Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

PRISCILA YONE FUJII

TESTE DE VULNERABILIDADE DE SISTEMAS: ASPECTOS SOBRE A ENGENHARIA SOCIAL

Assis/SP
2022

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

PRISCILA YONE FUJII

TESTE DE VULNERABILIDADE DE SISTEMAS: ASPECTOS SOBRE A ENGENHARIA SOCIAL

Projeto de Conclusão de Curso apresentado ao curso de Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando (a): Priscila Yone Fujii
Orientador (a): Prof. Fábio Eder Cardoso

Assis/SP
2022

FICHA CATALOGRÁFICA

PRISCILA, Yone Fujii.
Teste de vulnerabilidade de sistemas: aspectos sobre a engenharia social / Priscila Yone Fujii. Fundação Educacional do Município de Assis - FEMA - Assis, 2022.
55p.

Orientador: Prof. Me. Fábio Eder Cardoso
Trabalho de Conclusão de Curso - Instituto Municipal de Ensino Superior de Assis - IMESA

1.Engenharia Social. 2. Phishing. 3. Segurança da Informação

TESTE DE VULNERABILIDADE DE SISTEMAS: ASPECTOS SOBRE A ENGENHARIA SOCIAL

PRISCILA YONE FUJII

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador:

Prof. Me. Fábio Eder Cardoso

Examinador:

Prof. Dr. Luiz Carlos Begosso

Assis/SP
2022

RESUMO

Ainda que muitos de nós estejam familiarizados com a utilização da Internet devido ao trabalho, estudos ou lazer, existem pessoas, geralmente idosos, que não conseguem ter tanta facilidade no seu uso. Pessoas sem conhecimento algum sobre tecnologia da informação, às vezes, se deixam enganar por golpes, ligeiramente modificados, que ao longo do desenvolvimento tecnológico migraram para Internet. No entanto, os riscos que todas as pessoas correm, independentemente de ser usuário da tecnologia informática ou não, é a Engenharia Social. A Engenharia Social pode ser efetuada através de sites fraudulentos, como uma propaganda enganosa ou um aviso de recadastramento de dados. No entanto, não depende apenas de ferramentas tecnológicas ou da própria Internet, mas principalmente da confiança das pessoas. Por esse motivo, o fator humano é considerado o elo mais fraco dentro do sistema de segurança. Com o intuito de informar as pessoas e conscientizá-las de que os riscos à segurança da informação não estão restritos apenas ao fator tecnológico, mas também ao fator humano. Como método explicativo, neste trabalho é realizado um ataque de *phishing* em ambiente virtualizado. E para esse propósito, foram utilizadas ferramentas como *Virtual Box*, sistema operacional *Kali Linux*, sistema operacional *Linux Mint* e a ferramenta de penetração *Social Engineering Toolkit* (SET).

Palavras-chave: Engenharia social; *phishing*; Segurança da informação.

ABSTRACT

Although many of us are familiar with using the Internet due to work, study, or leisure, there are people, usually the elderly, who are not so easy to use. People without any knowledge of information technology sometimes get fooled by scams, slightly modified, which over the course of technological development have migrated to the Internet. However, the risk that all people run, regardless of whether they are users of information technology or not, is Social Engineering. Social Engineering can be carried out through fraudulent websites, such as a misleading advertisement or a re-registration notice. However, it does not depend only on technological tools or the Internet itself, but mainly on people's trust. For this reason, the human factor is considered the weakest link in the security system. In order to inform people and make them aware that information security risks are not only restricted to the technological factor, but also to the human factor. As an explanatory method, in this paper a phishing attack is carried out in a virtualized environment. And for this purpose, tools such as Virtual Box, Kali Linux operating system, Linux Mint operating system and the penetration tool Social Engineering Toolkit (SET) were used.

Keywords: Social Engineering; phishing; Information Security.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

Qualquer pessoa está sujeita a algum tipo de ataque, seja um funcionário de cargo importante, ou um comerciante que iniciou recentemente seu negócio online. Dito isso, o conselho dado por especialista, em geral, são: criação de mídia para backup, atualizar o sistema e aplicativos periodicamente e desconfiar de links enviados em mensagem por supostos amigos. Grande parte das pessoas que têm o costume de realizar backups utilizam mídias como CD, pendrive e HD externo. Mas estas mídias não estão livres de malwares e podem ser corrompidas igualmente que os arquivos no computador. Além disso, alguns desses malwares são desenvolvidos especificamente para serem ativados em determinadas condições, ou que se alojam em partes do dispositivo como teclado e entrada USB. No ano de 2016 foi identificado o USB Thief, um malware derivado do cavalo de Tróia[1].

Segundo Stancik (2016), o USB *Thief* é um cavalo de Tróia baseado em USB e, assim como vírus, sua execução é automática. Quando o usuário do computador insere o dispositivo USB infectado, por exemplo *pendrive*, o *Thief* localiza os dados e aplicativos compatíveis no próprio sistema e basta que o usuário execute um destes aplicativos para que o *Thief* execute em segundo plano. No entanto, este *malware* reside somente em dispositivos USB e seus criadores criaram um mecanismo de criptografia garantindo que não seja detectado facilmente, portanto não deixa rastros aparentes.

Quando se trata de *backup* para empresas de pequeno até grande porte, elas costumam utilizar um servidor dedicado a esse propósito. Apesar das pessoas utilizarem os serviços de *backup* online, isso só significa que os dados não estão armazenados em suas mídias de fácil acesso, nem em seu dispositivo, mas em um servidor dedicado dentro da empresa que prestadora desse tipo de serviço.

Ao utilizar o serviço para *backup online* o usuário está se prevenindo de ataques como Tróia e *ransomware*[2], pois a segurança de dados deve estar incluída no serviço prestado. No entanto, outro ataque pode acontecer permitindo o acesso do *hacker* aos dados de *backup online*. O *hacker* pode se passar pelo usuário utilizando suas credenciais. Este tipo de ataque é conhecido como *phishing*, no qual o *hacker* disponibiliza um *site* fraudulento para que o usuário digite as informações necessárias para acessar a mídia de

[1] Tipo de *malware* que no momento de sua instalação, encobre a instalação conjunta de outros *softwares* sem o consentimento do usuário.
[2] *Malware* que encripta todos os arquivos e impede o livre acesso do usuário a eles.

backup online, além de outros serviços importantes como *Internet banking*, mas na verdade elas são enviadas para o *hacker*.

Mesmo com esforços no desenvolvimento tecnológico para inibir ou, no mínimo, mitigar os ataques, outro fator pode ser considerado mais preocupante e vulnerável. Este é o fator humano, que sofre ataques de manipulação e, mesmo sem intenção, a vítima acaba realizando atos que permitem o *hacker* ter mais vantagem no seu ataque.

Para efetuar um ataque o *hacker* não precisa de ferramentas sofisticadas da tecnologia como a maioria pode pensar, alguns *hackers* com mais experiência na arte da manipulação utilizam a técnica da engenharia social. Essa técnica consiste em métodos de persuasão e manipulação para convencer e conquistar a confiança da vítima. Com isso, o *hacker* consegue obter informações pessoais, e até empresariais, apenas pedindo-as educadamente. Quanto a esse tipo de ataque, *firewalls* e antivírus não oferecem segurança, já que com a engenharia social, o *hacker* pode convencer a vítima que os desative.

É da natureza humana querer se sentir seguro, tanto que muitas pessoas depositam a segurança de seus dados em objetos, métodos e *softwares*. Mas no final das contas, os ataques de engenharia social podem ter sucesso em pessoas que desconhecem as boas práticas de segurança. (MITNICK; SIMON; 2002, p.15).

Por um lado, existe a preocupação em relação a ataques cibernéticos como, por exemplo, infecção por vírus, mensagens com conteúdo suspeito e roubo ou sequestro de informações importantes. Por outro, a metodologia utilizada pela engenharia social dificulta saber das reais intenções da outra pessoa, se ela é realmente de confiança ou não.

Nesse sentido, o objetivo deste trabalho é apresentar o que o usuário deve saber sobre segurança de informação e como o treinamento, feito de forma adequada, pode influenciar positivamente, as possíveis vulnerabilidades sociais e cibernéticas. Na sequência será conduzida uma demonstração de roubo de credenciais em ambiente virtualizado. Para essa demonstração serão utilizadas as ferramentas *Virtual Box* e imagens de sistema operacional *Kali Linux* e *Linux Mint*.

