Utilização da engenharia social em proveito das ações de Inteligência Cibernética: uma combinação de ataque de e-mail com ataque web utilizando a ferramenta social-engineer toolkit

Raphael Fernandes Silva[1]
Ricardo Argollo Santos do Espirito Santo[2]

1 INTRODUÇÃO

A sociedade da informação, para Tarapanoff (2001), "é o resultado de novos referenciais sociais, econômicos, tecnológicos e culturais, que resultam em um conjunto significativo de mudanças na sociedade e nas organizações. A informação passa a ser uma matéria prima essencial e que move o sistema."

O surgimento da Internet deu origem a um novo ambiente de interação, serviços e comunicação, transformando sobremaneira o modo como as pessoas, grupos ou organizações se relacionam e trabalham. Neste sentido, a dinâmica das relações sociais e os fenômenos de massa foram impulsionados pela informação em tempo real e, assim, surgiram diversos canais de relacionamentos horizontais e não hierárquicos (NASCIMENTO et al., 2015).

Nesse contexto apresentado, surge o denominado Espaço Cibernético (E Ciber). Este, por sua vez, é caracterizado como o espaço virtual composto por dispositivos computacionais conectados em rede, onde informações digitais trafegam, são processadas ou armazenadas (BRASIL, 2015).

Segundo a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética (ESIC), da Administração Pública Federal (APF) (2015):

> O cenário de uso da Internet e, consequentemente, de uso das Tecnologias de Informação e Comunicação (TIC) permanece crescente e sem dúvida além de qualquer expectativa e prospecção, operando-se em cifras bastante expressivas no mundo e no País, especialmente frente aos avanços do uso de dispositivos móveis, da computação em nuvem e da evolução da chamada "internet das coisas" (BRASIL, 2015).

Com o crescente uso das TIC's, percebeu-se a formação de um conjunto denominado de:

> Redes e conexões, que aproximam espontaneamente usuários que possuem valores e objetivos comuns, propiciando que as pessoas se comuniquem, organizem eventos, compartilhem mídias, organizando-se assim em um debate público, nos quais são abordados diversos temas, sendo que alguns destes são de interesse direto ou indireto da segurança pública (NASCIMENTO; BARRETO e MIRANDA, 2015).

[1] Oficial de Engenharia do Exército Brasileiro - Academia Militar das Agulhas Negras. Pós-graduado em Comunicações-EsCom. Pós-graduado em Operações Militares - Escola de Aperfeiçoamento de Oficiais. Pós-graduado em Inteligência Cibernética– Escola de Inteligência Militar do Exército. Fernandessilva.rafael@eb.mil.br

[2] Oficial de Comunicações do Exército Brasileiro - Academia Militar das Agulhas Negras. Pós-graduado em Operações Militares - Escola de Aperfeiçoamento de Oficiais. Pós-graduado em Inteligência Cibernética– Escola de Inteligência Militar do Exército. Ricardo.argolo@eb.mil.br

A abordagem de certos temas nas redes sociais acaba criando um grande volume de dados com potencial influência na formação de novos conflitos, principalmente os que culminam em criminalidade, violência, ou ações que afetem a ordem social (NASCIMENTO et al., 2015).

Uma das formas de se reunir informações é utilizando a disciplina de Inteligência OSINT (*Open Source Intelligence*). É a Inteligência baseada em informações coletadas de fontes de caráter público, tais como os meios de comunicação (rádio, televisão e jornais), propaganda de estado, periódicos técnicos, internet, manuais técnicos e livros (BRASIL, 2015).

Diante do exposto, e com base nos aspectos mencionados, chegou-se ao problema norteador deste trabalho: Ao esgotar as informações de coletas em fontes abertas (OSINT), como poderia se utilizar da Engenharia Social para potencializar a busca do dado protegido no E Ciber em proveito das ações de Inteligência Cibernética (CYBINT)?

A CYBINT é a Inteligência elaborada a partir de dados, protegidos ou não, obtidos no Espaço Cibernético. Realiza ações de busca e de coleta de informações para a produção do conhecimento de Inteligência (BRASIL, 2015).

Nesse contexto, um dos métodos que pode ser utilizado em proveito das ações de CYBINT é a Engenharia Social, que, de acordo com Rafael (2013) “é uma técnica muito utilizada por crackers[3] que buscam obter acesso a sistemas, redes ou informações que possuam valor estratégico para as organizações.”

Este trabalho visa apresentar a ferramenta S*ocial-Engineer Toolkit* (SET) como maneira de aplicar a Engenharia Social, explorando as fraquezas do ser humano, em proveito das ações de CYBINT.

Com a finalidade de responder o problema proposto, o presente estudo tem como objetivo geral verificar a funcionalidade da ferramenta SET e seu aproveitamento nas ações de CYBINT, utilizando o método de Engenharia Social por meio da técnica de *phishing*.

