UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
CURSO DE CIÊNCIA DA COMPUTAÇÃO

ÂNGELO CARLOS FORTES SILVA

SEGURANÇA DE APLICAÇÕES NA NUVEM:
Um estudo de caso com a Amazon AWS

SÃO LUÍS - MA
2023

ÂNGELO CARLOS FORTES SILVA

SEGURANÇA DE APLICAÇÕES NA NUVEM:
Um estudo de caso com a Amazon AWS

Monografia apresentada ao curso de Ciência da Computação da Universidade Federal do Maranhão, como parte dos requisitos necessários para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Mário Antonio Meireles Teixeira

SÃO LUÍS - MA
2023

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Diretoria Integrada de Bibliotecas/UFMA

Fortes Silva, Ângelo Carlos.
Segurança de aplicações na nuvem : um estudo de caso com a Amazon AWS / Ângelo Carlos Fortes Silva. - 2024.
58 f.

Orientador(a): Mário Antonio Meireles Teixeira.
Curso de Ciência da Computação, Universidade Federal do Maranhão, São Luís - MA, 2024.

1. Amazon Web Services. 2. Ataques de negação de serviço. 3. Relação cliente-provedor. 4. Segurança em nuvem. I. Meireles Teixeira, Mário Antonio. II. Título.

ÂNGELO CARLOS FORTES SILVA

SEGURANÇA DE APLICAÇÕES NA NUVEM:
Um estudo de caso com a Amazon AWS

Monografia apresentada ao curso de Ciência da Computação da Universidade Federal do Maranhão, como parte dos requisitos necessários para obtenção do grau de Bacharel em Ciência da Computação.

Data de aprovação:

Banca Examinadora

_____

Prof. Dr. Mário Antonio Meireles Teixeira

_____

Profa. Dra. Simara Vieira da Rocha

_____

Prof. Dr. Geraldo Braz Junior

AGRADECIMENTOS

Agradeço a Deus pelo êxito de ter alcançado meus objetivos durante a graduação.

Agradeço aos meus pais, Francisca e Antônio, por sempre me proporcionarem a melhor educação possível, o amor e apoio necessários para que eu pudesse persistir em busca dos meus sonhos.

A minha avó Maria Fortes, por sempre me passar ensinamentos que foram importantes para minha formação.

Ao meu irmão Anderson, que sempre me ajudou com conselhos sobre a vida acadêmica.

Aos meus familiares e amigos que sempre estiveram por perto me apoiando.

Agradeço a todo corpo docente do curso de Ciência da Computação da Universidade Federal do Maranhão, pelos ensinamentos que serão levados não só para a minha vida profissional, mas também pessoal.

Agradeço ao meu orientador, professor Mário, pelo seu tempo, disponibilidade e todos os ensinamentos passados durante o curso e principalmente, durante a realização deste trabalho.

E por fim, pela minha persistência por todos esses anos de estudos na minha graduação e por ter superado todos os obstáculos, sem nunca ter desistido.

“A segurança é um processo, não um produto.”

(Bruce Schneier)

RESUMO

Considerando o crescente aumento da utilização de serviços em nuvem pelas mais diversas organizações, a segurança se tornou uma preocupação central para os profissionais da Tecnologia da Informação. Este trabalho faz a utilização de serviços de segurança da plataforma *Amazon Web Services* para a proteção de aplicações em nuvem. Trata-se de um estudo de caso que implanta ferramentas da *Amazon Web Services* para a mitigação de ataques de negação de serviço, comparando como um *software* se comporta antes e depois das configurações de segurança implantadas. Os resultados deste estudo mostram que provedoras de serviços em nuvem como a *Amazon Web Services,* dispõem de ferramentas eficazes para lidar com ataques cibernéticos. Por fim, discute-se como a relação entre provedor de serviços em nuvem e cliente é fundamental para uma maior eficiência dos níveis de segurança em aplicações, além de que se sugere novos estudos que possam aprofundar o tema principal abordado neste trabalho.

Palavras-chave: Segurança em nuvem; *Amazon Web Services*; Ataques de negação de serviço; Relação cliente-provedor.

ABSTRACT

Considering the increasing use of cloud services by a wide range of organizations, security has become a central concern for Information Technology professionals. This work uses security services from the Amazon Web Services platform to protect cloud applications. It is a case study that deploys Amazon Web Services tools to mitigate denial of service attacks, comparing how software behaves before and after the security configurations are implemented. The results of this study show that cloud service providers such as Amazon Web Services have effective tools for dealing with cyber-attacks. Finally, it discusses how the relationship between the cloud service provider and the client is fundamental for greater efficiency in application security levels, and suggests further studies that can delve deeper into the main topic addressed in this work.

Keywords: Cloud security; Amazon Web Services; Denial of service attacks; Client-provider relationship.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ACK	Acknowledgement
ACL	Access Control List
AMI	Amazon Machine Image
AWS	Amazon Web Services
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
Dns	Domain Name System
DoS	Denial of Service
EC2	Amazon Elastic Compute Cloud
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
IP	Internet Protocol
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
RSA	Rivest-Shamir-Adleman
SaaS	Software as a Service
SQL	Structured Query Language
SSH	Secure Shell
SYN	Synchronize
TCP	Transmission Control Protocol
URL	Uniform Resource Locator
VPC	Virtual Private Cloud
WAF	Web Application Firewall
Web	World Wide Web
XSS	Cross-site scripting

SUMÁRIO

1 INTRODUÇÃO

A computação é uma área dinâmica e está em constante evolução. Novas tecnologias aparecem constantemente e mudam a forma como os profissionais desta área realizam seus trabalhos. A nuvem é uma tecnologia que se mostra extremamente bem vista nos últimos anos. Segundo pesquisa da Flexera (2023), mais de 90% das empresas já utilizam algum tipo de serviço em nuvem. O que mostra que esse tipo de tecnologia não deve demorar muito para dominar o mercado e mudar completamente como os serviços são oferecidos no ramo da computação.

De acordo com Statista (2023), a empresa líder do mercado de distribuição de serviços em nuvem é a AWS, que domina 32% do mercado em relação a este tipo de tecnologia.

Com a utilização cada vez maior dos serviços em nuvem, também vieram preocupações em relação a esta tecnologia, como a segurança. Ainda segundo Flexera (2023), a segurança é a segunda preocupação majoritária de empresas se tratando de nuvem, dado que exemplifica o desafio em relação a este item.

O *Check Point Software Technologies* (2023), uma empresa globalmente reconhecida na área de segurança para a internet, divulgou um estudo que indicava um aumento de 48% de ataques a redes baseadas na nuvem em 2022, comparado com o ano anterior.

Nessa perspectiva, diante do crescimento de ataques cibernéticos a computação em nuvem, este trabalho objetiva demonstrar a importância da segurança no ambiente da computação em nuvem, apresentar os principais riscos cibernéticos que esta tecnologia é vulnerável e mostrar a aplicação de serviços de segurança para a proteção de aplicações na nuvem, no âmbito da plataforma da AWS.

1.1 OBJETIVO GERAL

Este trabalho tem como objetivo geral propor uma configuração de segurança utilizando serviços da AWS para a proteção de aplicações na nuvem. A proposta de configuração visa proteger a aplicação contra ataques conhecidos, especificamente o ataque de negação de serviço (DoS), utilizado neste trabalho. A intenção é impor

uma maior resistência a esses tipos de ataques, evitando falhas de segurança que podem prejudicar a disponibilidade do software.

1.1.1 Objetivos específicos

a) Avaliar a segurança de aplicações hospedadas na nuvem, identificando potenciais vulnerabilidades a que o *software* possa estar exposto;
b) Demonstrar como um ataque cibernético, em especial o ataque de negação de serviço, pode impactar na utilização da aplicação;
c) Analisar como a aplicação e a infraestrutura da AWS reagem durante esse tipo de ataque;
d) Propor uma solução de segurança específica para o ataque de negação de serviço, utilizando ferramentas disponibilizadas pela AWS.

1.1.2 Isenção de responsabilidade (*Disclaimer*)

O ataque de negação de serviço utilizado neste trabalho foi conduzido exclusivamente para fins didáticos e de pesquisa, com o objetivo de avaliar as vulnerabilidades da aplicação em nuvem hospedada na AWS. O ataque foi realizado em um ambiente controlado, onde não houve adversidades a outros usuários ou serviços. O único intuito do ataque DoS (*Denial of Service*) foi demonstrar como aplicações em nuvem podem ser vulneráveis a ataques cibernéticos.

1.2 ESTRUTURA DO TRABALHO

Este trabalho está estruturado em 5 capítulos que se dividem em seções e suas respectivas subseções.

No capítulo 2, denominado fundamentação teórica, são apresentados conceitos importantes para o embasamento teórico deste trabalho. Dentre estes, as principais características da computação em nuvem, vantagens e desvantagens da utilização desta tecnologia, princípios de segurança na nuvem e as principais ameaças no ambiente em nuvem.

Por seguinte, no capítulo 3, é abordado sobre as principais ferramentas de segurança na AWS para aplicações hospedadas na nuvem da provedora. É

apresentado a empresa de serviços em nuvem AWS, comenta-se sobre o serviço EC2, que é de grande importância na parte prática deste trabalho, além de discorrer sobre os principais serviços de segurança que serão utilizados neste trabalho.

No capítulo 4 é apresentado o estudo de caso que se utiliza do serviço EC2 para a criação de uma máquina virtual em que a aplicação será hospedada. É mostrado passo a passo como foi realizado esse procedimento e como é a configuração padrão de segurança nesse tipo de ambiente. Com o ataque de negação de serviço, é observado como a aplicação se comporta e assim, é utilizado de ferramentas de segurança apresentadas no capítulo 3 para que seja feita a mitigação do ataque. Após a implantação das medidas de segurança, é mostrado como o sistema reage agora protegido e, por fim, comenta-se sobre o resultado do estudo de caso.

Por último, no capítulo 5 é feita uma recapitulação sobre os principais tópicos abordados neste trabalho, analisando se os resultados esperados foram alcançados, além de que se reporta a relevância deste trabalho para o tema de segurança na nuvem, além de serem realizadas considerações finais e a sugestão de futuros trabalhos na mesma linha do tema principal.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo será tratado o conceito de computação em nuvem, suas principais características, modelos de serviço, vantagens da utilização desta tecnologia e ainda será abordado o tema da segurança na nuvem. Todos esses temas, servem de embasamento teórico para o que será abordado neste trabalho.

2.1 COMPUTAÇÃO EM NUVEM

Segundo o *National Institute of Standards and Technology* (NIST, 2012), a computação em nuvem pode ser definida como um modelo de prestação de serviços na tecnologia da informação que permite acesso sob demanda a uma rede compartilhada que disponibiliza de recursos computacionais (como banco de dados, armazenamento, servidores, aplicações e serviços). Estes recursos podem ser facilmente acessados e gerenciados, facilitando assim, a manipulação desta tecnologia.

A nuvem se mostra uma solução tecnológica cada vez mais interessante nos dias atuais pelo dinamismo e facilidades que esta tecnologia proporciona. Em relação ao modelo de computação tradicional, o investimento nos recursos necessários a um sistema são muitas vezes, muito mais compensatórios computacionalmente e economicamente para as empresas, já que uma série de preocupações como a segurança e armazenamento ficam como responsabilidade da provedora de serviços em nuvem.

2.1.1 Características da computação em nuvem

Ainda segundo o NIST (2012), existem cinco principais características da computação em nuvem. São estas:

a) Serviço sob-demanda: O cliente pode provisionar recursos computacionais sem interação humana com o provedor de serviços. É um processo que é automatizado, onde o consumidor pode pedir por recursos computacionais em tempo real e pagar apenas pelos serviços consumidos;
b) Acesso amplo a rede: Refere-se a capacidade dos clientes de acessarem os serviços da nuvem independentemente da plataforma. Os usuários podem

acessar de computadores pessoais, celulares, tablets, entre outros. Este recurso está inteiramente ligado com a acessibilidade disponibilizada pela nuvem, o que gera um conforto aos usuários;

c) Agrupamento de recursos: Trata-se da prática do agrupamento de recursos computacionais para atender a diversos consumidores. Vários usuários compartilham dos mesmo recursos físicos ou virtuais, que são alocados dinamicamente de acordo com a demanda dos usuários. O cliente não tem acesso a localização física de recursos específicos que estão sendo utilizados, mas em determinados casos, eles podem configurar preferências de localização de servidores, por exemplo, como em países, estados ou um data center específico;
d) Elasticidade rápida: Refere-se a capacidade de elasticidade da computação em nuvem. Os recursos são provisionados de maneira escalável e flexível, permitindo que a infraestrutura em nuvem se adeque às necessidades do usuário de aumento ou diminuição da demanda. Essa capacidade de dimensionamento dos recursos, é uma das partes mais importantes se tratando de facilitações que a nuvem permite;
e) Medição de serviço: Relaciona-se com a capacidade da nuvem de medir e monitorar recursos de uma forma muito precisa. O monitoramento e relato de serviços é de fundamental importância tanto para o provedor da nuvem, quanto para o cliente, pois ambos podem ter clareza de como otimizar seus recursos, para que estes sejam alocados da melhor maneira.

2.1.2 Modelos de serviço

Os serviços de computação em nuvem podem ser oferecidos para os clientes em diferentes formas, dentre estas (NIST, 2012):

a) *Infrastructure as a Service* (IaaS): É um modelo onde os consumidores podem provisionar e gerenciar recursos computacionais como servidores virtuais, armazenamento, redes e outros. O cliente pode implantar por exemplo, sistemas operacionais e aplicativos, porém, neste modelo, o consumidor não pode gerenciar camadas subjacentes da nuvem. Um exemplo de provedora IaaS é a Amazon Web Services, que será bastante abordada neste trabalho;

b) *Platform as a Service* (PaaS): É um modelo que fornece e gerencia todo o ambiente propício para o desenvolvimento de aplicações na nuvem. Os desenvolvedores podem criar as aplicações sem se preocupar com as configurações da infraestrutura ou plataforma da aplicação. Isto fica por conta da provedora de serviço em nuvem;
c) *Software as a Service* (SaaS): Neste modelo, os clientes utilizam aplicações fornecidas pelo provedor de serviço na nuvem. Os aplicativos são acessados através de um navegador Web e o usuário não gerencia e nem controla recursos da camada de infraestrutura como os sistemas operacionais e armazenamento. Um exemplo do SaaS é o correio eletrônico do Google, o Gmail.

