INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SERTÃO PERNAMBUCANO
COORDENAÇÃO DO CURSO DE SISTEMAS PARA INTERNET
SISTEMAS PARA INTERNET

CÉSAR DE BARROS COSTA

ANÁLISE DE SEGURANÇA DOS SISTEMAS WEB DAS INSTITUIÇÕES FINANCEIRAS BRASILEIRAS

SALGUEIRO

2024

CÉSAR DE BARROS COSTA

ANÁLISE DE SEGURANÇA DOS SISTEMAS WEB DAS INSTITUIÇÕES FINANCEIRAS BRASILEIRAS

Trabalho de Conclusão de Curso apresentado à Coordenação do curso de Sistemas para Internet do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano, campus Salgueiro, como requisito parcial à obtenção do título de tecnólogo em Sistemas para Internet.

Orientador(a): Dr. Francisco Kelsen de Oliveira

SALGUEIRO

2024

Dados Internacionais de Catalogação na Publicação (CIP)

C838 Costa, Cesar de barros.

Análise de segurança dos sistemas web das instituições financeiras brasileiras / Cesar de barros Costa. - Salgueiro, 2024.
27 f. : il.

Trabalho de Conclusão de Curso (Sistemas para Internet) -Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano, Campus Salgueiro, 2024.
Orientação: Prof. Dr. Francisco kelsen de oliveira.

1. Rede de computadores. 2. information security. I. Título.

CDD 004.62

Gerado automaticamente pelo sistema Geficat, mediante dados fornecidos pelo(a) autor(a)

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

CÉSAR DE BARROS COSTA

ANÁLISE DE SEGURANÇA DOS SISTEMAS WEB DAS INSTITUIÇÕES FINANCEIRAS BRASILEIRAS

Trabalho de Conclusão de Curso apresentado à Coordenação do curso de Tecnologia em Sistemas para Internet do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano, campus Salgueiro, como requisito parcial à obtenção do título de Tecnólogo em Sistemas para Internet.

Aprovado em:

BANCA EXAMINADORA

_____

Prof. Francisco Kelsen De Oliveira

_____

Prof. Francisco Junio da Silva Fernandes

_____

Prof. Leão João Dehon Costa

AGRADECIMENTOS

Gostaria de agradecer primeiramente a Deus, que me deu saúde e forças para superar as dificuldades ao longo desses anos.

Agradeço também a minha família e amigos, que me ajudaram e incentivaram nos momentos difíceis. Em especial ao Lucas dos anjos e Marcos Antonio, colegas de curso e amigos.

Agradeço ao professor e orientador Francisco Kelsen de Oliveira por todo o suporte e atenção para a realização deste TCC. E por fim, agradeço à banca examinadora deste trabalho.

“Medir o progresso de um programa por linhas de código é como medir o processo de montagem de um avião pelo peso. “

Bill Gates

RESUMO

O avanço da internet permitiu a troca instantânea de informações, conectando a população global em tempo real por meio de diversos dispositivos. Com a transformação de serviços bancários para plataformas digitais, surge a necessidade de aprimoramento constante na segurança da informação (SI), devido a riscos de golpes, como a clonagem de páginas. A SI busca proteger sistemas e dados contra erros e furtos. Este estudo tem como objetivo analisar as vulnerabilidades básicas relacionadas aos golpes de phishing e pharming em páginas eletrônicas de instituições bancárias brasileiras, pois, desta forma poderá ajudar a entender como os golpistas podem criar páginas falsas para enganar os usuários. Com esse objetivo em mente, foi realizada inicialmente uma investigação bibliográfica para explorar os conceitos, as técnicas de teste de invasão e outras pesquisas relevantes já conduzidas acerca desse tema. As páginas eletrônicas das instituições Banco do Brasil, Caixa Econômica, Santander e Itaú os respectivos foram analisados à luz dos seguintes aspectos: clonagem de página eletrônica, acessos e respostas aos servidores das respectivas aplicações. Ao final do estudo, apresentou dados importantes em quesitos as suas informações, como também erros que possivelmente podem vir a ser usados por pessoas má intencionadas. Resultados esses que poderão ser utilizados para pesquisas futuras, podendo assim ser aplicados os mesmos comandos e assim possa fazer um comparativo com os resultados aqui adquiridos, propondo melhorias.

Palavras-chave: Segurança da Informação, Redes de Computadores.

ABSTRACT

The advancement of the internet has allowed the instant exchange of information, connecting the global population in real time through various devices. With the transformation of banking services to digital platforms, there is a need for constant improvement in information security (IS), due to the risk of scams, such as page cloning. SI seeks to protect systems and data against errors and theft. This study aims to analyze the basic vulnerabilities related to phishing and pharming scams on electronic pages of Brazilian banking institutions, as this can help to understand how scammers can create fake pages to deceive users. With this objective in mind, a bibliographical investigation was initially carried out to explore the concepts, penetration testing techniques and other relevant research already conducted on this topic. The electronic pages of the respective institutions Banco do Brasil, Caixa Econômica, Santander and Itaú were analyzed in light of the following aspects: electronic page cloning, access and responses to the servers of the respective applications. At the end of the study, he presented important data regarding his information, as well as errors that could possibly be used by people with bad intentions. These results can be used for future research, allowing the same commands to be applied and a comparison with the results acquired here, proposing improvements.

Keywords: Information Security, Computer Networks.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

SI: Segurança da Informação
ADSL: Asymmetric Digital Subscriber Line
RC: Redes de Computadores
DNS: Sistema de Nomes de Domínio
CMD: Prompt de Comando
TTL: Time to Live
IP: Internet Protocol
ZAP: Zed Attack Proxy
Ms : Milisegundos

SUMÁRIO

1 INTRODUÇÃO

Graças ao advento da internet, informações são trocadas instantaneamente e navegam entre a rede na velocidade da luz, chegando a todos os dispositivos em tempo real, onde todos podem ter acesso com apenas um aparelho. Com isso, a maior parte da população mundial já usufrui de todos os benefícios que a rede mundial de computadores oferece, assim, todos estão de alguma forma conectados, seja por um smartwatch, smartphone, tablet ou uma Smart TV.

Com tais avanços tecnológicos, trazem consigo a necessidade de melhorias constantes nas redes, seja em termos de velocidade da ou até mesmo, segurança nas informações que trafegam. Contudo, como tudo está conectado, os bancos digitais também entraram no mundo web, transformando seus serviços físicos em digitais. No entanto, as vulnerabilidades desses sistemas são buscadas por cibercriminosos, a fim de que possam aplicar golpes, que vão desde clonagem de página a outros possíveis golpes, no qual um hacker pode utilizar do mesmo para colher informações de segurança, dados pessoais e afins.

Deste modo, a segurança da informação (SI), vem se enriquecendo de pesquisas voltadas para área a fim de implementá-las para auxiliar na proteção de todas as informações pessoais dos usuários digitais.

Segurança da informação trata de tudo aquilo que envolve a proteção de sistemas e dados de um determinado indivíduo ou organização. É papel da segurança da informação garantir que estes dados/sistemas estão realmente protegidos contra erros, furtos ou quaisquer incidentes aos quais as informações estão dispostas (MENDES, 2021).

O interesse dos pesquisadores pela otimização da SI vem crescendo a cada dia, pois tem o intuito de melhorar a segurança dos usuários da rede, pois a evolução da SI tem que ser constante, visto que os hackers estão sempre procurando brechas para burlar os sistemas, onde a problemática se deu a partir da seguinte indagação: o quão vulnerável podem ser as páginas de internet de instituições financeiras no Brasil?

Portanto, o objetivo desta pesquisa foi analisar as vulnerabilidades básicas relacionadas aos golpes de phishing e pharming em páginas eletrônicas de instituições bancárias brasileiras. Isso foi feito através de dois métodos principais: Testes de rede: Esses testes são realizados para avaliar a segurança da informação a partir da busca de vulnerabilidades de interconexão e outros aspectos softwares desses bancos, que podem abrir os caminhos para outros golpes. Eles podem incluir a verificação de vulnerabilidades que podem ser exploradas por invasores.

Este trabalho divide-se em organizar as pesquisas existentes na literatura, a fim de auxiliar e reforçar como a internet e dispositivos conectados transformaram o acesso à

informação e aumentaram a vulnerabilidade dos sistemas., identificar as principais fragilidades dos sistemas web das instituições financeiras, avaliar a eficácia das medidas de segurança existentes, apresentar como a pesquisa foi desenvolvida e organizada, mostrar informações de como cada dado foi analisado e expor cada uma das informações adquiridas e por fim, reforçar o objetivo deste trabalho, apresentando sugestões de trabalhos futuros.

2 REFERENCIAL TEÓRICO

Com a chegada dos microcomputadores e da computação pessoal, a transmissão de informações por meio de redes tornou-se uma ferramenta crucial de comunicação. Atualmente, é a base de quase todos os outros tipos de comunicação, como, por exemplo, a telefonia celular 4G e telefonia fixa VoIP (Camargo et al., 2021).

No entanto, ao longo do tempo, a internet tem evoluído com novas tecnologias, dispositivos e meios de informação mais precisos e avançados. Isso proporciona cada vez mais facilidades aos usuários que a utilizam para realizar tarefas que antigamente eram complexas e de difícil acesso.

Juntamente com os avanços nos dispositivos, houve também uma expansão na cobertura e na velocidade de transmissão de dados na internet, principalmente devido ao progresso das tecnologias de comunicação com e sem fio, como Asymmetric Digital Subscriber Line (ADSL), Wi-Fi e 4G/5G (Silva, 2022). Assim, outro meio de comunicação são os aplicativos de smartphones que acompanharam essa evolução.