Virtual Box é um *software* que virtualiza, ou emula, um ambiente como se fosse outro computador, nele serão instalados os sistemas operacionais *Kali Linux* e *Linux Mint*. A primeira máquina será configurada para acessar a *Internet*, clonar o *site* e disponibilizá-lo

para a vítima através da conexão de rede interna. Já a segunda máquina, que será a vítima, não terá acesso à rede externa mas consegue se comunicar com outras máquinas na mesma rede interna. O método utilizado para roubar as credenciais será o *phishing*, através de uma ferramenta do *Kali Linux* denominada *Social Engineering Toolkit* (*SET*).

1.2 OBJETIVOS

1.2.1 OBJETIVOS GERAIS

O presente trabalho tem como objetivo principal informar que a segurança dos usuários de informática não se baseia somente em softwares de segurança como a maioria das pessoas pode imaginar, mas que existem outros meios de sofrer ataques e, principalmente as pessoas mais leigas em relação a informática, como elas devem se prevenir. Para isso, será explicado como é estruturada a segurança da informação e a importância da aplicação de suas políticas, formas de prevenção e identificação de ataques ou fraudes. Por fim, será apresentado um exemplo de ataque por phishing em ambiente virtualizado.

1.2.2 OBJETIVOS ESPECÍFICOS

Para alcançar o objetivo geral proposto neste trabalho, elaborou-se os seguintes objetivos específicos:

- Informar sobre o conceito de segurança da informação e as sugestões indicadas pela ISO (organização internacional de padronização);
- Informar sobre o conceito de engenharia social;
- Apresentar métodos de proteção pesquisados em materiais bibliográficos;
- Apresentar uma prática de ataque de phishing em ambiente virtualizado;

1.3 JUSTIFICATIVA

As pessoas se preocupam mais com os ataques que podem sofrer pelos hackers, mesmo sem saber exatamente como funciona esse processo, sendo que eles nem sempre utilizam ferramentas tecnológicas para invasão e roubo de dados. Não saber onde colocar a defesa cibernética e ser negligente sobre as informações de ativos da empresa são fatores que podem contribuir para um ataque. Portanto, é preciso que até mesmo as pessoas que usam a Internet somente para o lazer ou, principalmente, as pessoas que raramente têm contato com a informática precisam estar cientes dos riscos.

1.4 MOTIVAÇÃO

A motivação para realizar este trabalho foi o fato de que nem todas as pessoas utilizam a Internet para trabalho ou, somente, lazer estão cientes das consequências, principalmente, em relação a segurança da informação. Funcionários não treinados correm o risco de vazar informações de ativos da empresa para terceiros e, o caso que mais acontece, baixar e instalar softwares que comprometem o sistema. Mas os riscos cibernéticos não são o único problema, a exploração das vulnerabilidades, através da persuasão, no fator social é igualmente perigosa e dificilmente identificada. Dessa forma, estes são mais propensos a acontecerem novamente. Conhecer o método de ataque pode ser usado em uma metodologia de defesa.

1.5 PERSPECTIVA DE CONTRIBUIÇÃO

Este trabalho objetiva contribuir com os leitores em relação às causas das vulnerabilidades, tipos de ataques que os usuários estão sujeitos e sugerir alguns métodos de proteção para inibir ou, ao menos, mitigar tais vulnerabilidades.

1.6 METODOLOGIA DE PESQUISA

O passo inicial para atingir o objetivo proposto neste trabalho, foi realizar uma pesquisa das vulnerabilidades relacionadas à segurança da informação. Nessa pesquisa foram revisadas bibliografias e documentos relacionados à segurança da informação, onde são

especificados os critérios para aplicação das políticas de segurança da informação nas empresas e informar quais os princípios da segurança da informação. Posteriormente, seguindo nesse mesmo sentido, foi abordado o conceito da engenharia social, em uma revisão literária, e como esse conceito pode afetar a segurança da informação.

Com base nos referenciais estudados buscou-se apresentar os métodos para proteção que o usuário pode aplicar em seu dia a dia ou em seu trabalho. Esses métodos abrangem tanto a proteção de informações cibernéticas quanto a proteção social, de modo a identificar tentativas de golpes ou subornos.

Após a revisão literária foi criado, com a finalidade de conscientizar o usuário, um ambiente virtual que consistem em duas máquinas com sistemas operacionais diferentes e um deles foi responsável por executar o ataque de phishing. Enquanto o outro sistema, que fará o papel de vítima, terá seus dados capturados e enviados à máquina do atacante.

1.7 ESTRUTURA DO TRABALHO

O presente trabalho está organizado em seis capítulos:

- Capítulo 1 - Introdução: Neste capítulo é contextualizado os riscos que podem acontecer com o usuário do computador e apresentados os objetivos, justificativa, motivação, perspectiva de contribuição e metodologia de pesquisa.
- Capítulo 2 - Conceitos Básicos de Segurança da Informação: Neste capítulo o leitor é informado dos princípios que constituem a segurança da informação e as exigências das políticas de segurança da informação para os estabelecimentos.

- Capítulo 3 - Conceitos de Engenharia Social: Neste capítulo é apresentado o conceito de engenharia social e as fraquezas do fator humano na segurança da informação.
- Capítulo 4 - Métodos de Proteção: Neste capítulo são apresentados os métodos de proteção do sistema que o usuário pode aplicar em sua rotina de uso e, para o fator humano, recomendações e procedimentos para treinamento para prevenção de ataques de engenharia social.
- Capítulo 5 - Materiais e métodos: Neste capítulo é iniciado uma construção do ambiente virtual para testes de penetração, com a finalidade de mostrar ao leitor como ocorre o ataque, neste caso, de phishing.
- Capítulo 6 - Considerações Finais: Neste capítulo é feito uma conclusão dos resultados da pesquisa realizada para atingir objetivo proposto neste trabalho.

2. CONCEITOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

Segundo Velasco (2019), o termo se refere à defesa de dados e a garantia de que informações sigilosas sejam acessadas somente por seus responsáveis. No contexto corporativo, a segurança da informação evita que dados como margem, lucro, vendas ou concorrentes sejam distribuídos de forma indevida. Com tantas tarefas sendo realizadas simultaneamente, como, por exemplo, organização de e-mails com informações confidenciais, uma pequena distração pode causar grandes erros, portanto é necessário que se implemente níveis de proteção.

Muitas organizações consideram a segurança da informação uma necessidade para seus negócios. A prática segurança deve ser correspondente às condições da empresa, porém nem sempre isso é aplicado por consequência do alto custo com projetos, recursos e demanda de tempo. E mesmo investindo em projetos, não é totalmente isento de falhas. (Almeida; Souza; Coelho, 2010, p.2).

De acordo com Brostoff (2004, p.22) segurança da informação pode ser definida como proteção ou controle de acesso a determinada informação, esta informação diz respeito a uma pessoa física, pessoa jurídica ou bem material. O principal objetivo da segurança da informação é preservar as características básicas da informação, sendo elas: confidencialidade, integridade, disponibilidade, além de outros fatores associados como: propriedade, autenticação, severidade, autenticidade e não repúdio. Para isso utiliza-se de técnicas como prevenção, detecção e resposta. Estas técnicas estão inseridas no processo de análise de risco, onde são identificadas as ameaças e vulnerabilidades.

Segundo Garfinkel et al. (2003), os profissionais da segurança da informação têm dificuldades em definir seu significado, pois a segurança, privacidade e proteção são termos que podem ter mais de um significado. Dessa forma a aplicação da segurança da informação não está restrita apenas a sistemas computacionais, mas também a todos os aspectos de proteção em relação a itens materiais, garantia de qualidade, confiabilidade do hardware e até o fator humano.

2.1 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Antes de criar uma política de segurança é necessário compreender os princípios da segurança da informação, requisitos para sua implantação e sua gestão em prática. A

segurança da informação deve seguir os princípios de seus pilares, que é a garantia a confidencialidade, integridade, e disponibilidade da informação. Dessa forma é possível definir as informações que devem ser protegidas, qual deve ser seu nível de proteção e quais ferramentas serão utilizadas no ambiente corporativo.

A confidencialidade de uma informação diz respeito a sua proteção contra acesso não autorizado do proprietário da informação, deve garantir acesso somente às pessoas autorizadas e a irretratabilidade, que garante a autenticidade do proprietário da informação. A integridade deve garantir a exatidão, não alteração sem permissão do proprietário da informação durante seu armazenamento ou processamento. A disponibilidade é responsável por manter a informação acessível aos usuários autorizados quando precisam acessá-la. (ISO 27001, 2006).