2.1.3 Modelos de Implantação

Por último, NIST (2012) ainda fala sobre os modelos de implantação dominantes na computação em nuvem:

a) Nuvem pública: Um serviço que é oferecido para diversos consumidores por um provedor de nuvem. Isso significa que os recursos do provedor podem ser usados por diversas companhias. Isso gera mais flexibilidade e facilidade para empresas, pois estas não precisam investir muito financeiramente comparado a uma nuvem privada;
b) Nuvem privada: Um tipo de serviço em que a nuvem é exclusiva para uma determinada companhia, com dedicação exclusiva. Este tipo de nuvem é comumente utilizada por empresas que trabalham com negócios que requerem um grau de segurança muito elevado e que queiram ter um controle bem rígido sobre suas informações no servidor;
c) Nuvem híbrida: Um modelo que une as nuvens privadas e públicas. A organização usa uma combinação de recursos que ambas entregam para atender especificamente o negócio da companhia. Muitas empresas utilizam-se da nuvem híbrida para, por exemplo, aproveitar da maior segurança e controle de dados da nuvem privada e dos recursos mais baratos da nuvem pública;
d) Nuvem comunitária: Um modelo onde diversas organizações utilizam os mesmos serviços em nuvem. É comumente utilizado por companhias que

compartilham dos mesmos interesses e querem que os custos sejam reduzidos, utilizando-se de um grupo maior de consumidores.

2.2 VANTAGENS DA COMPUTAÇÃO EM NUVEM

A computação em nuvem veio como algo revolucionário na tecnologia da informação, pois apresentou uma nova maneira de criar e gerenciar recursos computacionais. Antes a complexidade que existia para empresas colocarem na prática sistemas complexos era imensa, o que passou a ser muito mais facilitado com o advento da nuvem.

Segundo Santos (2018), a utilização da nuvem trouxe inúmeros benefícios para companhias que passaram a utilizar esse sistema, como a diminuição de custos, a possibilidade de acesso remoto aos sistemas, a facilitação da análise de dados, o que gerou mais eficiência para as empresas nas tomadas de decisões, além de diversas outras vantagens.

A computação em nuvem proporciona às empresas a migração de todo o *hardware* e *software* físicos que eram necessários para a utilização de um sistema complexo para a internet. O sistema físico necessita, por exemplo, de um centro de dados que ocupa espaço físico e requer de toda uma manutenção, que precisa de manuseio humano e que muitas vezes, custa bem caro para as organizações. Muitas vezes, um problema em um *data center* pode colocar a perder todo um sistema complexo de uma empresa, o que é uma desvantagem grande de um sistema fora da nuvem. Além de todas as responsabilidades com armazenamento, *backup* e diversos recursos, são de responsabilidade da provedora de nuvem, o que gera menos dor de cabeça para as empresas (SANTOS, 2018).

Toda a complexidade de um sistema tradicional (fora da nuvem), é facilitado pelo serviço da computação em nuvem, sendo que as empresas têm custos apenas com o que elas consomem, o que é muito relevante do ponto de vista empresarial. A adaptabilidade da nuvem é uma característica extremamente importante na tomada de decisão das empresas em utilizar esta tecnologia (SANTOS, 2018).

Ainda segundo Santos (2018), a principal vantagem da utilização dos recursos em nuvem é a otimização do *hardware* e *software* de sistemas das empresas. A escalabilidade e flexibilidade apresentada a estes recursos na nuvem é muito valioso para as organizações, pois fornece um melhor gerenciamento, automatização e

compartilhamento de recursos. Além de que coisas como atualizações de software e colaboração de recursos são sistematizadas na nuvem. Ou seja, a computação em nuvem proporciona uma otimização dos recursos de *hardware* e *software* para as empresas.

2.3 DESVANTAGENS DA COMPUTAÇÃO EM NUVEM

Apesar de todos os benefícios que a computação em nuvem pode proporcionar a organizações, existem algumas dificuldades que esta tecnologia tem que podem ser uma barreira na adesão dela.

Segundo Pedrosa e Nogueira (2011), as maiores dificuldades para a implementação da computação em nuvem são: a segurança, escalabilidade, interoperabilidade, confiabilidade e disponibilidade.

A segurança é o maior desafio quando se trata do uso da nuvem. Haja visto que antes informações que eram guardadas em servidores físicos, agora são armazenadas na internet, onde não se tem exatidão sobre o local físico onde estão inseridas. A integridade e confidencialidade das informações é imprescindível para qualquer sistema e acaba sendo um desafio, principalmente nas nuvens públicas, que são mais suscetíveis a ataques de cibercriminosos.

A escalabilidade, que é umas das principais características da computação em nuvem, pode também acabar sendo um empecilho. Muitas organizações podem ter dificuldade no processo de adaptar aplicações e dados para que se tornem mais “flexíveis” de acordo com a nuvem.

A interoperabilidade trata-se da capacidade de diferentes sistemas em computação em nuvem cooperarem de maneira eficiente, mesmo que estejam em nuvens distintas. É uma característica completamente desejável na nuvem, porém pode ser difícil de ser colocada em prática. As organizações precisam preparar seus sistemas para que a portabilidade seja possível.

A confiabilidade trata-se de quanto um sistema é confiável, ou seja, quanto este não apresenta falhas e entrega tudo que o foi prometido. Isto pode ocasionalmente ser um problema na computação em nuvem dependendo de o quão bem as provedoras entregam os seus serviços e o quão confiáveis estes são.

A disponibilidade também pode ser um desafio se tratando da computação em nuvem, pois coisas como ataques cibernéticos, falta de conectividade e falhas no

serviço do provedor, podem causar uma indisponibilidade do serviço para os clientes. Mesmo provedoras de grande porte não estão a salvo de problemas como estes, pois, muitos destes empecilhos, são situações que demandam de um esforço considerável para serem superadas.

2.4 SEGURANÇA NA NUVEM

Com o avanço tecnológico, os sistemas de informação ficaram cada vez mais robustos e capazes de guardar um volume grande de dados. Desde informações simples, como nome de usuários, até informações importantes, como os dados financeiros de uma empresa, são armazenados em computadores nas mais diversas instituições. Esses dados são protegidos por padrões de segurança, independente do tipo de tecnologia usada, demonstrando a importância crescente da segurança da informação nos ambientes digitais, onde a proteção de informações relevantes é fundamental para o sucesso das operações institucionais.

Em um ambiente de segurança na nuvem deve haver um cuidado ainda maior em relação a padrões de segurança por conta da maior fragilidade que este ambiente está inserido. Logo, há uma série de protocolos que devem ser seguidos para que um ambiente possa ser considerado seguro na nuvem. Nas próximas seções, serão dados conceitos fundamentais que servirão como base para o desenvolvimento deste trabalho.

2.4.1 Princípios de segurança na nuvem

Segundo Machado (2014), os três pontos principais que norteiam qualquer programa de segurança são: confidencialidade, integridade e disponibilidade, também conhecidos como “CIA”, como mostra a Figura 1.

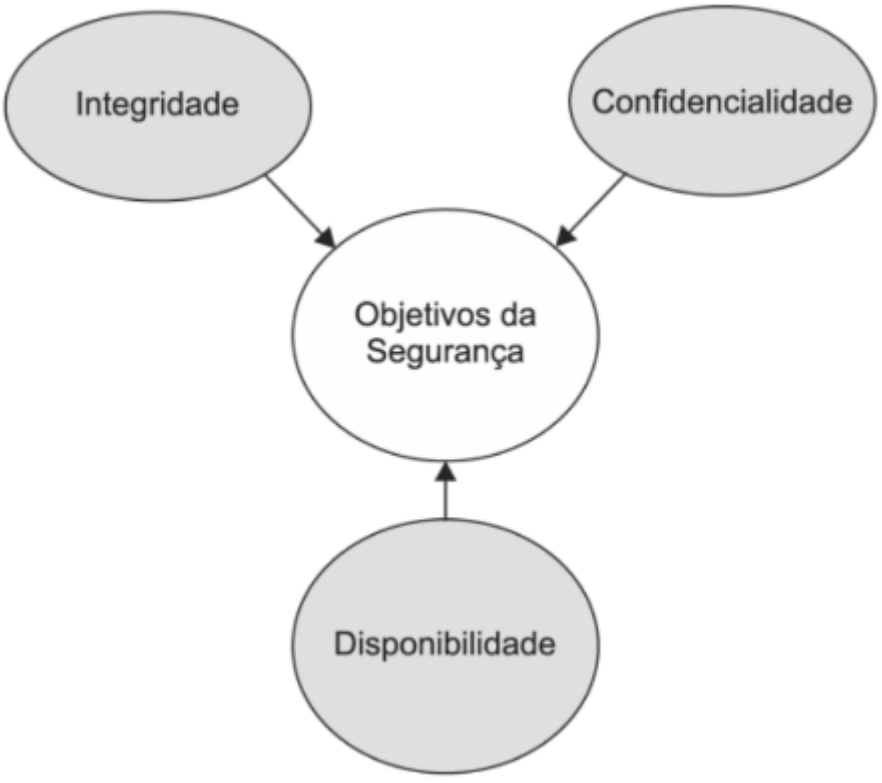
Dentre os princípios de segurança, a confidencialidade trata da preservação de informações importantes, permitindo apenas que pessoas autorizadas tenham acesso ao sistema, seguindo determinadas regras de acesso que serão implementadas pelos desenvolvedores (MACHADO, 2014).

A integridade refere-se a capacidade da manutenção inalterada dos dados de um sistema, prezando rigor e confiabilidade que dados não serão alterados sem permissão do proprietário do sistema. Ou seja, usuários não autorizados, não podem

modificar dados que o sistema previamente estabeleceu como inalterados (MACHADO, 2014).

Ainda em referência aos princípios de segurança, Machado (2014) cita a disponibilidade, que trata do sistema procurar sempre estar utilizável para os usuários, entregando os serviços como previsto para o projeto do sistema. Ele deve sempre estar preparado para a recuperação de disponibilidade, assim como dados importantes. A disponibilidade dos sistemas podem ser afetadas desde questões ambientais até os ataques de recusa de serviço (*denial of service*), que se tornam cada dia mais um desafio para os sistemas manterem a disponibilidade desejada.

Figura 1 - Tríade da segurança da informação.



Fonte: (MACHADO, 2014)

Estes três princípios são considerados pilares em qualquer sistema de informação, porém em relação a segurança na nuvem, entendeu-se que haveria uma necessidade de implementar alguns outros princípios fundamentais para sistemas em nuvem.

Winkler (2011) cita mais seis propriedades: O princípio do menor privilégio, autenticação, autorização, criptografia, auditoria e responsabilidade. O princípio de menor privilégio postula que os usuários ou sistema devem ter privilégio mínimo para a realização das tarefas específicas, ou seja, deve-se atribuir o menor conjunto de permissões para que determinada tarefa seja concluída.

A autenticação faz referência ao processo de verificação da autenticidade do usuário, onde o sistema pode utilizar dos mais variados métodos como senhas, biometrias, certificados digitais, para verificar a autenticidade do usuário. A autorização é um princípio complementar à autenticação pois refere-se ao controle de acesso e às permissões concedidas a usuários já autenticados em um sistema (WINKLER, 2011).

Ainda segundo Winkler (2011), a criptografia se baseia no uso de métodos matemáticos para realizar a segurança de dados na nuvem, onde há o processo de encriptação, que esconde dados relevantes e o processo de decriptação, que converte os dados que foram encriptados.

Winkler (2011) fala que a auditoria está relacionada ao processo sistemático de análise dos processos de segurança do sistema, verificando se as políticas e procedimentos estão de acordo com os padrões de segurança estabelecidos para o sistema.

Por último, Winkler (2011) cita que a responsabilidade trata-se da atribuição de responsabilidades a membros da organização para que a proteção de dados seja a mais efetiva possível. A designação de tarefas para cada aspecto da segurança, garantindo que os padrões de segurança sejam efetivamente bem implementados.

2.5 AMEAÇAS A COMPUTAÇÃO NA NUVEM

Quando se trata de ameaças a sistemas computacionais, existem diversas maneiras que se pode atacá-los. Hoje em dia, com uma infraestrutura computacional cada vez mais robusta, velocidade de transmissão de dados maior, acesso remoto à informação, dentre outras vantagens, os *hackers* têm maior facilidade de atacar diversas camadas em sistemas de informação.

Não diferentemente, com a popularização da computação em nuvem, o acesso a recursos computacionais mais poderosos trouxe também uma maior

preocupação em relação à segurança na nuvem. Agora, os atacantes têm acesso a esses sistemas, o que tornou os ataques cibernéticos mais eficientes.

Um exemplo de ataque famoso anos atrás, foi o ocorrido em uma rede da Sony. Ladrões virtuais utilizaram o serviço EC2 da Amazon para obter informações pessoais de usuários da empresa. Eles alugaram um servidor virtual e o utilizaram para realizar ataques a clientes da rede *Playstation,* o que resultou no comprometimento de contas de mais de 100 milhões de usuários (BLOOMBERG, 2011).

Logo, quando trata-se das vulnerabilidades da computação em nuvem, existem diversas ameaças a sistemas deste tipo, mas dentre as principais pode-se relatar: Ataque de injeção de *malware, wrapping attack* (ataque de encapsulamento) e ataque de negação de serviço.

2.5.1 Ataque de injeção de *malware*

É uma categoria de ataques baseados na web, no qual invasores aproveitam da vulnerabilidade em sites para inserir códigos maliciosos neles com os mais diversos objetivos, como manipulação de dados, roubo de informações sigilosas ou até mesmo para redirecionar usuários para outros sites perigosos. Este tipo de ataque também é cada vez mais usado em sistemas na nuvem, onde os *hackers* injetam código malicioso em máquinas virtuais, onde o módulo é detectado como uma instância legítima pelo servidor de nuvem, assim fazendo com que o invasor tenha sucesso na sua invasão (CHOU, 2013).

Dentre os diversos tipos de ataques de injeção de *malware* que existem, dois se destacam: Injeções SQL e XSS.

As injeções SQL têm como objetivo atacar servidores SQL onde estão os bancos de dados de determinada instituição. O invasor usa parte do código SQL para invadir o banco de dados, contornando o login de acesso, para assim, entrar em contato com informações importantes da empresa, de usuários, entre outros, no *backend* de um sistema. É um método muito utilizado desde antes da criação da computação em nuvem, porém foi aprimorado no decorrer dos anos e hoje ainda é usado para o ataque de informações na nuvem (CHOU, 2013).

Segundo Chou (2013), os ataques de *cross-site scripting* (XSS) injetam código malicioso utilizando tecnologias utilizadas na web como Javascript e HTML,

para deixar páginas dinâmicas em vulnerabilidade. O ataque é feito diretamente no navegador da vítima e utilizado para retirar informações da mesma. Roubar informações ou *cookies* são uma dos interesses de criminosos que utilizam desta técnica. O XSS difere-se um pouco de outras ameaças que existem porque o alvo do ataque não é necessariamente o aplicativo que está sendo explorado, mas sim o usuário do sistema.

