

**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO
SERTÃO PERNAMBUCANO
CAMPUS SALGUEIRO
CURSO DE TECNOLOGIA EM SISTEMAS PARA INTERNET**

DANIEL INÁCIO LEITE

**ANÁLISE DE SEGURANÇA À LUZ DOS TESTES DE INVASÃO EM
PLATAFORMAS DE E-COMMERCE**

SALGUEIRO - PE

2022

DANIEL INÁCIO LEITE

**ANÁLISE DE SEGURANÇA À LUZ DOS TESTES DE INVASÃO EM
PLATAFORMAS DE E-COMMERCE**

O Trabalho de Conclusão de Curso (TCC) foi apresentado na disciplina de TCC do curso de tecnologia em Sistemas para Internet, ofertado pelo Campus Salgueiro do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano (IFSertãoPE), como requisito parcial para obtenção do título de tecnólogo em Sistemas para Internet.

Orientador: Francisco Kelsen de Oliveira

SALGUEIRO-PE

2022

Dados Internacionais de Catalogação na Publicação (CIP)

L533 Leite, Daniel Inacio.

ANÁLISE DE SEGURANÇA À LUZ DOS TESTES DE INVASÃO EM PLATAFORMAS DE E-COMMERCE / Daniel Inacio Leite. - Salgueiro, 2022.
25 f. : il.

Trabalho de Conclusão de Curso (Sistemas para Internet) -Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano, Campus Salgueiro, 2022.
Orientação: Prof. Dr. Francisco Kelsen de Oliveira.

1. Rede de computadores. 2. e-commerce. 3. Marketplaces internacionais. 4. segurança web. I. Título.

CDD 004.62

**INSTITUTO FEDERAL DE EDUCAÇÃO CIÊNCIA E TECNOLOGIA DO
SERTÃO PERNAMBUCANO
CAMPUS SALGUEIRO
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS PARA INTERNET**

DANIEL INÁCIO LEITE

**ANÁLISE DE SEGURANÇA À LUZ DOS TESTES DE INVASÃO EM
PLATAFORMAS DE E-COMMERCE**

O Trabalho de Conclusão de Curso (TCC) foi apresentado na disciplina de TCC do curso de tecnologia em Sistemas para Internet, ofertado pelo Campus Salgueiro do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano (IFSertãoPE), como requisito parcial para obtenção do título de tecnólogo em Sistemas para Internet.

Orientador: Francisco Kelsen de Oliveira

Aprovado em 09 de Agosto de 2022.

COMISSÃO EXAMINADORA

Prof. Dr. **Francisco Kelsen De Oliveira** (IFSertãoPE)
Orientador

Prof. Ms. Orlando da Silva Oliveira. (IFSertãoPE)
Membro Interno

Prof. Ms. Leão João Dehon Costa (Uninassau)
Membro Externo

AGRADECIMENTOS

Quero primeiramente agradecer ao meu Senhor por toda sua misericórdia em minha vida, pela intercessão da Virgem Maria, que como filho me ensinou e me ensina a viver por amor, um amor que seria empobrecido, caso eu ousasse usar alguma palavra para defini-lo.

Agradeço aos meus pais, minha Mãe Laurinete e meu pai Geraldo, que com toda sua simplicidade me ensinaram o verdadeiro significado da perseverança e humildade, assim como cultivar a gratidão, mesmo nas pequenas vitórias, também trago aqui nessas linhas, meu irmão Gilmar. Hoje escrevendo esse texto de agradecimento, sinto grande alegria por chegar em mais essa grande vitória na minha vida. Minha noiva Edmaria, que me ajudou e motivou a tomar tantas decisões importantes, me auxiliou nos momentos difíceis e dolorosos.

Aos meus amigos Fabio, Yuri, Isabela, Vitória, e Alexandre, que caminharam junto comigo neste processo de ensino e aprendizagem. Quero também agradecer ao meu amigo e orientador Francisco Kelsen, grande professor que confiou em mim e me ajudou a superar as dificuldades aqui encontradas, também a todos do grupo de pesquisa GEPET, pela torcida.

Não posso deixar de citar também os professores, Francisco Junio, Augusto, Orlando, Heraldo, Patrícia, Woshington, Josenildo, Alexandre, Walfrido, Cintia, Alice, Raquel e Marcelo. Pessoas essas que são exemplos de educadores. Agradeço também a toda a banca avaliadora.

Por todas as orações, quero agradecer em especial a minha Comunidade Católica Mãe da Vitória, que me motivou e motiva a jamais desistir dos meus objetivos.

Por fim, agradeço ao IFSertãoPE como um todo, por tantas oportunidades oferecidas não só a mim mas também a todos os que junto de mim trilham esse caminho de puro aprendizado, não só educacional mas também humano.

RESUMO

As plataformas de comércio eletrônico internacionais se consolidaram no cotidiano dos milhões de usuários da web, pois é um meio prático, acessível e, muitas vezes, econômico. Neste sentido, a questão de segurança é de suma importância para seguir paralelamente ao desenvolvimento de serviços e novos produtos de suporte ao comércio eletrônico, pois de acordo com o crescente número de transações dentre outros processos desenvolvidos por meio da internet, o número de crimes digitais também aumenta, como por exemplo, a criação de páginas eletrônicas clonadas, cujos usuários por um descuido e ou desatenção informam seus dados pessoais, e esses são coletados por cibercriminosos. Este trabalho objetivou analisar os sistemas web para comércio eletrônico de *marketplaces* internacionais, à luz das técnicas para análise de teste de invasão. Logo, uma pesquisa bibliográfica foi realizada para compreender as definições, as possibilidades de teste de invasão e trabalhos já publicados sobre o assunto. Assim, os portais eletrônicos do Aliexpress e Shopee foram analisados à luz de critérios elencados a partir das técnicas de invasão. Além disso, foram utilizadas ferramentas como Wireshark, Setoolkit e outras disponíveis a partir da distribuição Kali Linux. Após estes testes, foi possível verificar o nível de estabilidade de conexão com as plataformas aqui exploradas, assim como sua segurança. As páginas aqui analisadas e submetidas ao teste de clonagem se mostraram resistentes a esse processo, não sendo possível a realização com êxito da clonagem, ocorrendo esta apenas em parte das páginas.

