Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

# EXPLORANDO A ENGENHARIA SOCIAL COM O SOCIAL ENGINEER TOOLKIT (SET)

# EXPLORING SOCIAL ENGINEERING WITH SOCIAL ENGINEERING TOOLKIT (SET)

Cristiane Aparecida Cavalcante Sales, Faculdade de Tecnologia de Americana (FATEC), cristiane.sales01@fatec.sp.gov.br
Ionara Helena Ferraz, Faculdade de Tecnologia de Americana (FATEC), ionara.ferraz@fatec.sp.gov.br
Henri Alves de Godoy, Faculdade de Tecnologia de Americana (FATEC), henri.godoy@fatec.sp.gov.br

**Resumo**

O objetivo deste trabalho é explorar um tema de extrema importância atualmente: a Engenharia Social e o *Phishing*. Hoje em dia, a recorrência desta prática se torna uma ameaça significativa para a segurança da informação e à segurança cibernética. Neste contexto, examinou-se como a Engenharia Social, em conjunto com o *phishing*, podem enganar suas vítimas, obtendo informações confidenciais, utilizando técnicas reconhecidas de testes de penetração para fins criminosos. Foi realizada a utilização do *Social Engineer Toolkit (SET)* para demonstrar a clonagem de um site legítimo, abordando sua facilidade de uso e levantando questões cruciais sobre segurança cibernética e conscientização dos usuários. O resultado demonstra a facilidade de acesso a ferramentas tecnológicas, tanto para profissionais da área de segurança quanto para qualquer usuário com qualquer nível de conhecimento em tecnologia, permitindo seu uso de forma ética ou maliciosa, por meio de engenharia social e *phishing*.

**Palavras-chave**: Engenharia Social, Phishing, Segurança da Informação.

***Abstract***

*The objective of this work is to explore a topic of extreme importance today: Social Engineering and Phishing. Nowadays, the recurrence of this practice becomes a significant threat to information security and cybersecurity. In this context, it was examined how Social Engineering, together with phishing, can deceive its victims, obtaining confidential information, using recognized penetration testing techniques for criminal purposes. The Social Engineer Toolkit (SET) was used to demonstrate the cloning of a legitimate website, addressing its ease of use and raising crucial questions about cybersecurity and user awareness. The result demonstrates the ease of access to technological tools, both for security professionals and for any user with any level of knowledge in technology, allowing their use ethically or maliciously, through social engineering and phishing.*

***Keywords****: Social engineering, phishing, cybersegurity.*

## 1. Introdução

A Engenharia Social é a prática de manipular as pessoas para obter informações confidenciais, como dados pessoais, credenciais, dados financeiros, e acesso não autorizado a sistemas ou para induzi-las a tomar ações prejudiciais, explorando aspectos psicológicos e comportamentais do ser humano (ABIN, 2023). A Engenharia Social é de extrema importância atualmente, devido ao crescente uso da tecnologia e da internet no cotidiano da comunidade. Esse tipo de ataque pode ocorrer por meio de e-mails de *phishing*, ligações telefônicas fraudulentas, perfis falsos em mídias sociais e outras táticas enganosas.

Será abordado neste projeto, como a Engenharia Social e o *Phishing* podem ser empregados facilmente por indivíduos mal-intencionados para prejudicar o patrimônio de suas vítimas, demonstrando como *Social Engineer Toolkit (SET)*, uma ferramenta utilizada por especialistas em segurança, pode ser utilizado para clonar sites legítimos e realizar ataques de engenharia social para ações criminosas. Em uma era, na qual a tecnologia se faz cada vez mais presente e necessária na vida do ser humano, o estudo e o desenvolvimento de técnicas de políticas de segurança, controles físicos e lógicos para evitar o roubo de informação de organizações públicas e privadas, estão se tornando cada vez mais importantes e essenciais. No entanto, embora possam existir controles para manter a segurança da informação e melhorar a segurança cibernética, há um assunto que deve ser abordado e levado em consideração pela sociedade: a engenharia social, uma vez que o ser humano é considerado por muitos, o elo mais fraco na segurança.

Serão definidos os conceitos da Engenharia Social e do *Phishing* para um melhor entendimento sobre o assunto. Para demonstrar um ataque de Engenharia Social, será utilizada a ferramenta *Social-Engineer Toolkit (SET)* no ambiente do Kali Linux. Realizou-se a utilização do método de clonagem de site para obtenção de credenciais e, posteriormente a demonstração de um ataque *phishing* com as próprias ferramentas do software. Foram efetuados estudos sobre o uso da ferramenta abordada, enfatizando algumas maneiras para se evitar cair em golpes. É importante destacar que, embora essa ferramenta seja frequentemente usada para testes de penetração e com intuito de conscientização dentro das organizações, elas também podem ser exploradas para atividades criminosas. Portanto, é essencial compreender a engenharia social e as maneiras de se proteger contra sua prática para atividades ilegais, podendo resultar em consequências extremamente prejudiciais para suas vítimas.

## 2. Referencial Teórico

A compreensão de conceitos fundamentais de engenharia social, *phishing* e sobre as ferramentas de *pentest* desempenham um papel crucial na proteção contra ameaças. Este referencial teórico visa explorar esses temas e destacar sua importância no contexto da segurança da informação.

### 2.1. Engenharia Social

Segundo a Agência Brasileira de Inteligência (ABIN, 2023) do Governo Federal, em seu guia de proteção elaborada pelo Programa Nacional de Proteção do Conhecimento Sensível (PNPC), é definido que a engenharia social é um método utilizado pelos engenheiros sociais para manipulação psicológica com o intuito de enganar, manipular ou explorar a confiança de suas vítimas, cujo objetivo é fazer com que a vítima passe voluntariamente informações sigilosas. A prática pode ser considerada crime, por exemplo, quando um indivíduo visa induzir outra pessoa a divulgar sua senha voluntariamente. Essa prática é utilizada para coletar informações, que podem ser de porte pessoal ou corporativo, sendo que esse método não utiliza violência física para obtenção de informações da vítima.