2.5.2 *Wrapping attack*

O *Wrapping attack* ocorre burlando o processo de autenticação e identidade de sistemas web. Em todo o processo de requisições HTTP na internet, este protocolo passa pelo *Web Services Security,* mecanismo de segurança entre clientes e servidores na internet. É um tipo de assinatura virtual, que é burlada pelo *wrapping attack* (CHOU, 2013).

Isso ocorre porque os invasores modificam a infraestrutura da assinatura digital de uma forma que ela ainda seja considerada válida pelo *Web Services Security,* mas modificando mensagens que podem conter coisas maliciosas para os sistemas atacados.

Como os usuários que utilizam os serviços em nuvem, normalmente usam navegadores web para acessar seus provedores, este tipo de ataque também pode ser utilizado para atacar sistemas na nuvem.

2.5.3 Ataque de negação de serviço

Segundo Erickson (2008), o ataque de negação de serviço tem como objetivo impedir que usuários utilizem determinado sistema ou recurso, negando operações que seriam normalmente disponibilizadas pelo sistema.

Os ataques de negação de serviço que vem de um único computador ou ponto de rede são referidos como DoS (*denial of service),* já aqueles que utilizam de diversas máquinas ou de redes de computadores diversos, são chamados de DDoS (*distributed denial of service)* (STALLINGS, 2017).

Segundo Stallings (2017), uma forma de classificar os ataques de negação de serviço é vendo que tipo de recurso esse ataque consome. Este pode ter um objetivo

de atacar um recurso específico no servidor-alvo ou pode exaurir a capacidade de transmissão de dados do sistema atacado.

Um dos ataques mais famosos e comuns é o ataque de inundação (*SYN flood attack*), que consiste no atacante explorar o protocolo TCP de comunicação entre cliente-servidor. O *hacker* manda vários pacotes SYN para o servidor-alvo, que responde com pacotes SYN/ACK, querendo estabelecer uma conexão com o cliente (que neste caso é o atacante). O servidor sempre manterá a conexão aberta esperando uma resposta do cliente que estará inundando o servidor com pacotes SYN, aumentando cada vez mais o tráfego de rede até o servidor-alvo não conseguir mais responder. Este método utiliza-se do procedimento *three-way handshake* do protocolo TCP para achar uma brecha de ataque a servidores vulneráveis (STALLINGS, 2017).

Já quando se trata de ataques que consomem recursos de transmissão de dados, a inundação de ping (ICMP) é um tipo muito usado também. Neste ataque, o atacante utiliza-se do ICMP, que é um protocolo para comunicação na camada de rede, para realizar ataques. O objetivo deste ataque é sobrecarregar o servidor-alvo, fazendo com que ele não consiga lidar com o número inesperado de solicitações ICMP. Normalmente atacantes utilizam-se de diversos endereços IP falsos para realizar o ataque, sendo que o servidor-alvo sofre com um aumento substancial no tráfego que este estava acostumado a lidar, resultando em uma possível interrupção no serviço de rede (CLOUDFLARE).

Ainda segundo Stallings (2017), outra forma de se classificar ataques de negação de serviço é em ataques diretos ou reflexivos. Nos ataques diretos, o atacante infecta vários *hosts,* chamados de máquinas zumbis. Estas são classificadas em “mestre” e “escravo”, onde o *hacker* coordena as máquinas “mestre” que por sua vez acionam as máquinas “escravo” até chegarem no servidor-alvo. Este tipo de ataque é considerado mais complicado de se mitigar, pois a utilização de duas “camadas” de ataque torna o processo de rastreio do atacante mais dificultoso.

Os ataques reflexivos adicionam mais uma camada de máquinas no ecossistema do ataque. Nele, o *hacker* instrui as máquinas zumbis a criar pacotes de dados com um endereço IP falso, que na verdade é IP real da vítima, não o endereço das máquinas zumbis. Os pacotes de dados com endereços IP falsificados é enviado para camada de máquinas chamadas “refletoras”, que não estão

infectadas, que respondem enviando uma mensagem ao remetente, que é a máquina-alvo. A vítima será então inundada com uma série de respostas dos refletores, assim, ocasionando um volume grande de tráfego que pode sobrecarregar os recursos da vítima, levando a uma negação de serviço. Este é um tipo de ataque altamente complexo de ser mitigado pois envolve mais máquinas e tem um maior tráfego que a versão direta. Além de que rastrear os pacotes de origem é muito mais difícil, pois eles vêm das máquinas não infectadas.

3 SEGURANÇA NO PROVEDOR AMAZON AWS

A Amazon Web Services é uma plataforma de serviços de computação em nuvem criada em 2006. É a plataforma de nuvem mais utilizada e abrangente do mundo, sendo uma das primeiras empresas a oferecer serviços de *cloud* sob demanda através da internet, com o pagamento do cliente sendo de acordo com o seu consumo (CLARANET).

A AWS disponibiliza seus serviços de nuvem a partir de inúmeros data centers que abrangem 102 zonas de disponibilidade em 32 regiões geográficas do Globo (AMAZON, 2023).

A AWS tem como objetivo oferecer serviços que são flexíveis, efetivos, escaláveis, elásticos e seguros. Neste contexto, a segurança desempenha um papel importantíssimo para a oferta dos serviços em nuvem de forma confiável (AMAZON, 2023).

A segurança na AWS é um processo compartilhado entre o cliente e a empresa, sendo descrito por esta como segurança da nuvem e segurança na nuvem (AMAZON, 2023):

a) Segurança da nuvem: A AWS é responsável pela parte de infraestrutura da nuvem, disponibilizando serviços específicos de segurança;
b) Segurança na nuvem: É a parte de segurança que fica responsabilizada pelo cliente, onde este estará livre para implementar medidas de segurança para seus sistemas, aplicações e afins, assim como este faria em um site não alocado na nuvem.

No meio dos mais de 200 serviços disponibilizados pela empresa, a AWS disponibiliza aqueles específicos em relação à segurança de aplicações na nuvem, que serão aprofundados neste trabalho.

Dentre os serviços de segurança de aplicações oferecidos pela Amazon, este trabalho foca em três principais: Grupos de segurança (EC2), AWS *Shield* e AWS *Web Application Firewall* (WAF).

Antes de prosseguir com a análise de cada grupo de segurança, é necessário uma breve explicação de um serviço importante que foi usado para o desenvolvimento deste trabalho.

3.1 EC2

O *Amazon Elastic Compute Cloud* (EC2) é um serviço que oferece uma capacidade de computação escalável sob demanda na AWS. É possível executar quantos servidores virtuais forem necessários e em qualquer região no globo terrestre disponível pela Amazon. A escalabilidade, que é a capacidade do sistema de se adaptar a um aumento ou diminuição de demanda mantendo a qualidade do serviço, é a principal característica do Amazon EC2. Para isso, o serviço oferece diversos recursos para que os clientes possam realizar o desenvolvimento de seus sistemas, dentre estes (AMAZON, 2023):

Instâncias: São os servidores virtuais.

Imagens de máquina da Amazon(*AMIs*): São modelos já pré-configurados para as instâncias que incluem o sistema operacional e softwares adicionais que serão necessários para o servidor.

Tipos de instância: É a parte relacionada a configuração de *hardware* para a instância.

Pares de chaves: Está relacionado a segurança da instância, onde a Amazon guarda uma chave pública e o cliente fica com uma chave privada para seu servidor.

Volumes de armazenamentos de instâncias: Onde ficam armazenados dados temporários que são excluídos quando uma instância é pausada, hibernada ou encerrada.

Volumes do Amazon EBS: Onde ficam armazenados dados persistentes, utilizando o *Amazon Elastic Block Store (*Amazon EBS).

Regiões, zonas de disponibilidade, zonas locais, AWS *Outposts* e zonas do *Wavelength:* São vários locais que o cliente tem acesso para alterar a localização da sua instância pelo Mundo.

Grupos de segurança: Um firewall virtual que faz parte dos processos de segurança do EC2.

Endereços IP elásticos: São endereços IPv4 estáticos utilizados para computação dinâmica.

Tags: Onde ficam os metadados(informações adicionais que descrevem os dados que estão sendo armazenados), onde o cliente pode criar e atribuir aos recursos do EC2.

Nuvens privadas virtuais (VPCs): São redes virtuais que podem ser criadas para a instância, que estão logicamente separadas do resto da nuvem AWS. O cliente pode conectar as redes virtuais à sua própria rede, se for necessário.

3.1.1 Segurança no Amazon EC2

A segurança de instâncias desenvolvidas no Amazon EC2, se passa principalmente pelo *Identity and Access Management* (IAM), por pares de chaves e pela aplicação dos grupos de segurança.

a) *Identity and Access Management* (IAM):
   O IAM são credenciais de segurança que servem como controle de acesso a serviços e recursos encontrados no Amazon EC2. Com ele é possível implementar políticas de permissão de acesso ao serviço, assim por exemplo, permitindo apenas que usuários autorizados possam ter acesso a determinado recurso requerido (AMAZON, 2023);
b) Pares de chaves:
   São um par de chaves que estão relacionadas, compostas por chave pública e chave privada. É uma forma de garantir a identidade do usuário que está acessando a instância no EC2 (AMAZON, 2023):
   - **Chave pública:** A chave pública serve como meio de criptografar os dados trocados entre a instância e a AWS. É armazenada pela própria Amazon e só pode ser descriptografada com a chave privada do cliente correspondente;
   - **Chave privada:** Já a chave privada é única e armazenada pelo cliente. Ela será usada para descriptografar os dados da chave pública. A Amazon não mantém uma cópia da chave privada, sendo de total responsabilidade do usuário mantê-la de forma segura;
c) Grupos de segurança:
   Os grupos de segurança são um recurso gratuito oferecido pela Amazon para proteção das instâncias no EC2 da AWS. Eles funcionam como um firewall virtual que visa controlar o fluxo de entrada e saída no tráfego de rede (AMAZON, 2023).

Por padrão, é criado um novo grupo de segurança para uma rede virtual privada (VPC), onde é permitido a comunicação entre portas e protocolos dentro da rede, e bloqueia tráfego de fora da rede, ao menos que o cliente crie regras adicionais que modifiquem esse padrão (AMAZON, 2023).

Apesar do grupo de segurança padrão da VPC oferecer certo nível de segurança inicial, a empresa recomenda que sejam criados grupos de segurança personalizados de acordo com as necessidades específicas de aplicativos que possam estar rodando nas instâncias criadas. A criação de novos grupos de segurança específicos, permite uma maior restrição no acesso à instância, podendo assim ser mais adequado para uma infraestrutura específica do cliente no Amazon EC2 (AMAZON, 2023).

3.1.2 Regras de grupos de segurança

O principal recurso relacionado aos grupos de segurança são as regras de entrada e saída do tráfego de rede. As regras de entrada são responsáveis por controlar o tráfego que tem acesso a instância e as de saída estão relacionadas ao tráfego que pode deixar a instância (AMAZON, 2023).

Dentre as principais características das regras de entrada e saída, se sobressaem as seguintes (AMAZON, 2023):

a) O tráfego de rede pode ser filtrado a partir da inserção de portas e protocolos específicos;
b) O tráfego de saída da rede não tem nenhuma restrição por padrão, podendo ser alterado pelo usuário;
c) Os grupos de segurança visam manter uma conexão, logo se o usuário configurar o tráfego de saída para uma determinada porta, o tráfego de entrada será também permitido para aquela porta;
d) É possível adicionar regras de entrada e saída quando o usuário quiser, e estas serão sempre associadas a instância que estão direcionadas;
e) É permitido associar diversos grupos de segurança a uma mesma instância, sendo que o Amazon EC2 irá agregar estas regras para determinar o que será ou não permitido no tráfego de rede;

f) Os grupos de segurança permitem a criação de regras baseadas em funções. Logo, se o cliente tiver uma arquitetura com servidores web, banco de dados e outros, ele poderá criar regras específicas para cada tecnologia.

Os grupos de segurança desempenham um papel fundamental na proteção de aplicações nas instância do Amazon EC2, pois, com a criação de regras apropriadas para as necessidades do usuário, este pode evitar muitos problemas comuns relacionados à segurança de aplicações na nuvem.

3.2 SEGURANÇA DE APLICAÇÕES

A *Amazon Web Services* apresenta diversos serviços em seu catálogo de ferramentas referentes a proteção de aplicações Web em seu provedor na nuvem. Esta seção do trabalho irá tratar dos dois principais serviços oferecidos pela empresa:

a) AWS *Shield:*

O AWS *Shield* é um serviço de segurança gerenciado pela Amazon que fornece proteção contra ataques de negação de serviço (DoS) e ataques distribuídos de negação de serviço (DDoS). O serviço ajuda a proteger as aplicações e recursos da AWS contra ataques de grande escala que podem prejudicar a disponibilidade das tecnologias.

O AWS *Shield* apresenta dois planos de proteção oferecidos pela Amazon: AWS *Shield Standard* e AWS *Shield Advanced*. O primeiro é oferecido gratuitamente para todos os clientes da AWS de forma automática, sem custo adicional. Ele defende as aplicações contra os ataques DoS e DDoS mais comuns nas camadas de rede e transporte, que podem ter como alvo o aplicativo do cliente na nuvem. Para mitigar esses tipos de ataques, o Shield Standard utiliza como filtragem de pacotes e modelagem de tráfego de rede com base em uma determinada prioridade, para de maneira mais rápida mitigar ataques na camada de rede.

Já o AWS *Shield Advanced* é um serviço pago e avançado de proteção contra ataques direcionados às aplicações executadas na AWS. Ele foi projetado para oferecer uma camada de segurança mais robusta e abrangente em

relação ao AWS *Shield Standard*, ajudando a proteger os recursos críticos contra ameaças DDoS mais complexas e sofisticadas como os ataques de saturação de rede, amplificação de DNS, ataques de aplicativos e até ataques camuflados.

Outra característica importante é que ele tem a capacidade de detectar e mitigar ataques DDoS de forma automática, ajudando a responder e manter as aplicações no ar, além do serviço fornecer relatórios detalhados sobre tentativas de ataque ou possíveis ameaças.

O AWS Shield Advanced também tem a capacidade de integração com outros serviços de segurança como o AWS WAF, que será citado posteriormente. Além de que os clientes têm acesso a uma rede de especialistas da empresa disponíveis para suporte 24 horas por dia (AMAZON, 2023).

b) AWS WAF:

O AWS Web Application Firewall (WAF) é um serviço de *firewall* de aplicações da web que ajuda a protegê-las contra ataques maliciosos, como ataques SQL *injection, cross-site scripting (*XSS*)*, bots maliciosos e dezenas de outros ataques direcionados às aplicações web.

