INTERFACE TECNOLÓGICA

ATAQUES DE ENGENHARIA SOCIAL

SOCIAL ENGINEERING ATTACKS

Igor Henrique de Souza Tieso – igor.142@hotmail.com
Faculdade de Tecnologia (Fatec) – Taquaritinga – SP – Brasil

Felipe do Espirito Santo - felipe.santo@fatecq.edu.br
Faculdade de Tecnologia (Fatec) – Taquaritinga – SP – Brasil

DOI: 10.31510/infa.v17i2.947
Data de publicação: 18/12/2020

RESUMO

Este artigo tem o objetivo de compreender como funciona um ataque de engenharia social utilizando uma distribuição Linux, demonstrar o funcionamento das ferramentas usadas para os ataques, apresentar boas práticas que podem ajudar o usuário a ter uma segurança maior e se proteger dos ataques desse tipo, falaremos sobre os principais tipos de ataques utilizando engenharia social. A informação é um dos ativos com mais valor em uma organização, exatamente por isso também é o mais visado e cobiçado por pessoas más intencionadas que tem como objetivo roubar informações, uma vez compreendido o funcionamento de um ataque cibernético utilizando a engenharia social, podemos nos proteger e minimizar os riscos de sofrer um golpe e ter prejuízos tanto morais como financeiros. O trabalho consiste em uma revisão bibliográfica sobre o tema e apresentação de um exemplo de ataque de engenharia social sendo feito passo a passo, com a ferramenta SET, o objetivo é demonstrar a facilidade de operação dessas ferramentas e como o risco de sofrer um ataque deste tipo tem crescido exponencialmente nos últimos anos.

Palavras-chave: Kali Linux, Ataque de engenharia social, Segurança da informação**.** ferramenta SET

ABSTRACT

This article aims to understand how a social engineering attack works using Kali Linux, demonstrating how the tools used for the procedures work, presenting good practices that can help the user to be more secure and protect themselves from the types, we will talk about the main types of methods that occur frequently in our current society, they all use methods to deceive the victim, we are increasingly dependent and using more and more systems to improve our daily lives, such as bank applications for example, due to this frequent exposure of our personal information on the internet we need to address this issue that has been occurring frequently, harming millions of people a year, once we understand how a cyber attack using social engineering works, we can protect ourselves and minimize the risks of being hit and have both moral and financial losses. The work consists of a bibliographic review on the theme and presentation of an example of social engineering attack being done step by step using Kali

Linux with the SET tool, the objective is to demonstrate the ease of operation of these tools and how to risk suffering such an attack has grown exponentially in recent years.

Keywords: *Kali Linux. Social engineering attack. Security. Information. SET Tool.*

1 INTRODUÇÃO

Segundo Carvalho e Galvão (2016) hoje em dia a informação é um dos ativos com mais valor em uma organização, exatamente por isso também é o mais visado e cobiçado por pessoas mal intencionadas que tem como objetivo roubar informações, seja apenas por curiosidade, por diversão, para fins lucrativos, ou até mesmo por motivo de vingança, devido a essas causas, devemos cada vez mais nos atentar e se preocupar com a segurança das nossas informações, tanto nas empresas como dentro de nossas casas, pois uma informação valiosa nas mãos de um *Hacker* ou *Cracker* pode levar a falência de uma empresa com anos de mercado, e até mesmo prejudicar a vida pessoal de quem for atacado.

As empresas concentram sua atenção em softwares de segurança, atualizando frequentemente esses *softwares*, utilizando recursos cada vez mais modernos. Essas tecnologias realmente são essenciais para uma boa proteção, mas não apenas isso, as empresas acabam esquecendo que o ser humano é falho, nesse ponto que entra a engenharia social, utilizando métodos que tiram vantagem e proveito da sua vítima, um *hacker* com essa habilidade consegue explorar os sentimentos da sua vítima, utilizando isso contra elas mesmas.