A engenharia social deve ser considerada um fator crítico, dada a gravidade das suas possíveis consequências. Os autores Mitnick e Simon (2003), argumentam que fator humano é o elo mais fraco da segurança, por ser possível obter informações sigilosas ao se passar por outra pessoa ou simplesmente pedindo as informações diretamente à vítima. Além disso, eles esclarecem que "a segurança não é um problema para a tecnologia – ela é um problema para pessoas e a direção", ou seja, a eficácia das medidas de segurança está diretamente ligada à forma como as pessoas e a liderança de uma organização lidam com essas questões.

A ABIN (2023), explica a razão pela qual a engenharia social demonstra sua eficácia. A técnica de engenharia social é eficaz porque aproveita as vulnerabilidades do funcionamento automático da mente humana. Muitas ações de nosso cotidiano são realizadas de forma automática sem que perceba-se, exigindo pouca reflexão e pensamento, a menos que algo pareça muito incomum, levando a acionar o pensamento mais lento. Os engenheiros sociais exploram que, se conseguirem alinhar uma situação com o modelo mental padrão, é improvável que questionem-se suas ações, facilitando assim que eles consigam as informações que desejam, sendo a engenharia social uma ferramenta básica no arsenal dos *hackers* não éticos.

Os ataques de engenharia social podem variar em complexidade técnica e até mesmo

ocorrer sem a necessidade de tecnologia. É amplamente conhecido, na área da segurança da informação, que os usuários representam uma vulnerabilidade importante. Mesmo que sejam implementados diversos controles de segurança, como físicos e lógicos, se um funcionário for persuadido a divulgar informações confidenciais da empresa, todas as medidas de segurança serão ineficazes. Muitos dos ataques mais conhecidos não envolvem exploração de falhas de sistemas, mas sim a exploração da natureza humana (WEIDMAN, 2014).

De acordo com Mitnick e Simon (2003), à medida que os especialistas em segurança aprimoram as técnicas de segurança e realizam melhorias contínuas em seus sistemas, torna-se cada vez mais difícil a exploração técnica, portanto, os engenheiros sociais tenderão a explorar cada vez mais a engenharia social. Neste caso, “quebrar o *firewall* humano” não requer investimentos significativos e envolve riscos mínimos, bastando ao atacante ter paciência e habilidades de persuasão para obter as informações desejadas.

## 2.2. *Phishing*

O *phishing* é uma forma de ataque cibernético em que os criminosos buscam enganar as pessoas para que revelem seus dados pessoais e financeiros. Esse ataque é feito pela utilização combinada de meios técnicos e engenharia social. Esse termo é de origem da palavra em inglês "*fishing*" resultado de uma analogia desenvolvida por criminosos, na qual eles empregam "armadilhas" (mensagens eletrônicas) com o objetivo de obter de forma fraudulenta senhas e informações financeiras dos usuários da Internet (CERT.BR, 2023).

Os ataques de engenharia social, juntamente com o *phishing*, envolvem utilizar e-mails, mensagens de SMS, contato por telefone e principalmente sites falsos para obtenção de dados de suas vítimas, uma vez que, devido à confiança depositada pela vítima, ela revela informações pessoais como credenciais e números de cartões de crédito. As técnicas de *phishing* e a engenharia social combinadas são extremamente perigosas, especialmente para usuários comuns que fazem uso da tecnologia, empresas, e organizações públicas e privadas.

Segundo Hadnagy e Fincher (2015), além de usuários comuns, os atacantes visam trabalhadores de empresas, pois fornecer credenciais de acesso pode permitir o acesso à toda rede da empresa. Isso pode ser o objetivo principal, se as recompensas forem grandes, ou pode ser uma maneira de ampliar o ataque. Além disso, alvos de alto valor incluem pessoas ligadas a grandes empresas e governos. Quanto mais elevado o cargo na hierarquia, maior a probabilidade de serem alvos de *phishing* direcionado (*spear phishing)*, devido ao esforço e às

recompensas envolvidas. Isso pode ter consequências significativas em termos de economias inteiras, não apenas de indivíduos.

Os atacantes se aproveitam de muitos temas e assuntos que despertam interesse e preocupação nas pessoas, como questões legais, promoções de produtos e serviços, ofertas de emprego e eventos de grande impacto emocional, como ataques terroristas e desastres naturais. Essa diversidade de abordagens visa atrair a atenção e confiança das vítimas, aumentando assim a probabilidade de elas caírem nos golpes (CERT.BR, 2015).

É importante destacar os vários tipos de *Phishing* existentes como forma de conscientização e prevenção. Conforme a Microsoft (2024), podem-se destacar algumas formas de ataque:

• ***Phishing*** **de E-mail:** esse é o meio de fraude *online* mais comum e utilizado por indivíduos mal-intencionados, no qual os criminosos enviam mensagens falsas fingindo ser de empresas ou pessoas conhecidas para enganar as vítimas para elas compartilharem informações pessoais e confidenciais. Eles geralmente usam *links* falsos que levam a sites falsos para roubar dados sensíveis como credenciais de acesso.

• **Ataque Direcionado (*Spear Phishing):*** essa é uma forma mais direcionada de ataque, na qual os criminosos pesquisam detalhes específicos sobre as pessoas e usam essas informações para personalizar suas mensagens. Eles miram em alvos específicos, aproveitando-se de dados sobre seus empregos e vida pessoal para aumentar a credibilidade das mensagens fraudulentas. Esses ataques são altamente eficazes, por serem altamente personalizados e podem contornar medidas de segurança cibernética mais básicas.