CARTILHA (2021), enfatiza a comunicação via internet como:

> "[...] Com o passar dos anos, a rede foi se transformando e conquistando cada vez mais espaço, fato que denomina o momento atual como "Mundo Globalizado", visto que a Internet permite que toda população mundial esteja conectada através da Internet."

Assim, os usuários usufruem da rede de forma eficaz, rápida e segura, utilizando diversos protocolos que compõem as redes de computadores. Especificamente, Redes de Computadores (RC) são conjuntos de máquinas destinadas ao processamento de dados independentes, com conexão entre seus sistemas operacionais por apenas um processo tecnológico (Tanenbaum, 2003). Quanto à própria rede de computadores em si (e.g., utilização e topologia da rede, falhas em roteadores e links, disponibilidade e desempenho de serviços e dinâmica de roteamento) (Coromela et al. 2022) são itens essenciais para que a mesma seja

disponibilizada seguindo conceitos de segurança para todos os usuários, especialmente os que utilizam em transações bancárias ou *home banking*, também chamado de *internet banking* ou *e-banking*.

Após o surgimento dos *smartphones* e o longo avanço da RC os bancos digitais começaram a sair do físico e entrar no mundo digital, as movimentações bancárias se tornaram mais práticas utilizando apenas um dispositivo. Com os avanços tecnológicos que levaram à popularização do mobile e do internet banking, a competitividade do setor bancário tornou-se mais acirrada. As informações sobre os produtos, serviços, custos e benefícios de cada banco estão mais acessíveis, o que aumenta a gama de informações possuídas pelo consumidor no momento de optar por um banco (Lacerda, 2022).

Contudo, para usufruir desses meios, os usuários precisam de uma certa segurança e confiabilidade com seus dados. Considerando que instituições bancárias, por via de regra, se preocupam e investem muito mais em segurança da informação[...] (Bisso; Kreutz, 2022).

Com isso, nota-se que a dedicação em melhorar sua plataforma por parte das instituições bancárias segue cada vez mais séria, para que todos os dados de seus usuários sejam preservados. Portanto, assim como a evolução da internet, os *e-banking*s investem mais em profissionais qualificados para realizarem buscas de falhas em seus bancos digitais.

Portanto, os bancos até pouco tempo se davam muita atenção à privacidade e à segurança de dados. Entretanto, os dados e exemplos de penalidades mostram que o cenário mudou drasticamente nos últimos anos, isto é, estes assuntos tornaram-se uma prioridade de estado. (Lacerda, 2022). Visando a correção de possíveis problemas, é necessário ampliar as soluções de segurança a tradicionais, como: firewall; e, sistemas de detecção/prevenção de intrusões, para que possam lidar com o tráfego de rede de alta velocidade [...]

Eles, no decorrer dos anos, podem ou sofrem invasões em seus bancos de dados, podendo assim, vazar dados de usuários. Assim, as instituições optam por profissionais que possam realizar testes de invasões. Weidman (2014, p.30) relata que o teste de Invasão (ou Pentesting) pode ser interpretado como uma simulação de ataques reais destinada a avaliar os riscos e impactos associados a brechas de segurança identificadas (caso sejam exploradas).
Luiz e Lucas (2019), também destaca sobre teste de invasão como:

> [...] visa checar o cumprimento de controles previamente definidos e está a identificar e analisar vulnerabilidades sem necessariamente explorá-las, a finalidade de um teste de invasão vai além ao utilizar métodos e técnicas de um atacante para não somente identificar brechas de segu-rança, mas para também analisá-las profundamente, explorando-as quando viável, a fim de

> avaliar o que pretensos invasores poderiam obter após uma exploração bem sucedida das vulnerabilidades encontradas.

Entre as estratégias mais recorrentes empregadas por cibercriminosos estão a engenharia social e a clonagem de sites, métodos que se revelam bastante eficazes na captura de informações sensíveis. Essas abordagens aproveitam a desatenção e os comportamentos das vítimas, frequentemente levando-as a revelar dados confidenciais sem perceber que estão sendo coagidas em um ataque. Compreender o funcionamento dessas ameaças é crucial para reforçar as defesas e garantir a integridade dos sistemas de informação.

A engenharia social é uma estratégia de manipulação psicológica empregada por criminosos para obter dados sigilosos ou perpetrar fraudes. Ao invés de se aproveitar de falhas técnicas, os engenheiros sociais trabalham para explorar a confiança e a curiosidade das pessoas, levando-as a acreditar em mentiras. Por exemplo, uma pessoa pode ser levada a revelar senhas ou informações pessoais ao pensar que está se comunicando com uma entidade confiável, enquanto na verdade está sendo enganada. A efetividade dessa tática depende da habilidade do criminoso em elaborar situações que aparentam ser reais e urgentes, promovendo uma resposta rápida e sem reflexão (Hadnagy, 2010).

A clonagem de páginas é uma estratégia empregada por criminosos virtuais para reproduzir, tanto em aparência quanto em funcionalidade, um site autêntico. Os invasores produzem uma réplica fiel de uma página, como a de uma instituição financeira ou rede social, com o objetivo de fazer com que o usuário insira suas credenciais de acesso, que acabam sendo capturadas pelos golpistas. Essa técnica é frequentemente utilizada em esquemas de phishing, nos quais os usuários são levados à página clonada por meio de links enganosos enviados via e-mail ou mensagens instantâneas (Hider; Shabir, 2024).

Ambas as técnicas exploram o comportamento humano, porém diferem em seus mecanismos. Enquanto a engenharia social depende da interação direta entre o atacante e a vítima para manipular psicologicamente a situação, a clonagem de página atua de forma mais passiva, induzindo a vítima a acreditar que está acessando um site legítimo. Embora o objetivo em ambas seja obter informações sensíveis, a primeira técnica se baseia na persuasão e confiança, enquanto a segunda depende da dissimulação técnica, criando uma falsa sensação de segurança no ambiente digital.

Alguns testes podem ser realizados para obter resultados que possam indicar riscos potenciais para os usuários dessas instituições. Dentre eles destacam-se dois, sendo o Testes de rede: Esses testes são realizados para avaliar a segurança da informação a partir da busca de

vulnerabilidades de interconexão e outros aspectos softwares desses bancos, que podem abrir os caminhos para outros golpes. Eles podem incluir a verificação de vulnerabilidades que podem ser exploradas por invasores. Clonagem de páginas: Este método envolve a criação de uma cópia de uma página da web do site que cada instituição com o objetivo de identificar possíveis falhas de segurança. Isso pode ajudar a entender como os golpistas podem criar páginas falsas para enganar os usuários. A finalidade desses métodos é obter resultados que possam indicar riscos potenciais para os usuários dessas instituições. Especificamente, a pesquisa está interessada em identificar possíveis golpes que podem ser realizados usando páginas da web falsas. Esses golpes podem comprometer a segurança dos usuários, levando a perdas financeiras ou ao roubo de informações pessoais.

Devido a esta inovação tecnológica, é crucial ressaltar a importância de realizar testes de segurança para assegurar uma experiência de uso mais eficiente para os usuários. Visto que atualmente os usuários buscam a praticidade e preferem utilizar os serviços digitais ao ter que se deslocar ao prédio físico dos bancos. Contudo, para apoiar essas análises, as seções seguintes apresentam: metodologias de meios para análise *e-bankings* bem como algumas considerações finais e conclusões.

Como mencionados na seção anterior o phishing e o pharming são alguns dos possíveis golpes que podem a vir ser utilizados por cibercriminosos. phishing: é um tipo de ataque em que criminosos tentam enganar para que forneçam informações pessoais ou financeiras, como senhas, números de cartão de crédito ou dados bancários. pharming: é um ataque em que criminosos redireciona o tráfego da web de um site legítimo para um falso. é feito através da manipulação do sistema de nomes de domínio (DNS).

3 METODOLOGIA

O intuito dessa pesquisa, buscou analisar a segurança da informação (SI) nas principais páginas eletrônicas das instituições financeiras do Brasil, na qual, apresentaram algumas informações que em mãos erradas, podem ser utilizadas para aplicação de golpes.

De acordo com Appolinário (2011), este estudo é classificado como aplicado, pois realizou testes diretos para avaliar os níveis de segurança. Em termos de profundidade, é descritivo, pois inicialmente identificou materiais já publicados e também pode ser considerado experimental, uma vez que procura explicar a razão por trás de um determinado fenômeno, manipulando conscientemente algum aspecto da realidade. Isso envolveu uma série de testes ao longo de uma semana para comparação dos dados coletados.

Contudo, ela utiliza também a metodologia apresentada por Marconi e Lakatos (2017) na qual foi definida como qualiquantitativa, pois a mesma versa a análise da segurança dos bancos, em se enquadra na qualitativa e em termos de análises de segurança dos sistemas web, ela também aborda e apresenta dados das páginas eletrônicas, onde eles foram analisados.

Foi preciso listar as funcionalidades a serem levadas em conta nas análises das aplicações, devido à possibilidade de clonagem das páginas e à conexão dessas funções com os servidores das páginas eletrônicas clonadas. Assim, foram elencadas as funções comuns presentes nos serviços mencionados, como mostrado no quadro 1.