Outros princípios como conformidade e autenticidade também foram incorporados no documento ABNT NBR ISO/IEC 27002, publicado em 2013. De acordo com o dicionário Aurélio (2022), conformidade é estar em concordância, que possui uma relação de correspondência e estar sujeito ao que foi estabelecido. Portanto, a conformidade da informação estabelece que sistemas de gerenciamento das informações devem estar de acordo com a política e normas estabelecidos para a empresa. Em relação a autenticidade, é esperado que as informações sejam de fonte confiável, confirmando a sua veracidade. Para estabelecer o pilar da autenticidade, é necessário manter o registro do autor da informação e, para segurar sua integridade, o registro de modificação quando preciso. (ISO 27001, 2006).

No pilar da autenticidade são colocadas técnicas usadas para distinguir os usuários autorizados dos não autorizados. O processo de autenticação assegura que somente pessoas com autorização, ou proprietário, tenham acesso após comprovarem a legitimidade da permissão. Neste pilar existem três formas de autenticação baseadas em conhecimento, token e biometria. (BROSTOFF, 2004, p.24).

Toda autenticação baseada no conhecimento tem a vantagem de não requerer hardware extra e não exige alto custo de mudança caso sejam comprometidos. O sistema que usa a autenticação baseada no conhecimento é de login e senha, comumente usados em autenticação de e-mail, redes sociais e serviços em nuvem. Autenticação baseada em token submete um objeto único do usuário, físico ou digital, para ser examinado pelo computador comprovando a autenticidade. Na autenticação biométrica existem duas formas de autenticar o usuário um através de sua estrutura física e por seus

comportamentos. Autenticar um usuário pelas suas características físicas permite o acesso rápido sem extenuá-lo, no entanto exige recursos caros em comparação com a autenticação por conhecimento. Outra complicação da autenticação biométrica por característica física é o fator humano, que envelhece e, consequentemente, alterando suas características. A autenticação por comportamento não é tão popular, devido a sensação invasiva causada pelo monitoramento de suas atividades (BROSTOFF, 2004, p.24).

Apesar dos esforços em criar meios de autenticação para melhorar a segurança, os atacantes conseguem burlar esses sistemas, o fator humano sempre será o elo mais fraco da segurança. No caso da autenticação baseada em conhecimento, não ter uma política bem definida quanto a informação, e do responsável por usá-la, o atacante também identificado como engenheiro social, conseguirá obter as informações em pouco tempo. Os itens usados na autenticação por token como cartão inteligente ou token físico (dispositivo semelhante a uma chave de carro) podem ser perdidos ou roubados, gerando um custo adicional para fabricação. A atualização do usuário em relação a autenticação biométrica deve ser realizada anualmente devido às mudanças biológicas. (BROSTOFF, 2004, p.24-25).

2.2 CICLO PDCA

Independentemente do tamanho da empresa todas têm suas informações confidenciais, e estas devem ser protegidas contra as ameaças, seja pelo fator humano quanto ou cibernético, portanto é indispensável a criação de um modelo de política de segurança de acordo com as necessidades e objetivos da empresa. A organização internacional de padronização (ISO) estabelece normas específicas para operar, manter e aprimorar o sistema de gestão da segurança da informação(SGSI). A norma ISO/IEC 27001 de 2006 sugere que os usuários enfatizem a importância da compreensão dos requisitos de segurança, da implementação e operação de controles de gerência de riscos, monitoramento e análise crítica do desempenho. Para realizar tais processos, a norma 27001 adota um modelo conhecido como plan-do-check-act (PDCA) para estruturar todos os processos do SGSI levando em consideração os requisitos de segurança da informação referente à organização. O ciclo PDCA auxilia na definição dos objetivos,

levantamento de requisitos, planejamento de classificação dos ativos[3], monitoramento das equipes e medição de desempenho para que possa ser determinada a efetividade.

No processo de plano devem ser estabelecidas as políticas, objetivos, processos e procedimentos do SGSI que sejam relevantes para a gestão de riscos e a melhoria da segurança da informação. A primeira etapa do processo de planejamento é a identificação do problema, podendo ser a falta de recursos ou falta de treinamento dos funcionários. Com a identificação do problema, os passos seguintes são a observação de suas características e detalhes, análise do motivo de seu surgimento e executar um plano de ação. Também é preciso identificar os ativos, para serem classificados e protegidos de forma adequada, e as vulnerabilidades nos processos e os impactos que a perda do C.I.D pode causar. Dessa maneira, são produzidos resultados seguindo as políticas e objetivos globais da organização. A empresa deve definir um escopo dos limites do SGSI em relação às características do negócio, estabelecer sua abordagem de avaliação de riscos seja adequada aos requisitos jurídicos. O planejamento deve preparar um inventário dos ativos que devem ser protegidos de acordo com a sua classificação de risco, seguindo os critérios da avaliação de riscos e os objetivos de tratamento de riscos são selecionados. (ISO 27001, 2006).

No processo de fazer (do) é realizada a implementação, ou seja, a execução, e operação da política estabelecida no processo de planejamento para alcançar os objetivos da organização. Neste processo devem ser realizados programas de treinamento e conscientização dos funcionários e a gerência dos recursos e operações do SGSI. Procedimentos de detecção de incidentes e controles de acesso devem ser implementados para melhor segurança da informação. Deve ser formulado um plano de tratamento de riscos que identifique a ação de gestão apropriada, recursos, responsabilidades e prioridades para gestão dos riscos de segurança e definir uma medição eficaz dos controles selecionados e como se deve avaliar essas medidas, de modo que os resultados sejam comparáveis. (ISO 27001, 2006)

Em checagem (check) os resultados do processo de execução (do) são submetidos a uma análise crítica para medir o desempenho e determinar se a política foi eficaz, e se os objetivos poderão ser alcançados, os resultados da análise crítica devem ser enviados para a diretoria. O monitoramento constante deve, prontamente, detectar erros nos

[3] Qualquer elemento que agregue valor ao negócio e, podendo ser digital ou físico, que sua manipulação indevida trará prejuízo, ou a ruína da confiança.

resultados de processamento e identificar tentativas de violações contra a S.I. Esta análise deve ser realizada regularmente, dessa forma é possível compará-las e determinar a eficácia e, quando precisar, discutir melhorias para o futuro. (ISO 27001, 2006)

No processo de *act* (ação) são executadas ações de correção e prevenção visando a melhoria contínua do SGSI. Neste processo os resultados da auditoria do SGSI e da análise crítica são levados em consideração para atingir os objetivos. As ações corretivas são efetuadas para eliminar as causas de não-conformidade com os requisitos do SGSI. De acordo com a norma, a ação corretiva deve definir requisitos para identificar as não-conformidades, determinar suas causas e registrar os resultados das ações executadas. Após identificar as não-conformidades para correção, a organização deve efetuar a ação de prevenção e assim evitar novas ocorrências. (ISO 27001, 2006)

Todo conceito de segurança da informação se aplica em cada processo do PDCA com a finalidade de inibir os ataques à organização ou empresa. A política de segurança estabelece que as categorias de risco definidas pelo objetivo de controle estejam em conformidade em cada processo ou subprocesso do PDCA. Os objetivos de controle podem ser classificados em categorias como conformidade, relatório financeiro, estratégica, operações ou desconhecido. Após a identificação do objetivo de controle, os riscos associados a esse objetivo de controle podem ser definidos. Por exemplo, o objetivo de controle do departamento de RH é chamado de ‘equipe’, o risco associado pode ser “conflito de ética entre os objetivos da empresa e os funcionários envolvidos”. Para manter a segurança dos processos são estabelecidos controles que devem ser obedecidos, esses controles são definidos no processo de planejamento. Os controles também contribuem para mitigar as vulnerabilidades. (ISO 27001, 2006).

Na gestão de ativos são determinadas as responsabilidades sobre os mesmos para manter a proteção adequada. Para um inventário, o controle determina que todos os ativos devem ser identificados e, os mais importantes devem ser estruturados e mantidos de forma organizada. Para os proprietários dos ativos, todas as informações e ativos associados com os recursos de processamento deve ter um proprietário designado pela organização. O controle estabelece que a classificação das informações seja feita de acordo com seu valor, requisitos legais, sensibilidade e criticidade para a organização. (ISO 27001, 2006).

Em relação a segurança dos recursos humanos, o objetivo é assegurar que funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com seus papéis, reduzindo o risco de roubo, fraude ou mau uso de recursos. O controle de papéis e responsabilidade requer que os funcionários, fornecedores e terceiros devem ser definidos e documentados de acordo com a política de segurança da informação. (ISO 27001, 2006).

O objetivo do gerenciamento das operações e comunicações é garantir a operação segura e correta dos recursos de processamento da informação, o controle para sua documentação estabelece que todas as operações e procedimentos devem ser documentados, atualizados e devem estar disponíveis a todos os usuários que precisem deles. (ISO 27001, 2006).