• ***Whaling:*** *"whaling"* ou pesca de baleias, esse termo é utilizado quando criminosos miram em figuras importantes, como executivos de grandes empresas ou celebridades. Eles investem tempo em pesquisas extensivas sobre seus alvos, buscando oportunidades para roubar informações confidenciais ou credenciais de *login* valiosas.

• ***Vishing:*** o *vishing* é uma tática em que criminosos ligam de centrais de atendimento falsas e tentam enganar as pessoas para compartilharem informações confidenciais por telefone. Eles muitas vezes usam truques psicológicos para convencer as vítimas a instalarem aplicativos maliciosos em seus dispositivos.

• ***Smishing:*** Uma combinação das palavras “SMS” e “*phishing*”. As pessoas estão mais vulneráveis aos golpes por SMS, porque as mensagens de texto são entregues em texto simples

e parecem mais pessoais.

### 2.3. Ferramentas de Pentest

As ferramentas de *pentest* (teste de penetração) são projetadas para identificar, mapear e expor vulnerabilidades em diversos tipos de sistemas, como em redes de computadores, sistemas operacionais, aplicativos *web* e banco de dados. Através do *pentest*, é possível descobrir falhas, para que as organizações criem mecanismos de defesas contra possíveis invasões de cibercriminosos. No entanto, essas mesmas ferramentas também podem ser utilizadas maliciosamente por indivíduos com intenções de cometer crimes, visando obter acesso a informações confidenciais de empresas e indivíduos, comprometendo assim a integridade de seus alvos (MORENO, 2019). Tais ferramentas, como *Social-Engineer Toolkit (SET)*, abordado neste trabalho, são geralmente desenvolvidas para serem acessíveis a profissionais de segurança em tecnologia, mas também podem ser obtidas por criminosos com fins ilegais. O fácil acesso a essas ferramentas através da internet significa que criminosos podem adquiri-las e utilizá-las sem a necessidade de desenvolver suas próprias soluções. Muitos até mesmo adquirem ferramentas prontas na internet e inclusive obtêm informações confidenciais como credenciais em casos de vazamento de dados.

O Kali Linux é um sistema operacional de código aberto, baseada no Debian, projetado especificamente para uma ampla gama de atividades relacionadas à segurança da informação. Ele é usado principalmente para realizar testes de penetração, investigações de segurança, análise forense digital e outras práticas relacionadas à segurança cibernética. É um sistema operacional que possui uma vasta gama de ferramentas e utilitários já instalados prontos para uso, incluindo o *Social-Engineer Toolkit* (KALI, 2024).

Pessoas com algumas habilidades técnicas em tecnologia, ou até mesmo sem nenhum conhecimento na área, podem empregar ferramentas de *pentest* para explorar sistemas e redes de maneira maliciosa. Eles podem usar essas ferramentas para encontrar vulnerabilidades e explorá-las para ganho pessoal, roubo de informações confidenciais, espionagem industrial, fraude financeira, entre outros crimes, e até mesmo disseminação na *web* de informações confidenciais e arquivos sigilosos (MORENO, 2019).

Diversas das ferramentas de *pentest* permitem a automação de certos tipos de ataques, o que facilita para os criminosos lançarem ataques em grande escala. Isso pode incluir ataques de negação de serviço (DDoS), ataques de força bruta contra nome de usuários e senhas,

ataques de *phishing*, exploração de vulnerabilidades conhecidas e ataques de engenharia social baseados em pretextos convincentes conforme exemplos destacados neste trabalho.

Ao utilizar essas ferramentas de *pentest*, os criminosos podem tentar ocultar sua identidade e localização, tornando-se mais difíceis de serem rastreados pelas autoridades. Isso é especialmente verdadeiro quando os criminosos utilizam técnicas de anonimato *online*, como redes privadas virtuais (VPNs) ou redes anônimas, para ocultar sua atividade na internet. De acordo com Moreno (2019), há também a possibilidade de utilizar redes e computadores de vítimas como "laranjas" para facilitar outros tipos de crimes virtuais.

Quando se trata da utilização dessas ferramentas, é frequente que as pessoas as associem a indivíduos que utilizam seus conhecimentos e recursos para atividades criminosas, sendo frequentemente rotulados com o termo conhecido "*hacker*". No entanto, é importante destacar que *hackers* são classificados em diferentes grupos, isso com base em suas motivações e na maneira como usam suas habilidades e as ferramentas. O uso inadequado das ferramentas para clonagem de sites e obtenção ilegal de credenciais, por exemplo, é tipicamente atribuído aos *hackers* de chapéu preto. Os *hackers* de chapéu branco — ou *hacker*s éticos — são indivíduos que usam seus conhecimentos para encontrar vulnerabilidades em sistemas e fazer recomendações de melhorias dentro dos limites legais e em um escopo pré-determinado pela empresa que solicita seus serviços. Os *hackers* de chapéu cinza, por outro lado, são indivíduos que usam seus conhecimentos para encontrar vulnerabilidades em sistemas sem o conhecimento e consentimento da empresa alvo. Frequentemente, eles informam posteriormente a empresa sobre as falhas encontradas motivados por recompensas financeiras ou simplesmente em busca de reconhecimento (KASPERSKY, 2024).