Quadro 1: Funções e Objetivos

ID	Funções	**Objetivo**
01	Pagamentos	Realizar pagamentos por meio do Internet Banking
02	Transferências	Realizar a movimentação bancária sendo ela por pix ou não
03	Empréstimos	Pegar um valor antecipado ao banco tendo em vista o ressarcimento através do valor e de juros
04	Investimentos	Funcionalidade de investimento em cripto moeda ou ações
05	Dados dos Cartões	Informações pertinentes aos dados
05	Consulta de Saldo e Extrato	Informa valores armazenados na conta e movimentações realizadas
06	Fatura	Amostra de todos os gastos que estão acometidos no presente mês.
07	Controle Total de Limite	Ação que possibilita controlar o valor disponível de compra nos cartões.
08	Recarga de Celular	Realiza recargas para quaisquer operadoras e número de celular
09	Bloqueio/ Desbloqueio	Verificar a possibilidade de bloqueio e desbloqueio dos cartões (virtual ou físico)
10	Renegociação de Dívidas	Permite renegociar dívidas, sejam de faturas atrasadas ou de empréstimos não pagos.
11	Atendimento ao Cliente	Atendimento com operadores do banco através de um chat

Fonte: Pesquisa direta

As funções descritas no quadro 1 foram avaliadas em cada um dos sistemas web das instituições financeiras que compõem os focos de análise deste estudo, com o intuito de verificar a presença destas funções em seus sites.

Essa pesquisa se deu com a coleta de dados através de testes realizados nas plataformas webs dos bancos digitais, não contemplou seus aplicativos móveis. Contudo, vale ressaltar que a escolha pela utilização de suas páginas eletrônicas se dá ainda pela facilidade de erros e falhas que muitas vezes passam despercebidas pelas empresas, fazendo assim com que também possam apresentar problemas futuros para seus respectivos apps.

As instituições financeiras escolhidas para o presente trabalho foram: Banco do Brasil, Caixa Econômica, Banco Santander e Itaú. Elas foram escolhidas com o critério de serem bancos que tiveram que se adaptar ao digital ao decorrer dos anos.

Portanto, para toda coleta de dados que serão apresentados na seção seguinte, foram utilizadas algumas ferramentas para os testes nas plataformas, como também, comandos para que pudessem ser colhidas todas as informações. Os comandos redes utilizados foram listados no quadro 2:

Quadro 2: Comandos de redes utilizados

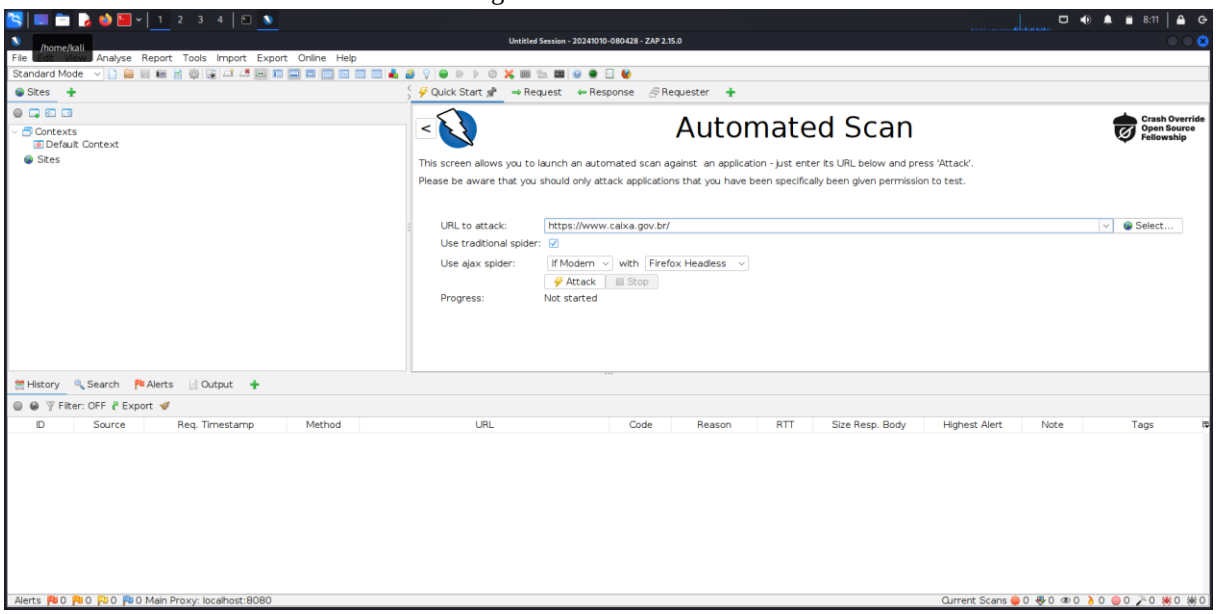
Comando	**Objetivo**
Ping	Testar a disponibilidade dos sistemas, através do CMD para que possa descobrir se a mesma responde corretamente com ‘Ms’, milissegundos avaliar possíveis perdas de pacotes e o número máximo de roteadores pelos quais o pacote pode trafegar através do *Time To Live* (TTL).
Traceroute	Analisar a quantidade de saltos que a requisição correu para chegar ao destino. Desde a saída (Computador local) e chegada (servidor da requisição)

Fonte: Pesquisa direta

A ferramenta utilizada para o procedimento da pesquisa foi o terminal do Kali Linux, para a execução do comando tracert e o ping seja realizado. Para os testes de vulnerabilidade e clonagem da página inicial de cada banco utilizou-se respectivamente o Zed Attack Proxy (ZAP) e Setoolkit do Kali Linux, pois os mesmos dispuseram de comandos para que pudessem ser efetivadas o teste de vulnerabilidade e clonagem.

Depois de iniciar o ZAP e selecionar o modo automático clicando em “Automated Scan” é necessário inserir a URL da instituição financeira que será testada no campo “URL to attack” e depois clicar no botão ataque, como podemos ver na figura 01.

