;

Implementação

O protótipo recebe uma requisição /GET com os seguintes dados: IP e porta da máquina infectada, conta do usuario infectado e seu e-mail. Com esses dados, a API seguirá o seguinte fluxo de atividades:

1. verificar se o IP e a porta são válidos;
2. verificar se o IP é público;
3. buscar a rede onde o IP se encontra;
4. buscar as máquinas gerenciáveis na rede;
5. enviar comando de bloqueio do IP para as máquinas gerenciáveis encontradas;
6. enviar e-mail para o dono da conta infectada;

Trojan

A defesa nesse tipo de ataque se resume a bloquear a máquina e solicitar ao administrador que faça uma varredura nela, a fim de neutralizar o malware.

Implementação

O protótipo recebe uma requisição /GET com os seguintes dados: IP e porta da máquina infectada, conta do usuário infectado e seu e-mail. Com esses dados, a API seguirá o seguinte fluxo de atividades:

1. verificar se o IP e a porta são válidos;
2. verificar se o IP é público;

3. buscar a rede onde o IP se encontra;
4. buscar as máquinas gerenciáveis na rede;
5. enviar comando de bloqueio do IP para as máquinas gerenciáveis encontradas;
6. enviar e-mail para o dono da conta infectada;

Worm

Com essa ameaça, o protótipo irá informar o usuário da máquina infectada e o administrador de rede para que desative a máquina da rede e realize a neutralização do malware de forma offline.

Implementação

O protótipo recebe uma requisição /GET com os seguintes dados: IP da máquina infectada, conta do usuário infectado e seu e-mail. Com esses dados, a API seguirá o seguinte fluxo de atividades:

1. verificar se o IP e a porta são válidos;
2. verificar se o IP é público;
3. enviar e-mail para o dono da conta infectada;

4.4.4 Ilustração do Funcionamento Real do Sistema

Para registrar neste documento escrito o funcionamento real do Módulo de Defesa/Proteção do Projeto, será apresentada a seguir uma sequência de figuras relativas ao procedimento realizado no sistema ao receber um ataque do tipo DoS. Os outros tipos de mecanismos de defesa para outros ataques deflagram ações do Módulo de Defesa/Proteção semelhantes às ações DoS e não serão apresentados neste documento a fim de evitar excesso de dados com pouca informação adicional.

Inicialmente, o Módulo de Defesa/Proteção recebe uma notificação de um ataque DoS oriunda de algum dos módulos do EB-CyberDef responsáveis por identificar os ataques. Para fins desta representação, fez-se o envio de uma notificação de exemplo manualmente, enviando os dados necessários para a correta defesa ser executada para o endpoint /api/denyofservice da API do Módulo de Defesa/Proteção, o que está ilustrado na Figura 8.

O Módulo de Defesa/Proteção invoca as funções pré-definidas para tratamento do ataque DoS, como inclusão na tabela de IPs de uma ordem para barrar o tráfego de rede vindo do IP do atacante (Figura 9) e notificar o administrador da rede do IP da vítima (Figura 10) sobre o ataque sofrido na rede administrada.