Palavras-chave: e-commerce, Marketplaces internacionais, segurança web.

Abstract

The international electronic commerce platforms have consolidated themselves in the daily lives of millions of web users because it is a practical, accessible and often cost-effective means. In this sense, the issue of security is of paramount importance to follow parallel to the development of services and new products to support e-commerce, because according to the growing number of transactions among other processes developed through the internet, the number of digital crimes also increases, such as the creation of cloned electronic pages, whose users by carelessness and or inattention inform their personal data, and these are collected by cybercriminals. This work aimed to analyze the web systems for electronic commerce of international marketplaces, in the light of techniques for the analysis of invasion testing. Therefore, a bibliographic research was conducted to understand the definitions, the possibilities of intrusion testing and papers already published on the subject. Thus, the Aliexpress and Shopee electronic portals were analyzed in the light of criteria listed from the invasion techniques. In addition, tools such as Wireshark, Setoolkit and others available from the Kali Linux distribution were used. After these tests, it was possible to verify the level of connection stability with the platforms explored here, as well as their security. The pages analyzed here and submitted to the cloning test proved to be resistant to this process, and the cloning could not be successfully performed, occurring only in part of the pages.

Keywords: e-commerce, International Marketplaces, web security

LISTA DE FIGURAS

Figura 01 - Interface Setoolkit em captura de tela do terminal do Kali Linux	15
Figura 02 - Clonagem Aliexpress	16
Figura 03 - Clonagem Shopee	17
Figura 04 - Captura de tela do prompt comando do Windows do Teste de ping Aliexpress	18
Figura 05 - Captura de tela do prompt comando do Windows do teste de ping Shopee	19
Figura 06 - Captura de tela do prompt comando do Windows com comando Tracert Aliexpress	20
Figura 07 - Captura de tela do prompt comando do Windows com Comando tracert no Shopee	
Figura 8: Comparativo de tempo entre Aliexpress e Shopee(ms).	22
Figura 9: Comparativo de de TTL Aliexpress e Shopee.	24

LISTA DE QUADROS

Quadro 1 - Quadro metodológico	13
Quadro 2 - Itens Verificados	14
Quadro 3 - Variáveis analisadas	16
Quadro 4. Média de TTL e Tempo(ms).	24

LISTA DE ABREVIATURAS E SIGLAS

SI - Segurança da informação

TTL - Time To Live

IP - Internet Protocol

URL - Uniform Resource Locator

ICMP - Internet Control Message Protocol

MS - Milissegundos

IPV4 - Internet Protocol Versão 4

EaD - Educação a distância

SUMÁRIO

1. Introdução	12
2. Fundamentação Teórica	13
3. Metodologia	14
4. Resultados e discussão	17
4.1 Clonagem	18
4.2 Ping	19
4.2.1 Ping Aliexpress	19
4.2.2 Ping Shopee	20
4.4 Traceroute Shopee	22
4.5 Análise geral	23
5. Considerações finais	24
6. Referências	26

1. Introdução

Desde o advento da internet até os dias atuais, é possível verificar o aumento no seu fluxo de usuários, assim como os diversos modos de uso e de serviços disponibilizados na rede mundial de computadores.

Com a conexão de alta velocidade que atualmente possuímos, estando esta mais acessível e inserida no dia a dia de bilhões de pessoas, transações via web tornam-se uma realidade mais comum no nosso cotidiano, sendo assim, o acesso e uso de plataformas de comércio eletrônico (*e-commerce*) internacionais tornam-se cada vez mais facilitados, mobilizando diversos consumidores para aquisição de produtos via plataformas disponíveis na web sem a necessidade de deslocar-se geograficamente, sendo esse também um ponto de grande valência quanto às vantagens desse tipo de transação.

Ressalta-se que, apesar das inúmeras vantagens já consolidadas em relação a estas formas de aquisição de produtos, existem ainda pontos a serem discutidos, tendo em vista a segurança web das transações feitas por consumidor e fornecedor.

Segundo Mello *et al.* (2006), a segurança da informação (SI) envolve os seguintes conceitos basilares, como, confidencialidade, disponibilidade, integridade e autenticidade, sendo estes pilares da SI, sejam realidade nesse meio de grande fluxo de informações gerada pelo acesso cotidiano a tais plataformas, visando diminuir riscos ocasionais, voltados a ataques, em virtude da exploração de vulnerabilidades associadas a estes conceitos basilares da SI.

Evidencia-se o conceito de vulnerabilidades na SI, que possui forte ligação com fatores voltados para processos de desenvolvimento falhos, prazos de entrega de sistemas e ou plataformas, muito curtos, reduzindo assim o modelo de testes a rápidas verificações de *bugs*, sem um detalhamento adequado e sólido, na construção de estratégias de testes (MONTEVERDE, 2014).

Este trabalho objetivou analisar os sistemas web para comércio eletrônico de *marketplaces* internacionais, à luz das técnicas para análise de teste de invasão. Nesse sentido, buscou-se alcançar o objetivo geral a partir das execuções dos seguintes objetivos específicos:

- Identificar as técnicas utilizadas para análise de vulnerabilidades, com o objetivo de verificar a segurança de sistemas web de comércio eletrônico.
- Explorar e comparar os resultados obtidos a partir dos testes realizados.

A metodologia deste trabalho traz em seu escopo a caracterização da pesquisa aqui desenvolvida a partir das caracterização de Appolinário (2011), assim como a exemplificação dos principais comandos e ferramentas utilizadas no decorrer dos testes.

As seções a seguir contemplam a fundamentação teórica, ambas contextualizando e explicitando pesquisas relacionadas assim comparativos com esta, metodologia, resultados e discussão, explorando assim as considerações finais e explicação dos resultados obtidos a partir dos testes realizados e por último referências bibliográficas.

2. Fundamentação Teórica

A sociedade está extremamente conectada à rede mundial de computadores, a Internet, a partir dos diversos serviços e plataformas. Isso favoreceu os processos que antes eram custosos tanto no sentido de tempo como econômico, de tal modo a torná-los mais simples, práticos, acessíveis e possivelmente baratos.

