Segurança e Computação em Nuvem: Uma Abordagem Utilizando Instância AWS EC2 com AWS Inspector e GuardDuty

André Ferreira Caetano
Graduando em Redes de Computadores pela Fatec Bauru
E-mail: andre.caetano2@fatec.sp.gov.br

Erick Cesar Domingos Barbosa
Graduando em Redes de Computadores pela Fatec Bauru
E-mail: erick.barbosa@fatec.sp.gov.br

Lucas Del Rei Silva
Graduando em Redes de Computadores pela Fatec Bauru
E-mail: lucas.silva587@fatec.sp.gov.br

Gustavo Cesar Bruschi
Docente na Fatec Bauru
E-mail: gustavo.bruschi@fatec.sp.gov.br

RESUMO:

Atualmente, as empresas buscam meios mais rentáveis e seguros para suas organizações e para isso eles voltaram seus olhos para as infraestruturas em nuvem para reduzir custos e aumentar a capacidade produtiva. Entretanto muitas dessas aplicações não são seguras e nos propusemos a verificar a segurança e confiabilidade de umas das infraestruturas em nuvem mais populares do momento, a AWS. Este artigo tem como proposta de trabalho estudar e avaliar a segurança e as ferramentas da AWS. Neste artigo foram utilizadas o GuardDuty e o Amazon Inspector quando utilizadas em uma instância EC2. Para realizar esse teste foi criada uma instância AWS EC2 disponibilizada após ter sido criada um starter account do qual foi instalada na máquina física de um dos nossos integrantes. Em seguida foi gerado um grande tráfego de dados em nossa instância e foi feita uma varredura pela ferramenta Wireshark para verificar a estabilidade dos dados, em seguida foi utilizada a ferramenta Amazon inspector para verificar irregularidades em nossa instância; enfim utilizamos a ferramenta GuardDuty para avaliar se haviam acontecido invasões provenientes de terceiros. Após realizado os testes, o Amazon Inspector nos informou de um problema de segurança nas portas, enquanto o Amazon GuardDuty barrou ataques direcionados a essa porta. Conclui-se, portanto, que as ferramentas trabalharam muito bem em conjunto para assegurar a segurança de nossa instância.

Palavras-chave: Computação em Nuvem, AWS, Segurança, GuardDuty, Inspector.

ABSTRACT:

Nowadays, companies are looking for more profitable and safer measures for their organizations and because of that they have turned their eyes to cloud infrastructures to reduce costs and increase production capacity. However, many of these applications are

not safe and we set out to check the security and reliability of one of the most popular cloud infrastructures of the moment, AWS. This article has as its work proposal to study and evaluate the safety of AWS tools, in this article Guarduty and Amazon Inspector were used in an EC2 instance. To perform this test, an AWS EC2 instance was created, made available after a starter account was created from which it was installed on the physical machine of one of our members. Next, we generated a large amount of data traffic in our instance and a scan was performed by the Wireshark tool to check the data stability, then the Amazon Inspector tool was used to check irregularities in our instance; finally, we used the GuardDuty tool to assess whether invasions had taken place from a third party. After testing, Amazon Inspector informed us of a security issue with the ports, while Amazon GuardDuty stopped attacks targeting that port It is concluded therefore that the tools worked very well together to ensure the security of our instance.

KEYWORDS: Cloud Computing, AWS, Security, GuardDuty, Inspector.

1 INTRODUÇÃO

Atualmente as empresas buscando reduzir gastos com a infraestrutura, muitas estão recorrendo a computação em nuvem (*Cloud Computing*), com o objetivo de obter armazenamento de dados e capacidade computacional. Oferecendo aplicação, plataforma e infraestrutura a custos reduzidos. (TAURION, 2009)

Um exemplo de infraestrutura atual que oferece serviços em nuvem seria a *Amazon Web Service (AWS)*, que oferecem serviços online através de um preço acessível como armazenamento de dados, máquinas virtuais, ferramentas para desenvolvedores e banco de dados entre outros. (AMAZON, 2019)

Entretanto as plataformas de Cloud Computing assim como qualquer serviço, ele está sujeito a falhas e vulnerabilidades principalmente no quesito de segurança de dados. Como por exemplo o vazamento de dados ocorrido no dia 21 de março pela *Playstation Network* (PSN) onde as informações de mais de 100 milhões de usuários foram expostos como cartões de crédito e senhas dos usuários. (ZANUTTO, 2018)

Por essa razão, inúmeras empresas que oferecem esses serviços na nuvem endossam para que terceiros realizem *Penetration Test (*Pentest*)* com finalidade de verificar se existem vulnerabilidades ou falhas na rede com o objetivo que essas falhas sejam corrigidas o mais breve possível para garantir a integridade e segurança do serviço. (COSTA NETO; SANTOS; TEIXEIRA, 2018)

Este trabalho teve como propósito avaliar a eficiência das ferramentas de segurança, Amazon Inspector e GuardDuty em um ambiente controlado utilizando o serviço AWS *Elastic Compute Cloud* (EC2), buscando identificar ameaças e vulnerabilidades.

Inicialmente foi realizado um cadastro na própria plataforma da AWS que disponibiliza inúmeros sistemas operacionais, tanto Windows quanto Linux (pode-se realizar testes controlados nesses SOs pelas diretrizes da Amazon). Após feito o cadastro criamos algumas falhas intencionais na instância escolhida e em seguida foi utilizado duas aplicações: o Amazon Inspector e o Amazon GuardDuty que em conjunto devem ser capazes de identificar as falhas propositais de nossa instância e sendo assim gerar automaticamente um relatório de falhas e soluções para os problemas apresentados.

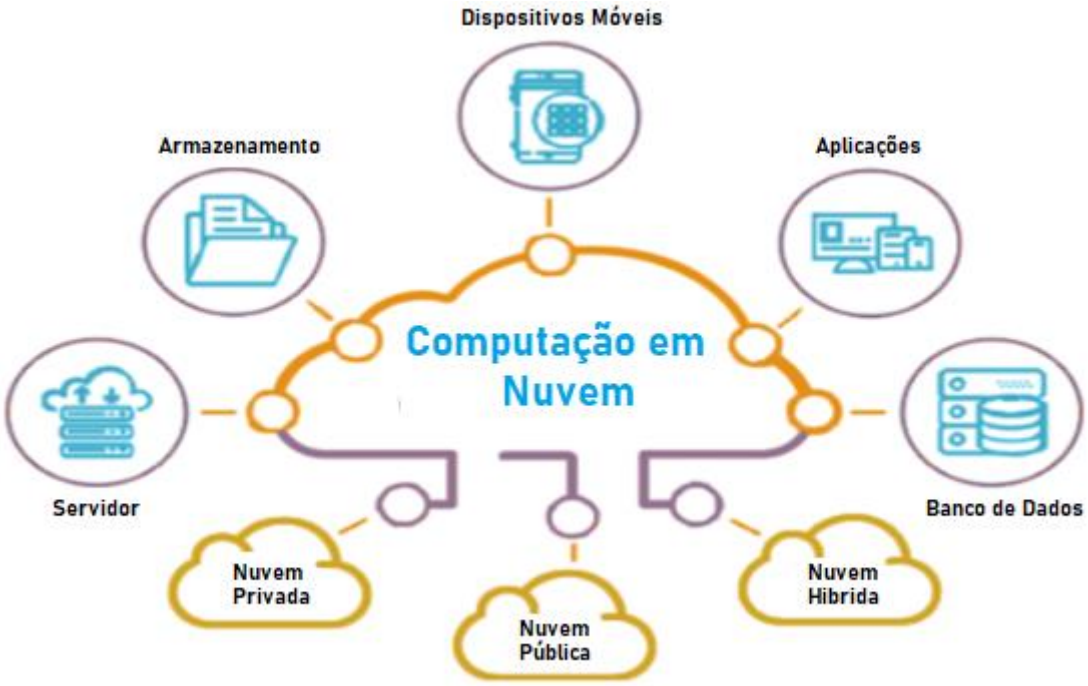
Realizados todos os testes, a ferramenta Amazon Inspector tinha como objetivo detectar falhas de conformidade e vulnerabilidade que poderiam ser aproveitadas por invasores. Ele nos alertou sobre uma vulnerabilidade de uma porta específica, porém não foi capaz de detectar os sistemas de segurança padrão desligados, enquanto o Amazon GuardDuty impediu várias invasões que estavam alvejando a porta especificada pelo Amazon Inspector.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Cloud Computing