No Brasil, existe a lei que trata especificamente dos crimes cometidos no ambiente digital, conhecidos como crimes cibernéticos. A legislação referente a crimes cibernéticos no país é precisamente delineada pela Lei nº 12.737/2012, reconhecida como a “Lei Carolina Dieckmann”, que deixa claro que o acesso a um sistema informático de outro indivíduo, esteja ele conectado à internet ou não, através da violação injustificada de suas medidas de segurança, visando obter, modificar ou apagar dados sem a permissão explícita, ou implícita do dono do dispositivo, ou de introduzir vulnerabilidades visando benefícios ilegais, pode resultar em penalidades legais que incluem detenção e multa, conforme estabelecido na legislação brasileira de 2012 Art. 154-A (BRASIL, 2024)

### 2.3. Estatísticas

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR) apresenta as estatísticas detalhadas das páginas falsas identificadas e acompanhadas ao longo do ano de 2023. Esses dados são cruciais para entender a extensão do problema referente ao *phishing* e à engenharia social e orientar ações para mitigar ameaças cibernéticas. Durante o período de janeiro a dezembro de 2023, foram acompanhadas um total de 10.923 páginas falsas. Ao analisar a distribuição dessas páginas, conforme sua influência geográfica, verifica-se que 7.422 delas tinham impacto nacional, enquanto 3.501 afetaram organizações no Brasil. Vale destacar que esses dados são calculados sempre que uma tentativa de *phishing* é notificada ao CERT.BR, podendo o número ser bem maior do que o apresentado, pois muitos casos não são relatados. Algumas categorias de páginas falsas acompanhadas pelo CERT.BR são: criptomoedas, fidelidade, financeiro, governo, infraestrutura de nuvem, pagamentos, provedores, redes Sociais, seguros e saúde, serviços de nuvem, varejo, webmail corporativo. Essas estatísticas fornecidas por eles ajudam a entender a amplitude e a natureza dos ataques de *phishing* e tem como objetivo permitir que as organizações identifiquem os principais tipos de assuntos em *phishing* que possam afetar suas operações (CERT.BR, 2023).

## 3. Metodologia

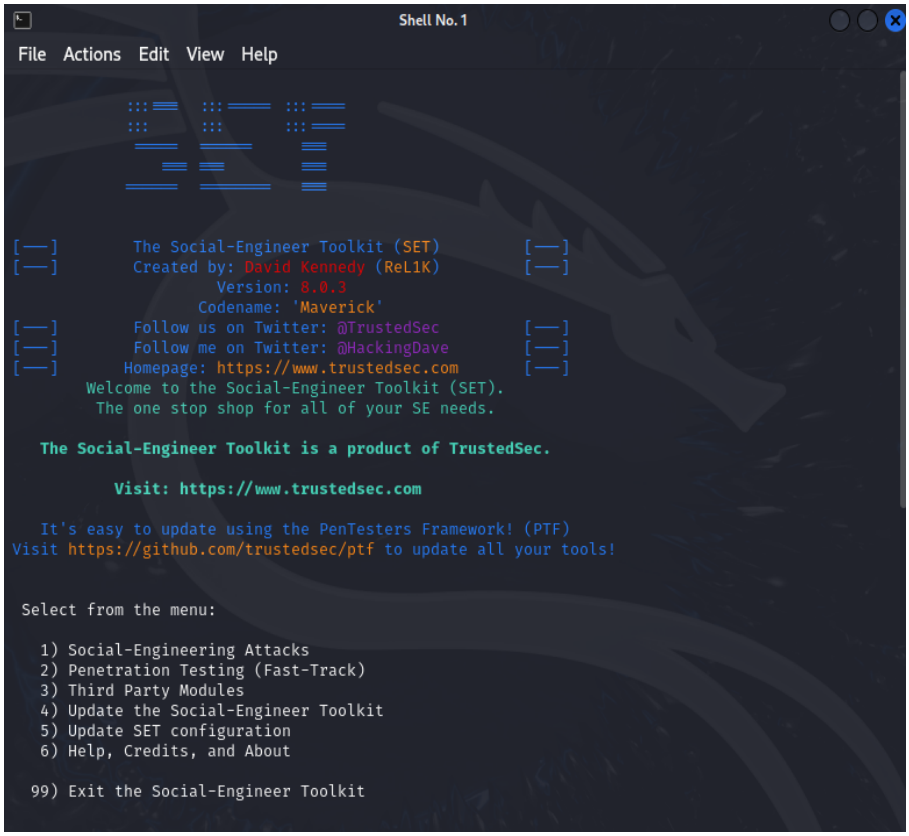
Para a realização da proposta informada neste processo de pesquisa, foi desenvolvido um ambiente virtual fictício com o propósito de realizar uma simulação de clonagem de um site legítimo e demonstração de um ataque *phishing*. Isso foi realizado através da utilização do software de virtualização Oracle VM VirtualBox 7.0, executando o sistema operacional Kali Linux 2024, uma distribuição Linux de código aberto baseada em Debian, para uso do *Social-Engineer Toolkit (SET)* versão 8.0.3, uma vez que a ferramenta já vem pré-instalada nesse sistema operacional. O objetivo principal foi avaliar e demonstrar a facilidade de utilização do *Social-Engineer Toolkit (SET)* para realização de ataques *phishing* e clonagem de sites.

Para fundamentar a pesquisa proposta, foi procurado obter informações atualizadas de fontes diversas, incluindo artigos, livros e sites publicados entre 2015 e 2024. O objetivo foi estabelecer uma base de conhecimento sólida para a realização da parte teórica e prática deste artigo, por meio de nomes renomados no setor de segurança da informação. Foram utilizadas ferramentas de pesquisas voltadas para este nicho, como o Google, Bing e o Google Acadêmico, sendo este último com o propósito de localizar conteúdo de carácter confiável e

válido. Além disso, para a parte prática, também foi utilizado a documentação fornecida pelos desenvolvedores dos *softwares* utilizados.

O *Social-Engineer Toolkit (SET)* é uma ferramenta desenvolvida por David Kennedy, fundador da empresa *TrustedSec*. É um software de código aberto baseada em *Python* amplamente reconhecida e utilizada pela sua versatilidade e pela variedade de técnicas que oferece para simular ataques realistas. Ela é uma ferramenta muito utilizada por profissionais de segurança para avaliarem a segurança de sistemas, redes e indivíduos, explorando vulnerabilidades por meio de técnicas de manipulação psicológica e social, técnica conhecida como engenharia social. A engenharia social é um dos ataques mais difíceis de se proteger e um dos mais prevalentes na atualidade. O software possui mais de 2 milhões de *downloads* e é amplamente utilizado, possuindo forte suporte na comunidade de segurança. O programa é pré-instalado por padrão no Kali Linux, no entanto, também é possível fazer o *download* e instalá-lo diretamente caso não esteja instalado através do repositório do GitHub (TRUSTEDSEC, 2023). Observa-se na Figura 1 a tela inicial do software.