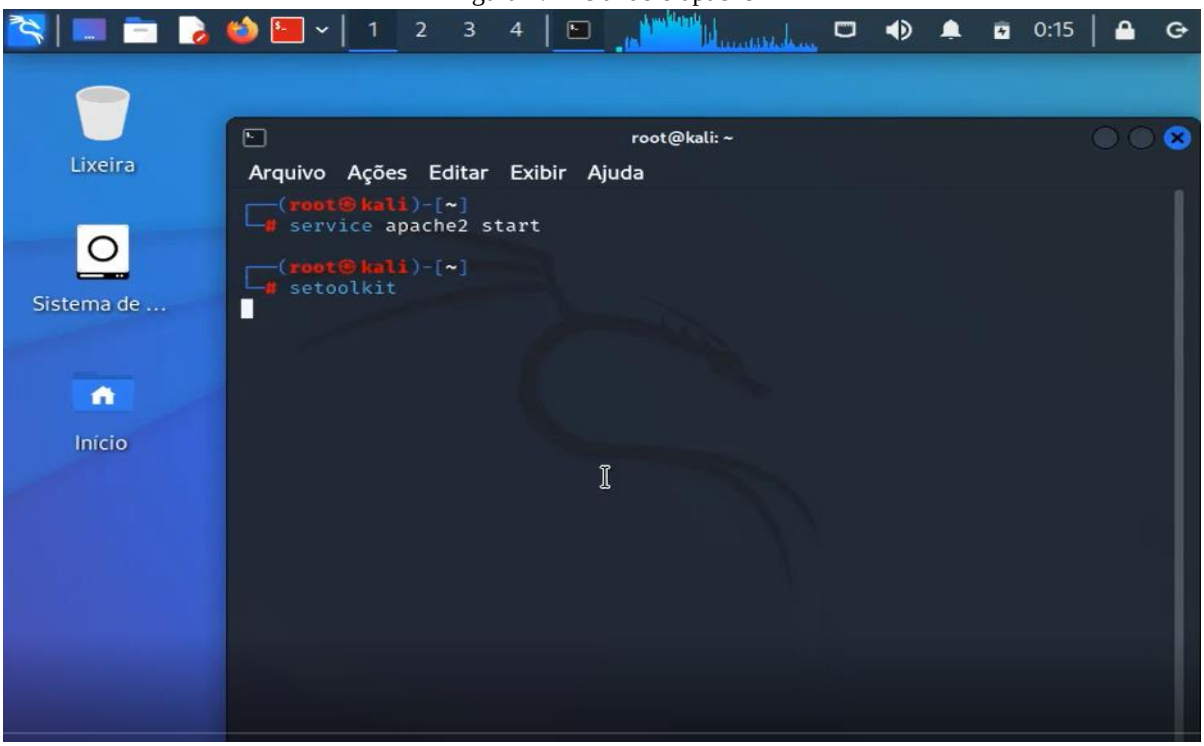
Figura 1: Iniciando o ZAP



Fonte: Pesquisa direta

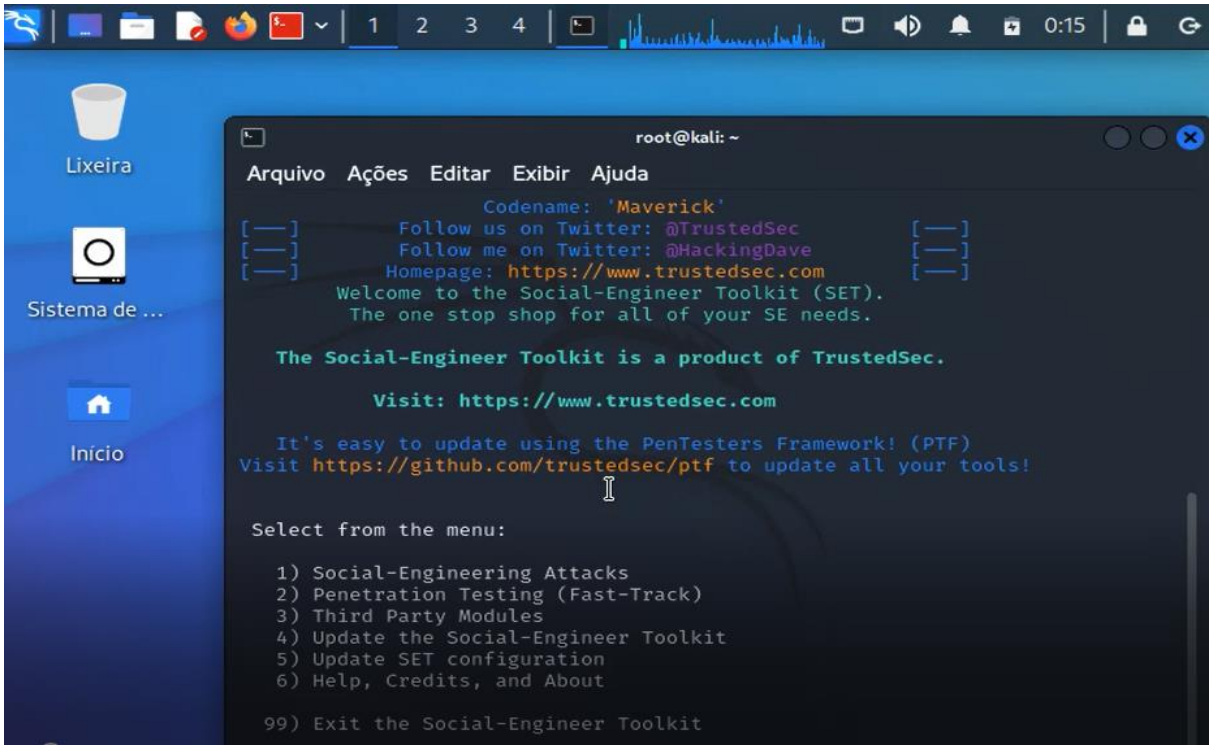
Com a ferramenta setoolkit, foram executados alguns comandos para a clonagem da página. Primeiramente, o comando apache2 start foi inicializado para que o apache pudesse ser ativado e em seguida iniciando a ferramenta setoolkit, como mostra na figura 2 e 3.

Figura 2: Iniciando o apache



Fonte: Pesquisa direta

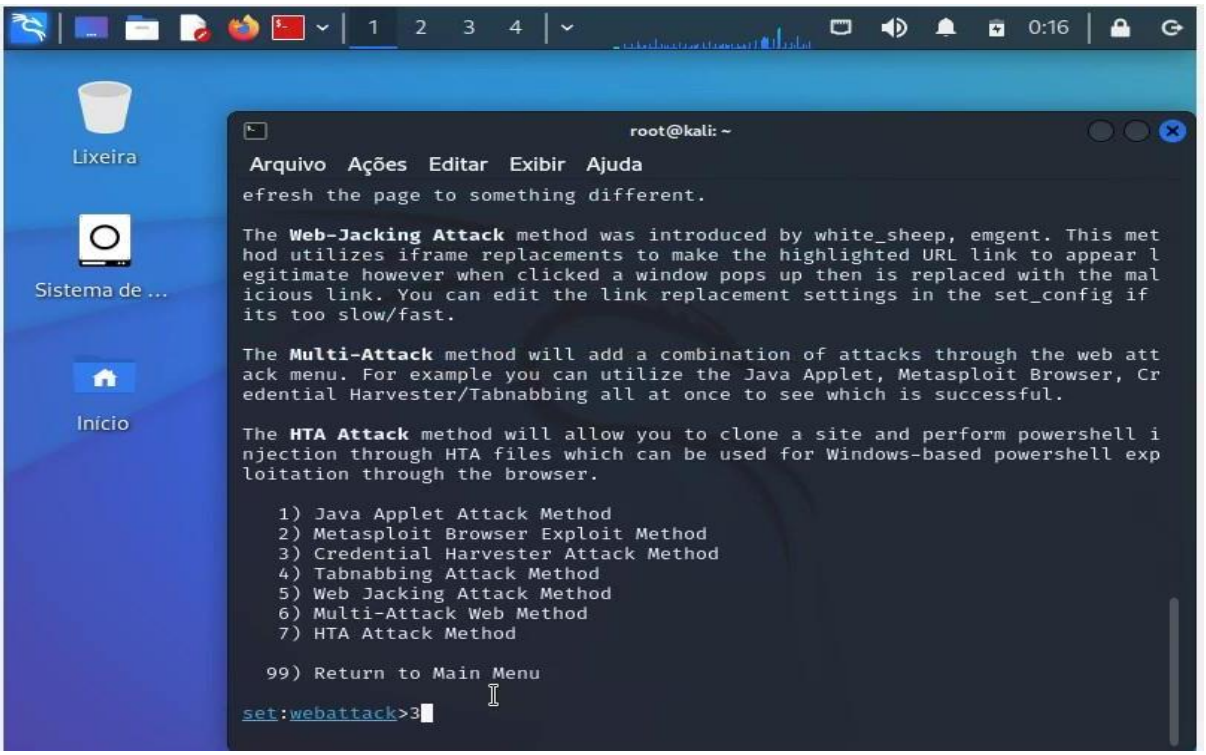
Figura 3: Inicialização do Setoolkit



Fonte: Pesquisa direta

Assim a ferramenta apresentou várias informações que a mesma dispõe, contudo, a escolhida foi a opção 1, Social-Engineering Attacks onde a mesma apresenta outra lista de opções, como mostra a figura 4.

Figura 4: Escolha das opções para clonagem

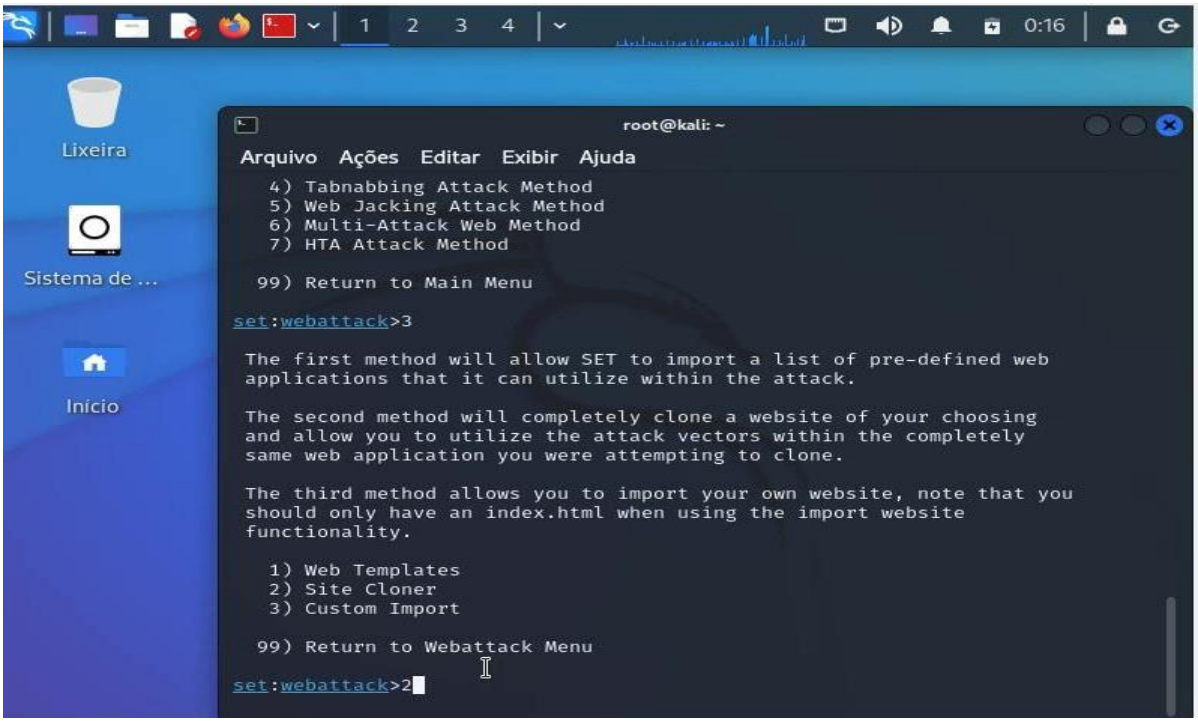


Fonte: Pesquisa direta

Com a opção 1 escolhida, a ferramenta habilita novas informações para os próximos passos, como mostra a figura 4 e com isso a opção na qual encaixa para a clonagem, escolheu-se a 3) Credential Harvester Attack Method. Na qual, tem a opção de criar um método de ataque para clonar a página, em outras palavras, o mesmo irá usar esse sistema para tentar buscar informações na página que contenham credenciais ou logins e senhas dos clientes.

Com a escolha da opção 3, ela apresenta novas informações para realizar a clonagem, portanto, para a realizar a clonagem na próxima opção, precisou-se que fosse escolhida a opção 2, na qual denomina como Site Cloner, ou seja, onde de fato o site seria clonado, como mostra a figura 5.