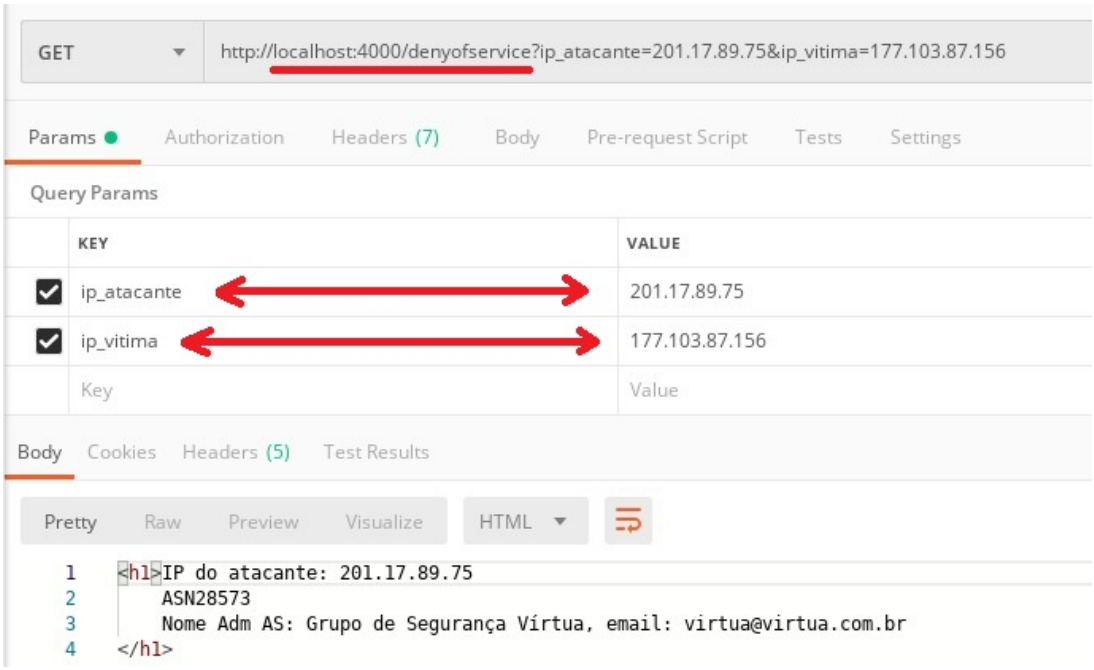

Figura 8 – Notificação de ataque DoS em curso enviada ao Módulo de Defesa/Proteção

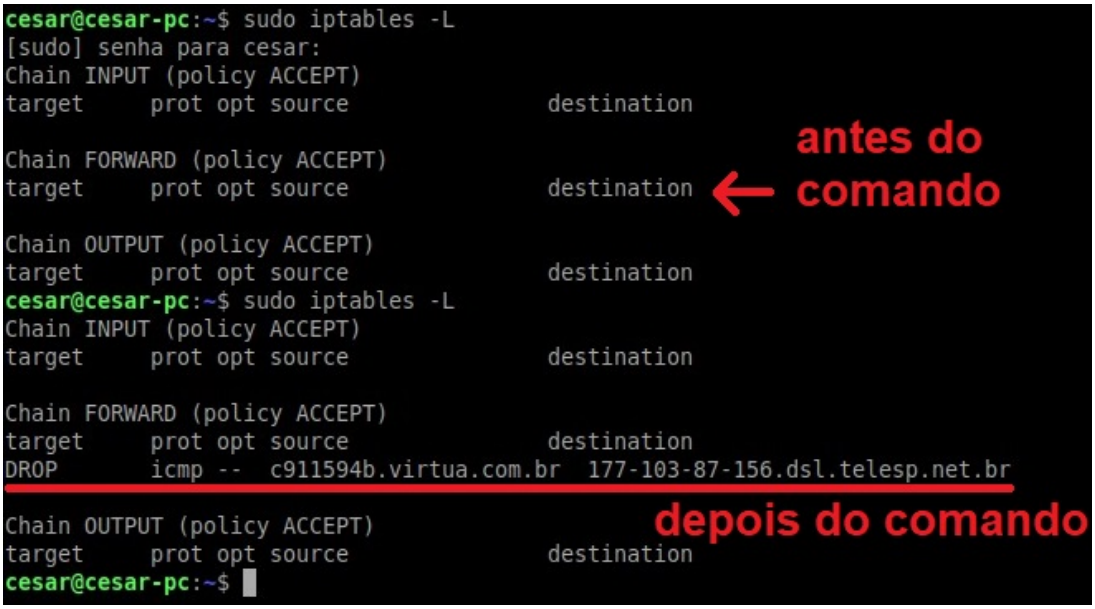

Figura 9 – Inclusão na Tabela de Roteamento de instrução para bloquear IP do Atacante

Por fim, o Módulo de Defesa/Proteção gera automaticamente um relatório de ataque tratado e o envia para o chatbot do Módulo via aplicativo Telegram, para que o administrador do Módulo possa ter o log dos ataques já tratados para fins estátisticos e de análise posterior do desempenho do sistema. Esta notificação está representada na Figura 11.