Figura 1. Apresentação do *Social-Engineer Toolkit (SET)*




Fonte: Autoria propria

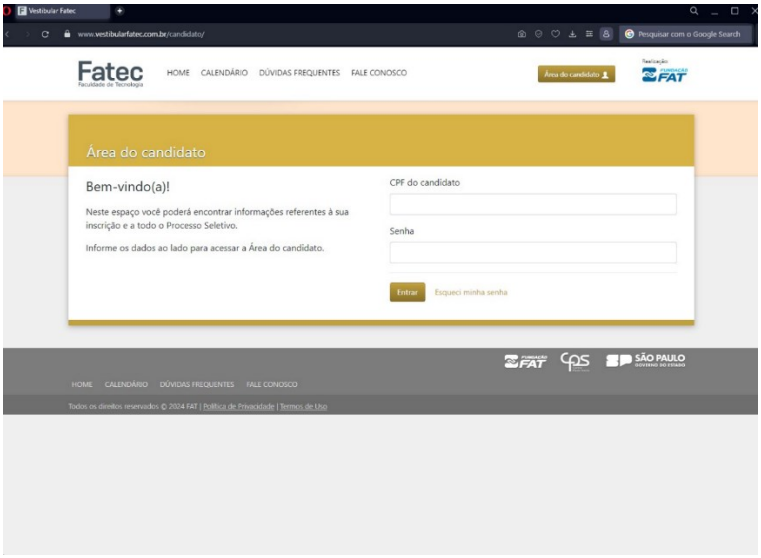
O *Social-Engineer Toolkit (SET)* possui diversas ferramentas para ajudar os profissionais de segurança na realização de testes com objetivos específicos. O propósito principal é encontrar vulnerabilidades e lacunas na segurança de uma organização através da engenharia social.

No capítulo 4, apresenta-se uma visão resumida dos resultados obtidos com o uso essa ferramenta para clonar um site alvo e, posteriormente, seguida pela exposição dos resultados obtidos da execução de um ataque de *phishing* por e-mail. Foram exploradas as funcionalidades disponíveis na ferramenta com a seleção cuidadosa dos métodos de ataque mais adequados para alcançar esses objetivos.

## 4. Resultados e Discussões

Para a realização da parte prática, iniciou-se com a etapa de clonagem de um site alvo. O site escolhido como alvo para demonstrar a técnica de clonagem foi o site do vestibular da própria instituição de ensino da FATEC, disponível no link "https://www.vestibularfatec.com.br/candidato/".

Figura 2. Site Alvo




Fonte: Autoria própria

Conforme demonstrado na Figura 2, é possível confirmar a autenticidade do site em questão ao analisar detalhes cruciais, tais como a URL (*Uniform Resource Locator*) e a presença de um certificado digital, que tem por objetivo autenticar o proprietário do site e assegurar uma comunicação segura, confiável e criptografada entre o navegador do usuário e o servidor, garantindo uma confiabilidade do processo de comunicação e troca de informação.

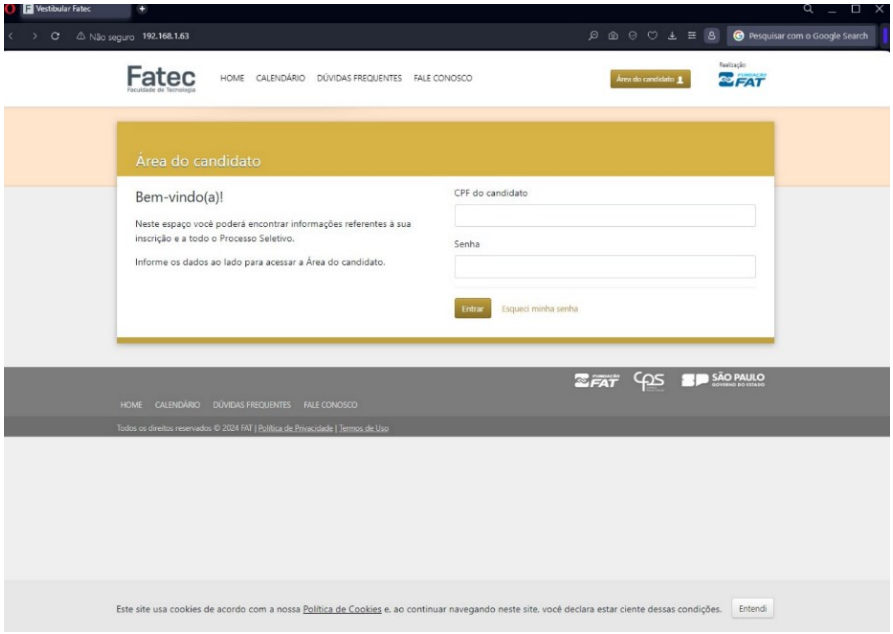
Escolhendo a opção *"Social-Engineering Attacks"* disponível no *Social-Engineer Toolkit (SET)*, procedeu-se à clonagem do site alvo, utilizando a opção *"Website Attack Vectors*", seguida da opção *"Credential Harbester Attack Method*" e selecionando o *"Site Cloner*", conforme ilustrado na Figura 3. Os parâmetros passados foram o endereço IP para o *POST Back* e a URL do site alvo.