Para possibilitar a consecução do objetivo geral do estudo, foram formulados objetivos específicos, de forma a encadear logicamente o raciocínio descritivo apresentado neste trabalho:

a) Apresentar a definição de Engenharia Social segundo a literatura;

b) Esclarecer como a vulnerabilidade humana é um fator decisor na aplicação da Engenharia Social;

c) Explicar a técnica de *phishing*; e

d) Demonstrar a ferramenta S*ocial-Engineer Toolkit* e sua aplicabilidade na CYBINT;

O trabalho de natureza aplicada, valeu-se de pesquisa bibliográfica e exploratória relacionada ao tema, com uma abordagem qualitativa, sendo dividido em introdução, três capítulos de desenvolvimento e uma conclusão.

A Introdução aborda uma breve contextualização e os objetivos da pesquisa. O Capítulo 2, intitulado “A Engenharia Social”, versa sobre a revisão da literatura do

[3] Cracker utiliza o conhecimento em informática, computação e outras tecnologias para invadir sites, servidores, bancos de dados para ter ganho financeiro ou pessoal (BRASIL ESCOLA, 2021).

conceito de Engenharia Social, dando ênfase às vulnerabilidades humanas e explicando a técnica de *phishing*. O Capítulo 3, “O SET e a Exploração Cibernética”, relaciona a ferramenta com a capacidade operativa em questão que é ligada a CYBINT.

O Capítulo 4, denominado “A ferramenta *Social-Engineer Toolkit*” discorre sobre a demonstração da ferramenta SET. Finalizando, uma conclusão, na qual são recordados os aspectos mais importantes do artigo e são dissertados os resultados da pesquisa, demonstrando a importância que a Engenharia Social pode exercer na CYBINT.

2 A ENGENHARIA SOCIAL

De acordo com estudos realizados: a definição de Engenharia Social que melhor se aplica ao contexto do trabalho é:

> A ciência que estuda como o conhecimento do comportamento humano, pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de hipnose ou controle da mente, as técnicas de Engenharia Social são amplamente utilizadas por detetives (para obter informação) e magistrados (para confirmar se um declarante fala a verdade). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos (KONSULTEX, 2004 APUD PEIXOTO, 2006, p.4).

Para Mitnick e Simon (2003), “Engenharia Social é a habilidade de se manipular pessoas para obter informações necessárias para conseguir acessar um sistema, roubar dados de bancos ou qualquer outra coisa.”

De acordo com Hadnagy (2011), “Engenharia social é a arte ou, melhor ainda, a ciência, de habilidosamente manobrar seres humanos a realizar ações em algum aspecto de suas vidas.”

Verifica-se, então, que a utilização da Engenharia Social em proveito da CYBINT na busca do dado protegido é uma oportuna ferramenta que pode ser utilizada em seu benefício.

Com o conceito em mente, uma questão importante a ser ressaltada é que, independente do *software* ou *hardware* utilizado, o elemento de maior vulnerabilidade é o fator humano.

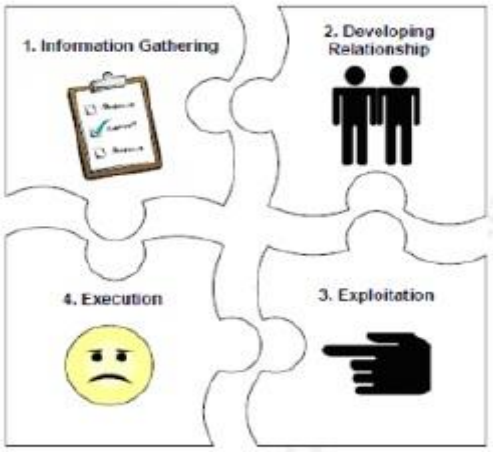
2.1 EXPLORAÇÃO DAS VULNERABILIDADES HUMANAS

A Engenharia Social assume diversas formas e pode ser compreendida como a “arte de enganar”. Não é apenas utilizada em sistemas informatizados é, também, usada para explorar falhas humanas nas organizações. Os ataques são ações que exploram a boa vontade das pessoas (MITNICK; SIMON, 2003).

Aproveitando-se dos aspectos psicológicos da mente humana e dos padrões de interação social entre as pessoas, possibilita-se que elas cumpram seus desejos. Os aspectos de interação humana, padrões de comportamento humano e estrutura social criam um estado de confiança com a vítima, tornando mais fácil de reunir informações e fazer a vítima executar alguma ação involuntária (HEIKKINEN, 2010).

Mitnick e Simon (2003) descrevem o Ciclo de Engenharia Social, como “quatro estágios distintos que são: a obtenção de informações, o desenvolvimento de relacionamento ou confiança, a exploração da confiança e a execução objetivando a realização”, conforme a figura 2.

Figura 1 – O Ciclo da Engenharia Social



Fonte: Allen (2007).

Diante do exposto, percebe-se que um dos elos mais fracos da segurança é o fator humano, uma vez que está sujeito a diversas condições que afetam o seu comportamento e dispõe de traços psicológicos que o deixam vulnerável a ações que se utilizam da Engenharia Social.