Nesse artigo falaremos sobre os principais tipos de ataques cibernéticos que ocorrem frequentemente na nossa sociedade atual, muitos deles utilizam métodos para enganar a vítima, estamos cada vez mais dependentes e utilizando cada vez mais os sistemas para melhorar nosso dia a dia, como aplicativos de banco por exemplo, devido a essa exposição frequente de nossas informações pessoais na internet precisamos abordar esse assunto que vem ocorrendo frequentemente, prejudicando milhões de pessoas por ano, uma vez entendendo como funciona um ataque cibernético utilizando a engenharia social, podemos nos proteger e minimizar os riscos de sofrer um golpe e ter prejuízos tanto morais como financeiros.

2 ENGENHARIA SOCIAL

Engenharia social é um termo usado para descrever um método utilizado de fazer um ataque, esse método é aplicado constantemente em diversas áreas. De acordo com Mann (2011) e Thomas (2007) o alvo desse ataque precisamente é o ser humano, já que o ser humano é o elo mais fraco na segurança de uma empresa, por isso ataques de engenharia social vem crescendo cada vez mais no brasil.

"Nos últimos três meses do ano, foram registrados 63,8 milhões de links maliciosos, um aumento de 12% em relação ao começo do ano. O documento mostra que o campeão de golpes são os links em apps de mensagem como WhatsApp" (WAKKA, 2017, n.p).

A engenharia social é um método muito eficaz, resume em basicamente enganar a vítima, criar uma familiaridade, abusando da sua inocência e da confiança, o atacante consegue explorar várias áreas do sentimento humano para fazer o ataque, como por exemplo, a curiosidade, onde a vítima recebe um *link* e por curiosidade e inocência acaba entrando no *link* sem saber que se trata de um *link* malicioso, muitas vezes em uma empresa, o atacante escolhe como alvo algum funcionário que tem acesso ao sistema, através de várias ferramentas e métodos, conseguindo assim adquirir informações que podem dar acesso ao sistema.

3 PRINCIPAIS TIPOS DE ATAQUE DE ENGENHARIA SOCIAL

3.1 PHISHING

Phishing é uma técnica comum e muito utilizada por *hackers* e *crackers,* esse ataque é simples e pode ser enviado para milhões de pessoas, esse ataque frequentemente consiste em um *e-mail* falso se passando por um *e-mail* real, com um arquivo anexado pedindo para atualizar informações ou senhas, como um *e-mail* de banco por exemplo, onde os detalhes são bem arquitetados e a vítima não consegue diferenciar que se trata de um *e-mail* falso. Muitas das vezes o texto escrito na mensagem é um alerta para problemas financeiros ou algo que chame a atenção da vítima, induzindo à baixar algum arquivo em um anexo para sanar o problema, assim infectando o computador. "Golpes de *phishing* com páginas que fingem ser plataformas como *Zoom*, *Google Meets e Microsoft Teams* estão cada vez mais comuns — surfando na onda

da realização dessas reuniões online por causa da pandemia do novo coronavírus" (TECHMUNDO, 2020, n.p).

Segundo Kleverson (2019) o *clone phishing* é outro segmento do *phishing* muito utilizada é a de sites falsos, que são muito parecidos com os sites legítimos, basicamente o golpista envia um *link* falso de um site que a vítima acessa frequentemente, mascarando o IP do *link* para parecer um site legítimo, nesse site a vítima faz *login* normalmente, porém o *login* e a senha foram enviados para o golpista, este tipo de ataque ocorre frequentemente, depois de enviado a vítima é direcionada automaticamente para o site real, e acaba não percebendo que foi vítima de um ataque cibernético.

3.2 SPEAR PHISHING

O *Spear Phishing* é outro segmento do *Phishing*, porém é mais perigoso, pois esse tipo de ataque cibernético tem um alvo específico, é um ataque direcionado , com foco em empresas e organizações, o ataque ocorre praticamente da mesma forma que o *phishing*, porém como ele tem uma vítima específica ele é mais elaborado nas abordagens, é um ataque personalizado. Um caso que ficou famoso ocorreu na eleição presidencial de 2016 nos Estados Unidos, segundo o site Gatefy (2020, n.p)

> Um dos casos mais emblemáticos de engenharia social é a eleição presidencial dos Estados Unidos em 2016. Ataques de *Spear phishing* levaram ao vazamento de e-mails e informações do Partido Democrata que podem ter influenciado o resultado da eleição, com a vitória de Donald Trump sobre Hillary Clinton.
> Os *hackers* criaram um *e-mail* falso no *Gmail*, convidando os usuários, por meio de um *link*, a alterar as suas senhas devido a atividades incomuns. Os fraudadores então tiveram acesso a centenas de *e-mails* contendo informações confidenciais sobre a campanha de Clinton.