Cloud Computing pode ser definido como a utilização de inúmeras máquinas, dispositivos de armazenamento, servidores e serviços oferecidos por empresas de terceiros, deste modo fornecendo poder computacional, desempenho e uso de softwares de alto custo, assim não necessitando que o usuário possua uma infraestrutura física preparada para atender as demandas da empresa, como demonstra a Figura 1. (ZANUTTO, 2018)

Figura 1 - Serviços oferecidos por Cloud Computing



Fonte - ANTRA (2020)

Qual é objetivo do Cloud Computing? De acordo com Veras (2012), o conceito surgiu com o objetivo de processar as aplicações e armazenar os dados fora do ambiente físico da empresa. Ou seja, transferir as informações para fora da infraestrutura interna da mesma, sendo assim reduzindo custos com equipamentos, espaço interno e otimizando o uso dos recursos.

Para todo o modelo do Cloud Computing é fundamental que possua essas seguintes características: autoatendimento sobre demanda (O usuário pode utilizar os recursos sem precisar da interação humana), acesso amplo a rede (Os recursos estão sempre disponíveis na rede sendo acessíveis através de dispositivos comuns), pooling de recursos (Os recursos de computação atenderão diversos usuários simultaneamente oferecendo armazenamento, processamento e memória de banda), elasticidade rápida (oferecendo recursos e serviços proporcional a demanda) e o serviço medido (O usuário será cobrado pelo recurso utilizado). (SZABÓ, 2018)

A Cloud Computing oferece então alguns modelos de serviço, explicados resumidamente: Infraestructure as a service (Este modelo oferece controle quase absoluto ao usuário como o sistema operacional, o armazenamento e as

aplicações submetidas, entretanto o controle sob a rede é limitado, assim como a infraestrutura interna da nuvem); Platform as a service (Este modelo permite que o usuário possa apenas submeter aplicações desenvolvidas por ele próprio e executá-las em ambientes de máquina virtual, porém o usuário não tem controle sob nada além das aplicações); Software as a service (É o modelo mais utilizado onde as aplicações são inteiramente executadas na nuvem como por exemplo google docs, slides, planilhas entre outros aplicativos). (ZANUTTO, 2018)

Cloud Computing possui diferentes modelos de implementação que servem para atender requisitos específicos do usuário final sendo essas implementações:

a) Nuvens Particulares: Elas estão localizadas em apenas uma organização específica e não dividias em várias firmas. Nuvens particulares são as nuvens com o maior nível de segurança; (JAIN; NARULA; PRACHI, 2015)
b) Nuvens Públicas: Em uma nuvem pública os vendedores armazenam as informações através de comerciantes de nuvem. O cliente não tem controle e nem visibilidade alguma pelo framework do dono da nuvem. Este tipo de computação é compartilhado entre diferentes companhias; (JAIN; NARULA; PRACHI, 2015)
c) Nuvens Híbridas: Esse formato de nuvem é escalável e que possui o melhor custo-benefício, Nuvens híbridas possuem esse nome porque combinam o uso de nuvens públicas e privadas, o seu foco seria de minimizar mudanças. (JAIN; NARULA; PRACHI, 2015)

2.2 Segurança em Cloud Computing

A segurança é um aspecto importante quando falamos do uso de Cloud Computing, onde migrar sistemas e dados significativamente importantes para empresas e usuários onde deixar que um único proprietário do sistema se encarregue da segurança, acaba parecendo um risco. É comum imaginar que em qualquer ambiente de Cloud Computing está passível a enfrentar vulnerabilidades e falhas tanto logicas como físicas e que podem prejudicar o

funcionamento, integridade e acessibilidade dos dados que estiverem armazenados. (CASTRO; SOUSA, 2015)

Contudo por se tratar de dados de diversos usuários é necessário que todo serviço cloud principalmente sendo um serviço distribuído em maior escala, retenha de robustos sistemas de segurança, pois, devido ao uso de servidores virtuais, onde são semelhantes aos servidores físicos, acabam necessitando de avaliações de segurança. Visando na busca desse objetivo uma das práticas mais importantes que agregam na detecção de possíveis falhas é a prática de Pentest, um modo efetivo na descoberta de brechas ainda não encontradas no sistema. Sendo assim cada vez mais necessário medidas que acelerem esse procedimento, pois, Pentest possuem tempo restrito e muito planejamento para que haja a detecção de erros e consequentemente um relatório preciso. (COSTA NETO; SANTOS; TEIXEIRA, 2018)

Também tomando como base outras medidas de segurança usadas pelos provedores, tendo em vista que as atitudes tomadas pelo maior provedor de serviço em Cloud Computing, a AWS é uma plataforma escalável com alto nível de confiabilidade, fornecendo versatilidade que permitem que os usuários possam criar uma ampla gama de aplicações. Medidas são tomadas pelos provedores buscando a melhoria na segurança, como as certificações (exemplo da ISO 27001), que tornam a mesma validada como um provedor de serviços nível 1 sobre o padrão de segurança de dados. (SHAHZAD; FARRUKH, 2014)

Apesar dos diversos meios que são tomados pelos provedores, vazamentos acontecem devido a vulnerabilidades, tendo necessidade de cada vez mais investimento para que alcance uma maior segurança e confiabilidade. Entretanto mesmo havendo diversas medidas de segurança, que ainda há um alto número de vulnerabilidades reportadas em Cloud Computing, principalmente quando observa-se as três maiores, Google, Amazon e Microsoft, que representam cerca de 56% de todos os incidentes reconhecidos. (COSTA NETO; SANTOS; TEIXEIRA, 2018)

Embora as companhias de Cloud Computing constantemente dizem garantir a integridade da informação para o lado do cliente é necessário criar um acordo de nível de serviço (ANS) para garantir a confiabilidade e garantia de que

não ocorrerão falhas que prejudicarão o funcionamento total da empresa e do cliente que contratou o serviço, assim evitando um dos pontos críticos de falha. (CASTRO; SOUSA, 2015)