Junior (2006), e Silva (2012, p. 2) descrevem algumas destas características que são exploradas pela Engenharia Social:

a) Vontade de ser útil: o ser humano, geralmente, age com cortesia, procurar ajudar os outros quando necessário;

b) Busca por novas amizades: o ser humano costuma se agradar e sentir-se bem quando elogiado, ficando mais vulnerável e aberto a fornecer informações;

c) Vaidade: pode ser pessoal ou profissional. A identificação com argumentos que corroboram com a avaliação pessoal ou profissional gera aceitação espontânea e há uma receptividade e aceitação maior;

d) Autoconfiança: necessidade que os seres humanos têm de falar sobre o quanto é bom em realizar determinadas tarefas e ações, o quanto entende determinados assuntos; e

Devido à existência das redes sociais, onde é possível colher uma vasta gama de informações sobre o alvo, conhecê-lo melhor e traçar o seu perfil, percebe-se que há uma grande facilidade de explorar essas características de fragilidade.

Um dos maiores perigos da Engenharia Social é que os ataques não precisam funcionar contra todos. Uma única vítima bem-sucedida pode fornecer informações suficientes para acionar um ataque que afetará toda a organização. (CISCO, 2018).

É baseado nessas premissas da fraqueza humana que hoje uma das técnicas mais utilizadas da Engenharia Social é o *Phishing*, por isso o seu uso deve ser levado em consideração nas ações de exploração da CYBINT, em busca do dado protegido, quando se esgotam os recursos de coletas em fontes abertas.

2.2 O *PHISHING*

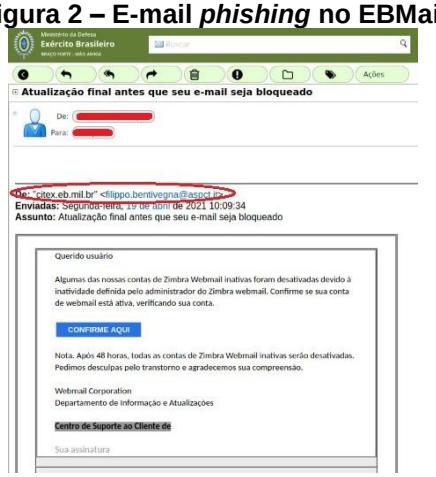
O *Phishing* pode ser considerado como uma das técnicas mais utilizadas para conseguir uma determinada informação. São e-mails falsos manipulados e enviados para pessoas e organizações, com o objetivo de fazer com que o usuário aceite o mesmo e realize as operações que são solicitadas (MAULAIS, 2016).

Comumente, são utilizadas páginas falsas, clonadas das reais; de instalação de códigos maliciosos de toda ordem, projetados para coletar informações sensíveis;

ou de preenchimento de formulários contidos na mensagem ou em páginas Web (CARDOSO; NUNES, 2020).

Trazendo o assunto para a realidade do Exército Brasileiro, um exemplo que ocorreu no ano de 2020, foi a disseminação, no EBMail[4] de diversos militares, de uma mensagem informando que seus dados de usuário (login e senha) deveriam ser atualizados, para que a conta de e-mail não fosse desativada de forma permanente.

Figura 2 – E-mail *phishing* no EBMail



Fonte: O autor.

O que ficou claro na utilização do *phishing* é a situação de urgência em que as vítimas foram colocadas, dessa forma, surge a necessidade por parte de alvo de resolver rapidamente o problema apresentado.

Segundo o site Agência Brasil (2021):

> Em 2020, o Brasil foi o país mais atingido por tentativas de roubo de dados pessoais ou financeiros de pessoas na internet, prática denominada em inglês de *phishing*. O percentual de usuários brasileiros que tentou abrir pelo menos uma vez *links* enviados para roubar dados representa 19,9% dos internautas do país. Em segundo lugar no *ranking* de países vem Portugal (19,7%), seguido da França (17,9%), Tunísia (17,6%), de Camarões (17,3%) e da Venezuela (16,8%).

3 O SET E A EXPLORAÇÃO CIBERNÉTICA

No Exército Brasileiro, de acordo com Brasil (2017), “As capacidades operativas (CO) da capacidade militar terrestre cibernética são três: a proteção cibernética, o ataque cibernético e a exploração”. Estas capacidades são descritas na tabela 3.

Tabela 3 – Capacidades operativas da capacidade militar terrestre cibernética

Capacidade Operativa	Descrição
Proteção Cibernética	Ser capaz de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente

[4] EBMail, e-mail corporativo do Exército Brasileiro.

Ataque Cibernético	Ser capaz de conduzir ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de computadores e de comunicações do oponente.
Exploração Cibernética	Ser capaz de conduzir ações de busca ou coleta nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados. Deve-se, preferencialmente, evitar que essas ações sejam rastreadas e sirvam para a produção de conhecimento ou para a identificação das vulnerabilidades desses sistemas.

Fonte: Brasil (2017).

Neste contexto, o Batalhão de Inteligência Militar (BIM), segundo Brasil (2017), “realiza a exploração cibernética em proveito da Força Terrestre Componente (FTC) apoiada. Conduz ações de proteção cibernética dos sistemas de informação da própria unidade.”

De acordo com Brasil (2019), “O produto da atividade de Inteligência é materializado, essencialmente, pelo conhecimento de Inteligência, cujo propósito básico é subsidiar a tomada de decisão, em todos os níveis.”

O uso do SET, orientado à exploração das vulnerabilidades humanas, em um contexto de Operações de Inteligência Militar, atua na capacidade operativa da exploração cibernética, visando a produção do conhecimento baseado no conteúdo buscado por meio das credenciais obtidas com a ferramenta, a fim de subsidiar a tomada de decisão.