Figura 3. Processo de Clonagem do Site-Alvo


Fonte: Autoria própria

O acesso à página falsa foi feito através do IP da Máquina Kali, 192.168.1.63, conforme a Figura 4, devido ao teste ter sido conduzido internamente na rede, sem exposição à Internet. Em um ambiente real, caso um invasor tenha acesso à rede interna de uma organização, técnicas como manipulação de arquivos DNS poderiam redirecionar um usuário para o site falso utilizando o próprio domínio ou poderia configurar a ferramenta para redirecionar o tráfego para um servidor externo, permitindo assim a obtenção de credenciais e tornando o ataque mais sofisticado, no entanto, este último exemplo requer uma configuração mais complexa.

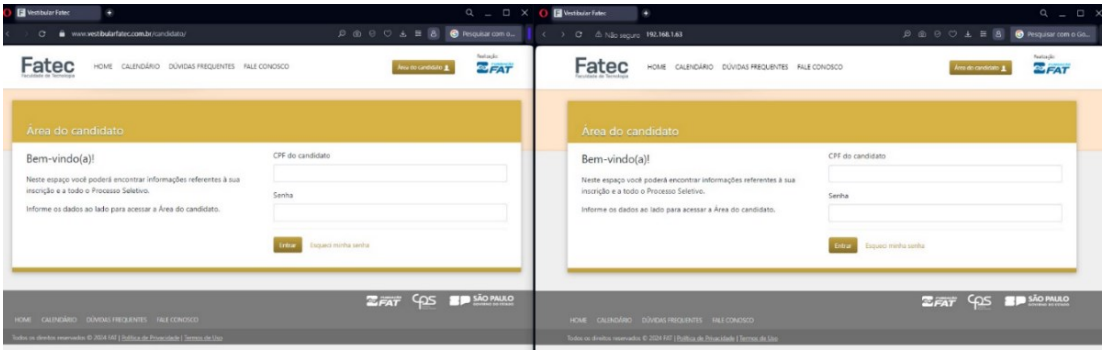
Figura 4. Réplica do site-alvo




Fonte: Autoria própria

A Figura 5 apresenta um comparativo dos sites onde o lado esquerdo representa o site original do Vestibular da FATEC e o lado direito representa o site clonado pela ferramenta.

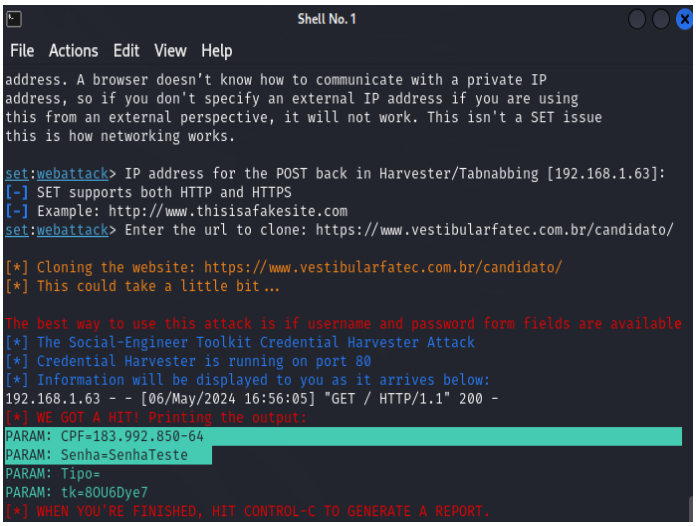
Figura 5. Comparação site Original e Falso




Fonte: Autoria própria

É evidente que há uma alta semelhança entre o site original e sua versão clonada, sendo a URL e a ausência de um certificado digital os únicos elementos distintos entre os dois. Ao acessar o site falso e tentar fazer login com uma credencial falsa para fins de teste, a ferramenta SET capturou tanto o nome de usuário, no caso, um CPF gerado aleatoriamente, quanto a senha, como ilustrado na Figura 6. Os dados capturados foram mostrados diretamente no terminal da ferramenta.

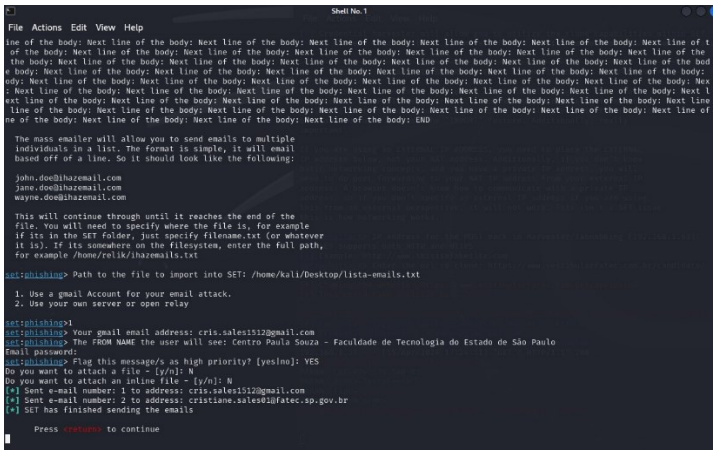
Figura 6. Sucesso na obtenção as credenciais




Fonte: Autoria própria

Posteriormente, foi realizado o envio de *e-mail* em massa para demonstrar como a ferramenta oferece recursos que podem ser utilizados para táticas de *phishing*. Ao selecionar a opção *"Social-Engineering Attacks"* e, em seguida, *"Spear-Phishing Attack Vectors"* e *"E-mail Attack Mass Mailer"*, o software solicitou informações específicas, tais como o endereço de e-mail da vítima ou uma lista de e-mails, o remetente do *e-mail* de *phishing*, o assunto, o corpo do e-mail e outros detalhes pertinentes. Uma conta no Gmail foi criada para possibilitar que o SET enviasse *e-mails* usando endereço de *e-mail* personalizado. Após as configurações adequadas, os e-mails foram enviados pela ferramenta. O conteúdo do *e-mail* gerou um código HTML, para tornar a abordagem mais realística.