Entretanto acaba sendo questão de tempo até cada vez mais a cloud ser usada como formato para um maior número de aplicações, pois seus diversos modos de operação a tornam um serviço abrangente, oferecendo cada vez mais segurança em diversos níveis. (MENEGATT; JOSIMAR, 2012)

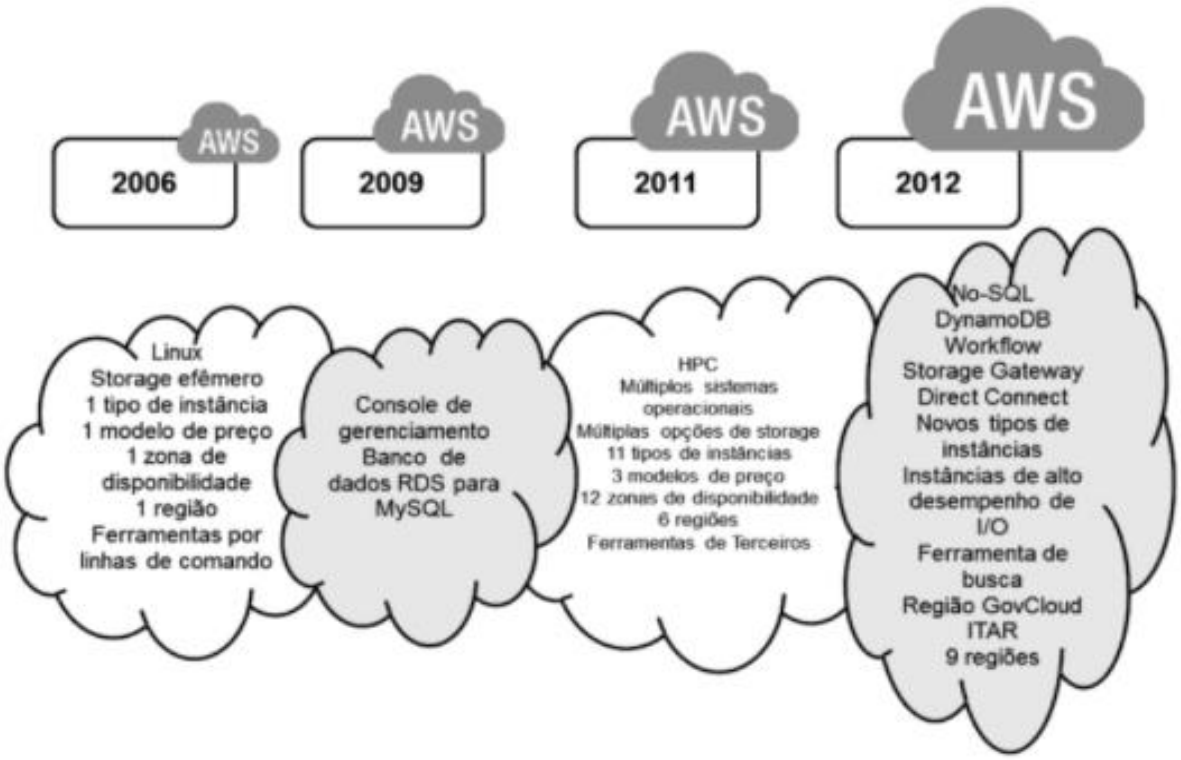
2.3 AWS

AWS é uma plataforma em Cloud Computing que é oferecida pela Amazon sendo uma junção dos serviços de infraestrutura, plataforma e software (IaaS, PaaS, SaaS) dos quais a plataforma pode oferecer ferramentas as organizações como poder computacional, armazenamento de banco de dados e serviços de entrega. (AMAZON, 2020)

A plataforma foi criada em 2006 pela própria Amazon desenvolvida inicialmente para lidar com o seu e-commerce, ela foi uma das primeiras companhias a introduzir o conceito de modelo de Cloud Computing *pay-as-you-go* (Pague o que usar), do qual é um padrão que fornece aos usuários armazenamento, computadores e a taxa de transferência conforme necessário. . (AMAZON,2020)

Embora a plataforma da Amazon hoje seja uma das maiores referencias em computação em nuvem e qualidade de serviços, este foi um processo gradual que se iniciou em 1995 e foi se aperfeiçoando até chegar ao modelo que foi oferecido ao público em 2006; e desde então eles continuam evoluindo quase que semanalmente para garantir a qualidade e flexibilidade de serviços e produtos. Em junho de 2012 a AWS já possuía 1 trilhão de aparelhos conectados a seu sistema de armazenamento, o Amazon Simple Storage Service, ou Amazon S3 como demonstra a Figura 2. (VERAS, 2013)

Figura 2 – Evolução da AWS



Fonte - Veras (2013)

Os serviços da AWS oferecem diversas ferramentas e soluções para empresas e desenvolvedores de software que podem ser utilizadas nos mais diversos datacenters que estão espalhados em até 190 países dos quais agencias governamentais, instituições de ensino, organizações privadas e sem fins lucrativos utilizam os seus recursos para desenvolver aplicações web, virtualizações para seus fins. (AMAZON, 2020)

Pode-se dizer que a AWS foi uma das precursoras do Cloud Computing, investindo nesta tecnologia muito mais cedo do que as outras empresas e sendo assim conseguindo sair na frente de todos os outros concorrentes. Após inúmeras variações e testes com sua estrutura, eles conseguiram aprimorar seu modelo de negócio até o formato que existe hoje, tornando assim a AWS como uma das principais líderes em IaaS de acordo com empresas de tecnologia como a Gartner. (VERAS, 2013)

Comparando a AWS aos Datacenters tradicionais existentes, a computação em nuvem possui muito mais vantagens levando em consideração fatores como a praticidade, custo, eficiência, desempenho e produtividade. As

empresas ao utilizar a AWS ainda podem garantir a integridade de suas aplicações pois ela oferece suporte total aos programas já existentes e aos que serão desenvolvidos. Foi observado que empresas de pequeno e médio porte tiveram seus rendimentos muito melhores utilizando a plataforma da Amazon em comparação aos datacenters que eram utilizados anteriormente. (VERAS, 2013)

2.4 SEGURANÇA NA AWS

Na AWS existe uma diversidade imensa de serviços e aplicações possíveis para serem utilizadas, algumas das ferramentas mais utilizadas são o Amazon Inspector e o Amazon GuardDuty, nos quais expandiremos mais nos próximos tópicos. (AMAZON, 2020)

2.4.1 AMAZON INSPECTOR

É um serviço de avaliação de segurança que age em segundo plano para identificar problemas de acessibilidade e vulnerabilidade em todas as instâncias instaladas, buscando por problemas de conformidade e logs. Após ser feita a varredura na instância, o Amazon Inspector gera o relatório automaticamente explicando e detalhando os problemas encontrados na instância priorizando as falhas de acordo como seu nível de severidade, assim como sugestões de como os resolver. (AMAZON, 2020)

2.4.2 AMAZON GUARDDUTY

É um serviço de segurança inteligente que busca constantemente por atividades suspeitas, maliciosas ou prejudiciais a instância vinda de fontes externas, muitas vezes com intenções maliciosos. O GuardDuty tem como objetivo proteger a integridade da instância, utilizando Machine Learning, ele busca aprender com as novas informações, para sempre estar atualizado contra as novas ameaças. (AMAZON, 2020)

Ele possui um terminal personalizado de fácil acesso e entendimento do qual, caso haja uma atividade suspeita ou maliciosa, essa ameaça foi barrada e catalogada pelo serviço, detalhando qual tipo de ataque/ameaça foi detectado, o IP e localização do invasor, junto a qual instância foi alvejada por eles. (AMAZON, 2020)

3 MATERIAIS E MÉTODO

Entre os diversos serviços na nuvem disponíveis pela Amazon para a realização de testes de desempenho, foi escolhido a AWS EC2 para aplicarmos testes de desempenho na plataforma utilizando de ferramentas desenvolvidas pela própria para identificar possíveis falhas.