4 A FERRAMENTA SOCIAL-ENGINEER TOOLKIT

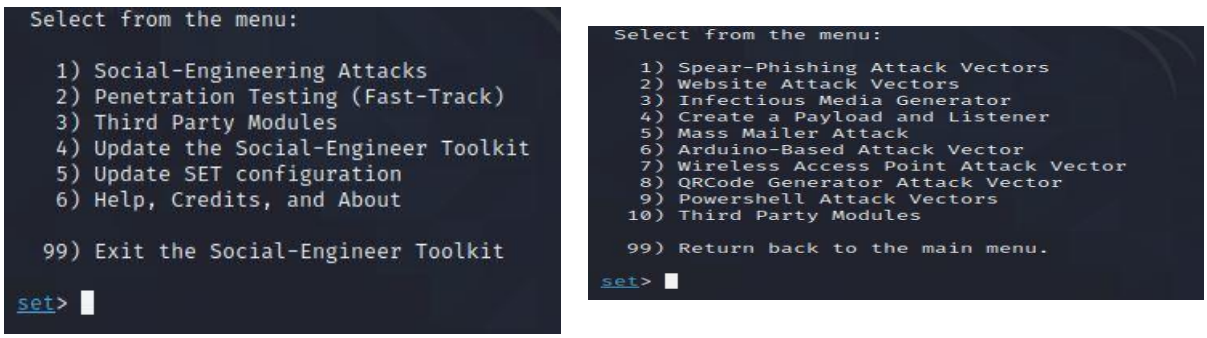
A distribuição *Kali Linux* traz nativamente a ferramenta de código aberto, baseada em Python, SET, que visa realizar explorações baseadas em Engenharia Social. (WEIDMAN, 2014).

Dentre as várias possibilidades do SET, o presente trabalho aborda a opção de clonagem de site e disparo de e-mails a fim de obter credenciais de interesse, utilizando a versão 2020.4 da distribuição *Kali Linux* e a versão 8.0.3 do SET.

4.1 INTERFACE DO SET

Para realizar explorações de engenharia social utilizando o SET, o usuário deverá digitar “*setoolkit*” no terminal do *Kali Linux*. Na tela inicial são exibidos os termos de uso do SET em que há um alerta em que os autores do software não se responsabilizam por danos diretos, indiretos, incidentais, entre outros e que a ferramenta deve ser utilizada para fins legais. Após aceitar os termos, a opção 1*, “Social-Engineering Atatacks”*, deverá ser selecionada. O Menu inicial e o submenu Social-Engineering Attacks do SET podem ser verificados nas figuras 3:

Figura 3 – Menu inicial SET (esquerda) e Submenu *Social-Engineering Attacks (direita)*



Fonte: O Autor.

Considerando o submenu Social-Engineering Attacks, neste trabalho serão utilizadas as opções 2 (*Website Attack Vectors*) e 5 *(Mass Mailer Attack*), que visam

a exploração por meio de clonagem de site e disparos de e-mail. Alguns dos métodos descritos por Weidman (2014, p. 311) da opção 2 podem ser inseridos na tabela 1.

Tabela 1 – *Website Attack Vecttors*

Método	Descrição
Credential Harvester Attack Method (Método de ataque para obtenção de credenciais)	Ajuda a **criar sites** para enganar os usuários de modo que eles forneçam suas credenciais
Tabnabbing Atack Method (Método de ataque com abas)	Conta com a propensão dos usuários em criar um conjunto de abas abertas no navegador. Quando o usuário abrir a página de ataque pela primeira vez, ela conterá "*Please wait*" (Por favor, espere). Naturalmente, o usuário irá tentar alternar para outra aba enquanto espera. Depois que a aba de ataque não estiver mais em foco, ela carregará o site de ataque (que pode ser um **clone de qualquer site** desejado), com o objetivo de enganar o usuário para que ele forneça suas credenciais ou interaja com o site malicioso. O pressuposto é que o usuário utilizará a primeira aba que encontrar que tiver uma aparência legítima

Fonte: Adaptado de Weidman (2014).

No método *"Credential Harvester Attack Method"* há 3 (três) opções: *Web Templates* (modelo web) que conta com modelos dos quais interessa os dos sites *Google* e *Twitter*; *Site Cloner* (clonador de site) efetua um clone de um site na web existente; e a opção *Custom Import* (importação customizada) se baseia em um site criado pelo próprio usuário.

Após selecionar o método, o usuário deve digitar o site ou selecionar o modelo, e em seguida escolher o endereço IP do site clone, sendo que se o objetivo for acessar da internet, o usuário deverá realizar configurações de redirecionamento de portas no roteador. Por fim, caso selecione a opção de clonar site diretamente da internet, basta digitar o site a ser clonado.