Cita-se como exemplo o serviço de troca de mensagens entre pessoas, cujos diversos mensageiros instantâneos surgidos nos últimos anos possibilitaram incluir voz e vídeo também no canal de dados. Além disso, a rede mundial de computadores permitiu o acesso ao conhecimento e à Educação, muitas vezes, de forma gratuita a qualquer momento. A educação a distância (EaD), por exemplo, possibilitou o acesso a conteúdos, materiais didáticos e aulas de diversos docentes, educadores, pesquisadores e outros profissionais em vários idiomas. Isso pode favorecer até mesmo a formação de novos profissionais em tecnologias ou metodologias e tecnologias de última geração, como ocorre com a área de programação.

O comércio também recebeu contribuição do modelo globalizado e conectado via Internet, inclusive players como Shein, Shopee, Aliexpress, Amazon e outros se tornam ameaças aos varejistas locais, regionais e até nacionais. É possível realizar compras on-line de forma fácil, simples e cômoda, sejam internacionais ou nacionais, independentes da distância.

Nesse sentido, a Internet favoreceu o avanço desse modelo. A rede mundial de computadores é a infraestrutura de redes que gerencia serviços para aplicações distribuídas sendo executadas em sistemas finais e trocando informações entre si, assim como um conjunto de componentes que envolvem tanto software como hardware (KUROSE; ROSS, 2013). Tanenbaum (2003) conceitua redes de computadores como sendo um conjunto de computadores autônomos, estando estes interligados por uma única tecnologia.

Seguindo o contexto anterior e tendo em vista as conceituações feitas por Kurose e Tanenbaum a respeito de redes de computadores, estas consistem em uma gama de dispositivos finais interconectados entre si, compartilhando, trocando dados e recursos. Esses dispositivos seguem regras ou protocolos de comunicação, para assim poder ser concretizada de fato esta compatibilidade de compartilhamento, sendo que essa troca de recursos pode acontecer através de redes físicas ou wireless.

Envolvendo métodos de análise de segurança, existem comandos que podem de forma direta verificar a qualidade de conexão com determinada aplicação web. Existem diversas formas de análises voltadas para os testes de invasão, dentre elas cita-se o uso de ferramentas de análise de tráfego ou popularmente conhecidos como *sniffers*, a exemplo do Wireshark, que é uma aplicação focada em analisar o fluxo de informações correntes na rede, podendo verificar o Time to Live (TTL), explorado de forma mais detalhada a frente, informações como a quantidade de saltos que determinadas requisições podem realizar até chegar no seu destino final, também pode verificar informações como a versão do ip trafegado por determinada requisição.

No contexto deste trabalho, foi utilizado uma análise longitudinal em um intervalo de tempo de baixo fluxo de acesso às plataformas aqui exploradas culminando em um dia de grande fluxo de compra, sendo uma data comemorativa do dia dos

namorados. Essa análise se deu com a ferramenta Wireshark, para verificar as requisições de Ping e Traceroute, assim como a Setoolkit, clonando as páginas eletrônicas dos respectivos portais, com o intuito de verificar seu nível de segurança.

O TraceRoute, é um utilitário que tem por finalidade identificar o caminho de um pacote através da rede até seu determinado destino, o comando tracert se utiliza de requisições ICMP para percorrer e identificar os pontos por onde este mesmo pacote passou. No contexto deste artigo, através do tracert é possível avaliar se as páginas eletrônicas estão barrando requisições do tipo ICMP através dos firewalls, fazendo com que o processo de clonagem venha a ser prejudicado.

O TTL consegue analisar a duração de tempo, até o destino final de uma solicitação feita pelo usuário, com esta verificação é possível analisar se o pacote enviado conseguiu ou não concluir sua rota normalmente verificando assim o tempo de “vida” do mesmo, e conseqüentemente verificar a conexão da rede. Já o comando de rede Traceroute consegue imprimir para o usuários a rota de IP’s percorrida pelo pacote até seu destino final

A tecnologia de troca de informações em rede (Internet) tem seu uso expandido a cada dia, os riscos relacionados à segurança dessas informações também, com isso os dispositivos finais conectados em rede necessitam de uma garantia que assegure o máximo possível todas as trocas de informações.

Tendo em vista a dependência gerada pela Internet para com organizações e ou usuários finais em razão de suas facilidades como por exemplo, transações quase que instantâneas, armazenagem de informações. A SI se torna uma área de investimento obrigatória pelas empresas responsáveis pelos respectivos *marketplaces*, pois a proteção de dados provenientes de usuários de tais portais é essencial para garantir o uso desses portais, tendo em vista que envolve dados pessoais e financeiros, que poderão ser utilizados para práticas criminosas, caso caia nas mãos estelionatários.

Nesse sentido, destaca-se a importância da criptografia e de outros mecanismos de proteção de dados. Silva (2013) faz uma análise em relação a criptografia para o modelo de segurança relacionados a páginas de comércio eletrônico, verificando e analisando as maiores plataformas desse segmento utilizados no Brasil. Como fator diferencial entre a pesquisa de Silva (2013) e o trabalho aqui desenvolvido, o foco deste trabalho incide em analisar de forma mais específica a estabilidade assim como fatores de segurança à luz dos testes de invasão, sendo que foram utilizadas duas das maiores páginas de comércio eletrônico internacionais do mundo.

3. Metodologia

A presente pesquisa visou analisar alguns critérios de segurança, vinculados às páginas eletrônicas de comércio eletrônico internacional, também chamado de marketplace. O escopo desta pesquisa está vinculado ao Aliexpress e Shopee, pois ambas compõem o rol de páginas eletrônicas do escopo desta pesquisa e possuem alto nível de popularidade e relevância em seu respectivo nicho de negócio.