3.3 VISHING

Segundo o site Kaspersky (s.d), o *Vishing* também um tipo de *Phishing*, basicamente utiliza o mesmo conceito e estratégia, só que sua aplicação ocorre juntamente com mensagens de texto via SMS, seu objetivo principal é adquirir números de cartão de crédito e informações para roubo de identidade das vítimas sem que ela perceba que se trata de um golpe, se passando por uma empresa real. A vítima recebe um SMS que supostamente teria sido enviado por um banco, geralmente essas mensagem está dizendo que a conta está sendo cancelada ou suspensa, pedindo uma autorização para poder ativar novamente a conta através de uma ligação para outro número, mas na verdade esse outro número é um sistema automatizado de atendimento que pede para a vítima confirmar as informações pessoais e os dados do cartão de crédito, nesse momento a vítima cai no golpe e acaba tendo seu cartão de crédito clonado. Especialistas em segurança cibernética preveem que os ataques de *phishing* em correio de voz, também conhecidos como *Vishing*, podem se tornar corriqueiros em 2020. Pesquisa sobre ameaças conduzida pela Mimecast, especializada em gerenciamento de *e-mail* baseado em nuvem, incluindo serviços de segurança, descobriu que as mensagens maliciosas de correio de voz não estavam apenas aumentando, mas evoluindo e com mais nuances do que nunca. (CISOADVISOR, 2019).

3.4 Pretexting

Outro segmento do Phishing é o Pretexting, o *Pretexting* é um método de ataque também muito utilizado por *hackers*, este tipo de ataque cibernético consiste em elaborar uma falsa situação para induzir a vítima a disponibilizar acesso às informações do sistema, identificando-se para a vítima geralmente como alguém com cargo superior ao dela, assim a vítima acaba sendo coagida e intimidada, segundo (PROOF, 2019)Para se informar e decidir por quem o atacante deve se passar para fazer o ataque normalmente são utilizadas as redes sociais para analisar o perfil da vítima, descobrindo dados importantes como por exemplo, onde a vítima frequenta, onde trabalha, a função dentro da empresa, os familiares, amigos, colegas de empresa, entre outras informações que nas mãos de um criminoso que especialista em *Pretexting* pode ser crucial para fazer um ataque efetivo, com todas essas informações adquiridas sem muito esforço, o atacante pode simplesmente mandar um *e-mail* para a vítima se passando por um familiar ou chefe, e solicitar o que deseja, muitas das vezes a vítima não percebe que se trata de um golpe cibernético e cede as informações para o criminoso.

3.5 QUID PRO QUO

O *Quid Pro Quo* é uma palavra do latim que significa “algo por algo”, o *hacker* oferece para sua vítima algo em troca de uma informação, que no caso seria informações específicas para consolidar o ataque. Geralmente o método usado pelos criminosos quando vai iniciar o ataque a uma empresa, é se passar por uma pessoa da área de tecnologia da empresa e fazer contato por *e-mail*, telefone, chamadas de vídeo, com várias pessoas de dentro da empresa até encontrar uma pessoa que está com algum problema real no computador, no caso esse é o alvo (MEUPOSITIVO, 2018).

Então o *hacker* mantém contato com a vítima e inicia uma conversa, a vítima acha que está realmente falando com alguém da área de suporte de TI da empresa, então concede o acesso da sua máquina ao *hacker*, uma vez dentro do sistema da vítima, o *hacker* juntamente com a vítima começa a modificar o sistema da empresa, desabilitando antivírus, e programas essenciais para a segurança do sistema da empresa, instalando *trojans*, *malwares*, e a vítima continua pensando que estão procurando soluções para o problema real que ela tinha antes, quando na verdade está facilitando a invasão de um criminoso.