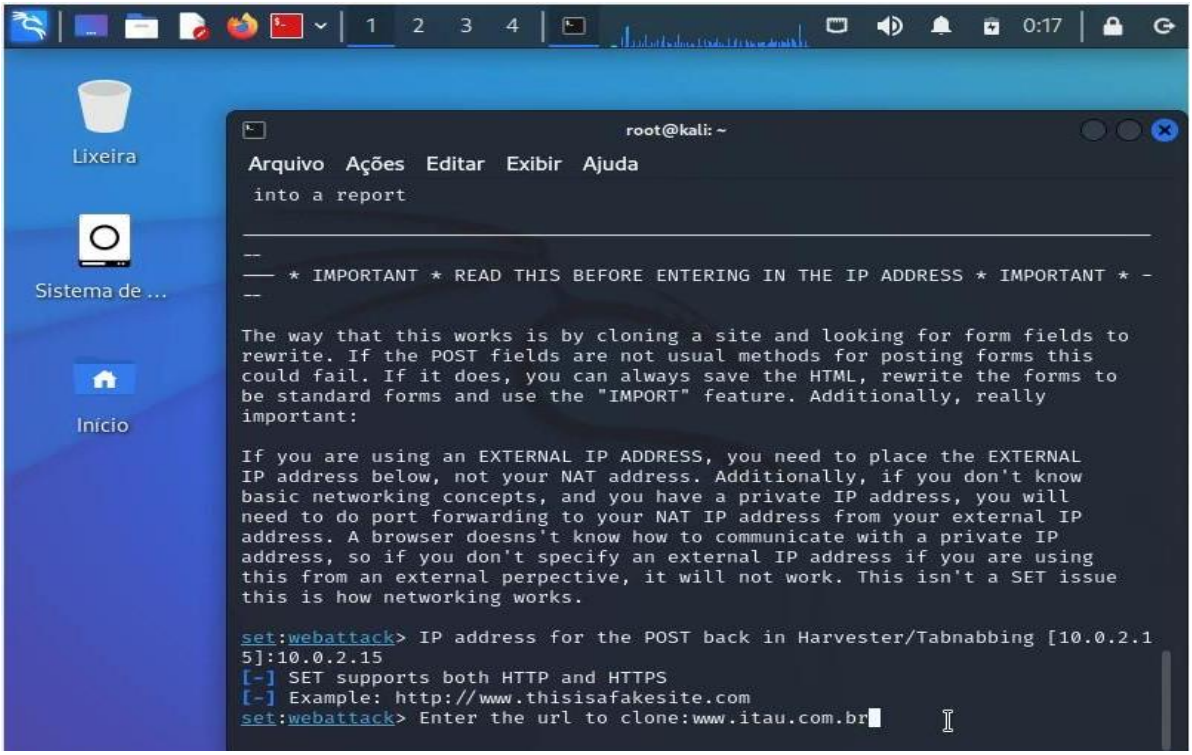
Figura 5: Escolha do comando para clonagem da página



Fonte: Pesquisa direta

Com a opção selecionada, a ferramenta pede mais informações detalhadas para a realização da clonagem, onde a mesma solicita a URL que será realizado a clonagem. A figura 6, exemplifica como realizou-se a requisição.

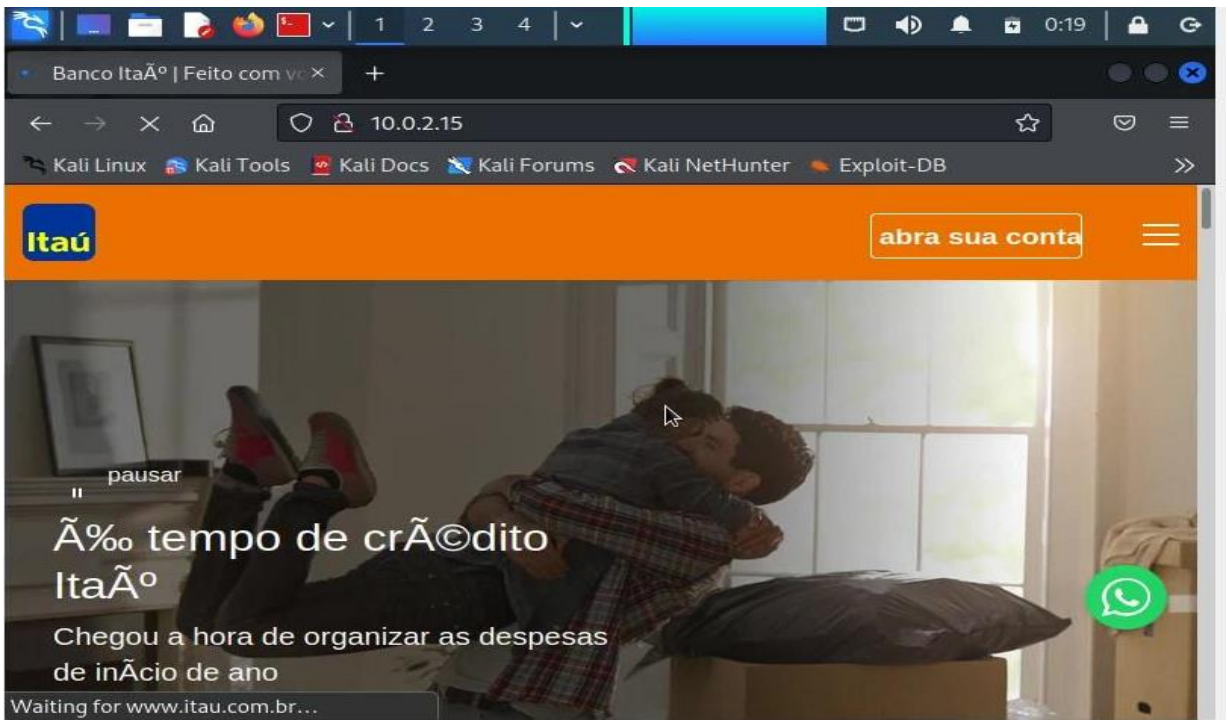
Figura 6: Inserindo URL para clonagem



Fonte: Pesquisa direta

Portanto, no determinado momento em que acontece com êxito sua clonagem, o site disponibiliza um IP local para analisar o site e suas informações da cópia, como mostra a figura 7 do site do Itaú.

Figura 7: Página do Itaú clonada



Fonte: Pesquisa direta

Assim, com todas as ferramentas e comandos selecionados para as análises, determinou-se que todas as principais páginas dos bancos seriam testadas no período de 5 úteis, para que a coleta de dados ocorresse de forma minuciosa e que pudessem ser encontradas oscilações de cada uma ao decorrer dos dias, possíveis latências e erros que poderiam ser descobertos.

Na seção seguinte, mostra-se como desenvolveu-se todo o estudo, informações, como foi testado todas as instituições, possíveis informações de segurança que foram coletadas e demais que serviram de dados para essa pesquisa.

4 RESULTADOS E DISCUSSÕES

Com base nas análises feitas nas atuais variáveis, foi viável obter informações relevantes e explicativas sobre as funcionalidades oferecidas pelos bancos digitais. Onde, após o login nos sites, foi observado a disponibilidade de algumas funções e serviços, descrito no Quadro 3.

Quadro 3: Variáveis Analisadas

Funções	**Dispositivo**	**Banco do Brasil**	**Caixa Econômica**	**Santander**	**Itaú**
Pagamentos	Browser	x	x	x	x
Transferências	Browser	x	x	x	x
Empréstimos	Browser	x	x	x	x
Investimentos	Browser	x	x	x	x
Consulta de Saldo e Extrato	Browser	x	x	x	x
Fatura	Browser	x	x	x	x
Controle Total de Limite	Browser	x	x	x	x
Recarga de Celular	Browser		x		x
Bloqueio/ Desbloqueio	Browser	x	x	x	x
Renegociação de Dívidas	Browser		x	x	
Atendimento ao Cliente	Browser	x	x	x	x

Fonte: Pesquisa Direta

No quadro 3, é possível observar de maneira clara e detalhada as funções de cada banco,

sendo perceptível em algumas das instituições financeiras possui funções específicas como a renegociação de dívidas e recarga de celular.

Como mencionado anteriormente, os testes em todos bancos digitais, foram feitos através de ferramentas disponíveis do Kali Linux, assim, foram testadas o ping, tracert, vulnerabilidade e a clonagem das páginas. Contudo, foi possível encontrar vários dados relevantes de cada uma. Como dados de cada pacote, tempo que o mesmo levou ao decorrer dos dias e outras informações.

Com o ping e tracert, recolheu e analisou dados de cada uma no decorrer 5 dias da semana e com horários diferentes, onde foi possível descrever como cada sistema disponibiliza as informações. Portanto, foi possível realizar uma média de cada tempo e saltos ao decorrer dos dias.

Quadro 4: Média das informações dos bancos

Bancos	**Tipo de IP**	**Tempo médio cada pacote - Ping em milissegundos (Ms)**	**Quantidade média de pulos (Tracert)**	**Método de teste**
Banco do Brasil	Estático	Não foi possível medir	14	Terminal do Kali
Caixa Econômica	Dinâmico	13	5	Terminal do Kali
Banco Santander	Dinâmico	46	9,5	Terminal do Kali
Itaú	Dinâmico	16	7	Terminal do Kali

Fonte: Pesquisa direta

Testes realizados ao longo dos dias mostram como cada uma contém um tempo de resposta diferente das demais, como por exemplo o Banco Santander, que possui uma média maior de tempo, enquanto as demais variam em uma média de 13 a 16 milissegundos (Ms). Assim, o comando tracert apresenta uma média de cada salto que cada pacote percorreu para chegar ao seu destino, onde, a instituição caixa econômica, teve a menor média de saltos e as demais, variaram de 7 a 14.