O AWS WAF permite a criação de regras personalizadas para controlar o tráfego da web que chega até as aplicações do cliente. Essas regras podem ser baseadas em endereços IP, padrões URL, cabeçalhos HTTP, entre outros parâmetros. O cliente cria essas regras definindo uma lista de controle (ACL), gerenciando o tráfego que deve ser permitido e bloqueado com base nas regras ACL. Um exemplo de ação utilizando o ACL, é a execução de CAPTCHA em um sistema web para verificação do uso padrão de um navegador por um usuário humano.

Assim como o AWS *Shield Advanced,* o AWS WAF permite integração com outros serviços de segurança da Amazon, além de fornecer logs detalhados que podem ser usados para análise de segurança e recursos de monitoramento em tempo real para a prevenção a possíveis ataques (AMAZON, 2023).

4 ESTUDO DE CASO: AVALIANDO A SEGURANÇA DE UMA APLICAÇÃO NA AMAZON AWS COM SIMULAÇÃO DE UM ATAQUE DE NEGAÇÃO DE SERVIÇO (DOS)

Neste capítulo será apresentada uma aplicação prática de algumas medidas de segurança fornecidas pela *Amazon Web Services* em um ambiente de uma aplicação *Wordpress* hospedada em uma instância no Amazon EC2.

Ao longo deste capítulo, serão apresentados todos os passos, desde a criação da instância até a avaliação de segurança da aplicação por meio de uma simulação de um ataque de negação de serviço.

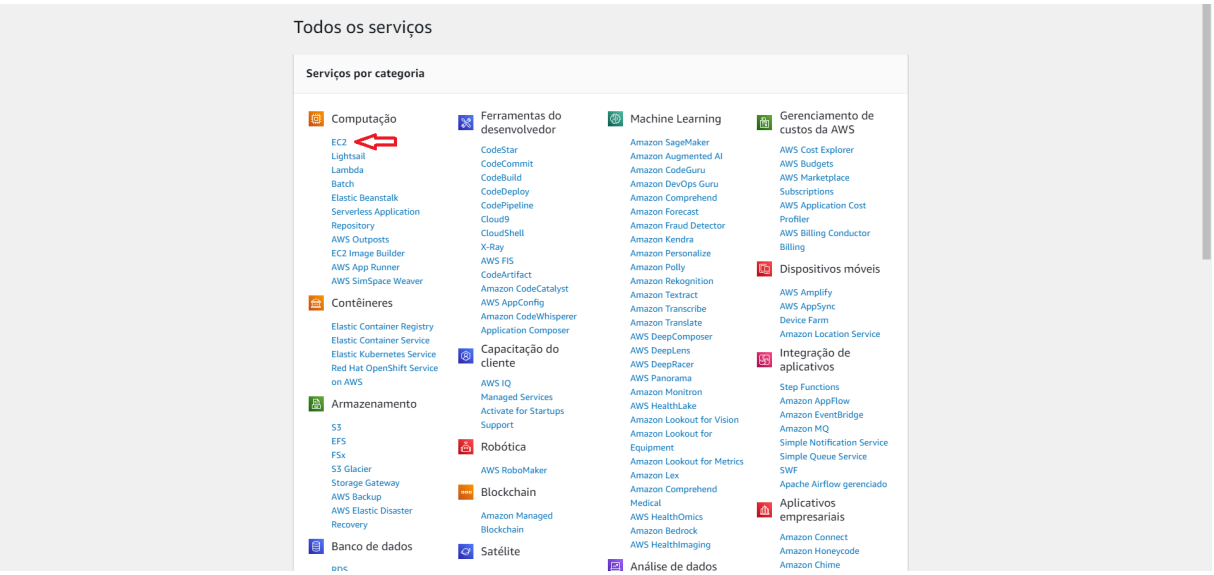
4.1 CRIAÇÃO DE UMA CONTA NA AMAZON WEB SERVICES

Para criar uma conta na AWS, foi necessário cadastrar um endereço de *email* válido, além de criar um nome para o usuário e senha. Após isso, foi indicado para a Amazon que a conta seria de nível pessoal (para projetos próprios), além de que foi preenchido um pequeno formulário contendo informações pessoais que a empresa pede. Além disso, a Amazon requer um cadastro de cartão de crédito e a inserção do número de telefone do usuário. Para a finalização do cadastro, a AWS pede para o usuário selecionar um plano de suporte, que vai desde o gratuito até ao “Suporte *Business”.* Após isso, os serviços da empresa já ficam disponíveis para a utilização do cliente.

4.2 CRIANDO UMA INSTÂNCIA NO AMAZON EC2 E SUBINDO UMA APLICAÇÃO WORDPRESS

Após a criação da conta na *Amazon Web Services*, o usuário tem acesso a página inicial do console da AWS, onde todos os serviços da empresa estarão classificados por categoria. Dentro da categoria “Computação”, encontra-se o serviço “EC2”, como mostra a Figura 2.

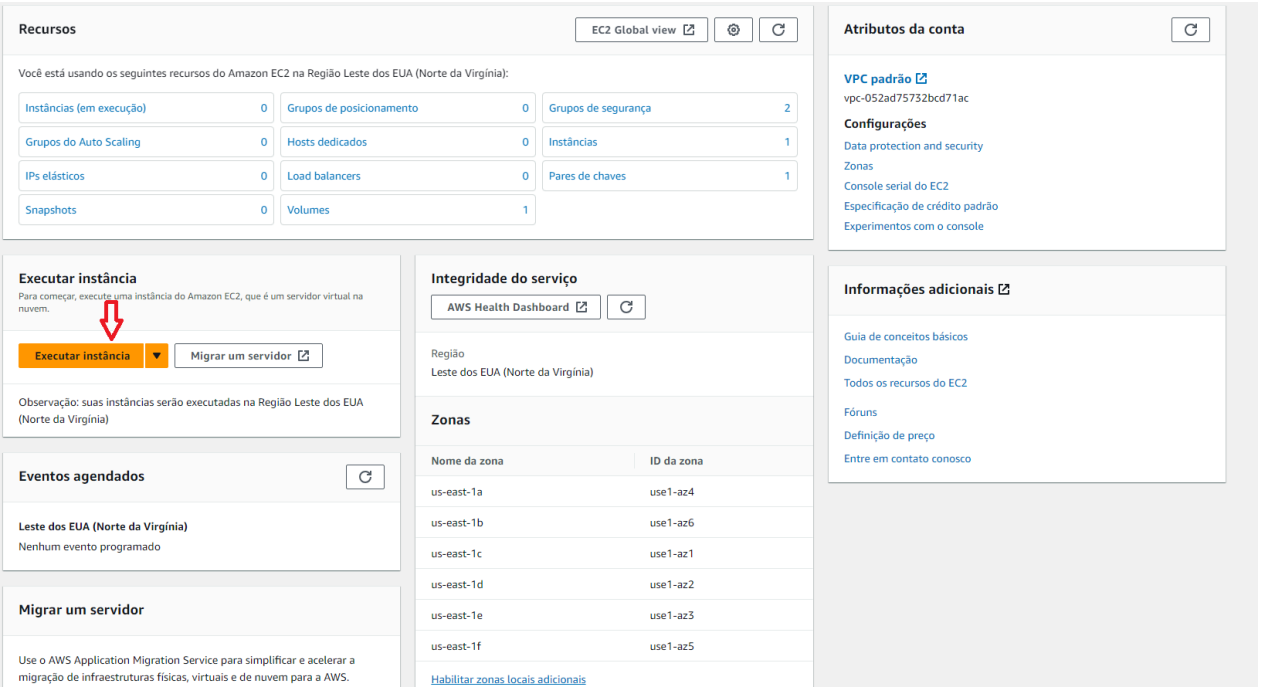
Figura 2 - Painel de serviços da AWS.



Fonte: AWS, 2023.

Ao clicar nesta opção, o *dashboard* do Amazon EC2 é apresentado, onde seleciona-se “Executar instância” para a criação de um novo servidor virtual na nuvem, como mostra a Figura 3.

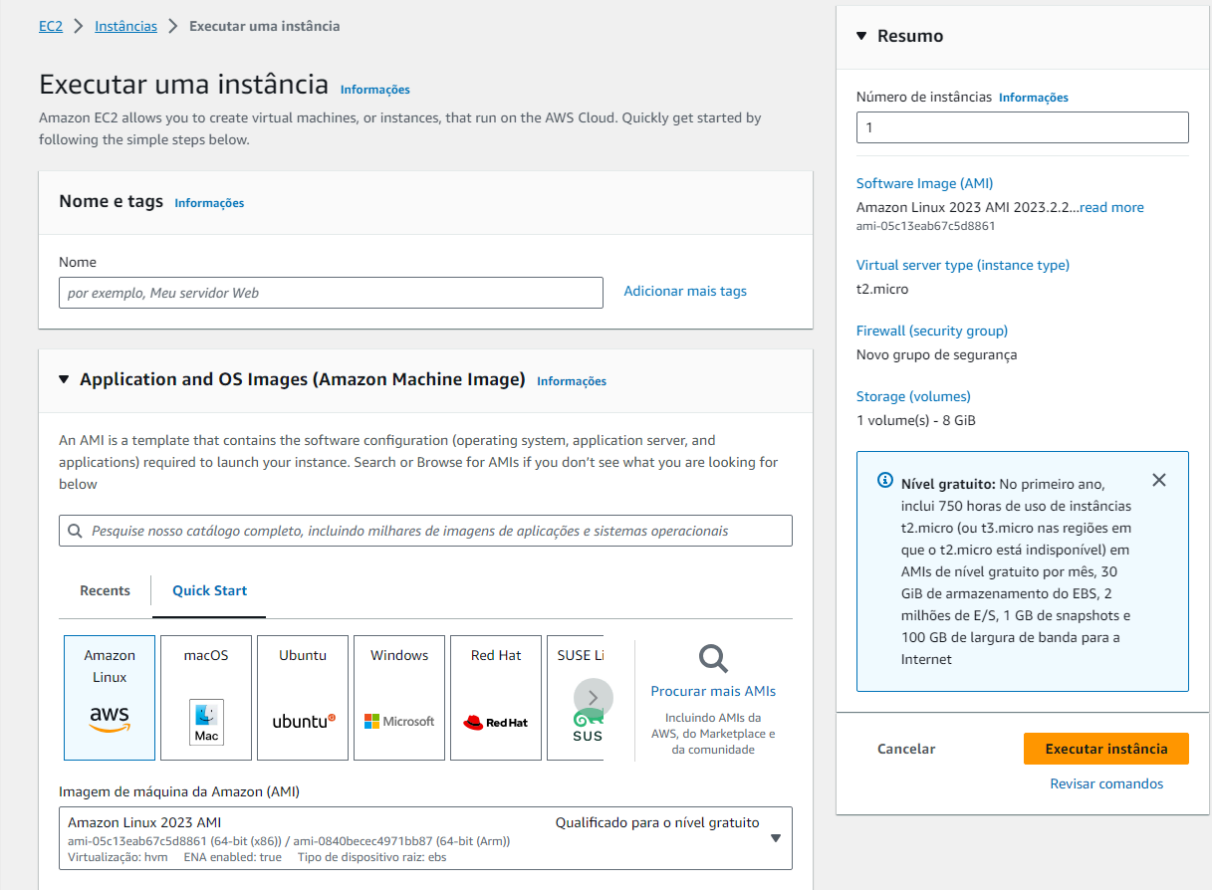
Figura 3 - Painel de recursos do EC2.



Fonte: AWS, 2023.

Após esta etapa, é apresentado um novo *dashboard* de configuração da instância. Inicialmente, é necessário designar um nome para o servidor, ao qual o autor nomeou de “Teste TCC ". Por conseguinte, no painel “Aplicações e imagens de sistemas operacionais”, a Amazon permite que o usuário selecione uma AMI (Amazon Machine Image), que é essencialmente uma imagem pré-configurada de uma instância do EC2, incluindo informações sobre sistema operacional, bibliotecas e aplicações, como apresentado na Figura 4.

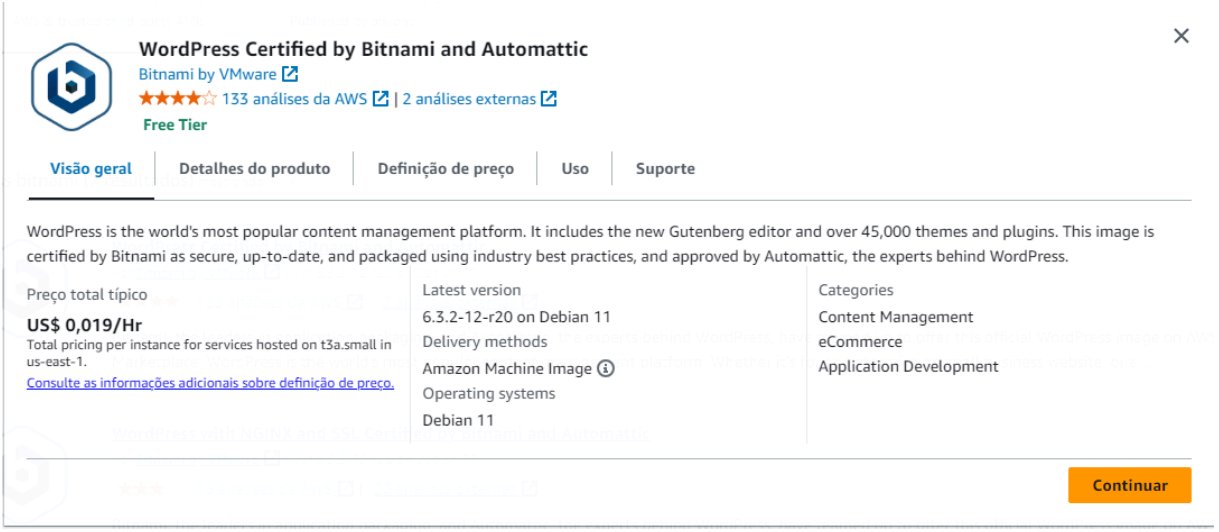
Figura 4 - Painel de configuração da instância.



Fonte: AWS, 2023.

Dentre as milhares de imagens disponíveis, foi procurada aquela referente ao “Wordpress” na aba “AMIs do AWS *Marketplace”* e selecionada a opção “*Wordpress Certified by Bitnami and Automatic”,* conforme mostra a Figura 5.

Figura 5 - Seleção da imagem Wordpress.