4 METODOLOGIA

Para o desenvolvimento deste artigo foi realizado um levantamento bibliográfico por meio de pesquisas em sites especializados, artigos e livros sobre o assunto, durante o processo de levantamento bibliográfico a ferramenta SET foi selecionada para uma demonstração prática da clonagem de um site que será apresentada na sequência.

5 SIMULAÇÃO DE UM ATAQUE DE PHISHING COM UM SITE FALSO

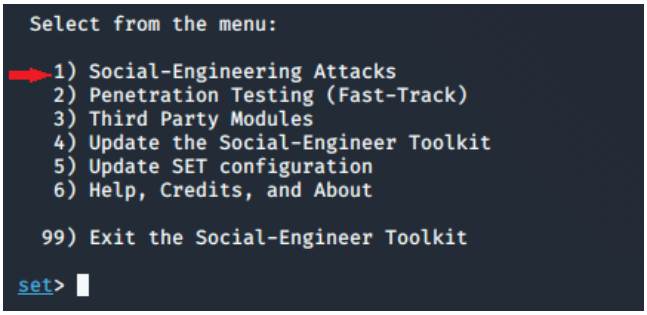
Neste exemplo será demonstrado uma simulação de como é simples fazer um site falso para poder enganar uma vítima, utilizando o sistema operacional Kali Linux. Segundo o site TerminalRoot (2019) o Kali é um sistema operacional muito utilizado por *hackers*, pois nele vem instalado bastante ferramentas de ataque, pentest, entre outras.

O *Kali Linux* é um sistema especializado e utilizado para testes de segurança, desenvolvido *pela Linux* baseado em *Debian*, para instalar o *Kali Linux* , é preciso de no mínimo 20 GB de espaço em disco, com o CD do software em mãos, após inserir no computador e iniciar a instalação, escolha a opção *Graphical Install*, escolha o idioma, especifique o seu idioma local, o instalador irá copiar a imagem para o seu disco rígido, e fazer teste, informe um nome para o sistema, defina o seu fuso horário, e também tem a opção para particionar o disco, fazer manualmente é um pouco mais complicado, recomendado para usuários experientes, o melhor a se fazer é deixar todos os arquivos em uma única partição, após o fim da instalação já com o sistema operacional funcionando.(TRENTINO,F ,2019).

Utilizando a ferramenta *Social-Engineer Toolkit* (SET) podemos escolher várias opções diferentes, testes, avaliações, porém o é para executar os comandos é e conseguir utilizar corretamente as ferramentas é necessário saber usar o prompt de comando, pois as ferramentas a maioria não tem interface gráficas, mas vamos falar dos ataques de engenharia social, que é o foco do assunto.

O primeiro passo é selecionar a opção 1 (*Social-Engineering Attacks*), esta opção nos levará a um outro menu com vários outros tipos de ataques de engenharia social (Autoria própria, 2020).

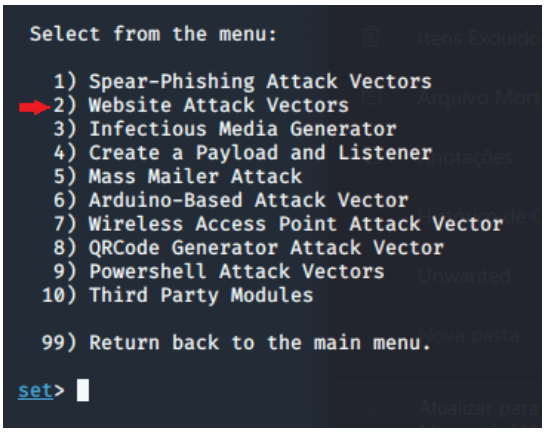
Figura 1. Selecionando Social-Engineering Attacks



Fonte: Autoria própria (2020)

Segundo passo é selecionar a opção número 2 (*Website Attack Vetors*), que nos proporcionará opções de ataque com website.