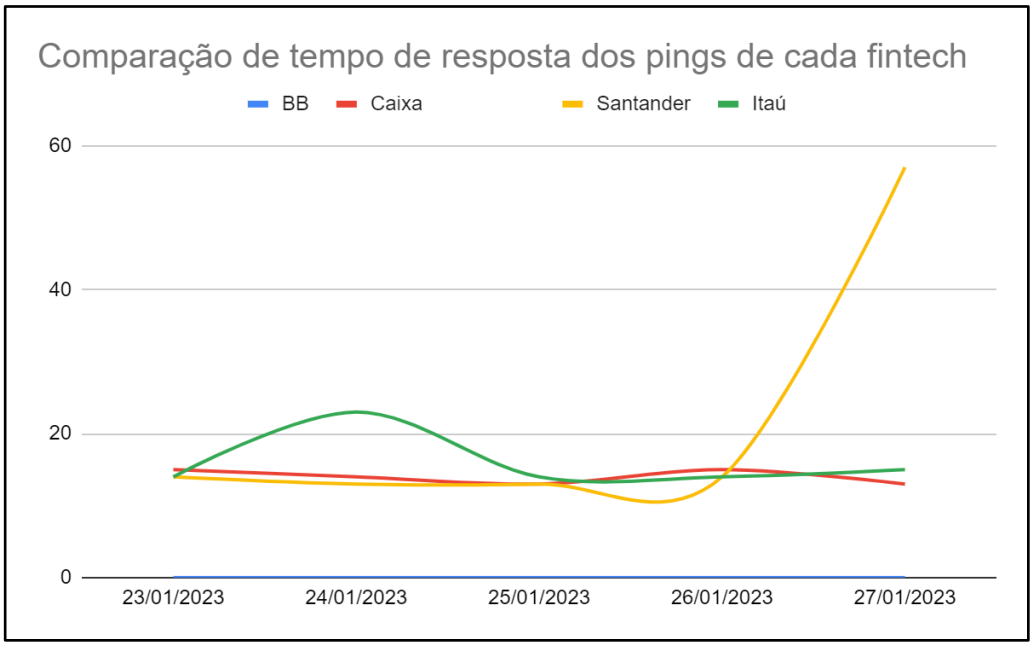
O Banco do Brasil, caracterizou-se como o que não obteve resposta quando solicitado o comando ping, sempre que realizado a solicitação, o mesmo apresentava “tempo esgotado”. Algumas causas podem ser levadas em consideração, como por exemplo, o servidor estava com várias demandas no decorrer do horário, ou até mesmo, que ele não aceita esse comando seja requisitado ao seu site. Contudo, seu IP não mudou ao decorrer dos dias, o mesmo se manteve presente com o IP fixo, desde o início dos testes, lavando a concluir que é uma falha grande de

segurança, pois o mesmo poderia sofrer ataques ao servidor e o mesmo vir a cair. Diferentemente dos demais bancos, onde, os mesmos permaneceram realizando a troca de seu IP ao decorrer dos dias, em média, no terceiro dia de teste, eles eram substituídos. Concluindo assim uma boa estratégia para fugir dos ataques no servidor.

Em testes semelhantes, realizados por Neto Junior (2022), onde o mesmo realizou teste através das ferramentas wireshark em dois sistemas operacionais distintos o Kali Linux e o Windows 10 e durante os testes mostrou que os IPs dos bancos digitais testados eram dinâmicos, levando a concluir que IPs estáticos podem sofrer ataques mais facilmente.

Ao decorrer dos dias, cada banco apresentou uma média em milissegundos de cada ping, diferente das demais, como mostra no gráfico 1.

Gráfico 1: Média do comando ping em milissegundos de cada banco



Fonte: Pesquisa direta

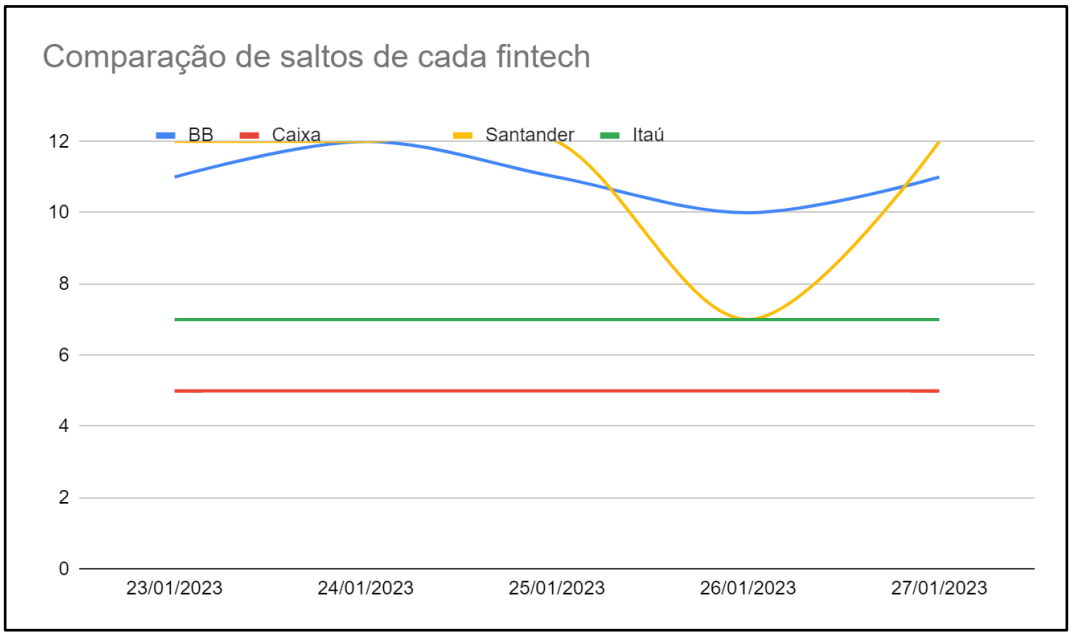
Observando o gráfico 1, nota-se que no dia 23/01, em uma segunda-feira, todos permaneceram respondendo bem às solicitações do ping, sem um tempo relativamente maior, com exceção do Banco do Brasil, que não retornou nenhum dado e Banco Itaú, no qual teve um pico maior na sua média. Esse pico pode ser devido às solicitações que o mesmo estava sendo requisitado, por ser início de semana.

No dia 26/01 nota-se que o Santander, respondeu com uma média bastante alta na solicitação. Contudo, o pacote demorou para voltar, mostrando que o banco estava com um pico alto de requisições. Essa demora de respostas pode entender-se que caso seja requisitado uma

tarefa neste dia, o usuário certamente poderia por uma certa demora ao solicitar o banco.

Dados levantados como o comando tracert, mostrou-se que além dos pings com um tempo médio relativamente alto por algumas solicitações da página principal, tiveram uma quantidade maior de saltos para que o pacote chegasse ao seu destino. Como mostra o gráfico 2, onde o banco Santander, teve uma quantidade maior.

Gráfico 2: Média de saltos de cada banco



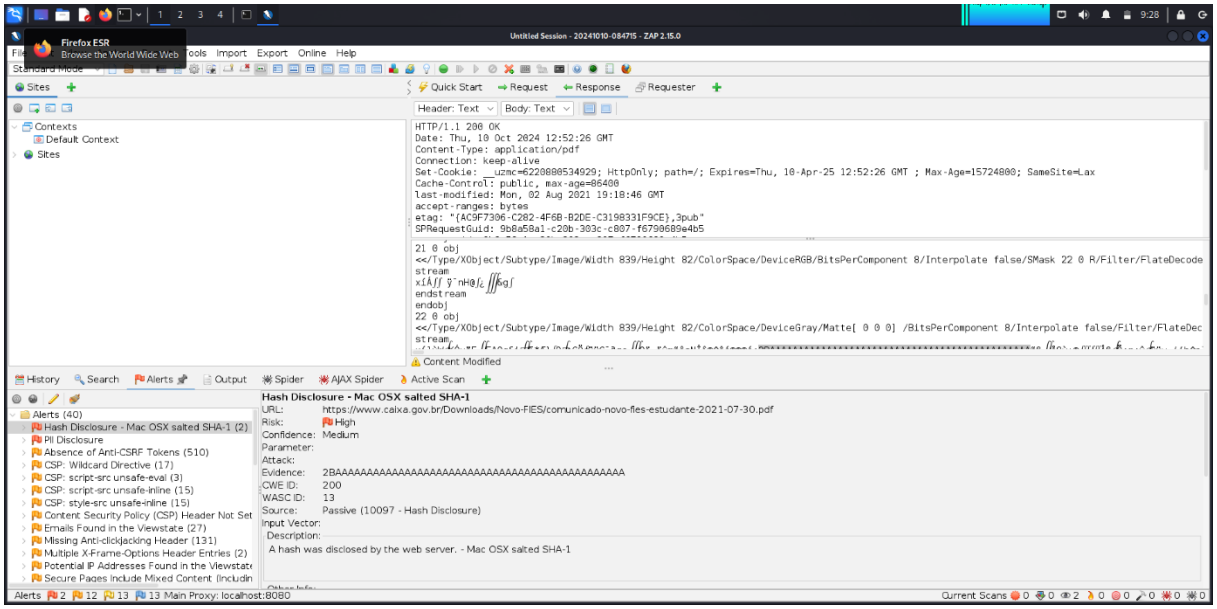
Fonte: Pesquisa direta

Entre os dias 25/01 a 27/01 o banco Santander teve um pico maior de saltos para que o pacote chegasse ao seu destino. Este mesmo dado pôde ser observado quando a requisição do ping foi executada, mostrando assim que entre esses dias o servidor se manteve bastante solicitado. Como mostra, foram 3 dias de oscilações, podendo levar um certo atraso na utilização deste banco.

Contudo, o Banco do Brasil, assim como o ping, o mesmo não pôde ser contado sua quantidade exata de saltos, pois o mesmo, ao realizar o comando com 10 a 12 saltos, informava que: “Esgotado tempo limite do pedido!”. O pacote se perdia ao longo dos saltos, fazendo assim que a mesma não permitisse a chegada deste comando.

No teste de vulnerabilidade realizado no ZAP, após dar o comando de ataque na URL da Caixa Econômica foram obtidos 40 aletas, sendo 2 de alto risco (vermelho) ,12 de médio (laranja), 13 de baixo risco (amarelo) e 13 avisos (azul), conforme figura 8.