Também foi utilizada a aplicação Amazon Inspector, um serviço capaz de realizar uma varredura em toda a instância AWS e em seguida gerar um relatório com todas as vulnerabilidades, falhas, acessos não autorizados e riscos de exposições de dados com seus devidos graus de severidade. (AMAZON, 2020)

Outro serviço utilizado que também é disponibilizado pela Amazon: o GuardDuty, muito utilizado em conjunto com o Amazon Inspector. Este que realiza um monitoramento continuo em todas as instâncias instaladas, procurando por atividades maliciosas, tentativas de intrusão e acessos não autorizados na instância. Esta ferramenta utiliza *machine learning* (aprendizado de máquina) para estar em constante evolução e identificar os milhares de malwares e ataques que surgem diariamente. (AMAZON, 2020)

Após ter sido realizado o cadastro no site da Amazon, a primeira ferramenta a ser testada foi o Wireshark, um analisador de protocolos de rede que permite analisar todos os pacotes que estão trafegando na rede para verificar a integridade e estabilidade da rede entre o servidor e a instância. Em seguida utilizaremos a ferramenta Amazon Inspector para realizar uma varredura completa em busca de erros de autorização, logs corrompidos e falhas de segurança do qual o programa irá emitir alertas e criar um log detalhado de todos os erros encontrados em nossa instância, todas essas ferramentas funcionam muito bem em conjunto e complementam umas às outras conforme mostra o quadro 1.

Quadro 1 - Recursos e funções das ferramentas utilizadas

Recursos Utilizáveis	Wireshark	Amazon Inspector	Amazon GuardDuty
Função	Analisar os pacotes da rede	Análise de vulnerabilidade e acessibilidade	Proteção contra atividades maliciosas ou suspeitas
Características	- Multiplataforma - Diversos filtros de busca - Análise de pacote minuciosa	- Alta Customização - Age de forma automatizada - Geração de relatórios automáticos e solução de problemas	- Terminal Intuitivo - Alta Disponibilidade - Relatório de ataque detalhado com o seu nível de severidade

Fonte - Elaborado pelos autores.

Caso o Amazon Inspector acabe deixando passar algum erro ou falha de segurança no banco de dados, o GuardDuty foi utilizado para auxiliar na identificação de invasões ao rodar em segundo plano, criando mais uma camada de segurança ao verificar se houveram tentativas de intrusão ou acessos não autorizados, utilizando técnicas de *machine learning* para verificar e manter a integridade e segurança das informações.

Utilizando essas ferramentas foi decidido realizar um teste de segurança na instância da Amazon AWS EC2 – Microsoft Windows Server 2019 Base sendo escolhida a versão gratuita t2-micro hospedado no servidor de Norte da Virginia us-east-1. A instância foi testada, primeiro com uma instalação limpa, utilizando apenas as aplicações e serviços padrões da AWS, em seguida foram realizados testes com o Amazon Agent instalado na instância, onde o mesmo funciona como um serviço de atualização, gerenciamento e configuração para as máquinas virtuais e instâncias, agindo como um intermediário que possibilita realizar requisições para a AWS.

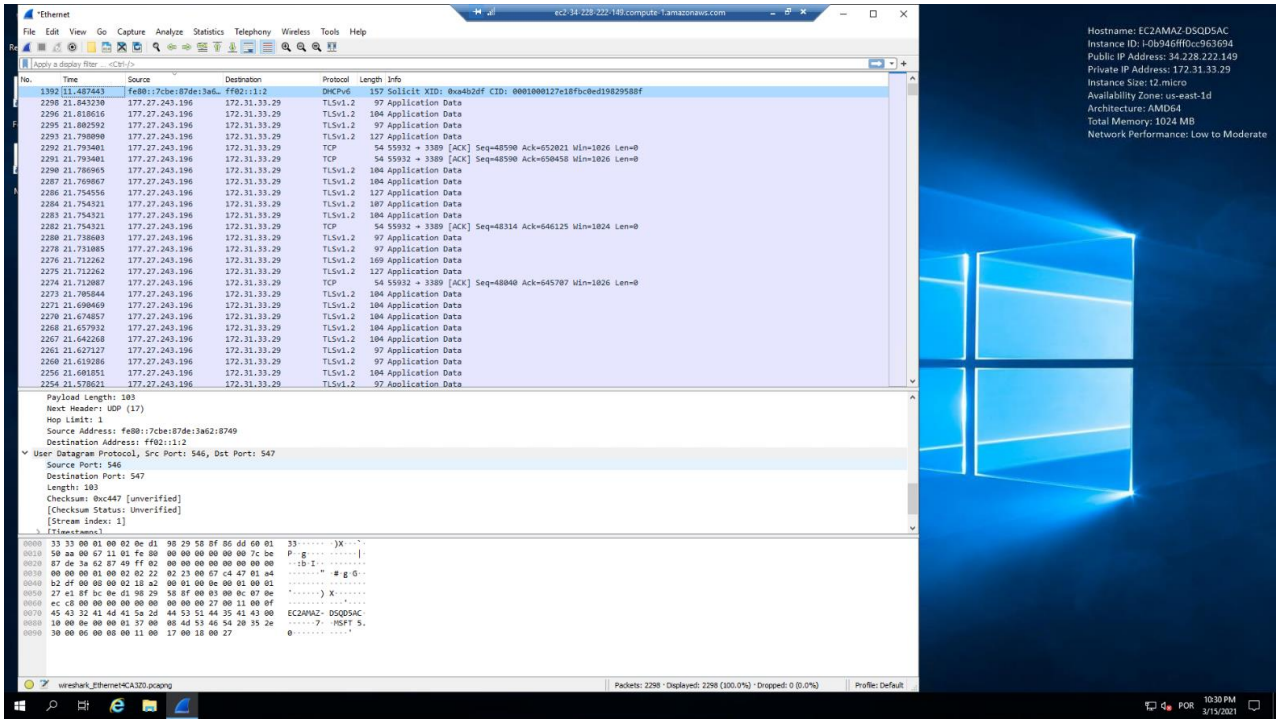
Para possuir resultados mais apurados a instância foi configurada no modo de rede aberta, com os padrões da AWS, para que o Amazon Inspector e GuardDuty pudessem realizar suas análises mais rapidamente. Por fim foi feita

uma análise os resultados obtidos para concluir e encontrar possíveis falhas de segurança na plataforma AWS EC2 e possíveis soluções para esses problemas.