As normas estabelecidas para o controle de acesso têm como objetivo controlar o acesso à informação, a política de controle de acesso deve ser implementada, documentada e analisada criticamente, para se tornar a base dos requisitos de acesso dos negócios e da segurança da informação. As normas do controle de acesso também definem os controles para o gerenciamento de acesso do usuário, cujo objetivo é garantir somente o acesso de usuários autorizados. (ISO 27001, 2006)

Na norma de gestão de vulnerabilidades técnicas é definido que, a informação sobre essas vulnerabilidades do sistema deve ser obtida em curto tempo, após confirmada a exposição da organização as medidas apropriadas devem ser tomadas para lidar com os riscos apropriados.

Todavia, as vulnerabilidades existentes não se aplicam somente à tecnologia do sistema como também ao fator humano. Por mais que uma empresa tenha investido em tecnologias de segurança, contratado os melhores guardas e trancado todos os segredos antes de irem para suas casas, a empresa ainda estará vulnerável. Os ladrões podem se passar por funcionários para conseguir se infiltrar e roubar informações (MITNICK; SIMON, 2002, p.15).

As empresas nunca devem focar somente na segurança tecnológica e deixar de lado a segurança social, pois o ser humano é considerado “falho”. No capítulo 3 será apresentado o conceito da engenharia social, as tendências do ser humano para ser manipulado e a gerência de políticas que tratam da segurança das informações.

3. CONCEITOS DE ENGENHARIA SOCIAL

Dentro do ambiente organizacional a informação é considerada um ativo e, neste caso, as informações têm valor considerável e precisam de proteção adequada. Com o aumento da interconectividade as informações ficam mais expostas e, consequentemente, vulneráveis (ABNT NBR ISO/IEC 17799, 2005).

Como foi apresentado no capítulo 2, a política imposta na norma ABNT NBR ISO 27001 de 2006, é determinado que os critérios de segurança sejam seguidos e um protocolo de conduta para o proprietário da informação que deve ser treinado.

Segundo Alexandria (2009, p.47), ” a segurança da informação é uma questão relacionada com aspectos sociais e humanos, portanto, para se ter sucesso na sua gestão deve-se conciliar tais conceitos às soluções adotadas, sejam elas tecnológicas ou administrativas“.

Um erro comum entre as organizações, que costuma conduzir os esforços da implementação de programa de S.I em direção ao fracasso, é desconsiderar os aspectos humanos no processo de implantação das políticas. Outras políticas como tecnológicas, não tecnológicas e administrativas são implementadas juntamente a política de segurança da informação, isso deve ser feito para atender todas as áreas da organização (ALEXANDRIA, 2009, p.43).

As pessoas que acreditam estar seguras somente instalando *softwares* de antivírus, ativando *firewall* do sistema e efetuando *backup* regularmente estão enganadas, pois a segurança da informação também envolve o fator humano. Este fator é considerado o elo mais fraco representando um potencial risco a política de segurança, isso porque os humanos são suscetíveis a erros.

A maior parte das pessoas tendem a imaginar que os produtos de segurança cibernética são o suficiente, no entanto esse mundo de fantasia não continuará para sempre, cedo ou tarde se tornarão novas vítimas de um incidente de segurança (MITNICK; SIMON, 2002, p.15).

A técnica conhecida como engenharia social foca justamente no fator humano para procurar brechas ou até mesmo criá-las. Essa técnica utiliza a persuasão como principal ferramenta de ataque, com isso o engenheiro social consegue conduzir a vítima para que ofereça as informações por vontade própria.

Segundo Mitnick e Simon(2002, p.18-19):

> Na maioria dos casos, os engenheiros sociais bem-sucedidos têm uma habilidade muito boa em lidar com as pessoas. Eles são charmosos, educados e agradam facilmente — os traços sociais necessários para estabelecer a afinidade e confiança. Um engenheiro social experiente pode ter acesso a praticamente qualquer informação-alvo usando as estratégias e táticas da sua habilidade. Os tecnologistas experientes têm desenvolvido soluções de segurança da informação para minimizar os riscos ligados ao uso dos computadores, mas mesmo assim deixaram de fora a vulnerabilidade mais significativa: o fator humano, Apesar do nosso intelecto, nós humanos — você, eu e todas as outras pessoas — continuamos sendo a ameaça mais séria à segurança do outro.

Em "A arte de enganar" de Mitnick e Simon (2002) são apresentados casos de engenharia social e é realizada uma análise crítica sobre a conduta dos atacantes e das vítimas. Um desses casos foi considerado como "o maior desfalque" e entrando no livro dos recordes na categoria de maior fraude de computadores. O autor do desfalque era Stanley .M Rifkin, funcionário do Pacific Bank e responsável pelo sistema de *backup* da sala de transferências, devido ao seu cargo ele tinha acesso aos processos de transferência. Depois de um tempo, analisou que precisava de três códigos para se passar por um consultor, membro do departamento internacional do banco, e assim solicitar a transferência para sua conta na Suíça. O caso de Rifkin ganhou destaque na época, manchando a reputação do banco, e tudo que ele precisou foi fazer um planejamento cuidadoso e ser bom de conversa.

A engenharia social tem o fator humano como alvo porque nosso "firewall interno" pode ser desativado por métodos persuasivos. De acordo com Cialdini, o engenheiro usa táticas de persuasão para afetar as seis tendências básicas do ser humano para obter uma resposta positiva. Essas tendências básicas da natureza humana são conhecidas como autoridade, similaridade, reciprocidade, consistência, escassez e validação social.

3.1 TENDÊNCIAS DA NATUREZA HUMANA

A sociedade desenvolveu aspectos para facilitar a comunicação, a autoridade eficiente para manter a ordem e organização entre os demais que, naquele local, devem obediência para alcançar um objetivo em comum. Segundo Mitnick e Simon (2002,

p.200), “as pessoas tendem a atender a uma solicitação que é feita por uma pessoa com autoridade.”

A autoridade é um dos fatores mais poderosos e motivadores das ações humanas. Um sistema de autoridade estratificada e amplamente aceita é de grande vantagem para a sociedade. A existência da autoridade permite o desenvolvimento de estruturas sofisticadas para a produção de recursos, comércio, defesa, expansão e controle social, que de outra forma estariam em perigo ou mergulhado na anarquia. E isto se deve a educação que recebemos ao longo do nosso desenvolvimento como cidadãos, somos educados a considerar a obediência para autoridades como algo positivo. E essa mensagem é constantemente transmitida por toda a cultura de forma subjacente. Por este motivo, em muitas situações cotidianas, quando somos por uma autoridade, nossa tendência é obedecê-la e desconsiderar todos os aspectos da realidade que a contradizem (CIALDINI, 2007, p.6).

Para Cialdini (2006), a tendência da similaridade, ou afabilidade, é o ato de ser simpático com aquele que é nosso semelhante e, aparentemente, possui os mesmos estilos de vida, gostos ou personalidade. Essa tendência tem quatro fatores importantes para chamar a atenção das pessoas alvo, esses fatores são atratividade física, semelhança, elogio e associação. A atratividade física consiste na boa aparência de uma pessoa, isso afeta nosso senso de pré-julgamento baseado nas características, o que nos leva a atribuir elementos positivos como honestidade, talento e inteligência. Quanto ao fator da semelhança, as pessoas preferem dar atenção àquelas que têm o mesmo estilo de vida, gostos e opiniões. Ou seja, que temos preferência a pessoas iguais a nós. Em relação aos elogios, o ser humano tem uma necessidade de recebê-los e acredita na bajulação, portanto se esforçará para ser reconhecido. Por fim a associação, este fator afeta os sentimentos de forma positiva quanto negativa, associar uma pessoa de status ou produto a marca ou um evento temporário é uma forma de agregação de valor. Supondo que um desodorante comum seja associado ao evento olímpico, e incluindo a estampa do evento, isso dá ao produto simples mais valor do que outros, dessa maneira a associação é importante do ponto de vista publicitário, para que se estabeleça uma associação, não necessariamente lógica, positiva.

O ato de ser recíproco é conhecido por mutualidade, troca equivalente ou cooperação. Quando recebemos um presente nos sentimos obrigados a retribuir de alguma forma para demonstrar gratidão pelo ato. “Podemos atender automaticamente a uma solicitação

quando recebemos ou temos a promessa de receber algo de valor. O presente pode ser um item material, um conselho ou ajuda” (MITNICK; SIMON, 2002, p.201).