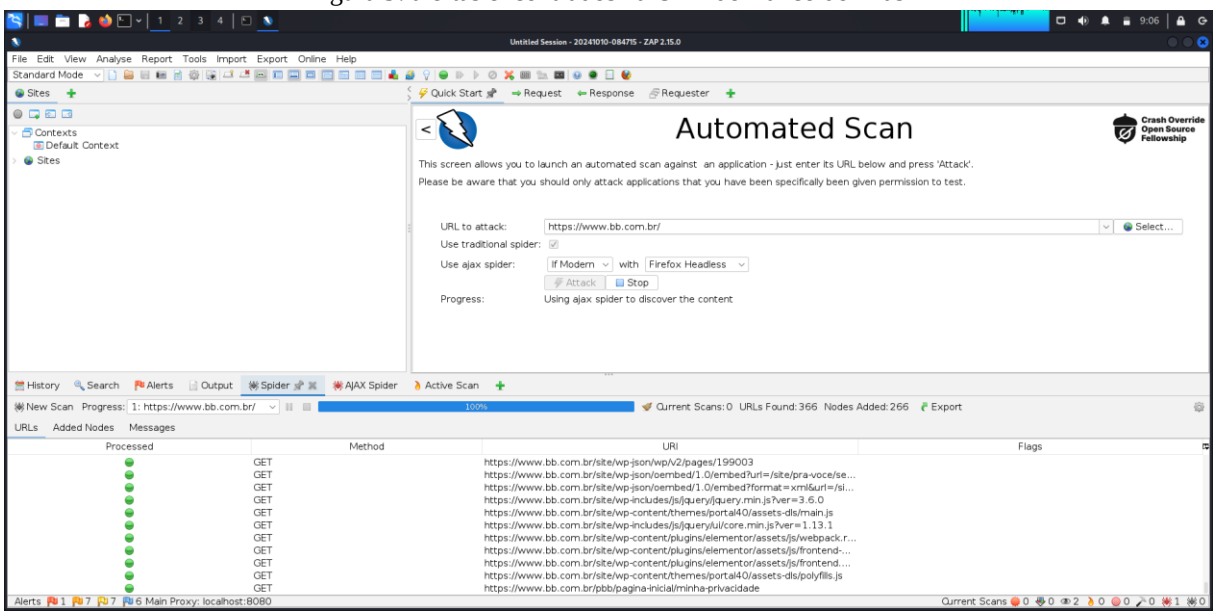
Figura 8: alertas encontrados na URL da Caixa Econômica



Fonte: Pesquisa direta

Para a instituição do Banco do Brasil, após os scan foi constatado 21 alertas, sendo 1 de alto risco, 7 de risco médio. 7 de risco baixo e 6 avisos, conforme a figura 9.

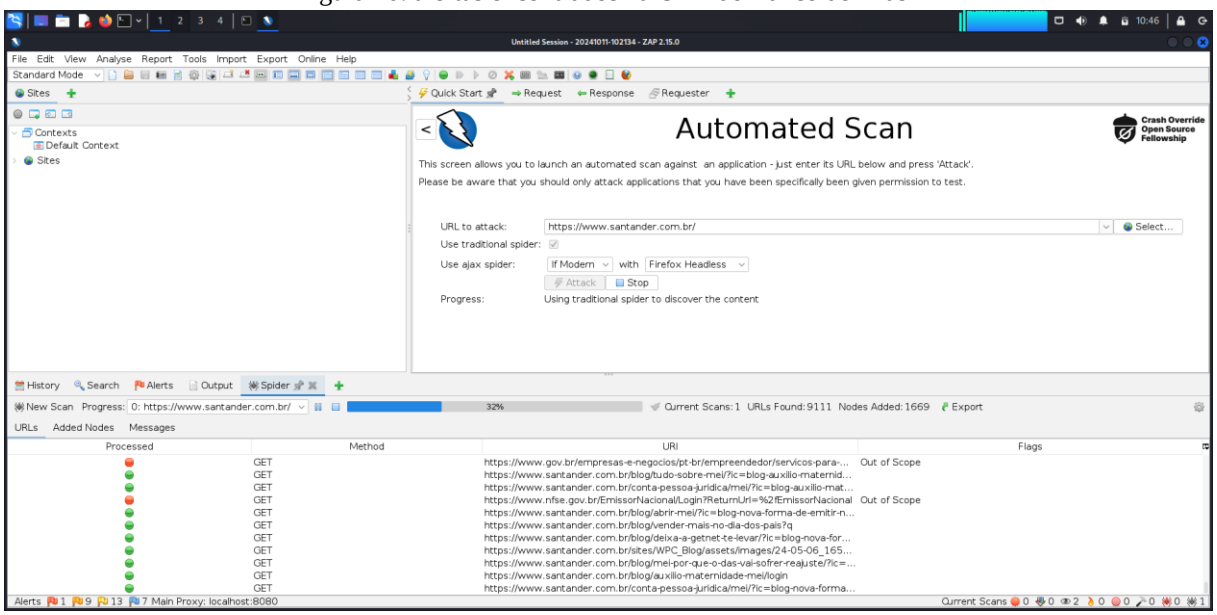
Figura 9: alertas encontrados na URL do Banco do Brasil



Fonte: Pesquisa direta

Para o banco Santander após o scan, foi descrito 30 alertas, sendo 1 de alto risco, 9 de risco médio, 13 de risco baixo e 7 avisos, conforme figura 10.

Figura 10: alertas encontrados na URL do Banco do Brasil

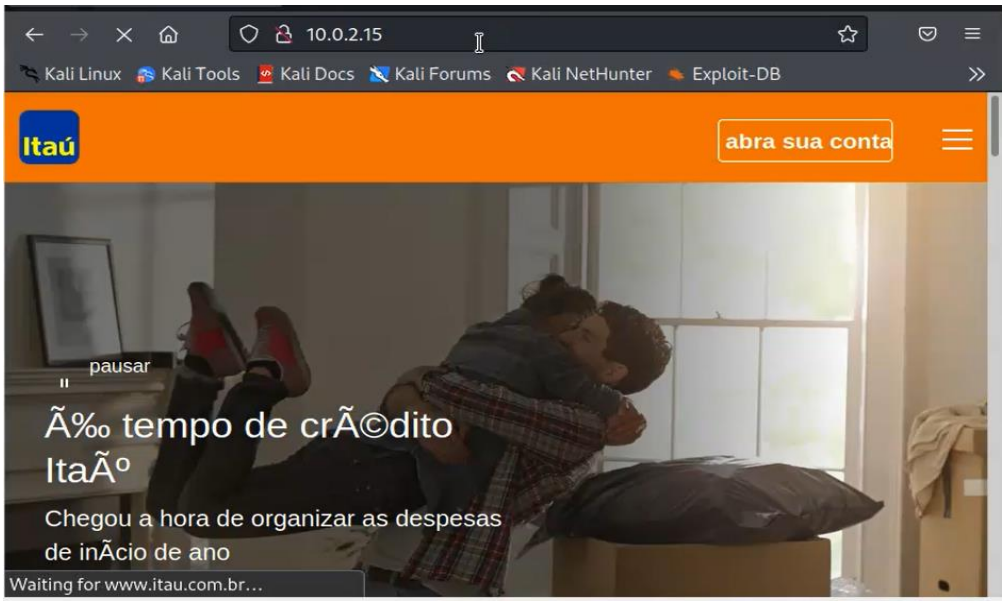


Fonte: Pesquisa direta

Não foi possível realizar o Scan do ZAP na URL do Banco Itaú, devido a presença de um erro desconhecido na realização do SCAN.

Nas clonagens das páginas observou-se alguns aspectos pertinentes, como o banco do Itaú, apresentou sua página sem sua formatação da página verdadeira, seus ícones, por exemplo, não foram atualizados na página falsa, levando assim um grau de dificuldade maior ao criarem um *phishing* de seu site.

Figura 11: Página do Banco Itaú clonada



Fonte: Pesquisa direta

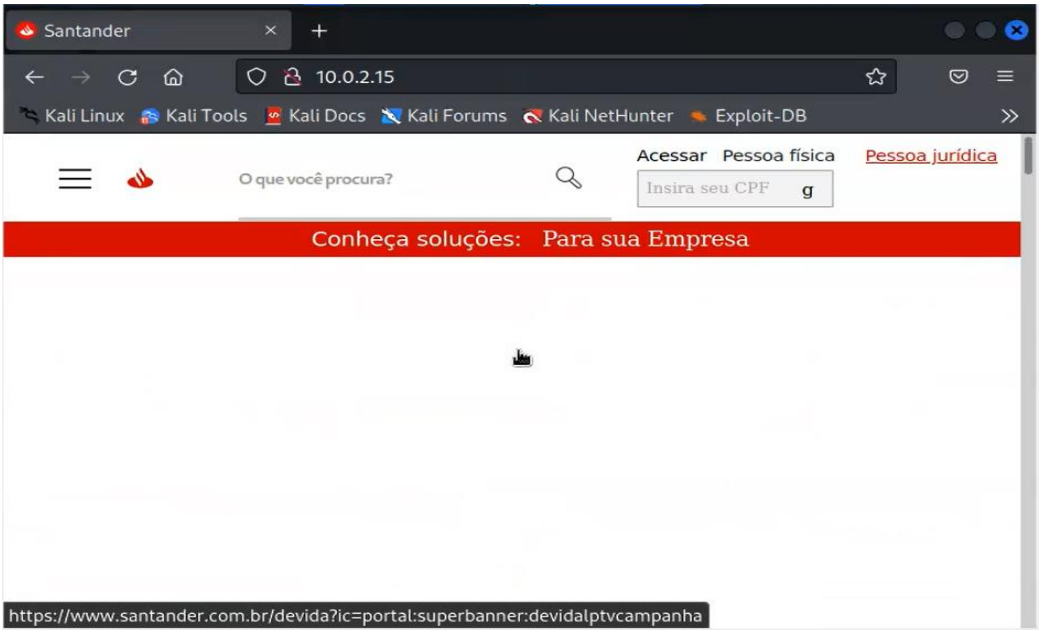
A instituição financeira Caixa Econômica, permitiu sua cópia da página, contudo, sua página inicial permanece idêntica a original, porém, quando é realizada a ação de clique sobre seus botões na lateral, a mesma não responde corretamente, apenas dispõe uma página em branco.