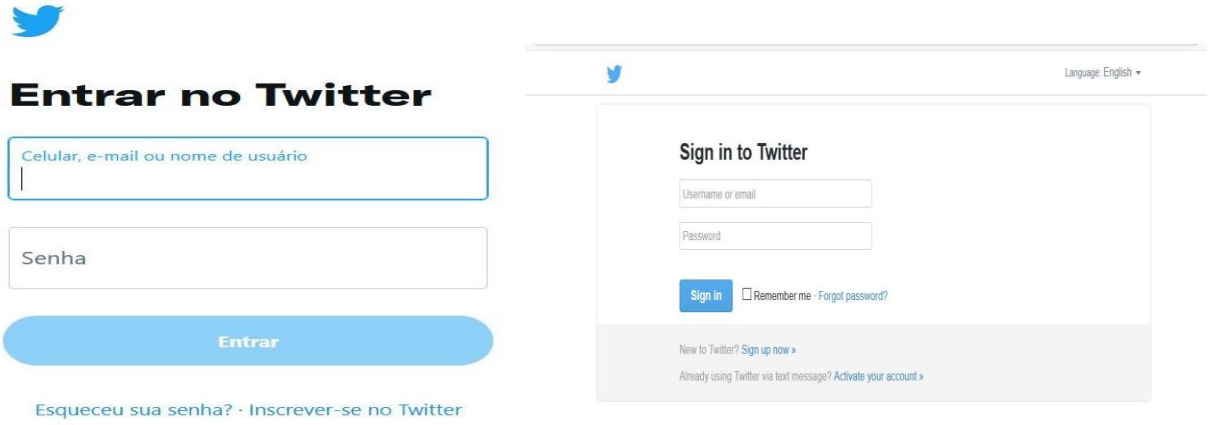
4.2 TESTES COM REDES SOCIAIS

Aprofundando nos modelos web, é possível verificar nas figuras 4 e 5 que os referentes aos sites *Google* e *Twitter* encontram-se desatualizados, sendo a imagem da esquerda o clone e da direita a original:

Figura 4 – Páginas Google

Fonte: O Autor.

Figura 5 – Páginas *Twitter*



Fonte: O Autor.

No clone do *Google*, o padrão do idioma é o inglês e está no modelo em que o login e senha são digitados na mesma página. No caso do Twitter, excetuando o idioma, as mudanças são mais discretas, porém perceptíveis.

Ao tentar realizar o clone do site da rede social *Instagram*, o resultado foi apenas uma página em branco, portanto inviável obter credenciais. No caso do *Facebook*, o resultado foi o seguinte:

Figura 6 – Clone *Facebook*

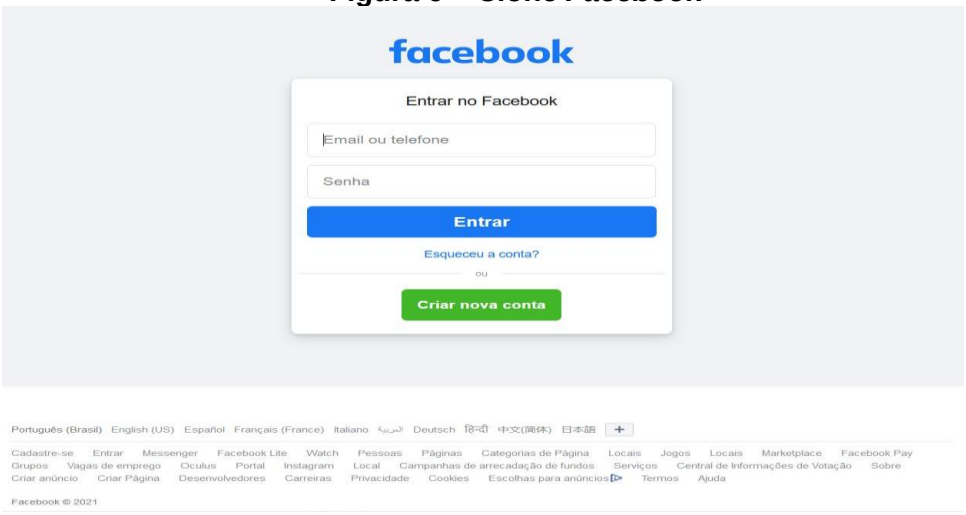
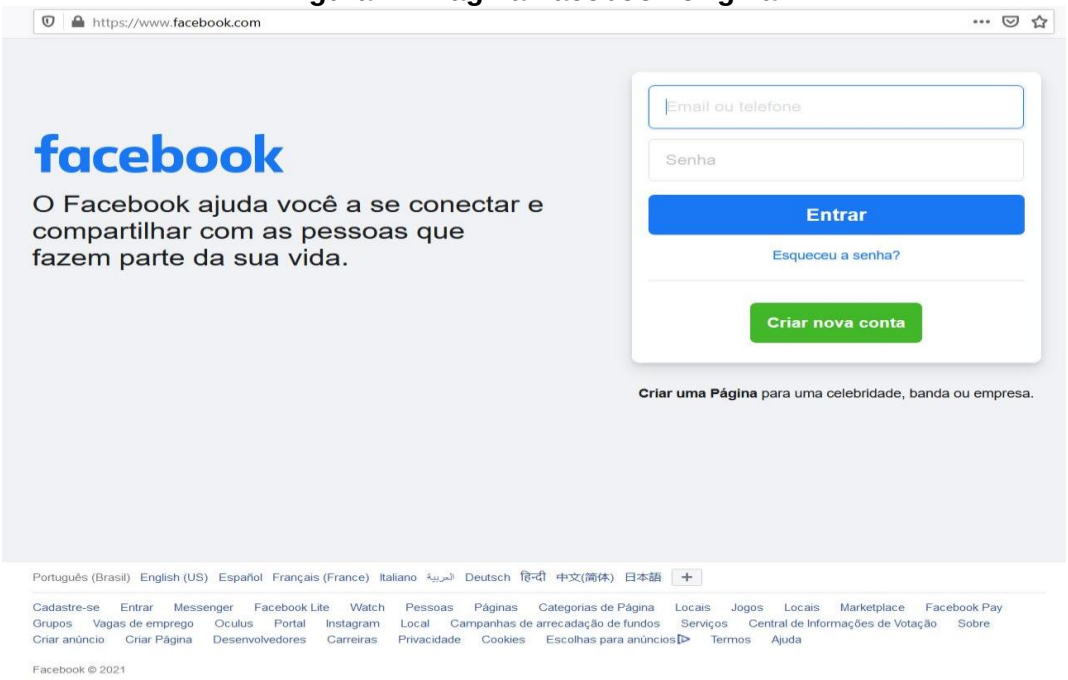