Fonte: AWS, 2023.

Após isso, ao retornar para o *dashboard* de configuração da instância, é necessário selecionar o tipo de instância adequada para a aplicação, ou seja, aquela que atenda as necessidades de computação, memória e armazenamento requeridas pela aplicação. No contexto deste estudo de caso, a instância selecionada foi a "*t3.small*", por ela ter características adequadas para o estudo de caso relatado neste capítulo, tais como:

a) Recursos de CPU e memória: A "*t3.small*" tem 2 CPUs virtuais, além de 2GB de memória (AMAZON, 2023);
b) Possui um recurso chamado "créditos de CPU", que acumula recurso computacional durante o período de inatividade da instância e consome esses créditos nos períodos de pico de utilização (AMAZON, 2023);
c) Possui uma largura de banda de rede de até 5 Gbps (AMAZON, 2023).

Em seguida, é necessário criar um par de chaves para a instância. Para isso, a Amazon solicita um nome para o par de chaves, além da escolha do tipo de algoritmo de criptografia e do formato do arquivo da chave privada. No caso, o nome do par chaves foi: "TesteTCC". Além de que optou-se pelo algoritmo de criptografia RSA (Rivest-Shamir-Adleman) e pelo formato ".pem".

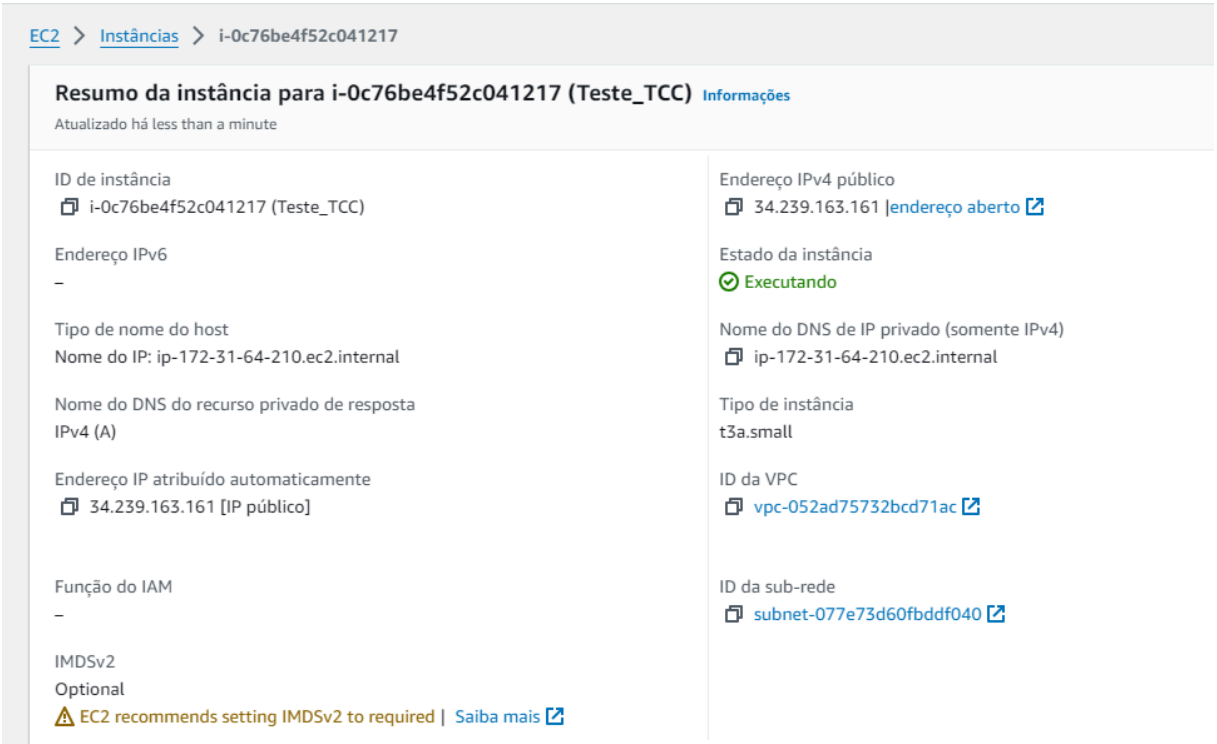
Após essa configuração, um arquivo “.pem” é baixado no computador local, contendo a chave privada associada àquela instância. É crucial que o arquivo seja armazenado de forma segura, pois ele pode ser necessário em caso de uso futuro.

Por fim, clicou-se no botão “Executar instância”, onde o usuário é levado a um novo *dashboard* chamado “instâncias” onde pode observar a instância iniciando o processo de execução. Após alguns minutos, a instância está completamente ativa e já pronta para ser utilizada pelo usuário.

4.2.1 Acesso a aplicação Wordpress

Para acessar a aplicação Wordpress, no *dashboard* “instâncias”, é preciso selecionar o ID da instância, o que direciona o usuário a outro *dashboard* chamado “resumo da instância”, contendo diversas informações relevantes sobre ela, como mostra a Figura 6.

Figura 6 - Painel de resumo da instância.



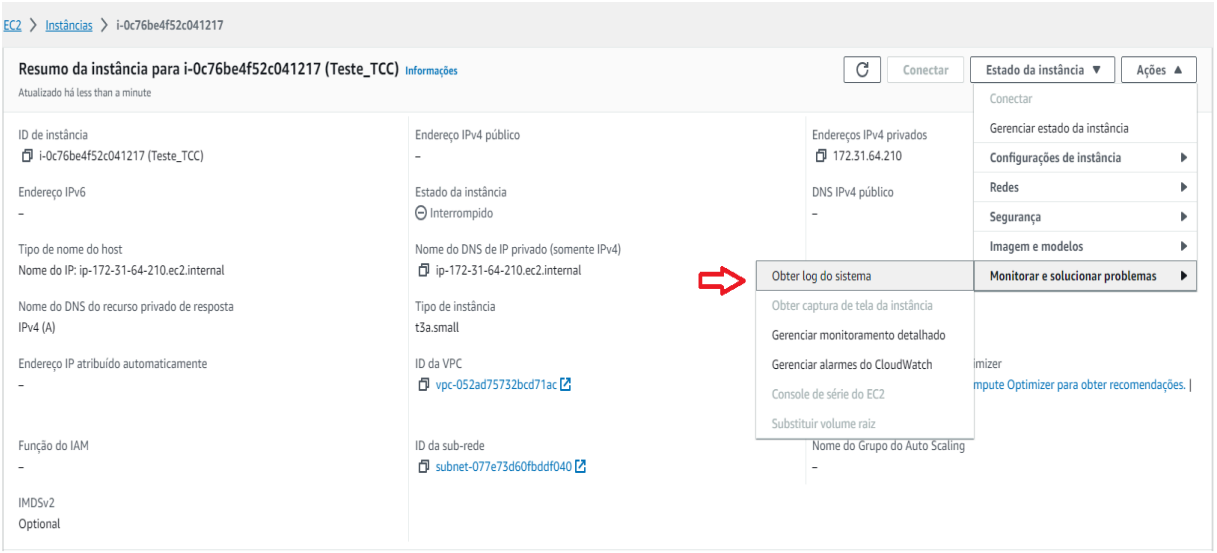
Fonte: AWS, 2023.

Dentre as informações mais relevantes, há o endereço IPv4 público da instância, que é copiado e inserido no navegador para possibilitar o acesso à aplicação.

Após o acesso, o usuário é redirecionado para o blog padrão do Wordpress. Para acessar o painel de controle, basta adicionar “/wp-admin” a URL do navegador, após o endereço IPv4 público da instância, e irá aparecer a área de login do Wordpress.

Com isso, o usuário tem acesso a área de login onde o mesmo deverá informar um nome de usuário e uma senha. Para encontrar estas informações de login, o usuário deve voltar ao *dashboard* “resumo da instância” e clicar na aba “Ações”, assim como em “Monitorar e solucionar problemas” e por último em “Obter log do sistema”, conforme a Figura 7.

Figura 7 - Acesso ao log do sistema.



Fonte: AWS, 2023.

Neste recurso, o cliente terá acesso a um nome de usuário padrão “user” e uma senha criptografada. Com essas informações, é possível fazer login na tela de administração do Wordpress e ter acesso ao painel de controle da aplicação. O nome de usuário e senha podem ser posteriormente alterados de acordo com a preferência do cliente.

4.3 PRIMEIRO ATAQUE DE NEGAÇÃO DE SERVIÇO (DOS)

Após os processos de criação da instância e colocar a aplicação Wordpress em execução, foi escolhida uma ferramenta de ataque de negação de serviço chamada “*slowloris”.*

O *slowloris* é uma ferramenta de ataque de negação de serviço (DoS) que foi desenvolvida com o intuito de explorar vulnerabilidades em servidores web. Este permite que o invasor sobrecarregue um servidor alvo mantendo inúmeras conexões HTTP entre o invasor e o servidor web alvo (CLOUDFLARE).

4.3.1 Como funciona o *slowloris*?

O *slowloris* utiliza requisições HTTP parciais para realizar um ataque em um servidor web. O ataque funciona abrindo estas conexões e mantendo-as abertas pelo maior tempo possível. O código envia periodicamente partes da requisição para que a conexão continue sempre aberta. Isso faz com que o servidor-alvo entenda que as requisições estão apenas “lentas”, e ele fica aguardando que elas sejam fechadas. O servidor de destino tem um número limitado de *threads* disponíveis para processar requisições HTTP. Quando este limite é excedido, as tentativas de conexões enviadas pelo ataque não serão atendidas pelo servidor-alvo, resultando assim em um ataque de negação de serviço (CLOUDFLARE).

Um ataque utilizando o *slowloris* ocorre em quatro etapas principais:

a) Inicialmente o invasor envia para o servidor-alvo várias requisições HTTP parciais (CLOUDFLARE,2023);
b) O servidor-alvo cria *threads* para lidar com as solicitações HTTP, e caso a conexão com o cliente (o invasor) esteja demorando muito, o servidor de origem fechará esta solicitação por tempo excedido, liberando os *threads* para novas requisições (CLOUDFLARE, 2023);
c) Para evitar que o tempo limite de espera do servidor seja expirado, o invasor continua a mandar várias requisições HTTP parciais com o objetivo de enganar o servidor-alvo, fazendo-o acreditar que a solicitação ainda está em andamento, assim mantendo a conexão aberta (CLOUDFLARE, 2023);

d) O servidor de destino não pode encerrar as requisições parciais que estão abertas enquanto aguarda o fim da solicitação. Em determinado momento, todos os *threads* disponíveis pelo servidor estarão em uso, fazendo assim com que o servidor não consiga mais lidar com novas requisições. Isso gera uma sobrecarga e incapacidade do servidor-alvo de responder a novas solicitações, resultando assim em um ataque de negação de serviço (DoS) (CLOUDFLARE, 2023);

O *slowloris* se mostra uma ferramenta de ataque de negação de serviço poderosa pela capacidade de gerar empecilhos significativos para um servidor web sem o consumo excessivo de largura de banda (CLOUDFLARE, 2023).

4.3.2 Utilizando o *slowloris*

Para o presente trabalho, foi utilizada uma versão do *slowloris* baseada no projeto "*Slowloris.pl",* hospedado no *Github* por *GHubgenius* (LAERA, 2013).

O código do *slowloris* foi executado no ambiente Kali Linux, uma distribuição do sistema operacional Linux especializada em testes de segurança e penetração em sistemas. (KALI LINUX, 2023).

A escolha do Kali Linux foi motivada pela sua vasta coleção de ferramentas de segurança integradas, bem como pela apresentação de um sistema intuitivo e simples para as avaliações de vulnerabilidade e testes de segurança exigidos neste trabalho (KALI LINUX, 2023).

Para executar o código, inicialmente, abriu-se o terminal do Kali Linux e navegou-se até o diretório onde o arquivo "*slowloris.pl*" estava localizado. Para a inicialização da ferramenta, é necessário inserir o nome da linguagem utilizada, que nesse caso trata-se do *Perl,* e o nome do arquivo onde o código está inserido, que é o "*slowloris.pl*".

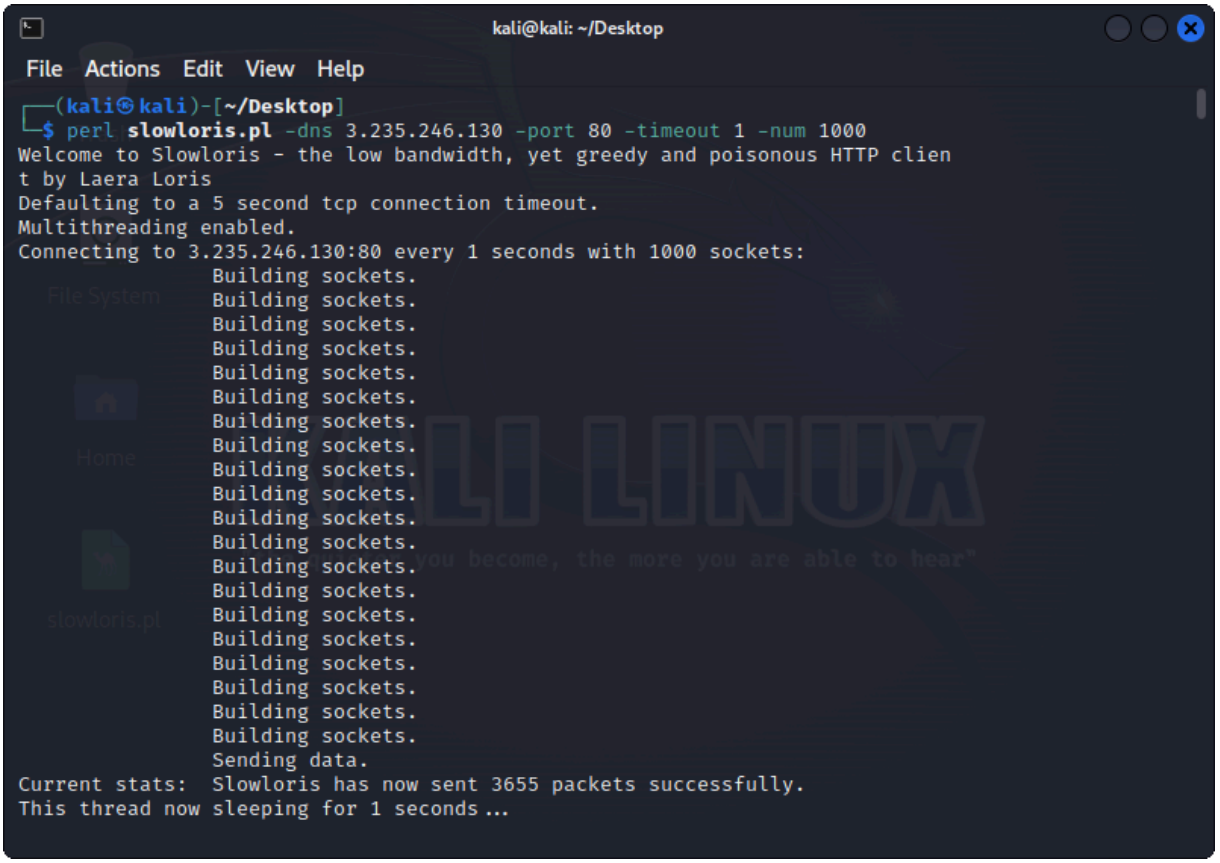
Após o *script* do programa ser executado, foi-se utilizado o comando padrão do *slowloris* para realizar o ataque de negação de serviço. Este comando tem os seguintes parâmetros exigidos (LAERA, 2013):

a. -dns: Parâmetro referente ao nome de domínio do site que será alvo do ataque ou o endereço IP público do site;

b. *-port*: Onde será referenciado o protocolo de internet no qual o alvo está inserido;
c. *-timeout:* Define o tempo limite para as requisições HTTP parciais enviadas pelo código do *slowloris;*
d. *-num:* Especifica o número de conexões simultâneas que serão mantidas abertas com o servidor-alvo;

Na linha de comando do terminal do Kali Linux, referenciou-se: *perl slowloris.pl -dns 3.235.246.130 -port 80 -timeout 1 -num 1000,* como mostrado na Figura 8.