4 RESULTADOS

Para os testes preliminares foi instalada a aplicação Wireshark para detecção de pacotes corrompidos e perdidos em nossa Instância AWS EC2. Para os escaneamentos não foram utilizados nenhum tipo de parâmetro especifico, o Wireshark foi utilizado apenas para análise se havia um tráfego de dados como mostra na figura 3.

Figura 3 - Escaneamento de portas utilizando Wireshark na instância AWS EC2

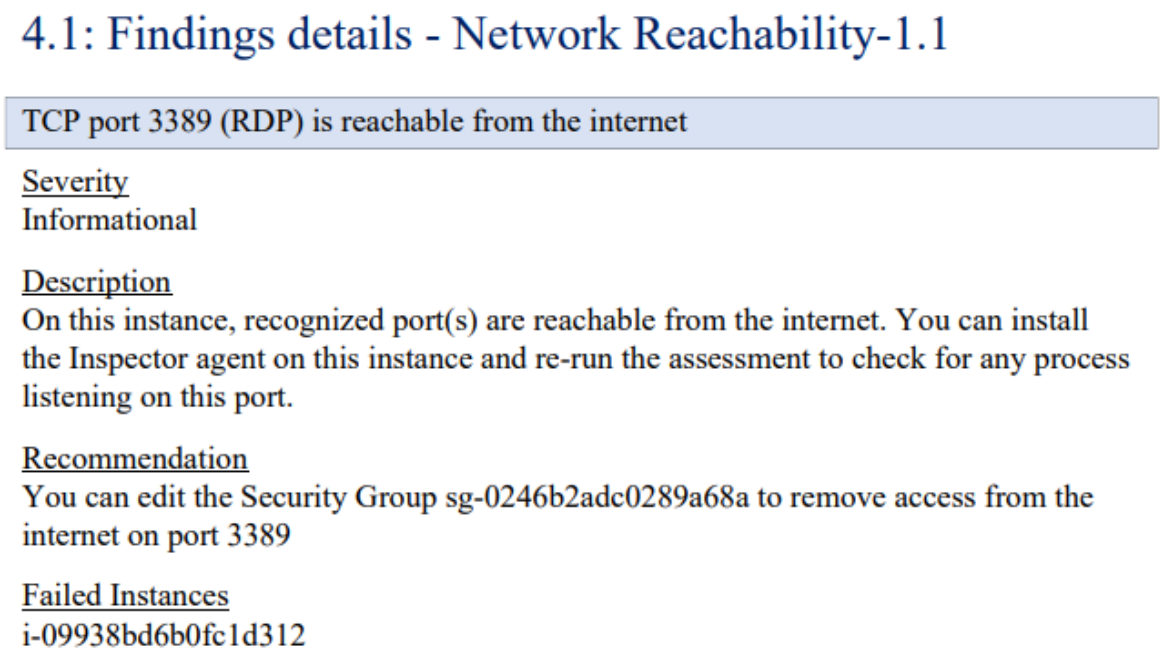


Fonte - Elaborado pelos autores.

Estes escaneamentos foram feitos com o intuito de verificar se o tráfego de dados da máquina virtual por estar no servidor us-east-1 não seriam corrompidos e também por ser um starter account não haveria uma perda grande de dados. Após esse teste preliminar não foi possível identificar portas vulneráveis ou pacotes corrompidos trafegando pela instância, não sendo identificado nenhuma tentativa de invasão ou golpe.

Em seguida foi executado o serviço Amazon inspector e realizado um teste na instância AWS EC2 criada para verificar se o serviço encontraria algum problema de conformidade ou segurança. Foram utilizados os pacotes de regras do modelo padrão do qual englobava todas as regras disponibilizadas. Após realizado o teste, foi gerado um relatório pela própria AWS detalhando a falha encontrada e medidas preventivas para solucionar o problema. Após a inspeção da instância foi gerado um relatório de ações corretivas a serem realizadas, como mostra a figura 4.

Figura 4 - Erros encontrados pelo relatório do Amazon Inspector



4.1: Findings details - Network Reachability-1.1

TCP port 3389 (RDP) is reachable from the internet

Severity
Informational

Description
On this instance, recognized port(s) are reachable from the internet. You can install the Inspector agent on this instance and re-run the assessment to check for any process listening on this port.

Recommendation
You can edit the Security Group sg-0246b2adc0289a68a to remove access from the internet on port 3389