Figura 10 – Notificação de ataque DoS enviada ao administrador da rede da vítima

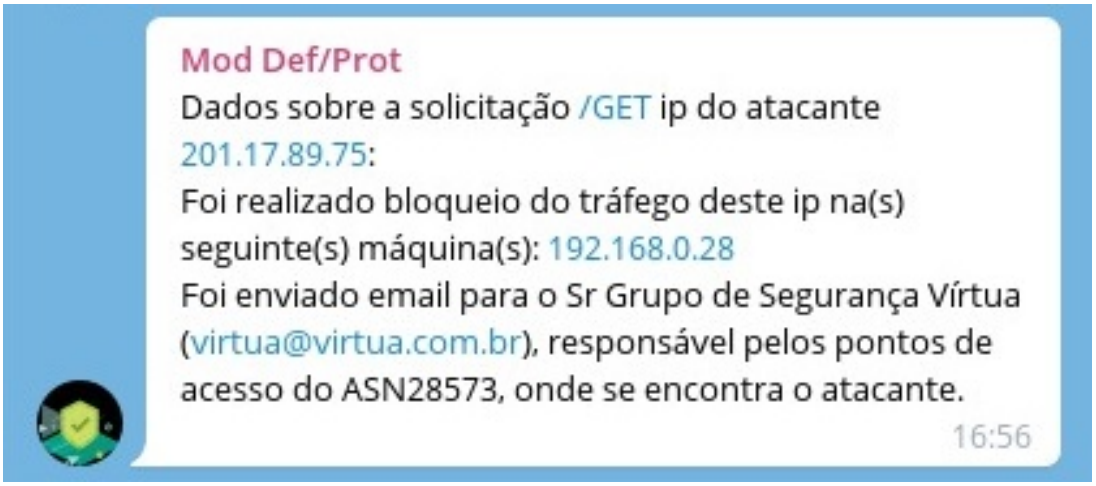

Figura 11 – Notificação de ataque DoS tratado pelo Módulo de Defesa/Proteção enviada ao Telegram para log

4.4.5 Interface Gráfica de Usuário do Módulo de Defesa/Proteção

A fim de facilitar a consulta de mecanismos de defesa já cadastrados no módulo e a adição de novos mecanismos a partir das funções de proteção já codificadas no sistema, foi desenvolvida uma interface gráfica de usuário. O modelo escolhido foi através da ferramenta Telegram, criando-se um chat-bot.

Este bot permite um login remoto e criptografado dos usuários com permissão de administrador do módulo e interações de Consulta e Adição de Novo Mecanismo de Defesa. A tela inicial permite ao usuário fornecer seu nome de login e sua senha, somente, como

mostrado na Figura 12.