Nesse sentido, segundo Appolinário (2011) e como exibido no Quadro 1 a classificação, este trabalho é caracterizado como sendo aplicado em relação à finalidade, pois buscou a

atingir a análise de um problema real, sendo este a verificação de segurança mediante o modelo dos testes de invasão, para as plataformas de comércio eletrônico do Aliexpress e Shopee. No que diz respeito ao Tipo, é considerada bibliográfica, pois inicialmente foi realizada uma identificação dos materiais já publicados sobre o assunto, bem como também se caracteriza como experimental pois foi realizado dois momentos de experimentos ao longo da pesquisa, no que se diz respeito ao fluxo de acessos aos sistemas de comércio eletrônico aqui referenciados sendo estes testes em datas específicas de grande quantidade de acesso, assim como de baixa quantidade de acesso.

Quadro 1. Quadro Metodológico

Finalidade	Tipo	Origem dos dados	Local de realização	Natureza	Temporalidade	Delineamentos
Aplicada	Experimental / Bibliográfica	Documental / campo	Campo	Qualitativa	Longitudinal	levantamento

Fonte: Pesquisa direta.

Em relação a origem dos dados, inicialmente classifica-se esta pesquisa como documental, por conta de sua coleta de informações baseada na pesquisa bibliográfica, somado a isso, essa pesquisa também tem sua origem de dados no campo, haja vista os testes e análises das ferramentas de e-commerce. A pesquisa será realizada em campo, analisando as variáveis do contexto das plataformas de comércio eletrônico aqui exploradas, ou seja, adequando-se perfeitamente ao modelo de campo no referente à localidade de realização da pesquisa. A natureza deste trabalho caracteriza-se como qualitativo, pois o mesmo analisará a qualidade da segurança em determinados aspectos.

A análise de segurança das plataformas aconteceu em dois momentos, sendo um com baixo pico de acesso e outro em momento de grande fluxo de acessos, caracterizando assim esta pesquisa em relação a sua temporalidade como longitudinal. Mediante o levantamento de dados no modelo descritivo, esta arguição molda-se no modelo delineamento de levantamento. Para análise de dados tomaremos como base as variáveis usadas no trabalho de Angelo e Oliveira (2019) *in prelo*.

Para aplicação do teste de clonagem, a ferramenta Social Engineering Toolkit (Setoolkit), presente no sistema operacional (SO) Kali Linux, foi explorada baseada na pesquisa de Angelo e Oliveira (2019) *in prelo*, que consistia em escolher uma página eletrônica e a partir do URL do página eletrônica, aplicar no Setoolkit e gerar uma clonagem do site, o nível de detalhes da clonagem, depende da segurança da página explorada. O Quadro 2, explicita e mostra as variáveis que foram analisadas e verificadas ao longo do desenvolvimento e aplicação dos resultados obtidos neste trabalho

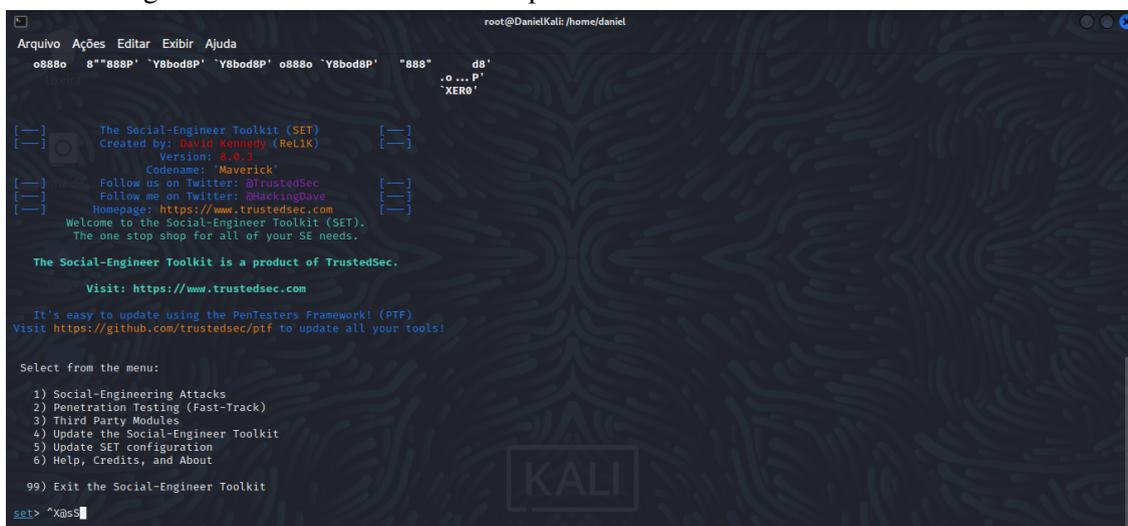
Quadro 2. Itens verificados

ID	Item avaliado	Descrição
01	Número IP	Identificar o número do IP a fim de verificar se há alteração do endereço em cada momento de teste.
02	Versão do IP	Verificar a versão do IP a fim de verificar se é IPV4 ou IPV6 em cada momento de teste.
03	Tipo do IP	Verificar se o IP é estático ou não.
04	TTL	Analisar se houve alguma perda de pacote baseada no TTL
05	Traceroute	Analisar quantos saltos o pacote fez até o destino final.
06	IP visível	Analisar se o IP está visível
07	Clonagem por URL	Realizar a clonagem das plataformas a partir da url correspondente.
08	Método de teste	Realizar o teste manualmente via prompt comando.
09	Ping (ms)	Verificar o tempo em milissegundos do pacote transitado

Fonte: Pesquisa direta.

A Setoolkit é uma ferramenta que clona páginas eletrônicas e verifica o nível de segurança, conforme a clonagem. Sendo assim, páginas de login de plataformas web, podem ser utilizadas por meio do Setoolkit para coleta de informações, podendo comprometer a confiança das mesmas como um todo. Na figura 4 é possível observar a interface inicial da ferramenta.

Figura 1: Interface Setoolkit em captura de tela do terminal do Kali Linux.



Fonte: Pesquisa direta.

Seguindo o protocolo de análise e pesquisa mostrado nesta seção, a próxima tratará de realizar as aplicações definidas e aqui delimitadas, a fim de analisar os dados coletados da pesquisa em tela.