Figura 7 – Página Facebook original



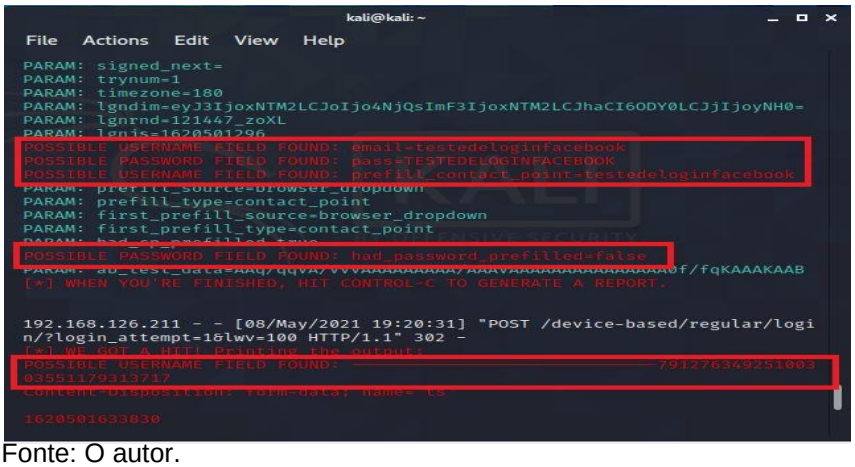
Fonte: O autor.

As diferenças entre as figuras 6 e 7 são basicamente observadas na posição do logotipo do *Facebook* que aparece na lateral da caixa de login. No entanto, ao digitar login e senha errados no site original, é exibida outra página com aparência semelhante ao clone da figura 6.

4.3 OBTENDO AS CREDENCIAIS

A exibição das credenciais pelo Terminal do *Kali Linux* pode ser observada na figura a seguir:

Figura 8 – Credenciais exibidas no SET



Fonte: O autor.

Os textos *"possible username field found"* (possível campo de nome de usuário encontrado) e *"possible password field found"* (possível campo de senha encontrado) indicam as possíveis credenciais digitadas pelo alvo. Vale destacar que são apresentadas falsas sugestões de usuário e senha, em que devem ser observados padrões para encontrar o verdadeiro.

Os resultados da tentativa de obter as credenciais das redes sociais *Twitter, Instagram, Facebook e Google*, no qual os resultados são exibidos de forma semelhante ao que consta na figura 8, podem ser resumidas na tabela 2.

Tabela 2 – Resultados do uso do SET em redes sociais

Site	Método	Exibição da página	Obtenção de credenciais
Twitter	Clone da página	Semelhante ao original (figura 5)	Foi possível obter login e senha (semelhante a figura 8)
	Modelo SET	Divergência de idioma e detalhes de posicionamento e formato da página (figura 5)	Foi possível obter login e senha (semelhante a figura 8)
Instagram	Clone da página	Não há	Não se aplica
	Modelo SET	Em branco	Não foi possível obter nenhuma credencial
Facebook	Clone da página	Página inicial com divergências na posição do logotipo, porém, semelhante após um erro de senha (figura 6)	Foi possível obter login e senha (figura 8)
	Modelo SET	Não há	Não se aplica
Google	Clone da página	Semelhante ao original (figura 4)	Foi possível obter apenas o e-mail, visto que as páginas de digitação do login e da são diferentes
	Modelo SET	Modelo de página antigo (figura 4)	Foi possível obter login e senha (semelhante a figura 8)

Fonte: O autor.

Conforme pode ser verificado na tabela, os melhores resultados foram obtidos através dos clones dos sites do *Twitter* e do *Facebook*. Para obter melhores resultados com o *Google* e *Instagram*, é possível utilizar o método importação customizada que requer habilidades de criação de páginas web.

As páginas criadas pelo SET são direcionadas para a página original após enviar o conteúdo digitado no formulário de login para o terminal do *Kali Linux*. Com isso, caso o alvo digite a credencial errada no clone do site, nas tentativas seguintes não será possível obter as credenciais.