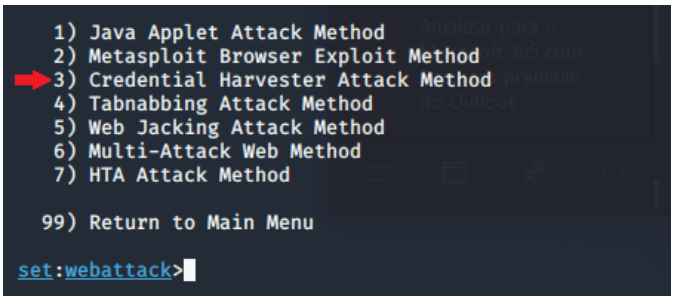
Figura 2. Selecionando Website Attack Vectors



Fonte: Autoria própria (2020)

Terceiro passo é selecionar a opção número 3 (*Credential Harvester Attack Method*), este método baseia-se em clonar um site com todas as características de um site real.

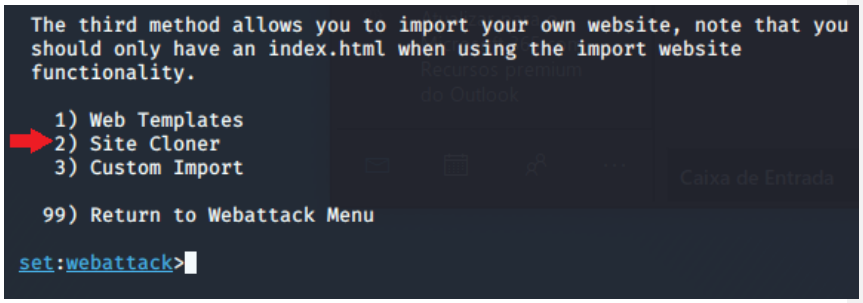
Figura 3. Selecionando Credential Harvester Attack Method



Fonte: Autoria própria (2020)

Em seguida selecionaremos a opção número 2 (Site Cloner)

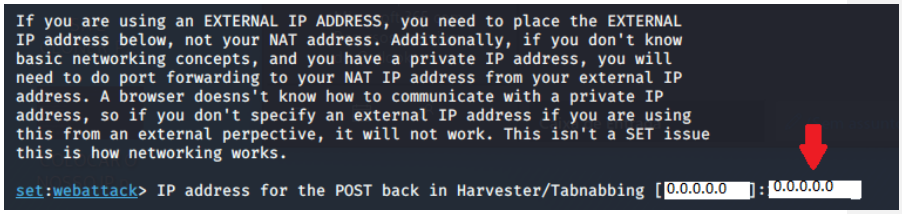
Figura 4. Selecionando Site Cloner



Fonte: Autoria própria (2020)

Feito isso, a ferramenta irá pedir para inserirmos um IP, as informações da vítima que acessar nosso site clone serão enviadas para este IP, então no caso teria que ser o seu IP.

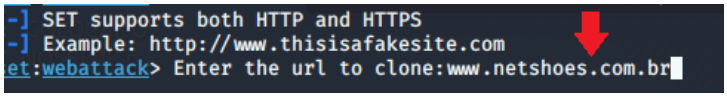
Figura 5. Colocando IP



Fonte: Autoria própria (2020)

Em seguida a ferramenta pedirá para inserir a URL do site que será clonado, o site pode ser da sua escolha, os hackers tendem a escolher sites bastante populares que são usados frequentemente, no caso eu escolhi a Netshoes.

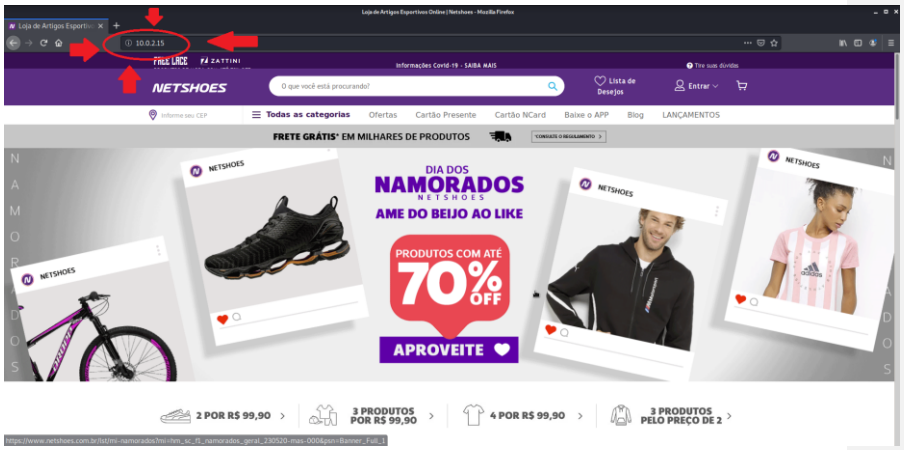
Figura 6`. Informando nome do site que será clonado