4. Resultados e discussão

No quadro 3, é apresentado as variáveis, Número IP, Versão do IP, Tipo do IP, TTL, Traceroute, IP Visível, Clonagem por URL, Método de teste, Ping(ms), que foram objetos de análises desta pesquisa, trazendo assim os resultados dos testes que a estas foram submetidos.

Quadro 3. Variáveis analisadas.

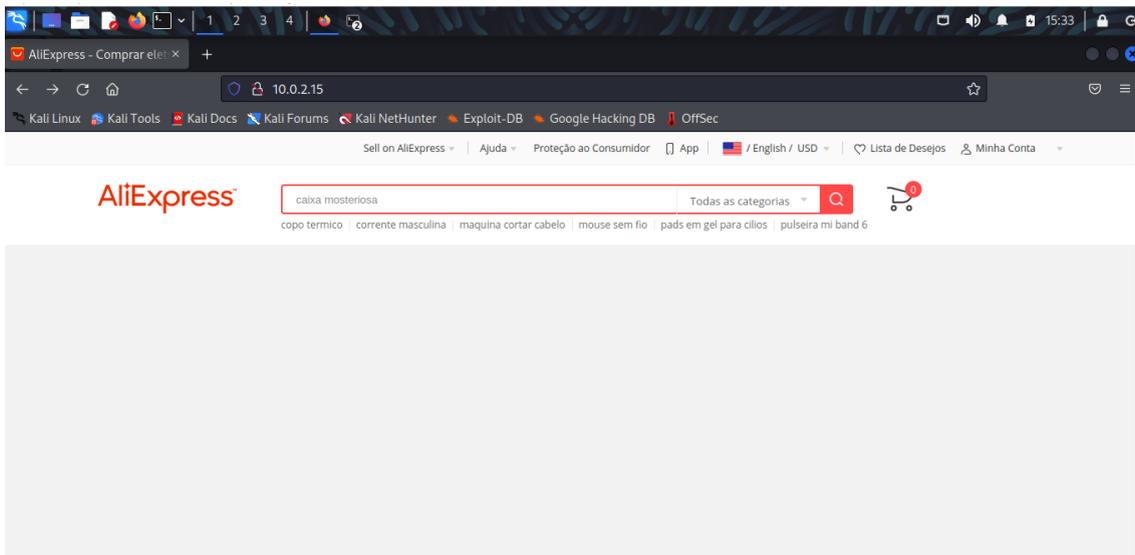
ID	Crítérios	Aliexpress	Shopee
01	Número do IP	sim	sim
02	Versão do IP	IPv4	IPv4
03	Tipo do IP	Dinâmico	Estático
04	TTL	sim	sim
05	Traceroute	sim	sim
06	IP visível	sim	sim
07	Clonagem por URL	Parcialmente	Parcialmente
08	Método de teste	Manual Prompt Comando do Windows	Manual Prompt Comando do Windows
09	Ping (ms)	sim	sim

Fonte: Pesquisa direta.

4.1 Clonagem

Referente à clonagem da Aliexpress, a ferramenta conseguiu apenas clonar o cabeçalho, juntamente com a barra de pesquisa e algumas informações como logomarca. Com isso informações e imagens de produtos não apareceram na clonagem e funcionalidades como a tradução da página. A sessão de clonagem não funciona, e não foi possível cloná-la. Concluindo assim que o processo de clonagem deu-se apenas em parte, não sendo possível a totalidade de sua eficiência.

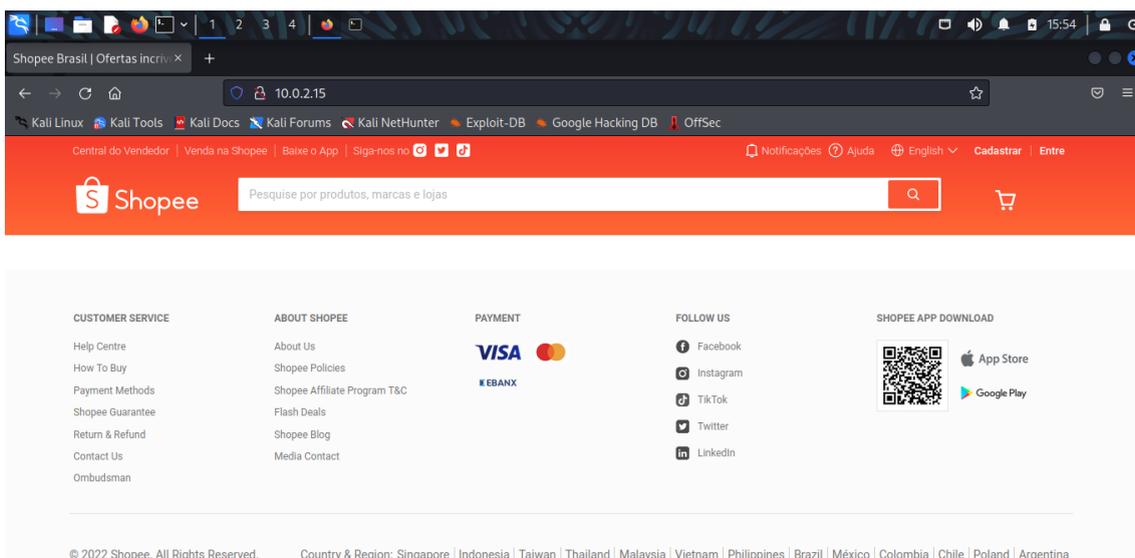
Figura 2: Clonagem Aliexpress



Fonte: Pesquisa direta

Quanto à clonagem da Shopee, foram identificados uma quantidade maior de elementos clonados na página, cabeçalho logo, rodapé, caixa de pesquisa. A sessão de login também foi clonada, contudo não ficou funcional. Seguindo o modelo conclusivo do teste feito na plataforma do aliexpress, o da shopee também deu-se por incompleto, sendo assim, a ferramenta Setoolkit não conseguiu realizar a clonagem da página como um todo, apenas fragmentos.