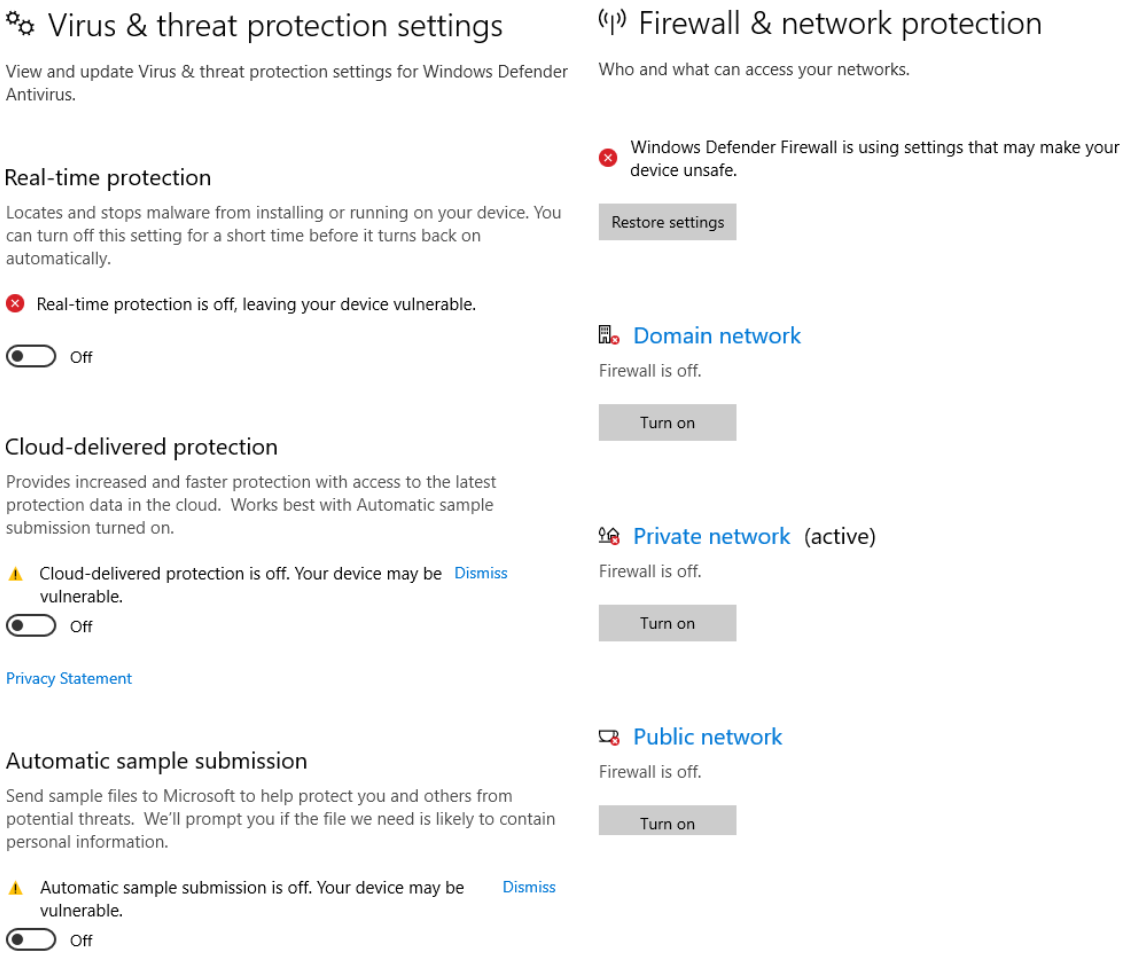
Failed Instances
i-09938bd6b0fc1d312

Fonte - Elaborado pelos autores

Foi identificado pelo serviço que a porta TCP 3389 (porta utilizada pelos sistemas operacionais do Windows para realizar comunicações remotas) podia ser acessada pela internet. Esta porta pode ser vulnerável a ataques de negação distribuída de serviço, no entanto, o tráfego de dados dela pode ser redirecionada para outra porta, melhorando a segurança dela ou como recomendado a instalação do Amazon Agent e em seguida utilizar novamente o Amazon Inspector.

Entretanto como pode se observar na figura 5:

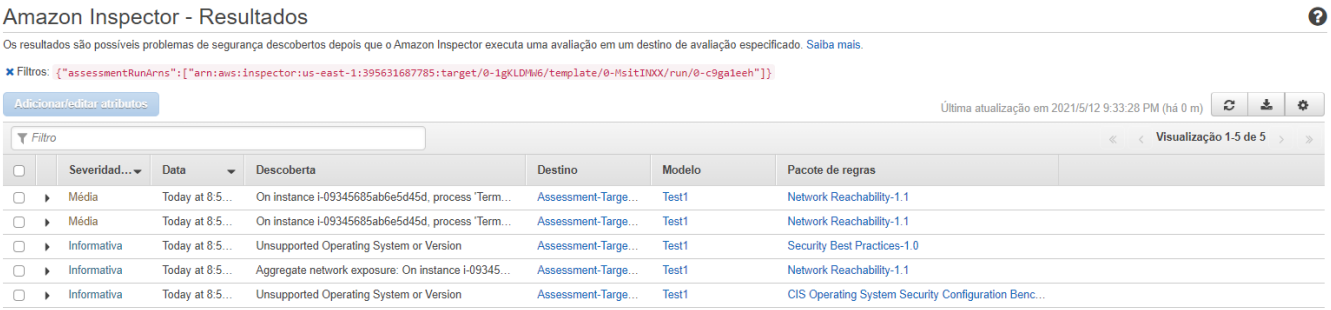
Figura 5 - Detalhes das ferramentas de segurança desabilitadas



Fonte - Elaborado pelos autores

De acordo com os pacotes de regras pré-estabelecidos pela própria Amazon, o serviço do Amazon Inspector não foi capaz de identificar que tanto o Windows defender e o firewall do Windows, como mostra a figura 6, desta instância estavam desligados, sendo assim este foi um erro grave e que pode acarretar em problemas muito piores no futuro.

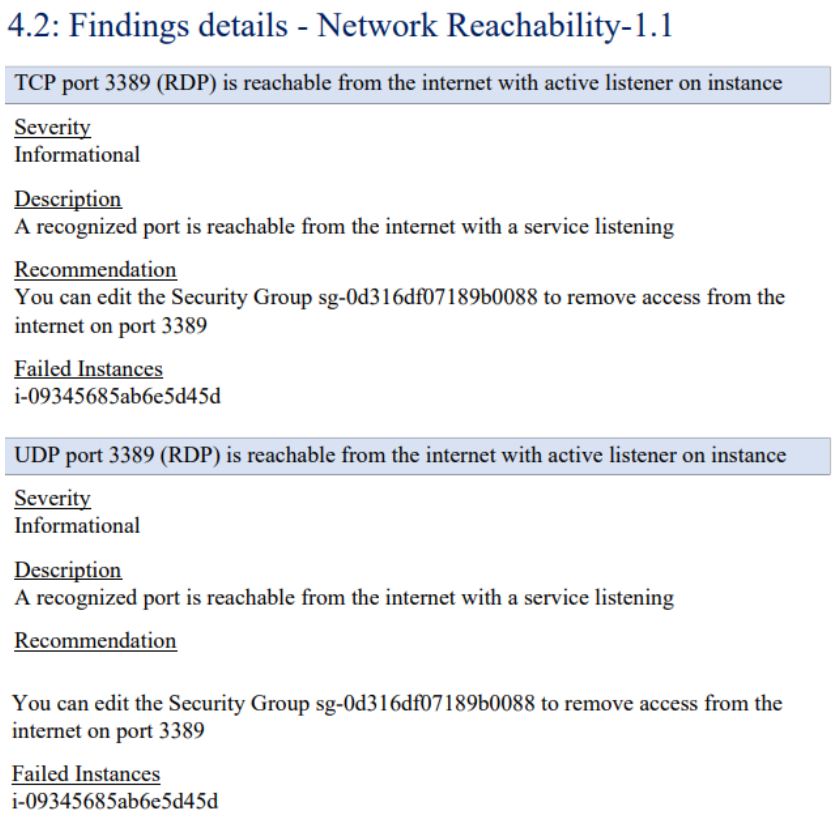
Figura 6 - Relatório gerado pelo Amazon Inspector em conjunto ao Amazon Agent



Fonte - Elaborado pelos autores

Este outro relatório, mais detalhes na figura 7, foi gerado após instalado uma aplicação auxiliar chamada de Amazon Agent, utilizado para permitir uma varredura mais profunda desta instância e recomendado pela própria AWS. Desta vez ele encontrou três outros problemas nessa instância, dos quais diziam que esta instância é de uma versão ultrapassada e que deveria ser atualizada para manter a segurança e integridade além de um relatório detalhado sobre o alcance de rede como mencionado na figura 4.