Fonte: Autoria própria (2020)

Em seguida, basta digitar no seu navegador o mesmo número de IP que você informou anteriormente, e abrirá o site clone.

Figura 7. Site Clonado



Fonte: Autoria própria (2020)

Repare que visualmente o site é idêntico ao site real, porém a URL (endereço do site) está aparecendo como um número de IP, porém isso também pode ser mascarado e alterado pelos *hackers*, para garantir que o usuário não consiga detectar que está utilizando um site falso.

Segundo Paulo Alves (2019) para verificar a autenticidade de um site, saber se ele é falso, existem algumas dicas importantes que podem ajudar e muito, conferir o link de domínio do site é sempre importante, pois sites clones costumam colocar nomes parecidos, exemplo: www.netfliix.com, no caso muita gente acaba não reparando que existe uma letra “i” a mais na palavra.

6 CONCLUSÃO

O objetivo proposto no trabalho foi atingido, a revisão bibliográfica proposta colaborou para a compreensão dos diferentes tipos de ataques de engenharia social e a demonstração prática de como um ataque desse tipo é realizado. O trabalho possibilitou demonstrar práticas que podem ajudar o usuário a não cair em golpes nesse formato.

Na sociedade moderna, as questões de segurança tornaram-se muito importantes. Apesar disso, muitas organizações esqueceram que seus próprios recursos humanos estão no centro da maioria das violações de segurança. Entre as práticas de ataque está a engenharia social, que encontrou uma grande terreno para ser explorado.

Não se trata somente de proteger nossos equipamentos tecnológicos com programas de antivírus ou apenas formatando nossos computadores, as pessoas devem saber como o invasor se comporta, pois um simples convite do *Facebook* pode comprometer a segurança do sistema, o exemplo de ataque apresentado neste artigo reforça essa fala ao demonstrar que um usuário mesmo sem um conhecimento profundo de programação poderia clonar um site para capturar dados de autenticação.

O sistema de segurança não está relacionado apenas à tecnologia em si, mas também ao processos por trás dela. Diante do exposto, por mais avançada que seja a tecnologia, ela de nada servirá se os fatores humanos não forem considerados e preparados. É preciso conscientizar as pessoas de que elas podem estar sendo observadas e que podem acabar se tornando um alvo potencial para engenheiros sociais, assim prejudicando a ela mesma e a empresa em que trabalha.

Trabalhos futuros poderiam observar como um grupo de usuários visualizam, ou não, que um site clonado através de ferramentas como o SET é um site falso e que eles deveriam sair antes de entrar com qualquer dado pessoal.

REFERÊNCIAS

ALVES, P. Sete dicas para descobrir se um site é falso e evitar golpes online. 25 mar.2019. Disponível em: <https://www.techtudo.com.br/listas/2019/03/sete-dicas-para-descobrir-se-um-site-e-falso-e-evitar-golpes-online.ghtml>. Acesso em: 02 set.2020.

BOCANEGRA, J. Spear phishing: técnica deu a hackers dados sobre a campanha de Hillary. 24 jul.2018. Disponível em:< https://exame.com/mundo/spear-phishing-tecnica-deu-a-hackers-dados-sobre-a-campanha-de-hillary/>. Acesso em: 19 mai.2020.

CISOADVISOR (ed.). Ataques de vishing devem se tornar comuns em 2020. São Paulo, 21 nov. 2019. Disponível em: https://www.cisoadvisor.com.br/ataques-de-vishing-devem-se-tornar-comuns-em-2020/. Acesso em: 20 maio 2020.