Figura 3: Clonagem Shopee



Fonte: Pesquisa direta

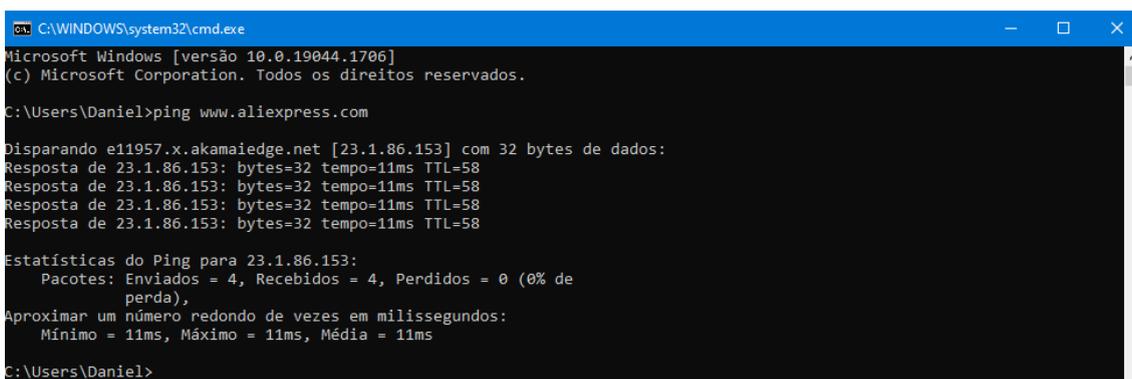
4.2 Ping

O ping é um utilitário que avalia a conexão entre terminais, se utilizando de requisições ICMP(Internet Control Message Protocol). Sendo assim o ping envia pacotes por meio do ICMP para um terminal determinado pelo usuário, conseguindo testar a conexão. Diante do exposto anterior o ping de uma forma geral, testa a conectividade, assim como o tempo de resposta das requisições feitas, de acordo com o tempo que os pacotes levam para percorrer o caminho é possível avaliar também a qualidade da conexão.

4.2.1 Ping Aliexpress

A figura 4 mostra o teste ping sendo realizado a partir do comando “ping www.aliexpress.com”.

Figura 4: Captura de tela do prompt comando do Windows do Teste de ping Aliexpress.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [versão 10.0.19044.1706]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Users\Daniel>ping www.aliexpress.com

Disparando e11957.x.akamaiedge.net [23.1.86.153] com 32 bytes de dados:
Resposta de 23.1.86.153: bytes=32 tempo=11ms TTL=58

Estatísticas do Ping para 23.1.86.153:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
    perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 11ms, Máximo = 11ms, Média = 11ms

C:\Users\Daniel>
```

Fonte: Pesquisa direta.

Os testes de ping realizados de forma longitudinal verificaram a estabilidade dos resultados exibidos para a página do Aliexpress, sendo pois constante as informações, não havendo variação crítica nos dados, ou alteração que viesse a modificar as conclusões aqui expostas. A variação de tempo, verificada em *ms*, como mostrado na figura 4, oscilou entre 11ms e 20ms, sendo uma variação de muito pouca amplitude.

Quanto à variável TTL, também não houve variação significativa, independente do período em que esta foi analisada, podendo-se observar uma micro variância entre 54 e 58 TTL. Da mesma forma em que foram analisadas as variáveis anteriormente exploradas, a questão de perda de pacotes também seguiu um modelo de estabilidade, consistindo em nenhuma perda de pacotes, segundo os testes realizados para conclusão deste projeto.

4.2.2 Ping Shopee

Figura 5: Captura de tela do prompt comando do Windows do teste de ping Shopee.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [versão 10.0.19044.1706]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Users\Daniel>ping shopee.com

Disparando shopee.com [103.115.78.65] com 32 bytes de dados:
Resposta de 103.115.78.65: bytes=32 tempo=317ms TTL=44
Resposta de 103.115.78.65: bytes=32 tempo=316ms TTL=44
Resposta de 103.115.78.65: bytes=32 tempo=317ms TTL=44
Resposta de 103.115.78.65: bytes=32 tempo=318ms TTL=44

Estatísticas do Ping para 103.115.78.65:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
    perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 316ms, Máximo = 318ms, Média = 317ms

C:\Users\Daniel>
```

Fonte: Pesquisa direta.

Realizado os testes de ping de forma longitudinal assim como no modelo definido para o aliexpress, os testes para a plataforma de comércio eletrônico, Shopee, foram observadas, assim como na plataforma anteriormente discutida, resultados estáveis, sendo pois, quanto a análise de tempo de resposta, discutida em *ms*, a variância seguiu-se de forma muito pequena, valores entre 317 ms e 321 ms, independente do dia da respectiva análise.

A variável TTL nos testes feitos em relação a Shopee, também seguiram de forma estável, em todos os dias de realização dos testes, variando de forma baixa, sendo valores entre 39 TTL e 44 TTL. Tanto na plataforma do aliexpress, como na da Shopee, independente do dia, os testes foram estáveis.

4.3 Traceroute Aliexpress

De acordo com os testes realizados a partir do comando Tracert no prompt de comando do windows, observou-se que o IP do servidor do aliexpress é dinâmico e possui a versão IPV4, alterando-se, caso o fluxo de requisições seja superior ao quantitativo suportado pelo próprio servidor, demonstrando assim que os servidores do aliexpress trabalham baseados no modelo de sistemas distribuídos.

Além disso, houveram variâncias no quantitativo de saltos, estando esta variação independente do dia do teste. Os valores variavam entre 7 e 12 saltos até terminar a execução do programa, o que de forma alguma, gerou algum tipo de gargalo no acesso à plataforma aqui explorada.