O princípio da reciprocidade é uma das armas mais influentes, poderosas e eficazes que possuímos. Quando alguém nos faz um favor ou recebemos um presente, nos sentimos na obrigação de retribuir com algo equivalente. Nenhuma sociedade humana desrespeitou esse princípio. De acordo com a antropologia, a reciprocidade é um mecanismo único de adaptabilidade humana que torna possível a divisão do trabalho, a troca de diferentes tipos de bens e serviços e a criação de uma rede interdependente entre os indivíduos, tornando-os em unidades eficientes. Este princípio costuma realizar um favor ou oferecer algo para obter o consentimento (CIALDINI, 2007, p.2-3).

Segundo Cialdini (2006), a consistência é um fator que, segundo a psicologia social, faz as pessoas se esforçarem para serem coerentes devido a necessidade de comprometimento com aquilo que acreditam ou alegam. Portanto, o compromisso de realizar ações correspondentes a suas crenças ou ideais para ser consistente. Caso contrário serão considerados indecisos, confusos ou hipócritas dentro da sociedade.

“As pessoas têm a tendência de atender alguém após fazer um comprometimento público ou adotar uma causa” (MITNICK; SIMON, 2002, p.202).

A tendência da escassez diz respeito a uma condição que representa falta de recursos ou algo necessário. As pessoas tendem a cooperar quando estão precisando de algo de valor, mas a demanda é excessiva e pode ser por tempo limitado (MITNICK; SIMON, 2002, p.202). “A ideia de uma possível perda desempenha um papel decisivo na nossa tomada de decisão. Aparentemente nós nos sentimos motivados pelo pensamento perder do que ganhar algo de igual valor (CIALDINI, 2007,p.6-7)”.

O engenheiro social pode usar a tendência da escassez e reciprocidade para conquistar a vítima e, consequentemente, obter as informações internas ou pedir para a vítima instalar algo no computador do serviço.

No princípio da conformidade (ou validação social), as pessoas seguem adiante com uma ação se esta for aprovada socialmente, isso nos faz sentir seguros e mais adepto a repetir quando a aprovação vem de pessoas semelhantes a nós. “O princípio da conformidade social afirma que descobrimos o certo ao conhecer a opinião dos outros sobre o que é certo” (CIALDINI, 2007, p.4).

De acordo com Mitnick e Simon (2002, p.202), “as pessoas tendem a cooperar quando isso parece estar de acordo com aquilo que as outras pessoas estão fazendo. A ação dos outros é aceita como uma validação de que o comportamento em questão está correto e apropriado."

Esse princípio é bastante usado em *marketing* por vendedores para enaltecer seu produto, mesmo sem provas de pesquisas eles alegam que pessoas com o mesmo estilo compraram e recomendam. Essa tendência sempre usará a similaridade para convencer outras pessoas a fazerem parte da maioria.

Para executar a engenharia social é preciso seguir quatro passos para obter informações a partir da vítima e com isso ter sucesso no golpe. Apesar de cada ataque ser distinto, pois varia de acordo com a vítima, todos precisam realizar a coleta de informações, o desenvolvimento de relacionamento, a exploração da vítima e a execução do plano final. Para coletar informações sobre a vítima, o engenheiro pode vasculhar seu lixo eletrônico, usar táticas de simpatia ou intimidação, implantar *spywares* e usar *phishing*. Com as informações sobre a vítima em mãos, o engenheiro social iniciará um vínculo que pode ser de extorsão, amigável e falsamente recíproco. Após um vínculo estabelecido o engenheiro social começará influenciar a vítima para que ela faça parte do seu plano, caso contrário ele poderá ameaçá-la com as informações obtidas. Por fim, depois de reunir informações suficientes, o engenheiro executará o plano (HASAN; PRAJAPATI; VOHARA, p.3-5).

Nesse contexto, a engenharia social é a porta de entrada para diversas formas de golpes tanto cibernéticas quanto sociais. O método mais usado na engenharia social para coleta de informações, como credenciais de banco digital e e-mail é o *phishing*. Segundo um relatório apresentado por Rodrigues (2021):

> Um em cada cinco brasileiros sofreu pelo menos uma tentativa de *phishing* em 2020. A estatística revelada por um novo relatório, coloca o Brasil como líder mundial em golpes dessa categoria, à frente de Portugal, França, Tunísia e Guiana Francesa, que completam a lista dos cinco países com maior índice de usuários alvos de roubo de dados ao longo do ano.

Conforme Nascimento e Yuge (2014), “*phishing* é um termo originado do inglês (*fishing*) que em computação se trata de um tipo de roubo de identidade online.” O hacker (engenheiro social) entra em contato com a vítima enviando e-mail contendo o link do site

falso, justificando que houve um problema com seus dados e precisa fazer uma atualização cadastral. Nesse momento o *hacker* pode usar a técnica da persuasão no texto do e-mail passando credibilidade. Ao clicar no link, a vítima será direcionada para um site falso previamente montado, ou simplesmente clonado. Após digitar as informações solicitadas e enviá-las, no caso de hackers experientes a página será redirecionada para o site oficial, dessa forma a vítima não perceberá que sofreu um golpe.

O *phishing* pode ser descrito como a tentativa de aceder, de forma fraudulenta, a informação financeira ou pessoal. Na maioria das vezes esses ataques acontecem por e-mail, chamadas telefônicas ou mensagens incluindo links. O atacante se passa por um colaborador legítimo ou uma instituição credível para obter as informações. Existe uma diferença tênue entre as técnicas de *phishing* e engenharia social. Se por um lado o *phishing* pode atingir várias pessoas sem uma pesquisa de seus interesses, por outro ambas as técnicas se complementam para alcançar o mesmo objetivo (Pais; Moreira; Varajão, 2013, p.6).

Ataques de *phishing* não estão restritos ao e-mail, é possível enviar o *link* falso para outras plataformas de comunicação como chat do Facebook ou Whatsapp. Todos os usuários devem sempre estar atentos aos links que recebem, muitas vezes falta apenas um caractere se comparado ao original. Pesquisar sobre a veracidade do link também é uma boa prática.

4 MÉTODOS DE PROTEÇÃO

4.1 PROTEÇÃO CIBERNÉTICA

A cartilha de segurança para Internet produzida pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) e o Núcleo de Informação e Coordenação do Ponto BR (NIC.br) apresenta recomendações e dicas de como o usuário deve se comportar para aumentar a segurança e se proteger de possíveis ameaças.

Os mecanismos de proteção contra-ataques cibernéticos podem variar de melhoria nas configurações de *firewall*, instalação de *softwares* específicos e adoção de políticas de segurança para sistemas. O usuário nunca deve se esquecer de cumprir com os requisitos da política de segurança estabelecida pela empresa, principalmente em relação aos ativos.

De acordo com a cartilha de segurança CERT.br e NIC.br, por mais que a Internet tenha inúmeros benefícios, ela não deve ser utilizada sem:

- A instalação de ferramentas *antimalware* (antivírus): responsáveis por procurar, anular ou remover códigos considerados maliciosos para o computador, o usuário deve configurá-lo para verificar todo tipo de extensão de arquivos e todas as mídias de armazenamento portáteis;
- Uso de *firewall* para computador pessoal: protege o computador de acesso não autorizado vindo da Internet bloqueando a possível exploração de vulnerabilidades e deve estar configurado para registrar o máximo de informações;
- Um navegador com configurações recomendadas: gerenciamento de cookies, gerenciamento de contas e senhas, e instalar extensões que inibem ou alertem ataques de malwares;
- Programas de criptografia de dados: empresas que usam canais de comunicação para compartilhamento de documentos devem ficar atentos a segurança das chaves criptográficas.

A instalação de *antimalware* é essencial para que códigos maliciosos não se instalem no computador e mesmo que isso aconteça, sua propagação para outros computadores será inibida. Entretanto, mesmo este recurso não é o bastante para a proteção completa do computador, desse modo é necessário a ativação do *firewall* pessoal (incluído no sistema

operacional). A configuração deste deve garantir o bloqueio de tentativas de invasão, coleta e envio de dados a terceiros vindos da Internet (CERT.br; NIC.br, 2012, p. 71).