Figura 7 - Erros encontrados pelo relatório do Amazon Inspector com o Amazon Agent instalado



4.2: Findings details - Network Reachability-1.1

TCP port 3389 (RDP) is reachable from the internet with active listener on instance

Severity
Informational

Description
A recognized port is reachable from the internet with a service listening

Recommendation
You can edit the Security Group sg-0d316df07189b0088 to remove access from the internet on port 3389

Failed Instances
i-09345685ab6e5d45d

UDP port 3389 (RDP) is reachable from the internet with active listener on instance

Severity
Informational

Description
A recognized port is reachable from the internet with a service listening

Recommendation

You can edit the Security Group sg-0d316df07189b0088 to remove access from the internet on port 3389

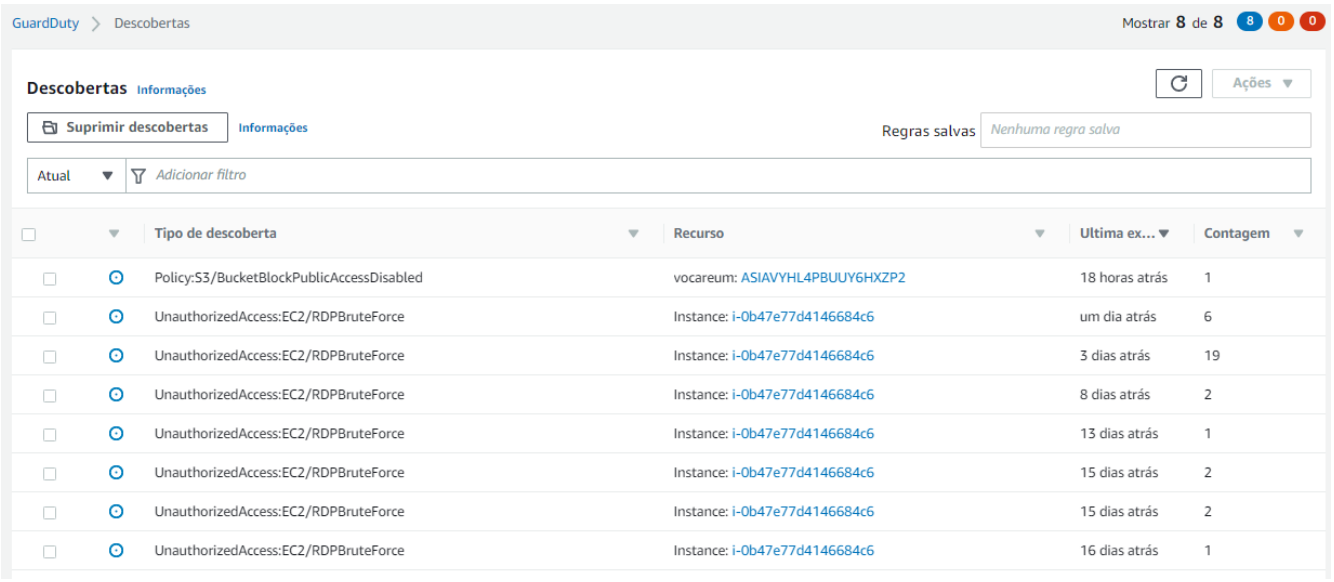
Failed Instances
i-09345685ab6e5d45d

Fonte - Elaborado pelos autores

A figura acima continua a mostrar o mesmo erro da figura 4 e que a melhor tomada de decisão a se fazer continua sendo editar o grupo de segurança da porta 3389 para que ela não possa mais acessar a internet.

Em seguida foi testado a aplicação GuardDuty, para que ela realizasse a segurança de nossa instância automaticamente durante os períodos de teste conforme a figura 8.

Figura 8 - Interface do GuardDuty



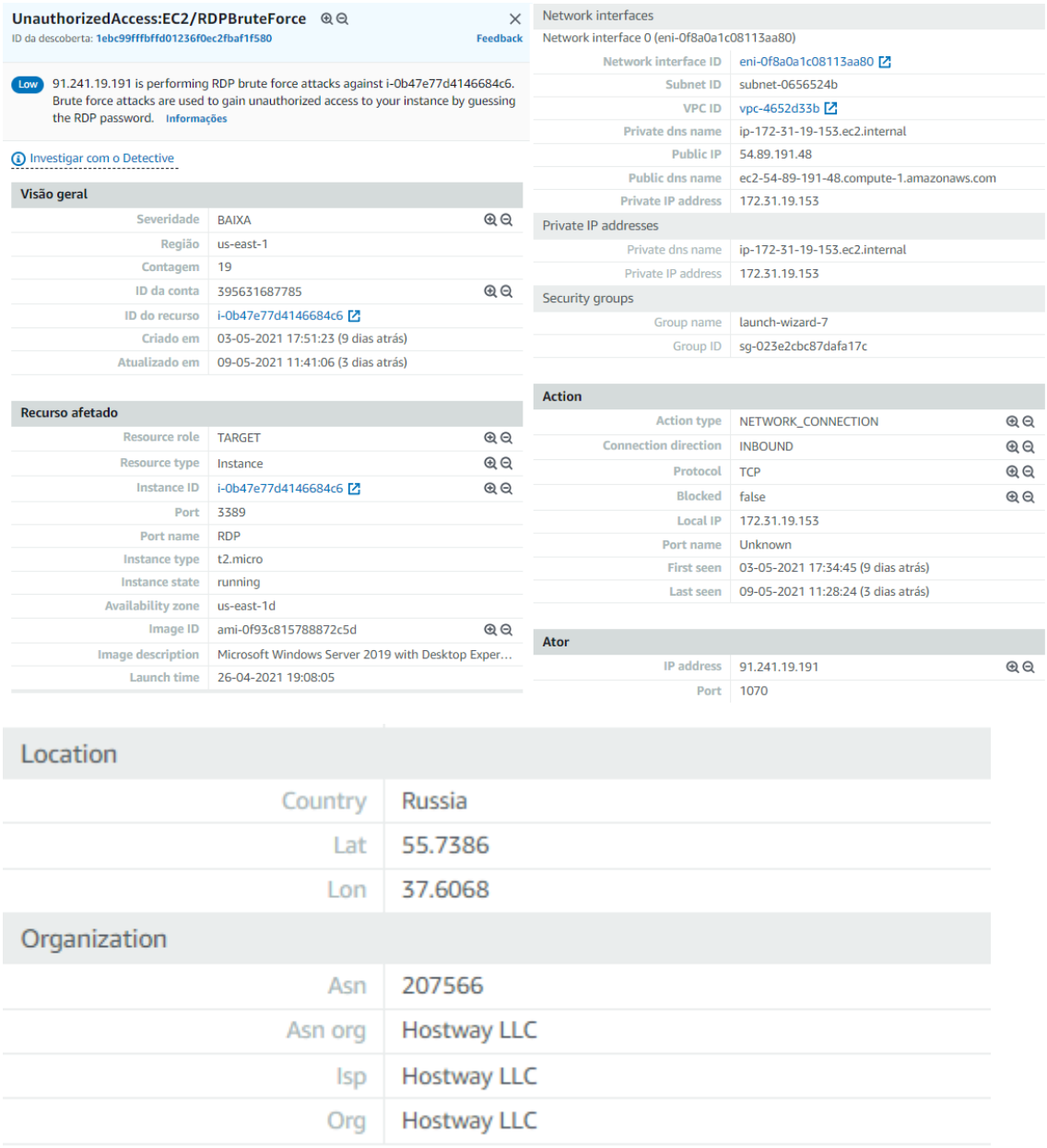
Fonte - Elaborado pelos autores

A figura mostra que houveram várias tentativas de invasão por força bruta (uma técnica de hacking que envolve uma máquina tentar constantemente adivinhar a senha do usuário por tentativa e erro, tentando dezenas de milhares de combinações até descobrir a senha) desta instância ao longo de 16 dias, do qual o Amazon Inspector detectou e relatou que a porta 3389 foi alvejada em todos esses ataques. Em um primeiro momento acreditava-se que a aplicação não havia funcionado corretamente, mas ela se provou muito eficiente ao barrar inúmeros ataques vindos de outras regiões do mundo.