Figura 6: Captura de tela do prompt comando do Windows com comando Tracert Aliexpress.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [versão 10.0.19044.1706]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Users\Daniel>tracert www.aliexpress.com

Rastreando a rota para e11957.x.akamaiedge.net [23.207.60.70]
com no máximo 30 saltos:

  1  1 ms      1 ms      <1 ms    192.168.1.1
  2  1 ms      35 ms     10 ms    10.105.1.1
  3  *          *          *        Esgotado o tempo limite do pedido.
  4  *          *          *        Esgotado o tempo limite do pedido.
  5  *          *          *        Esgotado o tempo limite do pedido.
  6  356 ms    565 ms    27 ms    170.79.214.157
  7  29 ms     33 ms     80 ms    170.79.213.9
  8  28 ms     23 ms     14 ms    170.79.213.11
  9  111 ms    40 ms     242 ms   170.79.213.41
 10  89 ms     35 ms     22 ms    170.79.213.64
 11  *          *          *        Esgotado o tempo limite do pedido.
 12  290 ms    103 ms    65 ms    a23-207-60-70.deploy.static.akamaitechnologies.com [23.207.60.70]

Rastreamento concluído.

C:\Users\Daniel>
```

Fonte: Pesquisa direta.

4.4 Traceroute Shopee

Com os testes de traceroute na plataforma Shopee, foi possível verificar que no período promocional da data 06/06/2022, houveram um maior quantitativo de saltos, assim como, um aumento na perda de pacotes, exibido na figura 7 abaixo.

Figura 7: Captura de tela do prompt comando do Windows com Comando tracert no Shopee.

```
C:\Users\Daniel>tracert www.shopee.com

Rastreando a rota para sg-eq.sgw.shopeemobile.com [103.115.78.65]
com no máximo 30 saltos:

 1  <1 ms     <1 ms     <1 ms    10.0.0.1
 2  3 ms      1 ms      1 ms     100.72.114.1
 3  1 ms      2 ms      1 ms     100.127.255.1
 4  10 ms     *          1 ms     10.222.101.1
 5  4 ms      4 ms      3 ms     10.222.99.1
 6  14 ms     12 ms     12 ms    172.16.200.53
 7  12 ms     12 ms     12 ms    172.16.128.85
 8  14 ms     12 ms     13 ms    8.243.156.205
 9  *          *          *        Esgotado o tempo limite do pedido.
10  80 ms     80 ms     120 ms   mai-b2-link.ip.twelve99.net [213.248.84.80]
11  123 ms    123 ms    124 ms   atl-b24-link.ip.twelve99.net [62.115.113.48]
12  *          157 ms    166 ms   atl-bb1-link.ip.twelve99.net [62.115.134.246]
13  105 ms    107 ms    103 ms   nash-bb1-link.ip.twelve99.net [62.115.137.55]
14  *          114 ms    *        dls-bb1-link.ip.twelve99.net [62.115.137.45]
15  164 ms    173 ms    178 ms   dls-b23-link.ip.twelve99.net [62.115.136.119]
16  *          *          *        Esgotado o tempo limite do pedido.
17  *          *          *        Esgotado o tempo limite do pedido.
18  *          *          *        Esgotado o tempo limite do pedido.
19  *          *          *        Esgotado o tempo limite do pedido.
20  *          *          *        Esgotado o tempo limite do pedido.
21  *          *          325 ms   sngc-b5-link.ip.twelve99.net [62.115.124.216]
22  343 ms    345 ms    343 ms   garena22246-ic350946-sngc-b1.ip.twelve99-cust.net [62.115.182.155]
23  318 ms    317 ms    317 ms   143.92.108.202
24  375 ms    332 ms    384 ms   143.92.108.150
25  333 ms    333 ms    334 ms   143.92.108.151
26  *          *          *        Esgotado o tempo limite do pedido.
27  341 ms    334 ms    333 ms   103.115.78.65

Rastreamento concluído.