Convém alertar que o planejamento da realização de *phishing* para obter credenciais deve atentar para o devido cuidado com a anonimização, de forma a dificultar a identificação dos autores. Entre as opções existem a rede TOR, Servidor Virtual Privado (VPS), Rede Privada Virtual (VPN), redes de acesso à internet alternativas, equipamentos exclusivos para a prática.

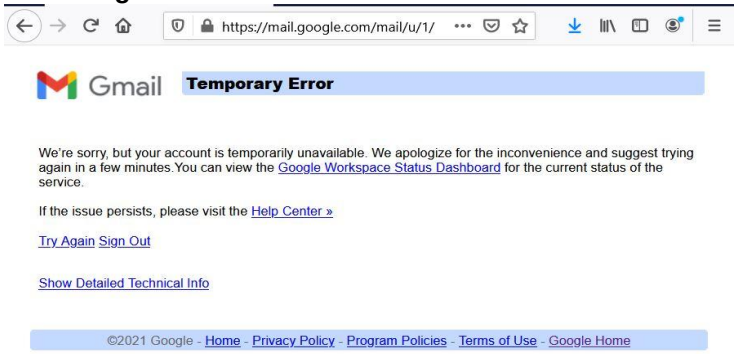
Os testes realizados foram apenas utilizando IP privado e sem servidor DNS, sendo facilmente percebido em uma situação real. É possível falsificar as entradas da cache do DNS (*Domain Name Service*), que correspondem aos mapeamentos entre nomes de domínio e endereços IP, de modo a encaminhar o tráfego destinado a um site para outro que possa ser controlado. O DNS mapeia (ou resolve) nomes de domínio como www.gmail.com para endereços IP (WEIDMAN, 2014).

4.4 DISPARO DE E-MAIL

Ao selecionar a opção 5 da figura 3, *Mass Mailer Attack,* o deve ser selecionada a opção 1 para e-mail individual, ou opção 2 para lista de e-mail. Seguindo na opção 2, para múltiplos destinatários, deve ser fornecido o caminho absoluto de um arquivo do tipo ".txt", que contenha os endereços de e-mail dos alvos. Após esta etapa, há a opção de utilizar uma conta do *Gmail* para o disparo das mensagens ou a utilização de algum servidor próprio de e-mail. Prosseguindo pela opção do *Gmail,* são fornecidos outros parâmetros como endereço de origem, senha, nome, assunto, anexo e o texto propriamente dito, em que é possível utilizar o formato HTML para a criação de links.

No teste realizado com a opção *Gmail*, a mensagem não chegou ao destino e a conta de e-mail tornou-se temporariamente indisponível, sendo exibida a página que conta na figura 9. Dessa forma, observa-se que a opção de utilizar um servidor de e-mail tende a ser mais viável.

Figura 9 – Erro ao acessar a conta do *Gmail*



Fonte: O autor.

Além dos resultados de disparos de e-mail acima, neste capítulo também foram testadas algumas funcionalidades do SET relacionadas ao clone de sites e disparos de e-mail, que tem a finalidade de obter credenciais por meio de *phishing*. Por meio da tabela 2 foram sintetizados os resultados dos testes em sites de redes sociais, de forma que o *twitter* e *facebook* apresentaram os melhores resultados ao possibilitar clones de sites semelhantes aos originais e com possibilidade de obter usuário e senha, visando obter informações úteis para produção do conhecimento de Inteligência.

5 CONCLUSÃO

Este trabalho teve como norte responder à pergunta: Ao esgotar as informações de coletas em fontes abertas (OSINT), como poderia se utilizar da Engenharia Social para potencializar a busca do dado protegido no E Ciber em proveito das ações de Inteligência Cibernética (CYBINT)?

Iniciando dela, o objetivo principal determinado foi o de verificar a funcionalidade da ferramenta SET, que se baseia na metodologia de Engenharia Social por meio da técnica de *phishing*, de modo a subsidiar o melhor aproveitamento das ações de CYBINT.

No decorrer da pesquisa, observou-se que algumas questões deveriam ser explicadas de forma a produzir o fundamento lógico e teórico para que se atingisse o objetivo proposto.

Diante do exposto, este trabalho abordou os conceitos de Engenharia Social com a finalidade de conhecer a metodologia utilizada para aplicação dessa técnica. Como consequência, percebeu-se que uma das vulnerabilidades que mais pode ser explorada é a fraqueza humana. Delimitou-se, ainda, na utilização do *phishing* como meio de empregar a Engenharia Social.

Face aos conceitos apresentados, verificou-se a aplicabilidade da ferramenta SET como proposta desta pesquisa, observando-se que é possível se obter credenciais de possíveis alvos utilizando tal metodologia, percebeu-se, porém, que o uso por si só da ferramenta não é suficiente, sendo necessário conhecer a ideia de como se trabalha a Engenharia Social no alvo e a fraqueza a ser explorada.

O uso da ferramenta SET com a finalidade de clonar sites demonstrou ser de simples utilização, facilitado por menus intuitivos. Nesta função, a ferramenta atendeu em parte as necessidades, tendo em vista que foi possível obter credenciais do *Facebook* e *Twitter*, porém, não foi possível clonar o site do Instagram, uma das principais redes sociais da atualidade. Além disso, o site do Google, por ter a página de digitação do usuário diferente da página da senha, restringiu a obtenção da credencial apenas do usuário, sem a senha.