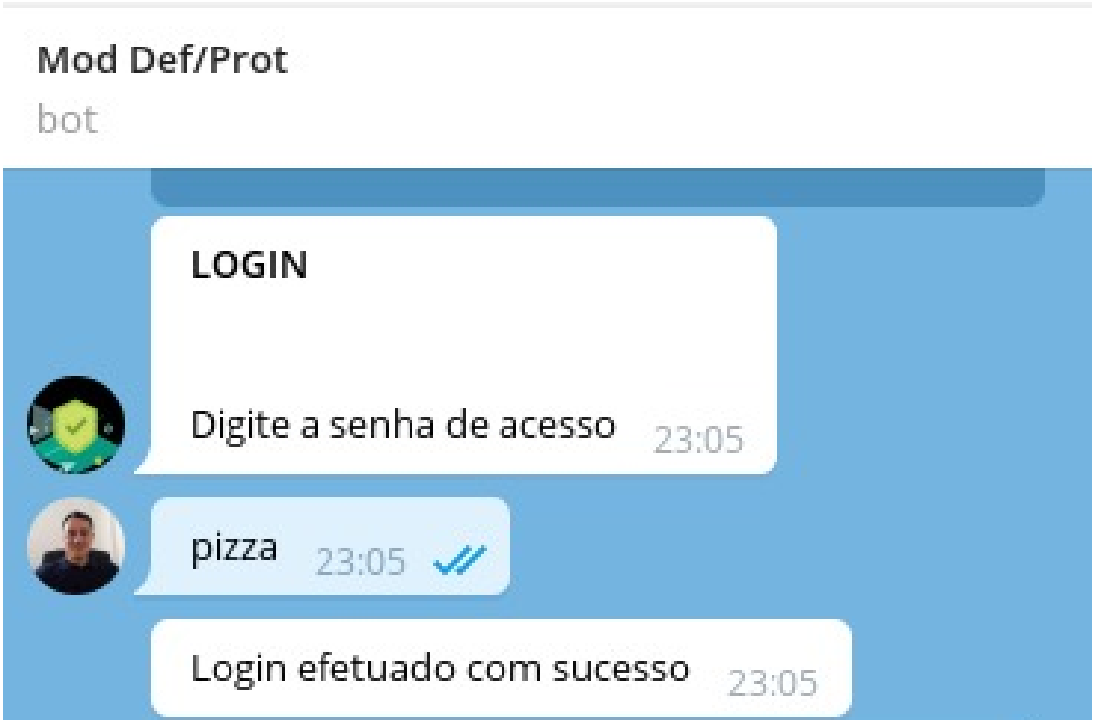

Figura 12 – Tela inicial do chat-bot no Telegram

Após o login, o usuário chega à tela do menu principal, onde tem as opções de visualizar mecanismos cadastrados, adicionar novo mecanismo, verificar o funcionamento de um mecanismo e verificar o status da API, como apresentado na Figura 13 a seguir.

Figura 13 – Tela inicial do chat-bot no Telegram

5 ESTUDOS DE CASO

A construção da API de Defesa/Proteção só se mostra completa após sua verificação em ambientes controlados, obtendo a formalização e execução de testes de rede, comprovando o nível de eficiência do programa.

A seguir, são expostas as diversas situações às quais o módulo foi submetido e alguns comentários a respeito delas.

5.1 Caso 1 - Tipo de Ataque: Negação de Serviço

5.1.1 Entradas recebidas

- IP da máquina do atacante
- IP da máquina da vítima

5.1.2 Ações tomadas pelo Módulo

Primeiramente o módulo verificará se os parâmetros são válidos, ou seja, se o IP do atacante e o IP da vítima estão no formato IPV4 e se eles são públicos, já que a princípio não faria sentido receber endereços privados. Caso não passe nessa verificação, o administrador irá receber uma mensagem por Telegram sobre a inconsistência dos dados.

Após a validação dos parâmetros, o Módulo tem por objetivo obter IPs de máquinas gerenciáveis próximas do atacante, a fim de bloquear o ataque mais próximo do atacante e minimizar os danos colaterais à rede de computadores. Duas estratégias verificadas para tal ação são:

- encontrar a rota que o atacante está utilizando para enviar os pacotes ICMP e encontrar máquinas gerenciáveis nessa rota o mais próximo possível do atacante para efetuar o bloqueio do fluxo malicioso e
- encontrar o AS do atacante e bloquear o fluxo malicioso que esteja saindo desse AS por todas as máquinas gerenciáveis desse Sistema Autônomo.

O módulo seguiu a segunda abordagem, buscando encontrar o ASN no qual o atacante se encontra, o nome e e-mail do administrador desse AS. Assim, ele lista as máquinas gerenciáveis e envia um comando de bloqueio do fluxo malicioso para essas máquinas. Juntamente a isso, o administrador do AS recebe um e-mail informando o ocorrido, a fim de adicionar esforços para minimizar a ação da negação de serviço.

5.1.3 Saídas do módulo

O administrador do EB-CyberDef receberá uma mensagem no Telegram com um relatório resumido das ações tomadas pelo Módulo de Defesa/Proteção, contendo dados das entradas e do tipo de ataque, lista das máquinas que receberam comando de bloqueio de tráfego e dados das notificações realizadas pelo e-mail e pelo Telegram.

Por fim, o módulo enviará uma mensagem para o EB-CyberDef com os dados das ações executadas.

5.2 Caso 2 - Tipo de Ataque: Trojan

5.2.1 Entradas recebidas

- IP da máquina da vítima do Trojan
- nome de usuário da vitima
- e-mail da vitima

5.2.2 Ações tomadas pelo Módulo

O módulo verificará se os parâmetros são válidos, ou seja, se o IP da vítima está no formato IPV4 e se ele é público, já que a princípio não faria sentido receber endereço privado. Verifica-se também se o e-mail encontra-se no formato usual. Se ele não estiver, esse parâmetro não será utilizado para fins de notificação. Caso não passe em alguma dessas verificações, o administrador irá receber uma mensagem por Telegram sobre a inconsistência dos dados.

Após a etapa de validação, a vítima receberá um e-mail com as instruções necessárias para eliminar o Trojan da máquina.