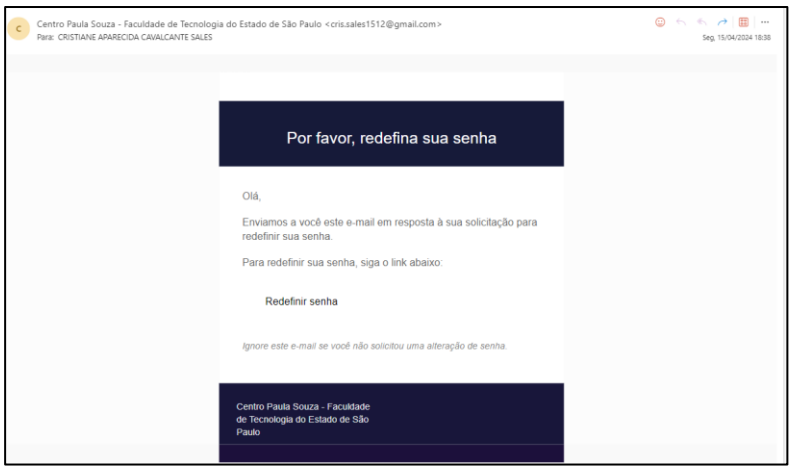
Figura 7. Configuração de envio de e-mail em massa




Fonte: Autoria própria

Após o sucesso do envio dos e-mails, como evidenciado na Figura 7, foi verificada a caixa de entrada de um e-mail alvo para assegurar que os e-mails foram entregues conforme o planejado e demonstrado na Figura 8.

Figura 8. Recebimento do e-mail




Fonte: Autoria própria

Os resultados representam como é possível utilizar facilmente algumas ferramentas destinadas para fins éticos dentro da área de segurança cibernética de maneira fácil e rápida, já que o Kali Linux por padrão, já vem com muitas ferramentas para esse propósito instalados. Sobre o *Social-Engineer Toolkit (SET)*, é evidente que não há necessidade de utilizar parâmetros de alta complexidade. Com o desenvolvimento do ambiente de testes concluído com êxito, fica clara a simplicidade dos processos abordados, os quais podem ter um impacto exponencialmente negativo, tanto em indivíduos, quanto em corporações caso sejam utilizadas para fins criminosos.

A engenharia social e o *phishing,* em conjunto com a utilização dessa ferramenta, são táticas altamente eficazes e prevalentemente usadas por atacantes cibernéticos para enganar vítimas e obter informações confidenciais. A ferramenta é acessível devido à sua interface amigável e à variedade de recursos disponíveis, o que significa que não é necessário possuir um grande conhecimento para utilizá-la. No entanto, é importante destacar que o sucesso de um ataque desse tipo não é garantido apenas pelo uso da ferramenta. Os resultados dependem significativamente da habilidade do atacante em dominar táticas persuasivas e eficazes para enganar suas vítimas. Portanto, embora a ferramenta simplifique todo esse processo, o conhecimento e a compreensão das estratégias de engenharia social continuam sendo componentes essenciais para obter êxito em um ataque. Os autores Mitnick e Simon (2003)

destacam em seu livro que há um ditado popular, que diz que um computador seguro é aquele que está desligado, porém, essa afirmação é relativamente falsa, uma vez que um *hacker* pode convencer alguém a entrar no escritório e ligar o computador. Isso demonstra que tecnologia em si não apresenta riscos, é o ser humano que frequentemente representa o elo fraco, uma vez que é suscetível a ser persuadido a tomar decisões erradas. Tudo então, torna-se questão de tempo, paciência e persistência para um engenheiro social alcançar com sucesso seus objetivos.

Apesar da existência de ferramentas e medidas de segurança para evitar ataques de sites falsos e *phishing*, a vulnerabilidade mais crítica em um sistema de segurança é a falha humana, pois um simples clique ou falta de atenção do usuário para medidas de segurança consideravelmente simples como verificação de *URL* e certificado digital, pode comprometer toda a segurança. Pode-se concluir que, para diminuir os impactos da falha humana em sistemas que necessitam de proteção constante, é de suma importância promover a conscientização em massa do público que possui acesso à informação, de forma que seja possível reconhecer uma ação de engenharia social e suas vertentes digitais, como o *phishing*, por exemplo. Isso, em consonância com a aplicação de técnicas e testes contínuos para a proteção do âmbito das informações desejadas, poderá promover um ambiente pessoal e corporativo mais protegido contra as ameaças proporcionadas por pessoas mal-intencionadas.

Não existe uma tecnologia no mundo reconhecida até o momento que seja capaz de combater um engenheiro social. As empresas que realizam testes de penetração em sistemas relatam que se torna muito mais fácil invadir um sistema através de métodos com engenharia social, por ser possível adquirir diversas informações cruciais sobre o sistema. Além disso, embora existam tecnologias capazes de tomar decisões pelo ser humano mediante análises técnicas, a única forma de se combater um engenheiro social é por meio de políticas de segurança, junto com educação e treinamento (MITNICK; SIMON, 2003).

Uma política de segurança da informação é fundamental, tanto na segurança da informação, quanto na segurança cibernética, por estabelecer as diretrizes, procedimentos e práticas que uma organização deve seguir para proteger seus ativos de informação contra ameaças cibernéticas. Isso torna evidente que, não somente usuários finais devem se preocupar com a segurança, mas as empresas e organizações também devem estabelecer políticas de segurança para seus colaboradores e investir em treinamentos e conscientização.