Durante o uso da ferramenta, ela esteve bastante estável, rápida e não houve qualquer tipo de travamentos ou fechamentos inesperados. Por ser nativa no *Kali Linux*, é possível usar esse sistema diretamente em um pen drive, por exemplo.

Em suma, foi possível constatar que a ferramenta, no geral, atende às necessidades da busca do dado protegido, uma vez que se verificou a capacidade de se adquirir credencias. Dessa forma, a partir delas, é possível realizar explorações e monitoramentos no alvo, obtendo informações que auxiliarão na produção do conhecimento de Inteligência.

Para além do esforço de investigação, este trabalho foi mais um passo no desenvolvimento contínuo de aprendizado e crescimento, aliado ao conhecimento teórico adquirido ao longo da pesquisa.

REFERÊNCIAS

ALLEN, Malcolm. **Social Engineering:** A Means To Violate A Computer System. 2007. Disponível em: https://www.sans.org/readingroom/whitepapers/engineering/socialengineering-means-violate-computer-system-529 . Acesso em: 1 maio 2021.

AGÊNCIA BRASIL. **Brasil é o país com maior número de vítimas de phishing na internet**. 2021. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-03/brasil-e-o-pais-com-maior-numero-de-vitimas-de-phishing-na-internet. Acesso em: 1 maio 2021.

BRASIL. Exército Brasileiro. Estado-Maior do Exército. **Guerra Cibernética**. EB70-MC-10.232. Brasília, DF: 2017.

BRASIL. Exército Brasileiro. Estado-Maior do Exército. **Inteligência Militar Terrestre**. EB20-MF-10.107. Brasília, DF: 2015.

BRASIL. Exército Brasileiro. Estado-Maior do Exército. **Produção do Conhecimento de Inteligência**. EB70-MT-10.401. Brasília, DF: 2019.

BRASIL. PRESIDÊNCIA DA REPÚBLICA. Gabinete de Segurança Institucional. **Estratégia de segurança da informação e comunicações e de segurança**

cibernética da administração pública federal 2015-2018: versão 1.0 Brasília: Presidência da República, 2015.

CAETANO, Érica. **"O que é hacker?"**; Brasil Escola. Disponível em: https://brasilescola.uol.com.br/informatica/o-que-e-hacker.htm. Acesso em: 3 de abr. de 2021.

CARDOSO, Félix; NUNES, Daniel. **Proteção contra ataques de phishing no Exército Brasileiro**. Disponível em: http://www.ebrevistas.eb.mil.br/OC/article/view/6011. Acesso em: 3 maio 2021.

CISCO. **Protect Against Social Engineering**. 2018. Disponível em: https://www.socialengineer.org/wiki/archives/AttackersMightUse/Ciscosocial-engineering.html Acesso em: 30 abr. 2021.

HADNAGY, Christopher**. The Art of Human Hacking**. 1. ed. Indianapolis: Wiley Publishing, Inc, 2011.

HEIKKINEN, Seppo. **Social engineering in the world of emerging communication technologies**.2010. 1 – 10 p. Disponível em: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.451.9154&rep=rep1&type=pdf. Acesso em: 1 maio 2021.

JUNIOR, Guilherme. **Entendendo o que é Engenharia Social**. Disponível em:https://www.vivaolinux.com.br/artigo/Entendendo-o-que-e-Engenharia-Social. Acesso em: 1 maio 2021.

MAULAIS, Claudio Nunes dos Santos**. Engenharia Social:** técnicas e estratégias de defesa em ambientes virtuais vulneráveis. 2016. Projeto de Pesquisa (Mestrado em Sistema de Informação e Gestão de Conhecimento) – Universidade Fumec, Belo Horizonte, 2016.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**: ataques de hackers: controlando o fator humano na segurança da informação. São Paulo: Pearson Education, 2003.

NASCIMENTO, Durbens; BARRETO, Erick; MIRANDA, Wando. A Obtenção de Dados em Fontes Abertas na Atividade de Inteligência de Segurança Pública do Estado do Pará: Desafios e Possibilidades de sua Utilização. *In*: **Defesa e Criminalidade: Em Busca da Convergência para a Segurança**. Durbens Martins Nascimento [et al...] (organizadores). – Belém/PA. NAEA/UFPA, 2015. p 133 – 156

PEIXOTO, Mário C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

RAFAEL, Gustavo de Castro. **Engenharia social:** as técnicas de ataques mais utilizadas. 2013. In: Profissionais de TI. Disponível em: https://www.profissionaisti.com.br/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/. Acesso em: 1 maio 2021.

SILVA, Pedro A. Lemes da. **Análise de redes sociais aplicada à Engenharia Social**. 2012. Disponível em: http://repositorio.uninove.br/xmlui/handle/123456789/163. Acesso em: 30 abr. 2021.

TARAPANOFF, K. (Org.). **Inteligência organizacional e competitiva**. Brasília: Ed. Universidade de Brasília, 2001. 344 p.

WEIDMAN, Georgia. **Teste de Invasão:** Uma introdução prática ao hacking. São Paulo: Novatec, 2014.