Apenas a primeira descoberta que não foi um ataque de invasão, sendo uma ação realizada pela própria AWS que bloqueia o acesso público a todos os nossos Buckets (são basicamente dados não estruturados sem tamanho definitivo no qual informações são armazenadas), impedindo que não haja mais ninguém vasculhando nossa instância.

Na figura 9 foi realizado uma análise de um destes ataques de força bruta realizada em nesta instância.

Figura 9 - Relatório de tentativa de invasão identificada pelo GuardDuty



Fonte - Elaborada pelos autores

A imagem acima está dando uma breve explicação sobre o que é um ataque de força bruta, qual recurso foi atingido e até mesmo o IP de quem está tentando aplicar o ataque nesta instância:

a) na coluna de visão geral está dando as informações sobre essa instância, como a região do servidor, data de criação, ID, etc.;
b) no recurso afetado está indicando que uma instância Windows Server 2019 que foi criado estava sendo alvejada;
c) em network interface estava mostrando o IP que foi disponibilizado pela AWS para esta instância;
d) em *private IP address* era a máquina primária;
e) em *security groups* é qual política de segurança essa instância está atrelada;
f) em *Action*, significa qual direção que este ataque estava vindo, tipo de protocolo, IP alvejado, primeira e última tentativa de ataque;
g) em Ator está nos mostrando o IP de quem tentou realizar este ataque e por qual porta ele tentou acessar, neste caso foi a porta 1070
h) em *Location*, está nos mostrando o país do invasor e sua região aproximada
i) e por fim em *organization*, nos diz qual a empresa de internet que estava provendo acesso a ele no momento do ataque.

Com todas essas informações que nos foi fornecido pelo GuardDuty pode-se avaliar que embora ele não tenha identificado as falhas propositais, ele foi capaz de identificar algo muito mais perigoso e que estava muito além de nosso alcance, e com isso ele tomou as medidas preventivas necessárias para garantir a integridade e segurança desta instância, além de fornecer informações necessárias para tomar outras medidas cabíveis caso seja necessário.

5 CONCLUSÃO

Este trabalho teve como objetivo avaliar e testar as ferramentas de segurança assim como comprovar a estabilidade em uma instância AWS EC2, sendo essas ferramentas: Amazon Inspector, GuardDuty e o Wireshark, todas são ferramentas populares e muito utilizadas para realizar testes e garantir a confiabilidade de que todas as informações, aplicações e dados nas máquinas virtuais terão sua segurança afirmada.

Utilizando a ferramenta Wireshark foi comprovado que a perda de dados e pacotes foi mínima, já o Amazon Inspector apresentou recomendações que seriam de extrema importância para garantir a segurança da instância, do qual a sua importância foi exacerbada quando foi utilizada o serviço Amazon GuardDuty, do qual estava defendendo a instância de ataques de força bruta na porta que foi indicada pelo Amazon Inspector. Entretanto, segundo os pacotes de regras disponíveis pela própria AWS, o Amazon Inspector não foi capaz de detectar a vulnerabilidade dos sistemas de segurança da instância estarem desligados.

A instância AWS se provou realmente muito estável e segura, tendo em vista que ele constantemente dava alertas de segurança para qualquer tipo de ação que poderia modificar ou alterar o funcionamento normal da máquina. Porém mesmo com toda a segurança padrão o uso de serviços adicionais de segurança trabalhando em conjunto podem reafirmar ainda mais a segurança, levando em conta que apenas um serviço não seria o suficiente para assegurar a segurança e estabilidade da máquina, já que a utilização de um único serviço poderia acabar acarretando em falhas ou erros que podem passar despercebidos por ele, sendo necessário o uso de outros serviços complementares.

5.1 TRABALHOS FUTUROS

Iremos propor como trabalhos futuros, a utilização de outros tipos de sistemas operacionais como o Linux, a utilização de outras ferramentas como o Amazon Detective ou o Amazon Macie devido ao acesso limitado de nossas contas.

REFERÊNCIAS

AMAZON.; Recursos do Amazon GuardDuty. **Amazon Web Service**. 2020. Disponível em: https://aws.amazon.com/pt/guardduty/features/. Acesso em: 19 mar. 2021

AMAZON.; Amazon Inspector. **Amazon Web Service**. 2020. Disponível em: https://aws.amazon.com/pt/inspector/. Acesso em: 15 out. 2020

AMAZON.; Segurança, identidade e conformidade na AWS. **Amazon Web Service**. 2020. Disponível em: https://aws.amazon.com/pt/products/security/?nc=sn&loc=2. Acesso em: 19 mar. 2021

AMAZON.; Segurança na Nuvem AWS. **Amazon Web Service**. 2020. Disponível em: https://aws.amazon.com/pt/security/?nc=sn&loc=1 Acesso em: 19 mar. 2021

CASTRO, R.C.; Sousa, V. P.; **Segurança em Cloud Computing: Governança e Gerenciamento de Riscos de Segurança**. 2015. Disponível em: https://cic.unb.br/~alchieri/disciplinas/posgraduacao/agi/g5/seguranca.pdf Data de acesso: Acesso em: 21 set. 2020

JAIN, A.; NARULA, S.; PRACHI, M.; **Cloud Computing Security: Amazon Web Service.** set. 2015**,** Fifth International Conference on Advanced Computing & Communication Technologies. Disponível em: https://ieeexplore.ieee.org/document/7079135 Acesso em: 21 set. 2020

COSTA NETO, R.P.; SANTOS, M.R.P.; TEIXEIRA, A.J.M.; **Proposta Metodológica de uma Plataforma para PenTest em Ambientes de Nuvem** Universidade Federal do Ceará Estácio – CEUT mai. 2016 Disponível em: https://www.researchgate.net/publication/306275477_Proposta_Metodologica_de_uma_Plataforma_para_PenTest_em_Ambientes_de_Nuvem Acesso em: 31 out. 2020

SHAHZAD, F.; **State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions.** The 6th International Symposium on Applications of Ad hoc and Sensor Networks, 2014. Disponível em: https://www.sciencedirect.com/ Data de acesso: Acesso em: 30 out. 2020

SZABÓ, R.; **Penetration testing of AWS-based Environments.** 2018. Dissertação (Mestrado em Cyber segurança) – University of Twente: Department of Computer Science EIT Digital Cybersecurity Specialization, nov. 2018.

TAURION, C.; **Cloud Computing: computação em nuvem, transformando o mundo da tecnologia da informação**. Rio de Janeiro: Brasport, 2009. p. 3/7.

VERAS, M.; **Arquitetura de nuvem: Amazon Web Services (AWS)**. Rio De Janeiro, Editora Brasport Livros e Multimídia Ltda, 2013.

VERAS, M.; **Cloud Computing: Nova Arquitetura da TI**, 2012. Rio De Janeiro Editora Brasport Livros e Multimídia Ltda, mar. 2012.

ZANUTTO, B. G.; **Segurança em Cloud Computing**. 2018. Universidade Federal de São Carlos, Sorocaba, São Paulo, fev. 2018. Disponível em https://dcomp.sor.ufscar.br/verdi/topicosCloud/Artigo-Seguranca-Cloud.pdf. Acesso em: 07 set. 2020