O navegador deve ter suas configurações alteradas para atender aos requisitos de segurança, principalmente os computadores de serviço. De acordo com CERT.br, o primeiro passo é definir os *cookies*[4] criados no navegador, eles contêm informações sobre o computador e o usuário que são usadas pelos *sites* acessados. Embora os *cookies* sejam práticos para agilizar o processo de preenchimento de formulários, acesso a contas cadastradas e identificação do tipo de equipamento (*hardware*), essas informações correm risco de serem exploradas pelo atacante em busca de vulnerabilidades ou por códigos maliciosos. A eliminação de todos os *cookies* também não é recomendada, isso pode impedir acesso e uso adequado de determinados *sites*. Portanto, a recomendação da configuração para *cookies* determina que o usuário nunca aceite *cookies* de terceiros, isso evita conteúdo de publicidade. Os *cookies* que não forem tão importantes para a rotina do usuário devem ser apagados automaticamente, assim que o navegador for fechado, caso contrário o usuário deve criar uma lista de exceções. Quando tiver que usar computador de terceiros sempre use a navegação anônima.

O segundo passo é seguir os critérios da política de segurança, estabelecida pela empresa, para criação de contas e senhas. Caso precise salvar senhas no computador é, extremamente importante, que utilize o método de criptografia e configure uma chave mestra. A opção de “lembre-se de mim” ou “continuar conectado” nunca deve ser usada em computadores de terceiros, devido aos *cookies* criados serem armazenados no computador e correm o risco de serem usados de forma indevida. Porém, o uso desta opção é recomendado somente para *sites* com um nível de risco muito baixo.

No terceiro, e último passo, as extensões adicionais ao navegador que permitem inibir ou alertar sobre ataques de *malwares*, no entanto, BELCIC (2021) afirma que “é impossível dizer que todas as extensões do navegador estão seguras. Se uma extensão é criada por um desenvolvedor confiável, você pode se sentir confiante. O código-fonte aberto é um bom sinal”. Portanto, o usuário deve estar ciente de que ao instalar uma extensão para prover segurança e privacidade, significa confiar os dados, pessoais e sigilosos, ao provedor. BELCIC (2021) oferece algumas dicas para avaliar e escolher extensão com segurança. Antes de instalar qualquer extensão é importante que usuário:

[4] *Cookies* são pequenos arquivos gravados no computador que contém informações do usuário e do próprio computador (sistema operacional e *hardware*).

- Ler as avaliações profissionais;
- Ler e analisar o depoimento de outras pessoas que já usaram;
- Ler com atenção as descrições na loja;
- Verifique as permissões solicitadas, desinstale a extensão caso algumas permissões não parecerem certas;
- Procure e avalie o site do desenvolvedor;
- Procure notícias sobre violações de dados ou incidentes semelhantes relacionados ao desenvolvedor e o produto.

Para melhor segurança das mensagens, os programas leitores de *e-mails* devem ter suporte para programas de criptografia. Isso garante que somente o destinatário terá acesso a mensagem. A criptografia proporciona proteção aos dados armazenados no computador, aos *backups* contra acesso indevido e encriptação automática de partição específica do computador.

A segurança do próprio *hardware* também deve ser levada em consideração, por exemplo, em caso de infecção por *malwares* ou perda do equipamento, o que deve ser feito quando o computador for comprometido.

Alguns indícios que o usuário deve perceber quando o computador estiver infectado por algum malware, de acordo com CERT.br et al.(2012), são:

- Lentidão para inicialização, desligamento, acesso à Internet e execução de programas;
- Desligamento não solicitado ou agendado;
- Mensagens de logs são apagados e seus arquivos apagados;
- Impossibilidade de atualização do sistema operacional e antimalware.

Para esses indícios a cartilha de segurança recomenda que o usuário deve seguir os passos para reverter o problema:

a. Certificar-se que o sistema operacional está na versão mais atual, caso contrário atualize-o de imediato;
b. Certificar-se de que o *antimalware* está sendo executado e se está na versão mais recente, se não estiver atualize e execute;
c. Execute o *antimalware*, configurando-o para verificar todos os discos e analisar todas as extensões de arquivos;
d. Os arquivos que o antimalware detectar como infectado devem ser limpos;
e. Caso deseje executar o *antimalware online* para tirar dúvidas sobre a situação, o *antimalware* local deve ser temporariamente encerrado;
f. Verifique a ativação e configuração do *firewall* pessoal;
g. No caso de o sistema operacional não estar atualizado, deve ser feito de imediato e também instalado todos os aplicativos novamente;
h. Os dados pessoais devem ser recuperados por meio de *backup*.

Todas as configurações do navegador no novo sistema operacional devem ser feitas novamente, os mecanismos de segurança precisam estar em dia dessa vez.

4.2 PROTEÇÃO SOCIAL

“A empresa pode considerar que o treinamento está atingindo o seu objetivo final se todos os que realizarem o treinamento estiverem convencidos e motivados por uma noção básica: a noção de que a segurança das informações faz parte do seu trabalho” (MITNICK; SIMON, 2002,p.199).

Apesar disso, alguns funcionários são negligentes em relação à segurança da informação não por arrogância, mas, às vezes, por não conseguirem tempo para absorver tudo que foi ensinado durante seu expediente. Talvez, a minoria considere ler sobre a segurança durante sua folga ou final de semana. Portanto, é necessário que a empresa organize pequenos grupos para receberem uma introdução básica, interativa e motivadora para que os funcionários se acostumem rápido.

A sessão inicial do treinamento deve ser focada em prender a atenção do empregado, seu conteúdo deve ser resumido para que seja fácil de lembrar. Apesar da grande

quantidade de material para ser apresentado, o importante no primeiro momento é fornecer a conscientização e motivação juntamente com pouco número de mensagens essenciais, por exemplo o mal que a empresa e os empregados podem sofrer.

Segundo Mitnick e Simon (2002, pg.202):

> Se as sessões de treinamento de conscientização puderem mudar o comportamento das pessoas para que cada empregado sempre teste toda solicitação que contraria esses critérios, o risco associado aos ataques da engenharia social reduz-se à de modo impressionante.

Após a sessão de treinamento inicial, devem ser criadas sessões mais longas de educação sobre as vulnerabilidades específicas e técnicas de ataques relativos a sua posição. A natureza da ameaça e os métodos para explorá-la estão sempre mudando, isso significa que o material do treinamento deve acompanhar a atualização. Os empregados que mudam de setor devem se adequar às novas políticas. O programa de treinamento e conscientização da segurança das informações deve incluir a metodologia utilizada pelos engenheiros sociais para abordar suas vítimas. Também deve fornecer dicas de reconhecimento e procedimentos de possíveis ataques, as obrigações de cada empregado em atender as políticas e as consequências caso não sejam respeitadas. Nas primeiras sessões de treinamento talvez fique bem claro que a característica principal da engenharia social é a fraude. Portanto, caso o empregado se depare com uma pessoa supostamente de autoridade, ele deve verificar sua veracidade, se a pessoa é realmente quem diz ser.

Mesmo que a prática de engenharia social seja mais voltada para ataques sociais, na sua aplicação não são dispensados a utilização de ferramentas tecnológicas e, portanto, de acordo com o material fornecido por Mitnick e Simon (2002, p. 202), as políticas também deve incluir:

- Uma descrição do modo como os atacantes usam as habilidades da engenharia social para enganar as pessoas;

- Os métodos usados pelos engenheiros sociais para atingir seus objetivos;
- Como reconhecer um provável ataque da engenharia social;
- O procedimento para o tratamento de uma solicitação suspeita;
- A quem relatar as tentativas da engenharia social ou os ataques bem-sucedidos;
- A importância de questionar todos os que fazem uma solicitação suspeita independentemente da posição ou importância que a pessoa alega ter;
- O fato de que os funcionários não devem confiar implicitamente nas outras pessoas sem uma verificação adequada, embora o seu impulso seja dar aos outros o benefício da dúvida;
- A importância de verificar a identidade e a autoridade de qualquer pessoa que faça uma solicitação de informações ou ação;
- Procedimentos para proteger as informações confidenciais, entre eles a familiaridade com todo o sistema de classificação de dados;
- A localização das políticas e dos procedimentos de segurança da empresa e a sua importância para a proteção das informações e dos sistemas de informações corporativas;
- Um resumo das principais políticas de segurança e uma explicação do seu significado. Por exemplo, cada empregado deve ser instruído sobre como criar uma senha difícil de adivinhar;
- A obrigação de cada empregado de atender às políticas e as consequências do seu não-atendimento.

Além do treinamento e conscientização dos funcionários deve haver uma forma de, conquistando o lado positivo da reciprocidade e validação social, segundo Mitnick e Simon (2002, p. 204), “...recomendo um programa ativo e bem divulgado de recompensas. Você deve reconhecer os empregados que detectaram e evitaram uma tentativa de ataque de engenharia social, ou que de alguma outra maneira contribuíram para o sucesso de segurança das informações…”

Para a criação de políticas de segurança a empresa ou organização deve designar uma pessoa para essa função, os planos para desenvolvimento das políticas devem ter o apoio e comprometimento por parte da gerência da empresa. A pessoa designada, ou

proprietário das informações, deve estar consciente de que precisa incluir o fator tecnológico nas políticas, seguindo as recomendações descritas na cartilha de segurança CERT.br e que a política deve se adequar a realidade da empresa, portanto não poderá ser inflexível.