Figura 8 - Linha de comando rodando no terminal do Kali Linux.



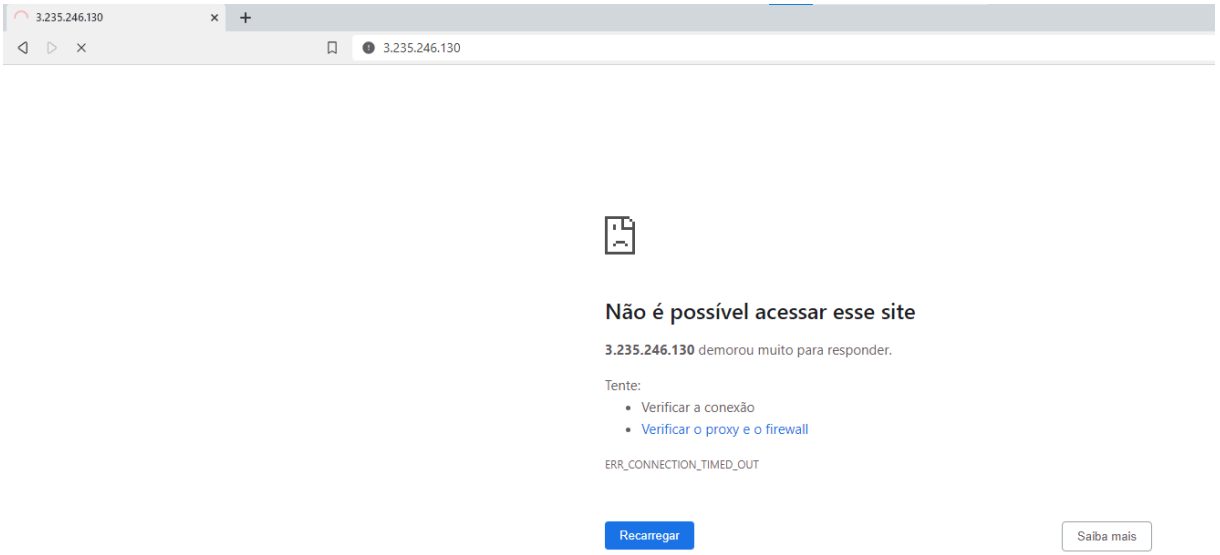
Fonte: O autor.

O número mostrado no parâmetro “*dns”* refere-se ao endereço IPv4 público da aplicação Wordpress na instância do Amazon EC2, enquanto que em “*port* 80” está referenciado a porta padrão de serviços HTTP. No parâmetro “*timeout”* fica

definido que o tempo limite para as requisições HTTP parciais são de 1 segundo, assim como fica decretado as 1000 conexões simultâneas no parâmetro “*num”.*

Após o script ser executado, o ataque de negação de serviço ocorre, esgotando os recursos disponíveis do site hospedado na instância do Amazon EC2 e consequentemente levando à queda da aplicação, conforme mostrado na Figura 9.

Figura 9 - Falha ao carregar a página após o ataque de negação de serviço.



Fonte: O autor.

4.4 ANÁLISES MÉTRICAS

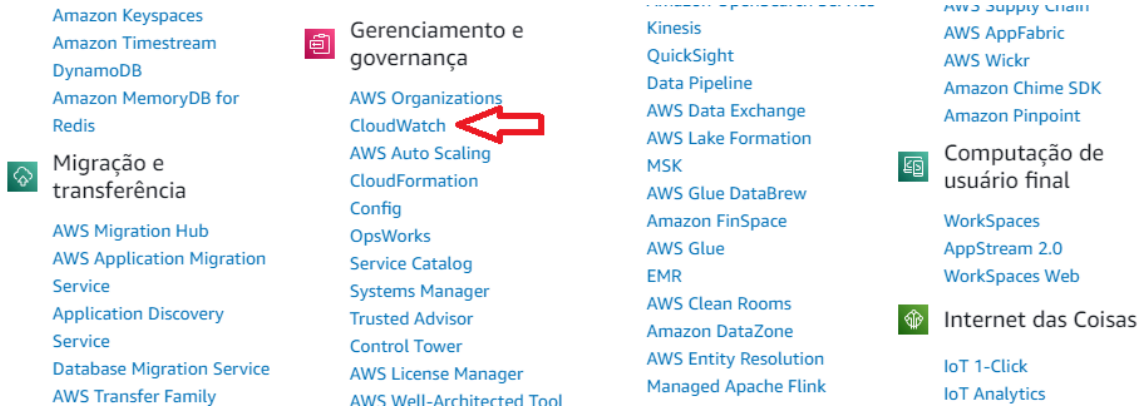
A AWS disponibiliza recursos para o monitoramento de instâncias que podem ser muito úteis para a tomada de decisões precisas em caso de falhas na segurança da nuvem. Dentre os serviços disponíveis, um dos mais acessíveis é o *CloudWatch*.

O *CloudWatch* é um serviço que coleta logs e métricas dos recursos e aplicações que rodam em um servidor da AWS em tempo real. Com ele é possível otimizar recursos e definir ações a serem tomadas em caso de algum comportamento indesejado em uma aplicação, por exemplo (AMAZON, 2023).

Esse serviço foi utilizado neste trabalho para a melhor compreensão do comportamento da instância no Amazon EC2 durante a realização do ataque de negação de serviço e no processo de mitigação.

Para usar o serviço, foi selecionado no agrupamento “Gerenciamento e governança”, como mostra a Figura 10.

Figura 10 - Painel de seleção do serviço *CloudWatch.*



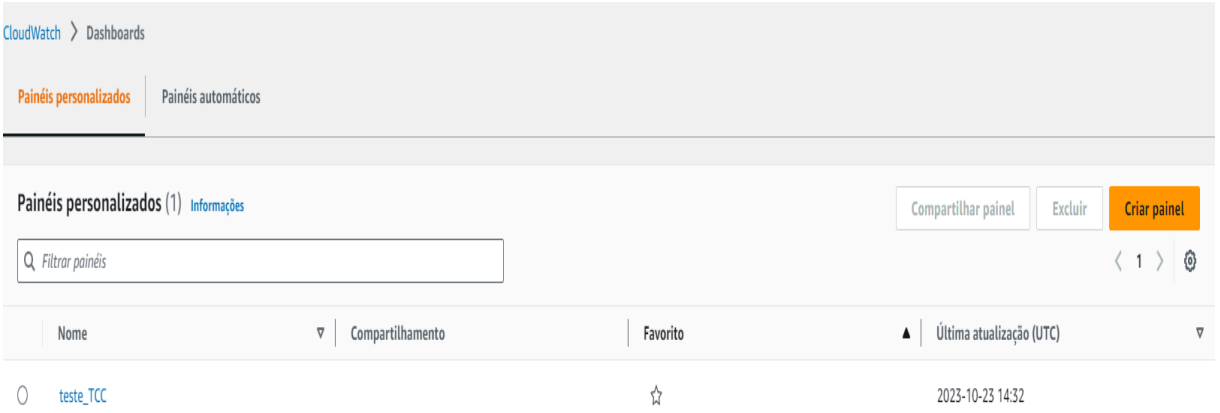
Fonte: AWS, 2023.

Após isso, o usuário é direcionado ao *dashboard* principal do *CloudWatch,* onde é apresentado um *overview* das principais funcionalidades do serviço, incluindo a criação de painéis para as métricas e a definição de alarmes, para caso alguma métrica ultrapassar um limite especificado pelo usuário.

No *dashboard*, foi selecionada a aba “Painéis”.

Em seguida, o usuário é direcionado ao *dashboard* de painéis, que podem ser personalizados ou automáticos. Neste trabalho, foi criado um novo painel específico para a acompanhar a aplicação Wordpress alocada na instância do Amazon EC2. Para isso, foi selecionado “Criar painel” e designado o nome “teste_TCC”, conforme a Figura 11.

Figura 11 - *Dashboard* de criação de painéis.

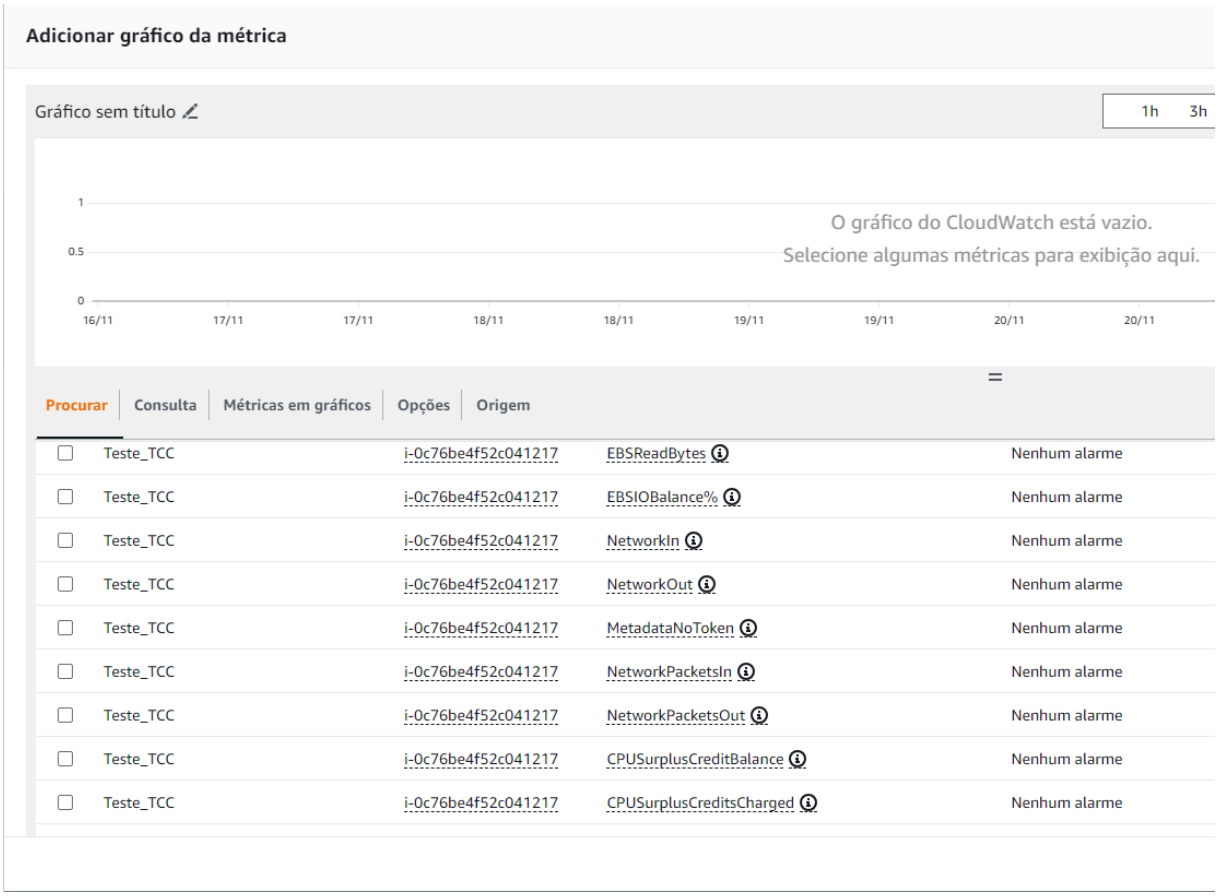


Fonte: AWS, 2023.

Ao criar um novo painel, é apresentada uma tela para que o usuário possa escolher o tipo de *widget* que será usado. A escolha depende de como o usuário deseja observar as métricas ou logs de seus serviços. No caso deste trabalho, o *widget* selecionado foi de gráfico tipo “Linha”, com a fonte de dados “Métricas”.

Após escolher o tipo de *widget,* é possível escolher um serviço que esteja sendo utilizado para criar a métrica referente a ele. Neste caso, foi escolhido o “EC2” e selecionado “Métricas por instância”, onde é apresentado diversas métricas para a instância “Teste_TCC”, conforme mostra a Figura 12.

Figura 12 - Painel de seleção das métricas.



Fonte: AWS, 2023.

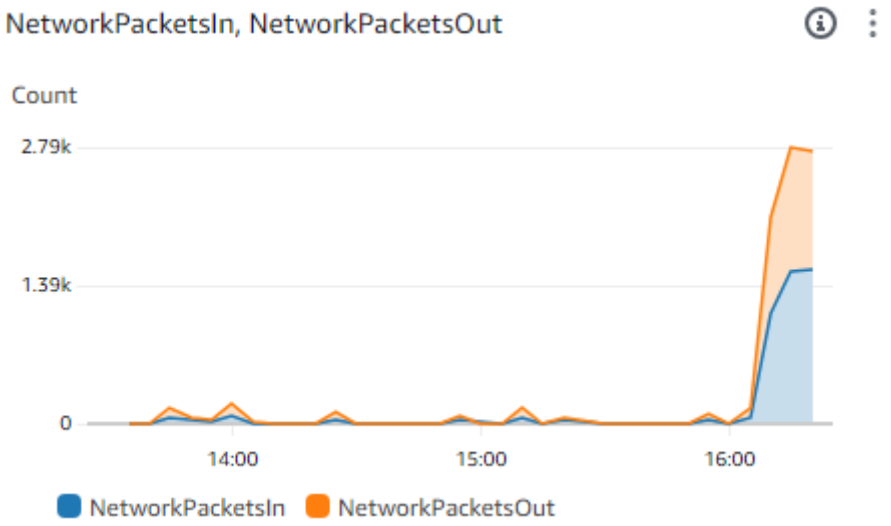
As métricas escolhidas para este trabalho foram:

a) “*NetworkPacketsIn*, *NetworkPacketsOut*”- Métricas relacionadas ao tráfego de rede na instância;
b) “CPU*Utilization*” - Corresponde a utilização dos créditos de CPU da instância durante um período de tempo.