Figura 12: Página da Caixa Econômica clonada

Fonte: Pesquisa direta

Assim, o banco Santander, mostrou-se com uma particularidade diferente das demais, pois a mesma ao ser clonada, não enviou juntamente com a página, suas imagens do site oficial, apenas textos, botões e links que foram adicionados a página falsa.

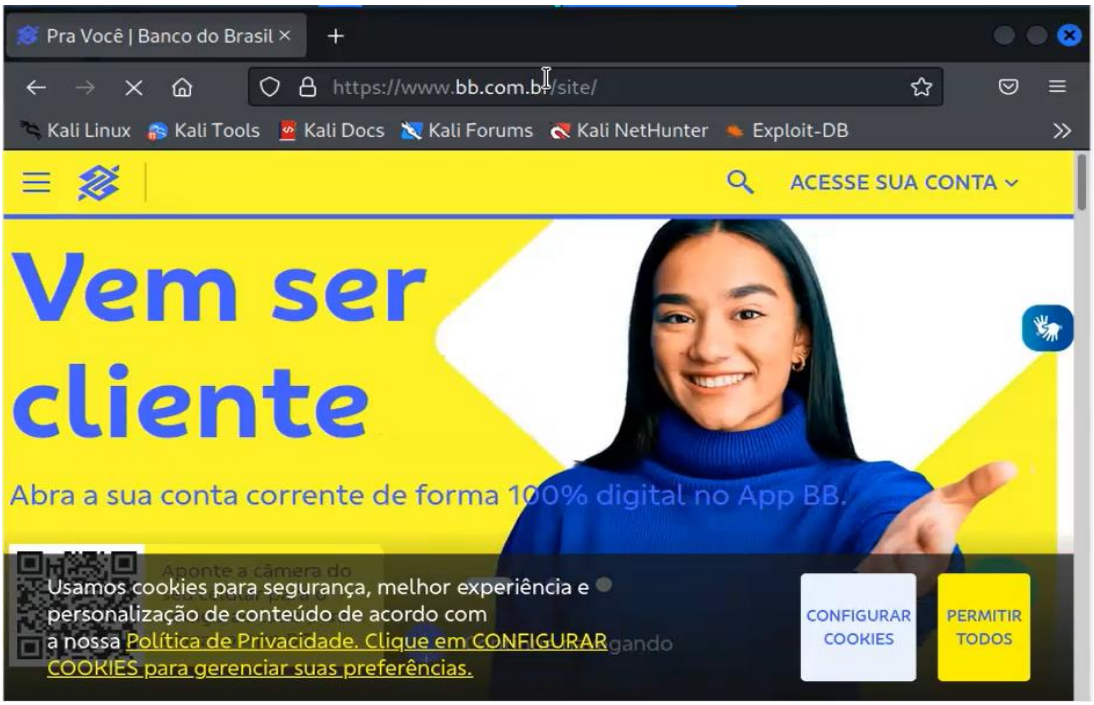
Figura 13: Página do Banco Santander clonada



Fonte: Pesquisa direta

O Banco do Brasil, ao realizar o teste com a ferramenta, não permitiu ser clonado. O mesmo quando o IP foi gerado e acessado no browser, sempre redireciona para a página oficial do Banco do Brasil, o que podemos considerar um site seguro e confiável, pois para realizar um site falso, seria precisa que o hacker, inicia-se na criação do mesmo sem utilizar elementos originais dele, fazendo assim que não saísse igual e que pudesse ser facilmente reconhecido.

Figura 14: Página do Banco do Brasil



Fonte: Pesquisa direta

Portanto, pode-se trazer algumas conclusões em relação a cada página eletrônica clonada, onde usuários dos respectivos bancos podem ser facilmente vítimas de golpes, como phishing. Contudo, apresentando algumas considerações sobre elas, enfatiza-se que todas contém um certo erro quando sua cópia foi realizada, contudo, o Banco do Brasil, é o único seguro em relação a todas elas, pois o mesmo, diante de teste de ping, tracert e clonagem, sempre apresentou dificuldades para a realização com erros, que poderiam ser consideradas como: “Erros de segurança” fazendo assim que as informações se tornem seguras.

Assim, das 3 que foram clonadas, observa-se que elas não trazem consigo informações de segurança que são relevantes aos usuários, como certificados digitais, cadeado na barra de pesquisa e selos de segurança.

5 CONSIDERAÇÕES FINAIS

A pesquisa teve como objetivo, realizar um estudo na área de redes de computadores com quatro instituições financeiras do brasil, explanando assim diversas informações de segurança da informação que as mesmas podem apresentar em suas páginas webs, onde levantou-se dados que podem ser utilizados para melhorias em suas informações. Apresentou dados importantes em quesitos as suas informações, como também erros que possivelmente podem vir a ser usados por pessoas má intencionadas.

Analisando mais detalhadamente os resultados, é importante destacar que os comandos de traceroute e ping foram executados com sucesso em todas as entidades. No teste de vulnerabilidade realizado pelo ZAP, O banco do Brasil teve destaque pois entre as instituições foi a que menos apresentou alertas, sendo um ponto positivo para a segurança da instituição. No entanto, o teste de clonagem de páginas apresentou desafios. Em todas as instituições, a clonagem não foi concluída corretamente, resultando em páginas com erros, fontes desalinhadas e outros problemas. Notavelmente, o Banco do Brasil se destacou, pois sua página não pôde ser clonada, indicando um nível superior de segurança.

Todos os resultados obtidos, poderão ser utilizados para pesquisas futuras, podendo assim ser aplicados os mesmos comandos e assim possa fazer um comparativo com os resultados aqui adquiridos, propondo melhorias. Assim, este trabalho pode ser expandido futuramente para a testagem com novos comandos, aplicação dos mesmos em mais dias da semana, como também seus respectivos aplicativos móveis, levantamento de dados com vários horários diferentes na testagem e análises mais a fundo nos códigos fontes de cada instituição ao realizar a clonagem.

REFERÊNCIAS

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

BISSO, Rodrigo; KREUTZ, Diego. Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteção de Dados. Disponível em: <https://sol.sbc.org.br/index.php/errc/article/view/9230/9133.> Acesso em: 21 out. 2022.

CAMARGO, Luiz Felipe de; REIS, Carlos; PAIOLA, Pedro Henrique; PAPA, João Paulo; BREGA, José Remo F.; COSTA, Kelton A. P. da. Voltar aos Detalhes do Artigo Métodos de Aprendizado de Máquina Adversariais na Detecção de Anomalias em Redes de Computadores. Disponível em: <https://sol.sbc.org.br/index.php/sbseg/article/view/17314.> Acesso em: 18 out. 2022.

COMARELA, Giovanni; FRANCO, Gabriel. Introdução à Ciência de Dados: Uma Visão Pragmática utilizando Python, Aplicações e Oportunidades em Redes de Computadores. XXXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos-SBRC,Disponível em: <https://sol.sbc.org.br/livros/index.php/sbc/catalog/download/65/289/538-1?inline=1.> Acesso em: 21 out. 2022.

HADNAGY. Christopher .Social Engineering: The Art of Human Hacking. New York: John Wiley & Sons, 2010

HIDER, B.; SHABIR, Ghulam. Cybersecurity Threats and Mitigation Strategies in the Digital Age: A Comprehensive Overview. 2024.

LACERDA, Matheus Soares de. Segurança de Dados em Nuvem através de Aprendizado de Máquina: uma Revisão Sistemática da Literatura. Sistemas de Informação. Disponível em: <https://sol.sbc.org.br/index.php/sbsi_estendido/article/view/13140/12993.> Acesso em: 21 out. 2022.

MARCONI, M.; LAKATOS, E. Fundamentos de metodologia científica. 8. ed. São Paulo, Brasil: Ed. Atlas, 2017. ISBN: 9788597010664.

MENDES , JOYCE DE ANDRADE. UMA ABORDAGEM SOBRE A SEGURANÇA DA INFORMAÇÃO NO MUNDO ATUAL. 2021. Monografia (Bacharel) - NS, [*S. l.*], 2021. Disponível em: <https://bdm.ufpa.br:8443/bitstream/prefix/4401/1/TCC_AbordagemSegurancaInformacao.pdf>. Acesso em: 4 fev. 2023.

NETO JÚNIOR, Fábio Demétrio. Análise de segurança dos sistemas web de Fintechs brasileiras. 2022.

SILVA, B. R. S. UMA ANÁLISE COMPARATIVA DE TÉCNICAS DE SUBAMOSTRAGEM PARA PROJETOS DE SISTEMAS DE DETECÇÃO DE INTRUSÃO EM REDES DE COMPUTADORES. Disponível em: <https://repositorio.ufc.br/bitstream/riufc/52808/5/2020_dis_brssilva.pdf.> Acesso em: 21 out. 2022.

WEIDMAN, G. Testes de Invasão. São Paulo: 1º Ed. Novatec, 2014.