4.3 CLASSIFICAÇÃO DE DADOS

Segundo Mitnick e Simon (2002, p. 210), “A política da classificação de dados define orientação para classificar as informações valiosas em vários níveis”. Para elaboração das políticas de segurança da informação é exigido que o proprietário das informações defina quais devem ser as informações que precisam de proteção, qual seu nível de importância e quem deve ter a permissão para utilizá-la. O proprietário das informações também é responsável pela reavaliação e alteração no nível da classificação das informações.

Ao classificar as informações os empregados conseguem ter uma noção da importância e, somado às sessões de conscientização e treinamento, serão capazes de proteger os dados de forma correta. Para exemplificar a classificação das informações, Mitnick e Simon (2002, p. 211) criaram quatro níveis de classificação considerados adequados para a maioria das empresas de médio a grande porte. Estas categorias são:

- Confidencial: Informações que devem ser usadas somente dentro da empresa, a quantidade de pessoas com autorização para compartilhamento deve ser limitada e sua divulgação não autorizada pode provocar um impacto sério em relação a parcerias e clientes. Geralmente são informações que se tratam de estratégia de *marketing*, segredos comerciais, código-fonte proprietário e informações do produto que pode ser vantajoso para concorrência;
- Particular: Informações de natureza pessoal que se destinam apenas dentro da empresa. Sua divulgação não autorizada pode provocar impactos sobre outros empregados, ou para a própria empresa caso uma pessoa não autorizada tenha acesso, como os engenheiros sociais. As informações particulares podem ser dados pessoais entre a pessoa e a empresa como histórico de salário, histórico médico dos empregados e informações de contas bancárias;

- Interna: Informação que podem ser compartilhadas livremente, somente dentro da organização, entre os empregados da organização. Sua divulgação para terceiros precisa de autorização, por exemplo, a assinatura contratual de confidencialidade. Essas informações incluem tudo o que é usado durante a atividade diária de negócios como gráficos organizacionais da corporação, números de discagem de rede, nomes de sistema interno, procedimentos de acesso remoto e códigos de centro de custos;
- Pública: São informações que podem ser liberadas ao público, sem qualquer restrição, como informações de contato de suporte ou brochura de produto;

Todas as informações que não forem consideradas públicas devem ser categorizadas como confidenciais, desse modo é possível minimizar a possibilidade de vazamento das informações.

Os empregados da organização também devem ser categorizados e designados a proteger determinadas informações, como foi estabelecido no treinamento, todos são responsáveis e devem ser conscientes em relação à gravidade das consequências em caso de vazamento. A categoria dada às pessoas que serão responsáveis pelas informações seguir as políticas de segurança são:

- Pessoa não verificada: Pessoa que não possui provas de ser membro organizacional, não é reconhecida pessoalmente ou que tenha um vínculo de parceria com a empresa, pelo menos, até o momento em que alguém de confiança concede sua autorização;
- Pessoa de confiança: Pessoa que é reconhecida como sendo membro da organização e, que possui um vínculo como cliente, membro de parceiros, empregado ou consultor, pertence a um cargo adequado para ter acesso às informações. Estas pessoas têm um relacionamento estabelecido pelo contrato de confidencialidade;
- Autorização de terceiro: São pessoas que precisam de autorização superior de uma pessoa de confiança, e que confirme seu vínculo empregatício, para solicitar informações ou uma ação. A pessoa de confiança que cedeu a autorização também deve ser verificada, para comprovar se ainda está empregada dentro da organização;

- Conta privilegiada: Trata-se de um computador, ou outro tipo de conta, que precisa de permissão de acesso, devido a política de autenticação. São contas com acesso privilegiado para impedir que pessoas não verificadas ou sem autorização tenham acesso aos arquivos e informações;
- Caixa de correio departamental geral: É uma caixa postal eletrônica de *voice mail* que possui uma mensagem genérica para o departamento. Tem como função proteger o número dos ramais de empregados que trabalham em determinado departamento;

4.4 PROCEDIMENTOS DE VERIFICAÇÃO

A política de segurança da informação estabelece critérios que todos os envolvidos dentro da organização são, por meio de contrato de confidencialidade, obrigados a seguir. Caso contrário, as informações confidenciais ou ativos importantes para a organização correm o risco de serem expostas, causando danos aos funcionários, à imagem da empresa e suas parcerias. Para evitar esse tipo de acontecimento, além da categorização dos empregados e classificação das informações, é essencial que os empregados recebam treinamento de procedimentos de verificação da pessoa solicitante da informação. Segundo Mitnick *et al.* (2002), os procedimentos recomendados para que os empregados verifiquem a identidade da pessoa solicitante, de informações, são divididos em três etapas, cada etapa possui métodos de verificação. Cada método de verificação tem seu ponto fraco em particular, são nos pontos fracos que o engenheiro social procura atacar.

4.4.1 Etapa de verificação de identidade

Nesta etapa são descritos métodos de verificação da pessoa solicitante das informações, como:

- Autorização: Quando uma pessoa de confiança concede autorização e assegura que a identidade do solicitante é legítima. Porém este método é o mais usado pelos engenheiros sociais para conseguir informações importantes, pois eles podem usar um pretexto, com as técnicas de persuasão, para convencer a pessoa de confiança a reconhecer sua identidade;

- Segredo compartilhado: Trata-se de uma senha ou código diário que é compartilhada por mais de um empregado, seu uso é restrito somente dentro da empresa. O fato de ser compartilhado torna esse método fraco em questão de segurança, o atacante pode consegui-lo com certa facilidade;

- Supervisor ou gerente: O empregado que recebe uma solicitação de informação deve, primeiramente, ligar para o supervisor do solicitante para verificação. Assim como o método de autorização este pode ser burlado. Mesmo que a ligação chegue ao ramal legítimo do gerente, a pessoa que atender a ligação pode ser um comparsa do atacante, afirmando credibilidade da identificação;

- E-mail seguro: Para confirmar a identidade do solicitante, o empregado solicita uma mensagem assinada digitalmente. Este método pode ser burlado se o atacante conseguir instalar *malwares* que detectam a digitação de teclas e, obtendo a senha da chave privada do empregado legítimo, acessando e-mail para envio do documento assinado;

- Pessoalmente com ID: O solicitante se apresenta pessoalmente e mostra o crachá, com foto, de um empregado ou outra identificação adequada. A possibilidade dos atacantes roubarem o crachá e falsificarem para parecer autêntico não é grande, pois com essa tática eles correm mais riscos de serem descobertos e detidos;

4.4.2 Etapa de verificação de status do empregado

Após a confirmação da identidade do solicitante, que realmente possui um vínculo empregatício com a organização, o seguinte passo é verificar o status do empregado. Isso se aplica tanto para o solicitante quanto para a pessoa que concedeu a autorização, ou seja, a pessoa supostamente de confiança também deve ser verificada.
Segundo Mitnick e Simon (2002, p.215):

> A maior ameaça à segurança das informações não vem do engenheiro social nem do invasor habilidoso de computadores, mas de alguém muito mais próximo: o empregado que acabou de ser demitido e que busca vingança ou espera abrir seu próprio negócio usando as informações roubadas da empresa.

Antes de liberar as informações confidenciais para outra pessoa, o empregado responsável deve verificar se o solicitante, ou a pessoa de confiança, ainda é empregado da empresa através dos métodos:

- Verificação na lista de empregados, se caso a empresa dispõe de uma lista *online* de empregados, com dados de status atualizados, para saber se ainda continuam ativos;
- Verificação com o gerente do solicitante, o número para verificação deve ser o que consta no cadastro da empresa, e não o número fornecido pelo próprio solicitante;
- Verificação do departamento ou grupo de trabalho do solicitante, o funcionário desse departamento deve confirmar que o solicitante ainda é empregado da empresa.