5.2.3 Saídas do módulo

O administrador do EB-CyberDef receberá uma mensagem no Telegram com um relatório resumido das ações tomadas pelo Módulo de Defesa/Proteção, contendo dados das entradas e do tipo de ataque e dados das notificações realizadas pelo e-mail e pelo Telegram.

Por fim, o módulo enviará uma mensagem para o EB-CyberDef com os dados das ações executadas.

5.3 Caso 3 - Ataque criado pelo usuário

5.3.1 Entradas recebidas

- nome do ataque
- IP da máquina da vítima
- IP da máquina do atacante
- nome de usuário vítima
- e-mail da vítima

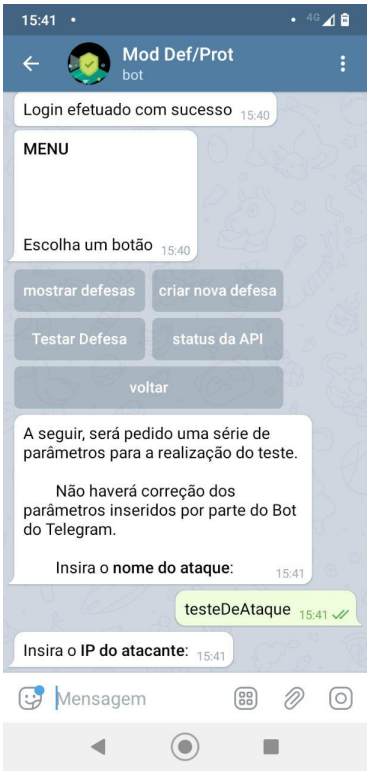

Figura 14 – Opção de teste de ataque do chatBot

5.3.2 Ações tomadas pelo Módulo

O módulo verificará se os parâmetros são válidos, ou seja, se o IP da vítima e o IP do atacante estão no formato IPV4 e se eles são públicos. Verifica-se também se o e-mail encontra-se no formato usual. Caso não passe nessa verificação, o administrador irá receber uma mensagem por Telegram sobre a inconsistência dos dados.

De acordo com o ataque criado, há um tipo de bloqueio a ser feito, podendo ser próximo ao atacante, próximo à vítima, em ambos os casos ou nenhum bloqueio a ser feito. O módulo seguirá o bloqueio de acordo com o ataque escolhido pelo usuário. Ele fará isso buscando o ASN do IP de interesse a fim de verificar quais são as máquinas gerenciáveis nesse AS.

Listando as máquinas gerenciáveis o módulo envia um comando de bloqueio do fluxo malicioso para essas máquinas.

Para o e-mail fornecido é enviada uma mensagem com informações que futuramente podem ser preenchidas com dados a fim de proteger a vítima desse ataque de características personalizadas.

5.3.3 Saídas do módulo

O administrador do EB-CyberDef e o usuário que está interagindo com o Módulo receberão uma mensagem no Telegram com um relatório resumido das ações tomadas pelo Módulo de Defesa/Proteção, contendo dados das entradas e do tipo de ataque e dados das notificações realizadas pelo e-mail e pelo Telegram.

Por fim, o módulo enviará uma mensagem para o EB-CyberDef com os dados das ações executadas.

5.4 Caso 4 - Tipo de Ataque: Worm

5.4.1 Entradas recebidas

- e-mail da vitima
- IP da máquina da vítima
- nome de usuário da vitima

5.4.2 Ações tomadas pelo Módulo

O módulo verificará se os parâmetros são válidos, ou seja, se o IP da vítima está no formato IPV4, verificando se foram passados quatro octetos separados por pontos,

em que cada octeto tenha um numero entre 0 e 255. Após isso é verificado se o IP é público. Verifica-se também se o e-mail encontra-se no formato usual. Se ele não estiver, esse parâmetro não será utilizado para fins de notificação. Caso não passe em alguma dessas verificações, o administrador irá receber uma mensagem no grupo do Telegram sobre a inconsistência dos dados.

Após a etapa de validação, a vítima do worm receberá um e-mail com as instruções necessárias para eliminar o malware da máquina.

5.4.3 Saídas do módulo

O administrador do EB-CyberDef receberá uma mensagem no Telegram com um relatório resumido das ações tomadas pelo Módulo de Defesa/Proteção, contendo dados das entradas e do tipo de ataque e dados das notificações realizadas pelo e-mail e pelo Telegram.