Estas duas métricas serviram de ajuda para a análise do comportamento da instância durante o período de ataques de negação de serviço (DoS), pois ao analisá-las, pôde-se entender melhor como a AWS agia em tempo real a uma situação de ataque inesperado.

Na Figura 13, observa-se o comportamento da métrica do tráfego de rede durante o ataque de negação de serviço.

Figura 13 - Gráfico do tráfego de rede.



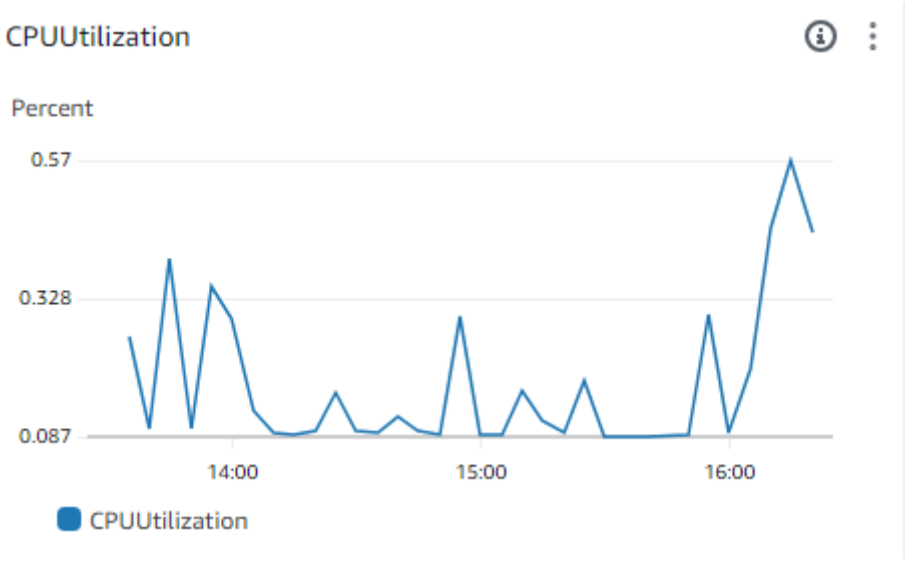
Fonte: AWS, 2023.

Como se pode notar no gráfico da Figura 13, o número de pacotes de rede recebidos e enviados alterou-se muito no intervalo das 14:00 às 16:00. Os pacotes de entrada foram representados em azul, enquanto os pacotes de saída em laranja, e nota-se que no período antes das 16:00, houve um tráfego baixo de entrada de pacotes de rede, o que pode ser explicado pelas poucas solicitações de cliente na aplicação Wordpress, já que havia um número de requisições controladas. Assim como havia pacotes em relação a saída de dados um pouco maiores que os de entrada, porém em situações muito semelhantes e em condições normais.

A partir das 16:00 (horário que o ataque de negação de serviço foi realizado), observa-se que o número de pacotes de entrada e saída aumentaram significativamente. Isso pode ser explicado pela instância ter que lidar com um número de solicitações HTTP muito maiores que anteriormente(relaciona-se aos pacotes de entrada), além da instância aumentar muito os pacotes de saída devido a necessidade da instância de gerar respostas a cada uma das requisições, o que gera um fluxo de pacotes de saída muito maior.

A outra métrica observada foi a de utilização da CPU, conforme mostra a Figura 14.

Figura 14 - Gráfico da utilização da CPU.



Fonte: AWS, 2023.

Como pode ser observado no gráfico, a utilização da CPU é medida em porcentagem no eixo Y em relação a passagem do tempo no eixo X. Esta métrica representa a carga de trabalho da CPU com o passar do tempo. (AMAZON, 2023)

Como observado, há um pico de utilização do processamento da CPU a partir das 16:00, mesmo horário em que foi realizado o ataque de negação de serviço, o que indica que os recursos de processamento da instância foram muito mais exigidos durante esse período do tempo. Em determinado momento do ataque, a CPU chegou no máximo de utilização de 0.57, o que indica que 57% da capacidade da CPU foi utilizada durante aquele período do ataque, o que é considerado um pico de utilização comparado a média que fica em 8,7% de utilização.

Essa métrica deu a informação valiosa que a instância teve uma sobrecarga de utilização durante o período do ataque de negação de serviço, o que pode causar problemas de desempenho na aplicação Wordpress, fazendo que os usuários tenham que esperar mais tempo para que a página seja carregada, por exemplo.

A partir da análise das métricas apresentadas previamente, foi possível compreender melhor como a instância reage em um caso de ataque de negação de serviço utilizando o *slowloris.* E tais parâmetros serviram como base para a implementação do método de segurança que visa mitigar tal ataque.

4.5 CONFIGURANDO A SEGURANÇA DA APLICAÇÃO

Conforme observado nas métricas, a aplicação se mostrou extremamente suscetível a ataques de negação de serviço. Logo, foi de interesse buscar métodos disponíveis pela *Amazon Web Services* para proteger a aplicação.

Como já foi visto neste trabalho, dentre os principais serviços de segurança da AWS, existem o AWS *Shield Standard* e os grupos de segurança das instâncias no Amazon EC2.

O AWS *Shield Standard* é um sistema de segurança agregado a todos os serviços disponíveis pela AWS, logo, as instâncias do Amazon EC2 estão incluídas no serviço (AMAZON, 2023).

Isto demonstra que a aplicação Wordpress já está sob proteção do serviço de segurança. O AWS *Shield Standard* trabalha em tempo real para detectar e mitigar ataques de negação de serviço. A forma que o serviço utilizou para tentar fazer a mitigação do ataque de negação de serviço da ferramenta *slowloris* foi o processo de “elasticidade”. O serviço de segurança é capaz de ajustar dinamicamente os seus recursos para acomodar várias áreas de tráfego, incluindo os picos de requisições que acontecem durante o ataque do *slowloris* (AMAZON, 2023).

O resultado da ação do serviço de segurança da Amazon é uma tentativa constante de entregar a aplicação aos clientes que a requerem. Logo, observou-se que mesmo com o ataque do *slowloris,* a AWS constantemente buscava recarregar a página para que esta pudesse ser acessada.

Entretanto, nota-se que isso demandou um esforço muito grande da AWS para que a aplicação fosse mantida, já que o AWS *Shield Standard* é um serviço de segurança básico e pode não ser o mais eficiente em muitos casos, incluindo o caso deste trabalho.

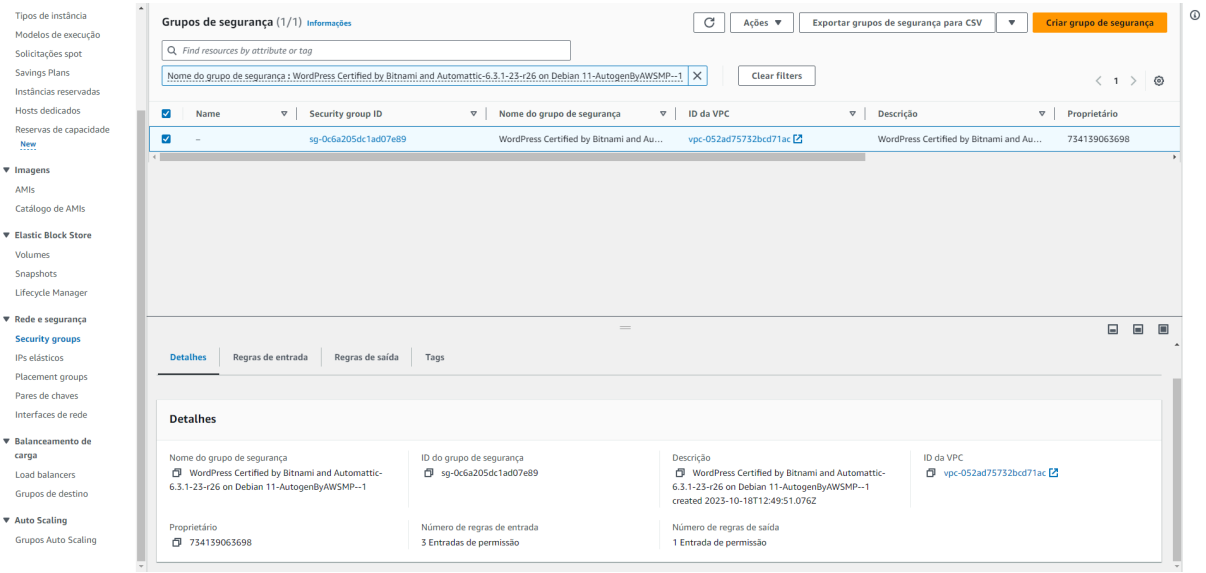
4.5.1 Implementação dos grupos de segurança

Para mitigar o ataque de negação de serviço utilizando o *slowloris,* mostrou-se necessário a implementação dos grupos de segurança do Amazon EC2. Como já foi relatado neste trabalho, os *security groups* funcionam como um *firewall* virtual que visa proteger o tráfego de entrada e saída de uma instância (AMAZON, 2023).

Para a implementação do recurso, foi acessado na aba “Rede e segurança” o nome “*Security Groups*”. Com isso, é aberto o *dashboard* principal que apresenta grupos de segurança já feitos e onde se pode criar novos.

No estudo de caso em particular, a aplicação Wordpress que foi utilizada já apresentava um grupo de segurança padrão referente a imagem disponibilizada pela Amazon. O nome deste grupo de segurança é: “WordPress Certified by Bitnami and Automattic-6.3.1-23-r26 on Debian 11-AutogenByAWSMP--1”, conforme mostra a Figura 15.

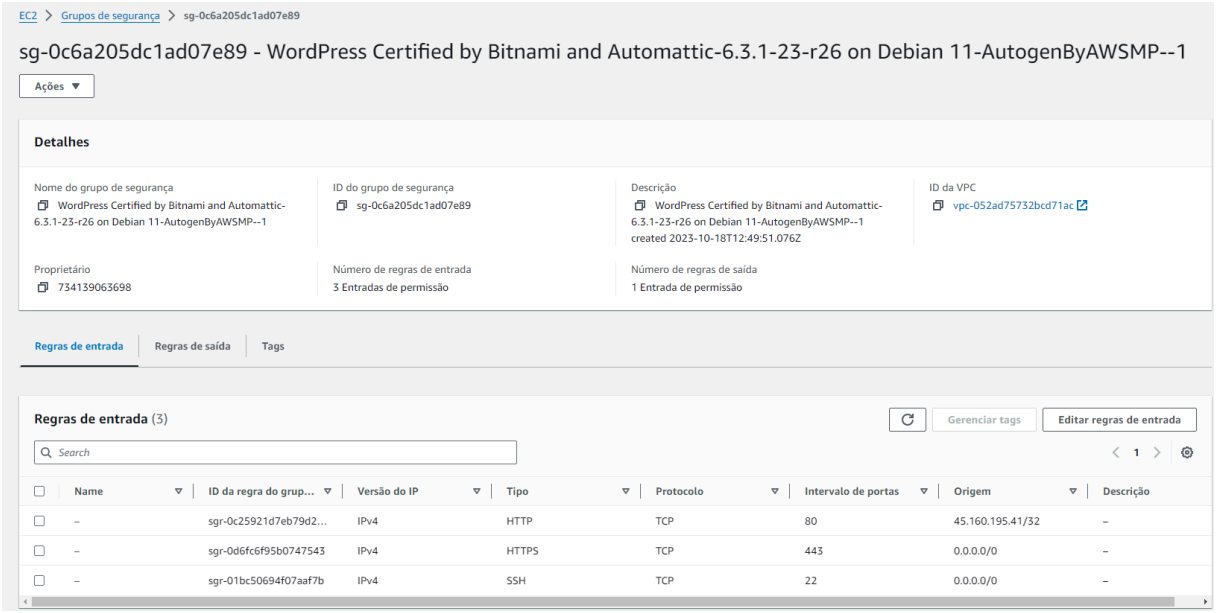
Figura 15 - Painel inicial dos grupos de segurança.



Fonte: AWS, 2023.

Ao acessar o grupo de segurança referente a instância onde a aplicação está alocada, um novo *dashboard* é apresentado contendo as regras de entrada e saída, conforme mostra a Figura 16.

Figura 16 - Painel da regra de segurança.



Fonte: AWS, 2023.

Primeiramente, foi selecionada a aba “Editar regras de entrada”, onde é apresentado um painel para a edição do tráfego de entrada na instância. Nas configurações, são apresentados alguns parâmetros que devem ser preenchidos, dentre eles:

a. O protocolo que terá acesso a instância: O Amazon EC2 disponibiliza uma série de protocolos dependendo da aplicação, estes podem ser do tipo SSH, HTTP, HTTPS e outros (AMAZON, 2023);
b. O intervalo de portas que podem acessar a instância: Uma porta será atrelada ao protocolo escolhido anteriormente (AMAZON, 2023);
c. Origem da regra: o parâmetro que determina o endereço IP ou o intervalo de endereços IP que terão acesso a instância (AMAZON, 2023);
d. Descrição: Uma parte opcional que pode ser usado para descrever a regra, comumente utilizado para que pessoas não familiarizadas com uma determinada regra, possam entender como ela funciona (AMAZON, 2023).

No tipo de protocolo, optou-se pelo HTTP, utilizando o protocolo de controle e transmissão TCP na porta padrão 80. O parâmetro crucial neste estudo de caso é o “Origem da regra”, onde se especifica o endereço IP autorizado a acessar à

instância, sendo configurado como: 45.160.195.41/32, o endereço IP referente a máquina do autor deste trabalho.

É relevante destacar que, em um cenário de ataque de negação de serviço com objetivos maliciosos, o administrador do sistema poderia adotar um intervalo de endereços IP permitidos a interagir com a aplicação, como os endereços dos clientes autorizados a acessar aquela instância.