C:\Users\Daniel>
```

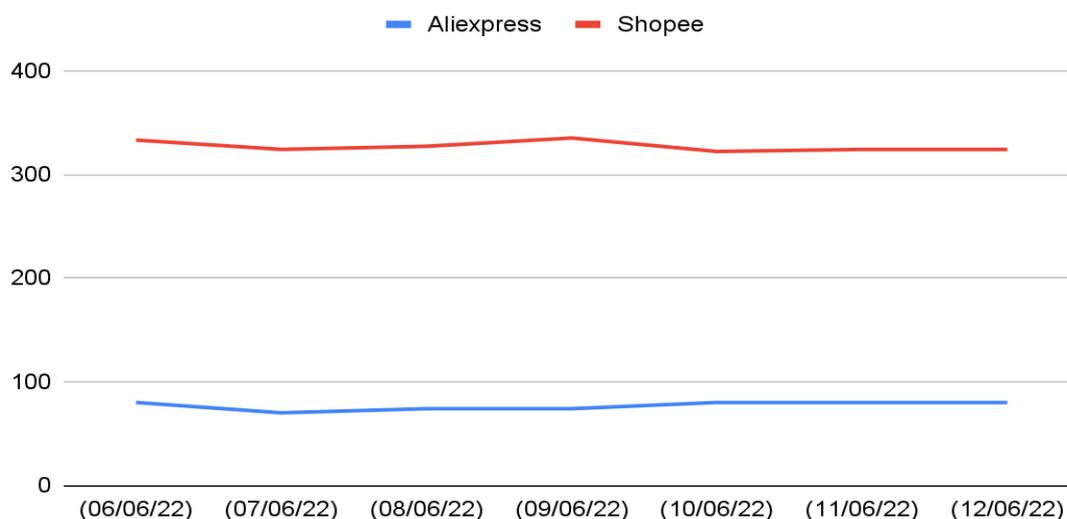
Fonte: Pesquisa direta.

Realizada a análise a partir do comando Tracert no prompt de comando do Windows, observou-se na plataforma da Shopee que o IP do servidor é estático e possui a versão IPV4. Além disso, houveram variâncias no quantitativo de saltos, os valores variavam entre 24 e 27 saltos até terminar a execução do programa, o que de nenhuma forma, assim como na plataforma do Aliexpress, não gerou gargalo no acesso à plataforma.

4.5 Análise geral

Para análise comparativa entre os valores correspondentes ao tempo de circulação do pacote ao longo dos dias da análise, verificou-se variações para os valores entre 70 ms e 80 ms para a plataforma do Aliexpress. Referente a plataforma da Shopee, que assim como a página eletrônica do Aliexpress, foi analisada ao longo de uma semana, trazendo um quantitativo maior, relacionado ao tempo em milissegundos, sendo esta variação entre 322 ms e 335 ms. As verificações de análise do tempo de circulação na rede dos pacotes, estão informados na figura 8.

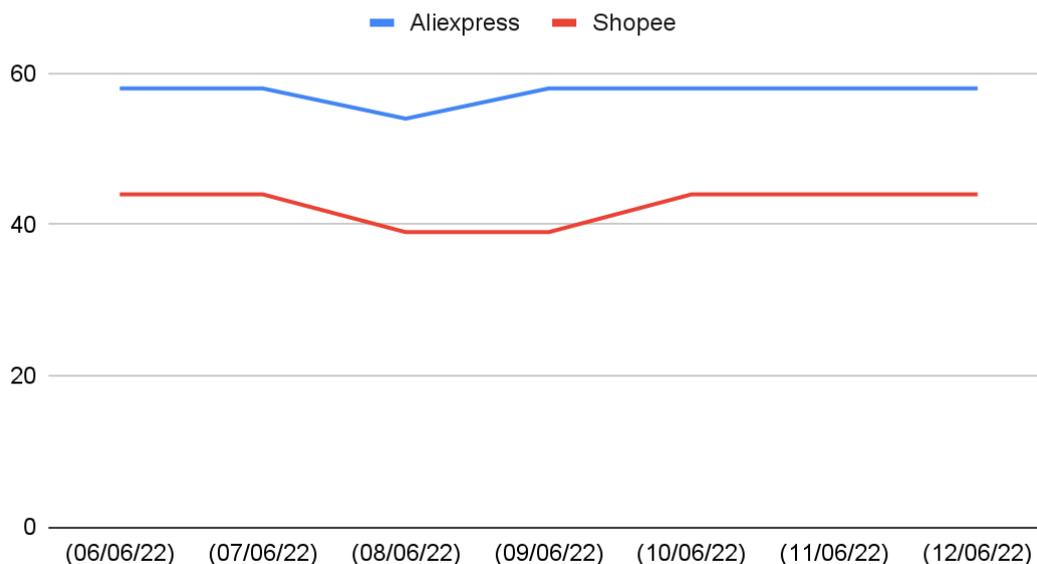
Figura 8: Comparativo de tempo entre Aliexpress e Shopee(ms).



Fonte: Pesquisa direta.

A figura 9, mostra um gráfico comparativo entre a variação do TTL em comparação com as plataformas vinculadas a este trabalho. A variação referente a página eletrônica do Aliexpress, mostra valores que variam entre 54 e 58 TTL. Quanto à página do Shopee esses dados oscilam entre 39 e 44 TTL.

Figura 9: Comparativo de de TTL Aliexpress e Shopee.



Fonte: Pesquisa direta

As figuras 8 e 9 anteriormente apresentadas, mostraram variações de valores referente ao TTL e o tempo dos pacotes em circulação para cada requisição do comando ping, sendo assim, no quadro 4, são exibidas as médias referente a esses dois valores, quanto aos pacotes transitados nos momentos dos testes realizados, nenhum foi perdido.

Quadro 4. Média de TTL e Tempo(ms).

Médias	Aliexpress	Shopee
TTL	58	44
Tempo (ms)	80	324

Fonte: Pesquisa direta

Através da análise geral das informações coletadas a partir dos testes, foi possível identificar variações ou a falta delas, em relação aos pacotes, de forma mais específica, quanto ao TTL, tempo em *ms*, assim como a perda de pacotes enquanto transitavam na rede, podendo esses resultados serem explorados a partir das figuras 8, 9 e do quadro 4.

5. Considerações finais

Este trabalho apresenta conceitos, análises e aplicações reais de métodos voltados para segurança da informação, à luz dos testes de invasão. Com isso, fica exposta a premissa objetivadora, sendo, pois, analisar as páginas web de comércio eletrônico internacionais, baseado nos métodos de testes de invasão.

Analisando-se a partir dos resultados obtidos dos testes feitos nessa pesquisa, é possível observar o êxito obtido na verificação e análise das plataformas com as variáveis definidas, foi possível também verificar a estabilidade das plataformas de comércio eletrônico internacionais, mediante análise longitudinal dos testes, assim como sua segurança, sendo pois concluído, que ambas possuem eficientes sistemas de servidores, para suportar todo o fluxo de acesso, mesmo em dias de grande fluxo. Com as análises realizadas, foi também perceptível o nível de segurança das mesmas, principalmente no que se refere a clonagem de páginas.

Diante dos fatos analisados e dos resultados obtidos, espera-se que ambos possam servir como base motivacional, para desenvolvimento de outras pesquisas baseadas em novas plataformas digitais de comércio eletrônico, assim como uma maior variação de métodos, a fim de extrair outros resultados.

Como o trabalho aqui apresentado, se objetivou analisar especificamente duas grandes plataformas, trabalhos futuros podem aumentar o leque de possibilidades, aumentando assim o número de páginas de comércio eletrônico analisadas juntamente com o quantitativo de variáveis analisadas.

6. Referências

ANGELO, R; OLIVEIRA, F. K. Engenharia Social e Phishing a partir da ferramenta SeToolKit. Trabalho de Conclusão de Curso. Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano (IFSertãoPE). Salgueiro, 2019. *in prelo*.

APPOLINÁRIO, F. (2011) “Metodologia da ciência: filosofia e prática da pesquisa”, 2ª edição, páginas 62-70.

DE MELLO, Emerson Ribeiro et al. Segurança em serviços web. Livro de Minicursos do VI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. Santos: SBC, p. 1-48, 2006.

KUROSE, J. F.; ROSS, K. W. Redes de Computadores e a Internet: Uma Nova Abordagem Top-down. 2013.

MONTEVERDE, Wagner Aparecido. Estudo e análise de vulnerabilidades web. 2014. Trabalho de Conclusão de Curso. Universidade Tecnológica Federal do Paraná.

SILVA, Alexandra Meca Bernardo da. O uso da criptografia na segurança da informação em e-commerce. 2013.

TANENBAUM, Andrew S. Redes de Computadores. Tradução da 4rd. Ed. em inglês. Editora Campus.2003.