Por fim, o módulo enviará uma mensagem para o EB-CyberDef com os dados das ações executadas.

5.5 Caso 5 - Tipo de Ataque: Intrusão

5.5.1 Entradas recebidas

- e-mail da vítima
- nome de usuário da vítima
- IP da máquina da vítima

5.5.2 Ações tomadas pelo Módulo

Primeiramente o módulo verificará se os parâmetros são válidos, ou seja, se o IP do atacante e o IP da vítima estão no formato IPV4 e se eles são públicos, como nos outros ataques. Caso não passe nessa verificação, o administrador irá receber uma mensagem por Telegram sobre a inconsistência dos dados e o módulo encerrará as medidas de defesa.

Após a validação dos parâmetros, o Módulo tem por objetivo obter IPs de máquinas gerenciáveis próximas da vítima, a fim de bloquear o ataque o mais próximo possível do atacante e minimizar os danos colaterais à rede de computadores.

Com isso ele irá encontrar o ASN no qual o atacante está localizado. Depois ele lista as máquinas gerenciáveis do AS e envia um comando de bloqueio do fluxo malicioso para essas máquinas. Juntamente a isso, o usuário recebe um e-mail informando do ocorrido, a fim de adicionar esforços para minimizar a ação da intrusão.

5.5.3 Saídas do módulo

O administrador do EB-CyberDef receberá uma mensagem no Telegram com um relatório resumido das ações tomadas pelo Módulo de Defesa/Proteção, contendo dados das entradas, lista das máquinas que receberam comando de bloqueio de tráfego e dados das notificações realizadas pelo e-mail e pelo Telegram.

Por fim, o módulo enviará uma mensagem para o EB-CyberDef com os dados das ações executadas.

6 CONCLUSÃO

O número de ataques cibernéticos contra organizações de todo o mundo, em especial os órgãos públicos, vem aumentando ano após ano e intensificam-se com a presença de eventos internacionais.

O presente projeto surgiu da necessidade de construção do sistema EBCyberDef a fim de dar apoio à detecção, a proteção e a defesa contra os comportamentos maliciosos em ativos do governo.

Assim, o objetivo do trabalho era elaborar o módulo de defesa e proteção desse sistema a fim de minimizar ou impedir os ataques sofridos por algum ativo de rede em conjunto com os outros módulos. O objetivo do projeto foi alcançado de acordo com as condições estabelecidas pelo projeto, de ser uma prova de conceito para a consolidação do EBCyberDef.

Vale lembrar que a construção do Módulo de Defesa/Proteção no EB-CyberDef proposta pelo presente projeto é fundamental para a eficácia do mesmo, já que ele é o vetor de proteção desse grande projeto estratégico.

O EB-CyberDef atuará neste ambiente com diversos sensores espalhados nas redes nacionais a fim de se antecipar aos possíveis ataques ou diminuir os danos de um ataque a um ponto sensível nas redes nacionais.

Como vetor de proteção, o módulo, seguindo comandos recebidos pelos outros módulos, irá mitigar os efeitos dos ataques através de diversos modos de operação, tomando o máximo de cuidado para não causar danos colaterais no ambiente cibernético.

O estudo de caso mostrou que quanto mais tipos de ataque cibernético forem estudados e implementados, mais funções de proteção serão criados e mais eficaz ele se torna diante de novas ameaças.

Durante a execução do projeto foram verificados vários pontos importantes para registrar para que projetos semelhantes possam ter mais chance de sucesso com os seus envolvidos.

O presente projeto envolveu assuntos de cibernética, ainda não tratados no curso de graduação até o recebimento do projeto, em fevereiro do ano de desenvolvimento do projeto. Este assunto traz consigo conhecimentos e vocabulário bastante particulares, o que fez com que as revisões bibliográficas fossem bastante custosas por parte dos integrantes do projeto, já que eles não possuíam familiaridade com o assunto.

Levando em consideração que o tema do projeto a ser desenvolvido foi recebido no

ano de seu desenvolvimento, uma sugestão para minimizar esse obstáculo seria receber os temas do Projeto Final de Curso (PFC) em anos anteriores, dando mais tempo para os alunos se familiarizarem com assuntos específicos dos seus temas de PFC.

Sobre os processos de gestão de projetos, alguns pontos importantes poderiam ser mais bem explorados pelos elementos da equipe.