No estudo de caso em questão, as regras de saída não precisaram ser alteradas do padrão pois em um ataque de negação de serviço do tipo apresentado neste trabalho, o relevante é a mitigação da conexão do invasor com a instância por meio do bloqueio dos parâmetros citados anteriormente nas regras de entrada dos *security groups.*

No entanto*,* é importante ressaltar que as regras de saída podem ser relevantes em casos específicos não presentes neste trabalho.

4.6 ATAQUE APÓS A CONFIGURAÇÃO DO SECURITY GROUP

Após a implementação do grupo de segurança, foi realizado um novo ataque utilizando a ferramenta *slowloris,* com o objetivo de verificar a eficácia da regra feita nos *security groups*.

Na realização do novo ataque, foram inseridos os mesmos parâmetros que já anteriormente foram citados neste trabalho, com a mudança apenas do parâmetro "*dns".* Por padrão, os endereços IP públicos nas instâncias do Amazon EC2 são do tipo dinâmicos, ou seja, cada vez que a instância é iniciada ou reiniciada, ela receberá um novo endereço IP. Logo, o "dns" desta vez foi: 3.236.122.210, conforme mostra a Figura 17.

Figura 17 - Ataque após configuração do *security group.*

Fonte: O autor

É importante destacar que, para o êxito do teste de segurança, foi necessário realizar o teste utilizando outro endereço IP público, identificado como 45.189.28.244/32, que agora passaria a ser o endereço IP utilizado pelo invasor na tentativa de um novo ataque.

Isso foi necessário pois, como visto anteriormente, a regra de segurança configurada permite que um único endereço IP (45.160.195.41/32) tenha acesso a instância, bloqueando todos os demais.

Conforme evidenciado na Figura 23, o ataque utilizando o *slowloris* não foi eficaz, pois a ferramenta não conseguiu enviar qualquer pacote de dados para a aplicação. Isto ocorreu pois na tentativa de comunicação do servidor de origem (invasor) com a aplicação Wordpress, a regra de segurança que foi definida para a instância agiu como um *firewall* virtual, identificando que o IP 45.189.28.244/32 não é o mesmo que foi estabelecido como acesso permitido no grupo de segurança. Logo, o tráfego de entrada foi bloqueado para o endereço IP do invasor e liberado apenas para o endereço especificado na regra de segurança.

4.7 RESULTADO

O ataque de negação de serviço utilizando a ferramenta *slowloris* mostrou-se inicialmente um desafio significativo para a aplicação Wordpress hospedada na instância do Amazon EC2. Como foi visto, os ataques DoS geram uma vulnerabilidade imensa a aplicações e serviços, e em especial, a ferramenta *slowloris* consegue causar danos graves utilizando pouco recurso computacional.

No entanto, os serviços de segurança da AWS demonstraram eficácia notável no processo de segurança da aplicação Wordpress que foi o alvo deste estudo. Com o AWS *Shield Standard*, observou-se uma resposta dinâmica na tentativa de mitigação do ataque de negação de serviço, utilizando-se da adaptação dinâmica para minimizar a degradação feita na aplicação.

Contudo, apenas o serviço padrão da Amazon não foi suficiente para a mitigação completa do ataque da ferramenta *slowloris*, sendo assim necessário a implementação dos *security groups*, que revelou-se vital na contenção do ataque. A restrição de acesso à instância utilizando o endereço IP permitiu controlar a interação com a instância e consequentemente com a aplicação Wordpress, bloqueando o tráfego não autorizado, como o do invasor.

É essencial salientar que em casos de ataques de negação de serviço reais, existem desafios muito maiores para serem enfrentados dos que os apresentados neste estudo de caso, o que salienta a utilização de recursos mais avançados disponibilizados pela AWS que já foram citados anteriormente.

O resultado positivo destaca a importância da configuração adequada do ambiente de segurança, reforçando a necessidade constante de aprimoramento de medidas de segurança em aplicações da AWS.

Em síntese, o estudo de caso apresentou perspectivas valiosas sobre a resistência da infraestrutura da *Amazon Web Services* a ameaças específicas, proporcionando um panorama que serve de orientação para possíveis vulnerabilidades em sistemas, e assim, realizar as tomadas de decisão adequadas para ataques futuros.

5 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo geral propor configurações de segurança para a proteção de uma aplicação em nuvem, visando protegê-las de ataques cibernéticos, em especial, o ataque de negação de serviço (DoS). Para isso, foram utilizadas ferramentas de segurança disponibilizadas pela AWS. Com base nos resultados encontrados no desenvolvimento deste trabalho, pode-se indicar que o objetivo proposto foi alcançado.

Constatou-se que a *Amazon Web Services* possui algumas vulnerabilidades de segurança como qualquer outra plataforma. No tocante a este trabalho, nota-se que as configurações inadequadas podem deixar uma aplicação vulnerável, mesmo em uma provedora mundialmente conhecida como a AWS. É importante destacar que, conforme a própria plataforma relata em seus documentos oficiais nos *websites* da empresa, a segurança na nuvem é uma responsabilidade compartilhada entre a provedora e o usuário. Logo, cabe ao cliente entender sua parcela de contribuição para que sejam tomadas as medidas de segurança mais efetivas.

No entanto, no que cabe a AWS, observa-se que esta dispõe de diversos recursos para manter o ambiente em nuvem mais seguro, como serviços inatos de proteção (AWS *Shield*), ferramentas de análise de recursos e proteção, além de serviços configuráveis pelos usuários, para manter a segurança de suas aplicações. Contudo, observou-se que na configuração padrão de segurança no ambiente em que realizou-se o estudo de caso deste trabalho, há brechas de segurança relacionadas a ataques cibernéticos.

Logo, foi necessário a utilização de mais ferramentas de proteção para que o resultado desejado fosse obtido. Com o serviço inato da AWS de segurança na nuvem (AWS *Shield*) e a implantação dos *security groups* na instância utilizada neste trabalho, foi possível realizar a mitigação de um ataque de negação de serviço (DoS) e assim, colocar a aplicação em um ambiente de maior segurança.

Os resultados aqui apresentados, oferecem evidências que a segurança na computação em nuvem é um tema cada vez mais relevante para profissionais da área, pois é uma preocupação que todas as empresas que utilizam deste recurso tem. A contribuição entre ferramentas disponibilizadas pela provedora e a utilização adequada destas pelo cliente, mostrou-se imprescindível para que se pudesse aumentar a segurança na aplicação desejada. Assim, este estudo contribui para que

o leitor possa entender melhor como funciona a segurança na computação em nuvem, como utilizar-se dos princípios de segurança adequadamente e como usufruir de recursos das provedoras para que possa aumentar a proteção de aplicações em relação a ataques cibernéticos.

No que tange às limitações deste trabalho, pode-se destacar a não utilização de ferramentas mais avançadas de mitigação a aplicações na nuvem disponibilizadas pela *Amazon Web Services* como o AWS WAF e o AWS *Shield Advanced* por serem ferramentas pagas. Essa restrição influenciou no quesito de facilidade da proteção da aplicação, haja visto que os serviços avançados são mais automatizados e detém maior poder de mitigação contra ataques cibernéticos. Outra limitação constatada foi relacionada ao ataque de negação de serviço utilizado neste trabalho, que é na camada de aplicação. Ataques mais poderosos como de amplificação e refletores, podem colocar à prova a implantação de segurança proposta neste estudo.

5.1 RECOMENDAÇÕES DE TRABALHOS FUTUROS

Referente às limitações colocadas anteriormente, recomenda-se para futuros trabalhos:

a) A utilização de mais ferramentas de segurança disponibilizadas pela AWS, visando aumentar ainda mais a segurança de aplicações na nuvem;
b) Testar aplicações na nuvem com ataques cibernéticos mais abrangentes e poderosos, como os ataques distribuídos de negação de serviço (DDoS);
c) Ampliar a discussão sobre as melhores práticas de segurança no ambiente de computação em nuvem, haja visto que essa é uma das maiores preocupações das organizações referentes a este tema;
d) Pesquisar sobre a utilização de inteligência artificial para a detecção avançada de ameaças e para que a resposta a essas seja de forma automatizada.

REFERÊNCIAS

Amazon CloudWatch. Monitoramento e observabilidade da AWS. Disponível em: https://aws.amazon.com/pt/cloudwatch/. Acesso em: 22/11/2023.

Amazon Web Services. Conceitos do Amazon EC2. Disponível em: https://docs.aws.amazon.com/pt_br/AWSEC2/latest/UserGuide/concepts.html. Acesso em: 31/10/2023.

Amazon Web Services. Grupos de Segurança no Amazon EC2. Disponível em: https://docs.aws.amazon.com/pt_br/AWSEC2/latest/UserGuide/ec2-security-groups.html. Acesso em: 01/11/2023.

Amazon Web Services. Identity and Access Management para o Amazon EC2. Disponível em: https://docs.aws.amazon.com/pt_br/AWSEC2/latest/UserGuide/security-iam.html. Acesso em: 31/10/2023.

Amazon Web Services. Infraestrutura global da AWS. Disponível em: https://aws.amazon.com/pt/about-aws/global-infrastructure/?pg=WIAWS. Acesso em: 31/10/2023.

Amazon Web Services. O que é a AWS? Disponível em: https://aws.amazon.com/pt/what-is-aws/. Acesso em: 31/10/2023.

Amazon Web Services. Pares de Chaves no Amazon EC2 e instâncias do Linux. Disponível em: https://docs.aws.amazon.com/pt_br/AWSEC2/latest/UserGuide/ec2-key-pairs.html. Acesso em: 01/11/2023.

Amazon Web Services. Perguntas frequentes sobre AWS WAF. Disponível em: https://aws.amazon.com/pt/waf/faqs/#:~:text=AWS%20WAF%20is%20a%20web,on%20conditions%20that%20you%20define. Acesso em: 01/11/2023.

Amazon Web Services. Recursos do AWS Shield. Disponível em: https://aws.amazon.com/pt/shield/features/. Acesso em: 01/11/2023.

Amazon Web Services. Regras de Grupos de Segurança no Amazon EC2. Disponível em: https://docs.aws.amazon.com/pt_br/AWSEC2/latest/UserGuide/security-group-rules.html. Acesso em: 01/11/2023.

Amazon Web Services. *Security groups - Amazon Virtual Private Cloud*. Disponível em: https://docs.aws.amazon.com/vpc/latest/userguide/security-groups.html. Acesso em: 01/11/2023.

Amazon Web Services. Segurança no Amazon EC2. Disponível em: https://docs.aws.amazon.com/pt_br/AWSEC2/latest/UserGuide/ec2-security.html. Acesso em: 31/10/2023.

Amazon Web Services. Tipos de instância Amazon EC2. Disponível em: https://aws.amazon.com/pt/ec2/instance-types/. Acesso em : 11/11/2023.

Amazon. Amazon Web Services Launches. Disponível em: https://press.aboutamazon.com/2006/3/amazon-web-services-launches. Acesso em: 31/10/2023.

Bloomberg. Sony Network said to have been invaded by hackers using Amazon.com Server. Disponível em: https://www.bloomberg.com/news/articles/2011-05-13/sony-network-said-to-have-been-invaded-by-hackers-using-amazon-com-server?embedded-checkout=true. Acesso em: 07/12/2023

Check Point Software Technologies. Check Point Press Releases: Cloud Security Threats Remain Rampant: Check Point Survey Reveals Heightened Concerns for 76% of Organizations Amid 48% Increase in Cloud-Based Network Attacks. **Check Point,** 2023. Disponível em: https://www.checkpoint.com/press-releases/cloud-security-threats-remain-rampant-check-point-survey-reveals-heightened-concerns-for-76-of-organizations-amid-48-increase-in-cloud-based-network-attacks/. Acesso em: 15 dez. 2023.

CHOU, Te-Shun. Security threats on cloud computing vulnerabilities. **International Journal of Computer Science & Information Technology**, v. 5, n. 3, p. 79, 2013.

Claranet. AWS: Entenda como funciona o serviço de nuvem da Amazon. Disponível em: https://br.claranet.com/blog/aws-entenda-como-funciona-o-servico-de-nuvem-da-amazon. Acesso em: 31/10/2023.

Cloudflare. Ataque DDoS de inundação ping (ICMP) - Cloudflare. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/ping-icmp-flood-ddos-attack/. Acesso em: 08/12/2023.

Cloudflare. O que é o *Slowloris?* - Cloudflare. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/ddos-attack-tools/slowloris/#:~:text=O%20Slowloris%20%C3%A9%20um%20ataque,abertas%20pelo%20maior%20tempo%20poss%C3%ADvel. Acesso em: 14/11/2023

ERICKSON, Jon. **Hacking:** The Art of Exploitation. 2. ed. [S.l]: No Starch Press, 2008.

Flexera. 2023 State of the Cloud Report. **Flexera,** 2023. Disponível em: https://info.flexera.com/CM-REPORT-State-of-the-Cloud-2023-Thanks?revisit#highlights. Acesso em: 15 dez. 2023.

GHubgenius. Slowloris.pl (2013). GitHub. Disponível em: https://github.com/GHubgenius/slowloris.pl. Acesso em: 23/09/2023

Kali Linux. What is Kali Linux? Disponível em: https://www.kali.org/docs/introduction/what-is-kali-linux/. Acesso em: 25/11/2023.

MACHADO, FELIPE NERY RODRIGUES. **Segurança da informação: princípios e controle de ameaças**. São Paulo, SP. Saraiva Educação SA, 2014.

National Institute of Standards and Technology. 2012. The NIST Definition of Cloud Computing. NIST Special Publication 800-145. Disponível em: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf. Acesso em: 12/12/2023.

PEDROSA, Paulo HC; NOGUEIRA, Tiago. Computação em nuvem. São Paulo, v. 6, 2011. Disponível em: https://www.ic.unicamp.br/~ducatte/mo401/1s2011/T2/Artigos/G04-095352-120531-t2.pdf**.** Acesso em: 13/12/2023.

RICHTER, Felix. Cloud Infrastructure Market: Amazon Maintains Lead in the Cloud Market. **Statista,** 2023. Disponível em: https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/. Acesso em: 15 dez. 2023.

SANTOS, Tiago. **Fundamentos da computação em nuvem**. São Paulo: Editora Senac São Paulo, 2018.

STALLINGS, William. **Network Security Essentials**: Applications and Standards. 6. ed. [S.l]: Pearson, 2017.

TANENBAUM, A.S. **Sistemas Operacionais Modernos**: 4ª edição. São Paulo, SP. Pearson Education, 2016.

VERAS, Manoel. **Arquitetura de Nuvem (AWS): Amazon Web Services**. São Paulo: Brasport, 2013.

WINKLER, Vic JR. **Securing the Cloud: Cloud computer Security techniques and tactics**. [S.l]: Elsevier, 2011.