Quanto ao *phishing*, existem muitas medidas de prevenção que podem ser tomadas. De acordo com o CERT.BR (2023) podem-se destacar algumas medidas: ficar atento às

mensagens de pessoas ou instituições que solicitem informações ou ações suspeitas, questionar a legitimidade de mensagens de pessoas e organizações com as quais não têm um relacionamento prévio, ser cauteloso com mensagens que buscam chamar excessivamente a atenção, como promoções ou ameaças como negativação de nome e não confiar em mensagens com base apenas no remetente, pois podem ser falsos. Além disso, digitar os endereços de sites diretamente no navegador, em vez de clicar em links suspeitos que estejam no e-mail para evitar redirecionamentos para sites fraudulentos, pois os criminosos podem tentar ocultar o endereço real do site. Outras medidas que também se destacam podem ser resumidas em: verificar se um site usa uma conexão segura ao inserir informações sensíveis como dados pessoais e dados de cartão de crédito, examinar as informações do certificado de segurança ao acessar sites, especialmente se parecerem diferentes do site verdadeiro e consultar o site da instituição para verificar a autenticidade de mensagens suspeitas, pois não faz parte da política da maioria das empresas o envio de mensagens.

Existem algumas outras técnicas e práticas de segurança que podem ser implementadas em conjunto para fortalecer a postura de segurança de uma organização contra ataques, abrangendo não apenas ataques de *phishing* e engenharia social, mas também outras formas de ataques cibernéticos e ameaças à segurança da informação. Por exemplo, os filtros de *e-mail* avançados para identificar e bloquear mensagens de *phishing* antes mesmo de chegarem à caixa de entrada dos usuários, utilização de *anti malware*, *firewall* pessoal e antivírus são outros exemplos. Além disso, os gerenciadores de senhas seguras, a autenticação de dois fatores (2FA) e as atualizações de software automáticas desempenham um papel fundamental na garantia da segurança cibernética. Essas medidas ajudam a mitigar vulnerabilidades conhecidas que os *hackers* poderiam explorar, enquanto a auditoria e o monitoramento de acesso são essenciais para detectar e investigar atividades suspeitas.

## 5. Considerações Finais

As ferramentas de teste de penetração são valiosas para melhorar a segurança cibernética. No entanto, embora sejam originalmente concebidas para fins legítimos de pesquisa e segurança, também podem ser exploradas com intenções maliciosas por criminosos para diversas finalidades.

Percebe-se, através do estudo, que o uso do *Social-Engineer Toolkit (SET)* é extremamente fácil, por possuir uma interface gráfica de usuário (GUI) amigável, que

simplifica todo o processo de configuração e execução dos ataques oferecidos pela ferramenta. Essa facilidade torna a ferramenta mais acessível mesmo para usuários com conhecimentos técnicos limitados, permitindo que até mesmo pessoas iniciantes realizem ataques complexos sem a necessidade de entender completamente os detalhes técnicos por trás da ferramenta. O programa automatiza muitos aspectos do processo de ataque, desde a criação de páginas falsas até a execução de envios de e-mail em massa para fins de *phishing*, conforme demonstrado.

Para evitar que as pessoas caiam em golpes, é crucial promover a conscientização sobre essas ameaças. Tanto indivíduos quanto as organizações devem estar cientes sobre as táticas usadas pelos criminosos, tanto quanto as táticas de engenharia social quanto as táticas de *phishing*, a fim de se protegerem de maneira eficaz. Além disso, a colaboração entre profissionais de segurança e usuários finais é fundamental para se proteger contra esses ataques. Um ataque direcionado a uma pessoa pode comprometer toda a organização, expondo dados internos e informações de clientes, o que pode causar danos irreparáveis à reputação da empresa. Além disso, as regulamentações rigorosas de proteção de dados, como a LGPD (Lei Geral de Proteção de Dados Pessoais), impõem severas penalidades por vazamento de informações, acarretando prejuízos financeiros significativos devido às multas. Portanto, é essencial adotar medidas preventivas e treinar todos os colaboradores para minimizar qualquer possibilidade de riscos, garantindo tanto a segurança da informação quanto a segurança cibernética.

## Referências


ABIN, Agência Brasileira de Inteligência. Engenharia social. Guia para Proteção de Conhecimentos Sensíveis. Disponível em: https://www.gov.br/abin/pt-br/acesso-a-informacao/acoes-e-programas/PNPC/boaspraticas/cartilha-engenharia-social-guia-para-protecao-de-conhecimentos-sensiveis. Acesso em: 20 out. 2023.

CERT.BR, Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Bra-sil (CERT.BR). Cartilha de Segurança para Internet Versão 4.0. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 20 out. 2023

CERT.BR, Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Brasil. Páginas Falsas Utilizadas em Tentativas de Phishing. Disponível em: https://stats.cert.br/phishing/#desc-categorias. Acesso em: 16 nov. 2023.

HADNAGY, Christopher; FINCHER, Michele. Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. Prólogo de DREEKE, Robin. Wiley, 2015.

KALI. Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution. Dis-ponível em: <https://www.kali.org/>. Acesso em: 28 Mar. 2024.

KASPERSKY. Hackers de chapéu preto, chapéu branco e chapéu cinzento – Definição e explicação. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/hacker-hat-types>. Acesso em: 29 mar. 2024.

LEGISLAÇÃO BRASILEIRA. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União, Bra-sília, DF, 3 dez. 2012. Disponível em: http://planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm. Acesso em: 17/09/2024

MICROSOFT. O que é phishing? Disponível em: <https://www.microsoft.com/pt-br/security/business/security-101/what-is-phishing>. Acesso em: 29 mar. 2024.

MITNICK, K. D.; SIMON, W. L. A Arte de Enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. Indianapolis, Indiana: Wiley Publishing, Inc, 2005.

MORENO, D. Introdução ao Pentest - 2a Edição. São Paulo: Novatec Editora Ltda, 2019.

TRUSTEDSEC. The Social-engineer Toolkit (SET). Disponível em: <https://www.trustedsec.com/tools/the-social-engineertoolkit-set>. Acesso em: 20 out. 2023.

WEIDMAN, Georgia. Testes de Invasão. Uma introdução prática ao hacking. São Paulo: Novatec Editora Ltda, 2014.