A não identificação das partes interessadas no produto desenvolvido fez com que a aceitação dele fosse dificultada, havendo dúvidas no transcorrer da construção do módulo que poderiam ser esclarecidas com o feedback de possíveis usuários. Também não foi identificado qual sistema de comunicação os patrocinadores do EB-CyberDef desejam adotar, dificultando a escolha de padrões de interface de comunicação com os outros parâmetros do módulo.

A coleta de requisitos do produto foi realizada de forma ineficiente, obtendo alguns requisitos pouco específicos. O próprio formato do projeto em que a criação do protótipo teria que ter suas partes alinhadas com os requisitos coletados pelas partes interessadas e com as revisões bibliográficas dificultou a estimativa de tempo de construção do mesmo.

A falta de registro de riscos fez com que a equipe tivesse que se ajustar aos problemas encontrados sem uma resposta previamente pensada, principalmente na construção, que com a falta de encontros pessoais entre os elementos do projeto dificultou a troca de experiências de programação e uso de ferramentas de rede de computadores.

Existem diversas oportunidades de melhoria e expansão do presente trabalho, que podem ser desenvolvidas por outros alunos em trabalhos futuros, sejam por meio de PFC, iniciação científica, etc. das quais são apresentadas 4 a seguir.

Token de autenticação:

O módulo não está utilizando nenhum protocolo de autenticação para fins de consumo dele. A implementação desse recurso selecionará somente clientes autorizados a consumir o módulo de Defesa/Proteção. Com isso, é de extrema importância a implementação desse recurso no módulo em produção.

Comunicação com as máquinas gerenciáveis:

O módulo realiza comunicação com as máquinas gerenciáveis através de envios de mensagens utilizando o protocolo SSH, de acordo com uma lista de máquinas no próprio módulo. Uma oportunidade de melhoria seria criar um módulo intermediário de comunicação com as máquinas gerenciáveis que fizesse esse gerenciamento dos ativos de rede e formas mais personalizadas de comunicação entre elas.

API RDAP:

A API RDAP do registro.br (31) apesar das diversas informações que nos transmite, não suporta IP de outros países, o que limita drasticamente a utilização dela no módulo de

Defesa/Proteção em produção. O consumo do módulo em APIs de outros países aumentará a capacidade de coleta de informações de forma significativa.

IPV6:

Os IPs utilizados no Módulo são apenas do tipo IPV4, sendo uma oportunidade de melhoria adicionar as mesmas funcionalidades ao IPV6, garantindo uma abrangência maior de requisições.

REFERÊNCIAS

1 VALLÉE, R. History of cybernetics. *Systems Science And Cybernetics*, v. 3, p. 22–33, 2009.

2 POST, F. *Move over oil, Big Data is the new fuel to run the world*. 2019. 31 abr. de 2020. Disponível em: <https://business.financialpost.com/technology/move-over-oil-big-data-is-the-new-fuel-to-run-the-world>.

3 MILLER, B.; ROWE, D. A survey scada of and critical infrastructure incidents. In: *Proceedings of the 1st Annual conference on Research in information technology*. [S.l.: s.n.], 2012. p. 51–56.

4 EB. *EBCyber-Def*. Rio de Janeiro, 2017. 18 p.

5 STALLINGS, W.; BRESSAN, G.; BARBOSA, A. *Criptografia e segurança de redes* . [S.l.]: Pearson Educación, 2008.

6 BARCELLOS, A. M. P.; GASPARY, L. P. Segurança em redes p2p: princípios, tecnologias e desafios. In: *Simposio Brasileiro de Redes de Computadores (24.: 2006 maio: Curitiba, PR). Anais dos minicursos. Curitiba:[sn], 2006.* [S.l.: s.n.], 2006. p. 3.

7 IGURE, V. M.; WILLIAMS, R. D. Taxonomies of attacks and vulnerabilities in computer systems. *IEEE Communications Surveys & Tutorials*, IEEE, v. 10, n. 1, p. 6–19, 2008.

8 NEUMANN, P. G. *Computer-related risks*. [S.l.]: Addison-Wesley Professional, 1994.

9 CYBERSECURITY, E. U. A. for. *Common Language Security Incident Taxonomy*. 2011. 27 abr. de 2020. Disponível em: <https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/figure11.png/view>.