GALVÃO, A. Engenharia social: uma análise de ameaças e cuidados aos funcionários das agências bancárias de santarém e itaituba - pará. Abril.2016. Disponível em:< https://www.researchgate.net/publication/319551455_ENGENHARIA_SOCIAL_UMA_ANALISE_DE_AMEACAS_E_CUIDADOS_AOS_FUNCIONARIOS_DAS_AGENCIAS_BANCARIAS_DE_SANTAREM_E_ITAITUBA_-_PARA>. Acesso em: 13 set.2020.

KASPERSKY (ed.). O que é vishing?. Brasil. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/vishing. Acesso em: 13 set. 2020.

KLEVERSON, K. o que é pishing e como se proteger de golpes na internet. 22 jan.2019. Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-phishing-e-como-se-proteger-de-golpes-na-internet/#:~:text=Geralmente%2C%20ao%20acessar%20o%20site,sem%20perceber%20que%20foi%20v%C3%ADtima>.Acesso em: 13 set.2020.

MEUPOSITIVO, Golpes de engenharia social: os 6 principais para ficar de olho. 6 jun.2018. Disponível em: <https://www.meupositivo.com.br/panoramapositivo/golpes-de-engenharia-social/>. Acesso em 18 mai.2020.

OLIVEIRA, R. Idosa perde mais de R$ 9 mil no golpe do falso sequestro. 27 mai.2020. Disponível em:< https://cgn.inf.br/noticia/idosa-perde-mais-de-r-9-mil-no-golpe-do-falso-sequestro>. Acesso em: 28 mai.2020.

PAIS, et.al. Engenharia social (ou o carneiro que afinal era um lobo).2013. Disponível em:< http://repositorio.uportu.pt/jspui/bitstream/11328/1347/1/144%20LivroEGP%20-%20EngenhariaSocial.pdf>. Acesso em: 31 mai.2020.

PROOF (São Paulo) (ed.). Ataques de Engenharia Social: tudo que você precisa saber!. São Paulo, jan. 2019. Disponível em: https://www.proof.com.br/blog/ataques-de-engenharia-social. Acesso em: 21 maio 2020.

ROCHA, D. Engenharia social: compreendendo ataques e a importância da conscientização. Disponível em:<https://gatefy.com/pt-br/postagem/7-casos-reais-de-ataques-de-engenharia-social/>. Acesso em: 19 mai.2020.

SEGINFO. Conheça o SET: Social-Engineer Toolkit. 22 set.2010. Disponível em:< https://seginfo.com.br/2010/09/22/conheca-o-set-social-engineer-toolkit-2/#:~:text=O%20Social%20Engineering%20Toolkit%20%C3%A9,ataques%20relacionados%20%C3%A0%20engenharia%20social.&text=Social%2DEngineer%20Toolkit%20(SET),from%20David%20Kennedy%20on%20Vimeo.>. Acesso em 2 jun.2020.

TECHMUNDO, Novo golpe finge ser link para videoconferência e rouba seus dados. 12 maio.2020. Disponível em: <https://www.tecmundo.com.br/seguranca/153035-novo-golpe-finge-link-videoconferencia-rouba-dados.htm>. Acesso em: 18 mai.2020

TERMINALROOT. As 22 Melhores Distros Linux para Hackers (Pentesting). 18 dez.2019. Disponível em: <https://terminalroot.com.br/2019/12/as-22-melhores-distros-linux-para-hackers-

pentesting.html#:~:text=Kali%20Linux,digital%20e%20teste%20de%20invas%C3%A3o.>. Acesso em: 02 set.2020.

WAKKA, W. Número de ataques cibernéticos no Brasil quase dobrou em 2018. 07 ago.2018. Disponível em: <https://canaltech.com.br/seguranca/numero-de-ataques-ciberneticos-no-brasil-quase-que-dobrou-em-2018-119600/>. Acesso em: 15 mai. 2020

TRETINO, F. Como instalar passo a passo o Kali Linux 2019. 31 jan.2019. Disponível em: https://sempreupdate.com.br/como-instalar-passo-a-passo-o-kali-linux-2019/. Acesso em: 01/12/2020.

Formatado: Sublinhado