10 LINDQVIST, U.; JONSSON, E. How to systematically classify computer security intrusions. In: IEEE. *Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097)*. [S.l.], 1997. p. 154–163.

11 KLIMOVSKY, A. Taxonomy of cyberattacks and its application to the task of creating scenarios for their implementation. *Proceedings of the Institute for System Analysis of the Russian Academy of Sciences*, Institute for System Analysis, Russian Academy of Sciences, v. 27, p. 78, 2006.

12 ANDERSON, J. P. Computer security threat monitoring and surveillance. *Technical Report, James P. Anderson Company*, v. 1, p. 7, 1980.

13 SIMMONS, C.; ELLIS, C.; SHIVA, S.; DASGUPTA, D.; WU, Q. Avoidit: A cyber attack taxonomy. In: *9th Annual Symposium on Information Assurance (ASIA'14)*. [S.l.: s.n.], 2014. p. 2–12.

14 TEYMOURLOUEI, H. Quick reference: Cyber attacks awareness and prevention method for home users. *World Academy of Science, Engineering and Technology International Journal of Computer and Systems Engineering*, v. 9, n. 3, p. 679,680, 2015.

15 MIRKOVIC, J.; REIHER, P. A taxonomy of ddos attack and ddos defense mechanisms. *ACM SIGCOMM Computer Communication Review*, ACM New York, NY, USA, v. 34, n. 2, p. 39–53, 2004.

16 BEITOLLAHI, H.; DECONINCK, G. Analyzing well-known countermeasures against distributed denial of service attacks. *Computer Communications*, Elsevier, v. 35, n. 11, p. 1312–1332, 2012.

17 REED, T. C. *At the abyss: an insider's history of the Cold War*. [S.l.]: Presidio Press, 2005.

18 ALVAREZ, G.; PETROVIC, S. A new taxonomy of web attacks suitable for efficient encoding. *Computers & Security*, Elsevier, v. 22, n. 5, p. 435–449, 2003.

19 L.V., H. A. P. Main types of cyberatacks on automated control system of technological process and means of protection from them. *FUNDAMENTAL RESEARCH*, Publishing House Academy Limited Liability Company ..., v. 1, n. 10-3, p. 507–511, 2017.

20 GARBER, L. Melissa virus creates a new type of threat. *Computer*, IEEE, v. 1, n. 6, p. 16–19, 1999.

21 EGOROV, I. S.; LUPANDIN, V. V. Main types of cyber attacks and methods of combating them. In: *SCIENTIFIC RESEARCHES OF HIGHER SCHOOL*. [S.l.: s.n.], 2020. p. 51–53.

22 BRASIL, M. D. B. Governo do. Livro branco de defesa nacional. *Lei Complementar nº 136, de 25 de agosto de 2010*, v. 1, n. 1, p. 71–72, 2012.

23 BRITO, R. C. de; BEZERRA, Y. F. Comitês de classificadores aplicados à detecção de padrões maliciosos no tráfego de rede de computadores. *Instituto Militar de Engenharia*, 2018.

24 ARAÚJO, R. T. A. de; VENTURA, T. B. Painel de apoio para uma central de detecção de padrões maliciosos. *Instituto Militar de Engenharia*, 2019.

25 RICHARDSON, C.; SMITH, F. Microservices: from design to deployment. *Nginx Inc*, v. 1, p. 24–31, 2016.

26 DEACON, J. Model-view-controller (mvc) architecture. *Online][Citado em: 10 de março de 2006.] http://www. jdl. co. uk/briefings/MVC. pdf*, 2009.

27 FLANAGAN, D.; MATILAINEN, P. *JavaScript*. [S.l.]: Anaya Multimedia, 2007.

28 NODEJS. *Node Js*. 2020. 28 maio. de 2020. Disponível em: <https://www.nodejs.org>.

29 TILKOV, S.; VINOSKI, S. Node. js: Using javascript to build high-performance network programs. *IEEE Internet Computing*, IEEE, v. 14, n. 6, p. 80–83, 2010.

30 NEWTON, A.; HOLLENBECK, S. *JSON Responses for the Registration Data Access Protocol (RDAP)*. [S.l.], 2015.

31 GETSCHKO, D. *RDAP - Registro.br*. 2018. 21 abr. de 2020. Disponível em: <https://registro.br/rdap/>.