4.4.3 Etapa de verificação da necessidade de saber

Além de verificar se o solicitante ainda pertence à empresa, ainda é necessário saber o motivo de sua solicitação das informações e se tem autorização específicas que afetam equipamentos e computadores relacionados. Essa verificação pode ser feita usando um dos métodos indicados por Mitnick e Simon, como:

- Consulta as listas de cargo de trabalho/responsabilidades, essas listas são informações de classe interna ou confidencial e por motivos de acesso rápido precisam estar disponíveis *online*. A responsabilidade pela manutenção e atualização dessas listas é do proprietário das informações, ou pessoa designada pela empresa para proteger as informações confidenciais. Entretanto, essa lista é um convite para o engenheiro social, caso o atacante tome conhecimento de sua existência terá um grande motivo para obtê-la. Após a obtenção da lista, novas portas de perigos se abrirão para a empresa;
- Obter autorização de um gerente, podendo ser o próprio gerente do setor ou do solicitante, para pedir autorização;
- Obter autorização do proprietário ou criador das informações, pois o proprietário é o juiz final que determina se uma pessoa deve ou não receber o acesso;

- Obter autorização por meio de um pacote de software proprietário, este software é desenvolvido para fornecer autorização de acesso às informações. Os usuários não podem examinar os direitos de acesso de cada indivíduo, mas podem digitar o nome do solicitante e do identificador associado às informações que estão sendo pedidas. Em seguida, o software fornece uma resposta indicando se o empregado está ou não autorizado a acessar tais informações. Essa alternativa evita o risco de criar uma lista de pessoal com os respectivos direitos de acesso a informações valiosas, críticas ou confidenciais que podem ser roubadas.

4.5 GERÊNCIA DAS POLÍTICAS

As políticas de segurança são constituídas por instruções que fornecem orientações de comportamento do empregado dentro da organização, estas instruções são elemento fundamental no desenvolvimento de contra-ataque a possíveis ameaças à segurança. É essencial que a gerência do primeiro escalão forneça apoio ao desenvolvimento de políticas de segurança e de um programa de segurança das informações. Um programa de segurança será bem-sucedido, somente se a gerência demonstrar um comprometimento pelo exemplo pessoal. Os gerentes são designados para reter e garantir o manuseio seguro das informações ou ativos críticos, para eles são aplicadas políticas como classificação de dados, divulgação da informação, administração de telefone e política diversas (MITNICK; SIMON, 2002, p.207-208, 216).

A política de classificação de dados oferece uma melhor organização das informações baseando-se na sua importância e nível de gravidade caso seja exposta. A política de divulgação das informações, após a classificação, é distribuída para diversas pessoas com base em suas identidades e necessidades de obter tal informação. Na política de administração de telefone é garantido que os empregados possam verificar a identidade do interlocutor, protegendo as próprias informações contra aqueles que ligam para a empresa. Em políticas diversas são aplicadas políticas como exame dos direitos de acesso em relação a mudança de posição do empregado, projeto do crachá, identificação especial para não-empregados e desativação das contas de computador dos contratados. Cada política contém itens importantes para sua estruturação, seu esclarecimento permite o fácil entendimento por parte de todos da organização durante o processo de treinamento.

Portanto, a seguir será mostrado algumas políticas, de forma resumida, indicadas por Mitnick e Simon (2002, p. 216-224):

1) Política de classificação de dados

    a) Designação da classificação de dados é responsabilidade da empresa classificar a confidencialidade das informações e designar um responsável para ser o proprietário, e este deve controlar quem pode ter acesso e seu uso;

    b) Publicação dos procedimentos confidenciais de tratamento, é estabelecido pela organização com a finalidade de estabelecer procedimentos para distribuição das informações conforme sua categoria;

    c) Rotulação de itens, são os materiais impresso e mídias de armazenamento que contém as informações confidenciais, privadas e internas marcados de acordo com a sua classificação.

2) Divulgação das informações

    a) Procedimento de verificação do empregado, antes de conceder a informação para terceiros é necessário saber de quem se trata. Para isso, a organização deve checar a identidade, *status* e a autorização de seu gerente. Como método de confirmar a identidade são usados tecnologias de autenticação;

    b) Distribuição de informações confidenciais, as informações que podem causar um dano substancial em caso se roubada, devem ser entregues somente à pessoas de confiança;

    c) Transferência de arquivos, como dados eletrônicos, não devem ser transferidos para nenhuma mídia removível sem permissão. Somente uma pessoa de confiança com identidade verificada e esclarecido sua motivação pode executar esse processo.

3) Política de administração de telefone

    a) Encaminhamento de chamadas nos números de discagem ou fax. Esse tipo de serviço permite o encaminhamento das chamadas para números de telefones externos, mas não deve ser usado em qualquer modem de discagem interna da empresa;

b) ID de chamadas, para capacitar a identificação da linha do interlocutor, instalados para distinguir as chamadas externas e internas;

c) Caixas postais de departamento, ou caixa postal de voz genérica, protegem os nomes e números de telefone dos empregados, consequentemente, limitando a coleta de informações pelos engenheiros sociais;

d) Ramais de telefone restritos, usados apenas para comunicação interna entre departamentos, bloqueia uma parte dos atacantes considerados amadores, porém permite a ligação de interna para externa caso um empregado seja convencido a ligar.

4) Políticas diversas

a) Projeto do crachá do empregado, deve melhorar a distinção de empregados e visitantes, para facilitar saber de quem se trata e o setor que pertence. De preferência com foto grande;

b) Identificação especial dos não-empregados, a empresa deve prover crachás exclusivos para visitantes, evitando que pessoas não autorizadas consigam entrar na empresa;

c) Desativando contas do computador dos contratados, evitando uma possível revolta, para que o ex-funcionário tenha acesso às informações depois de ser destituído de seu cargo. Isso deve incluir a exclusão no cadastro de autenticação, caso o funcionário tenha autenticação biométrica por exemplo;

d) Organização do relatório de incidentes, incluindo atitudes suspeitas, estabelecidos pelas empresas, dessa forma é possível determinar o que o atacante está querendo roubar e melhorar a proteção nos pontos atacados;

e) Teste de vulnerabilidade, é preciso que seja avisado para todos os departamentos, são um teste eficaz para avaliar o desempenho do treinamento de conscientização de segurança. Caso a empresa não notifique de que se trata de um teste, alguns funcionário podem sofrer danos psicológicos devido ao estresse e nervosismo.

5. MATERIAIS E MÉTODOS

No presente trabalho é demonstrado um exemplo de vulnerabilidade conhecida como *“phishing”* em ambiente virtualizado, portanto, o teste será seguro e não afetará o sistema do computador. Os materiais para realizar essa prática simulada são *Virtual Box*, sistemas operacionais *Kali Linux* e *Linux Mint* e a ferramenta *Social Engineering Toolkit* (*SET*). A metodologia para esta demonstração consiste em usar a *Virtual Box* para emular um ambiente virtual para o *Kali Linux* (sistema atacante) e *Linux Mint* (vítima).

De acordo com a documentação Oracle VM (2022), *Vitrual Box* é um *software* de virtualização que permite os usuários executarem vários sistemas operacionais em uma única máquina, sem riscos para sua máquina e seus arquivos internos.

Segundo Wilson (2022), *“Kali Linux* (anteriormente conhecido como BackTrack Linux) é uma distribuição Linux de código aberto, baseada no sistema operacional *Debian*, destinada a testes avançados de penetração e auditoria de segurança”. Uma dessas ferramentas é o *SET*, utilizado por pesquisadores para efetuar testes de penetração.

O sistema operacional *Linux Mint* é uma distribuição Linux com o propósito de ser potente, prático e, assim como o *Kali,* também é baseado no sistema operacional *Debian*. Este capítulo começará pela forma como o ambiente foi criado, as configurações de cada ferramenta para concretizar a demonstração de *phishing*.

5.1 CONFIGURAÇÃO DE AMBIENTE

5.1.1 *Virtual Box*

No emulador *Virtual Box* existem opções de configurações de *hardware* respectivamente para cada máquina virtual, para tal deve-se selecionar a máquina a ser configurada e, em seguida, clicar na opção “Configurações”, assim, será mostrado algumas opções de sistema como, opções de configurações de vídeo / monitor, memória primária e interface de rede. Para a máquina que irá realizar o *pentest*, neste caso o Sistema Operacional *Kali* é necessário realizar a configuração de duas interfaces de rede, sendo uma como rede interna ou *intnet* e outra como *NAT* (*Network Address Translation*). A máquina a ser explorada, neste caso, com o Sistema Operacional *Mint*, apenas uma interface deve ser

configurada como rede interna. Resumidamente, rede interna ou *intnet* é um tipo de rede que permite somente comunicação entre máquinas, mas impede o acesso a rede externa, como a *Internet*. Em contrapartida, a rede *NAT* é especificamente para acessar a rede externa, mas impede a comunicação entre máquinas na mesma rede local.

As placas de rede do *Kali* são apresentadas na Figura 1, esquerda: rede interna; direita: *NAT*, e na Figura 2 a placa de rede configurada como rede interna.

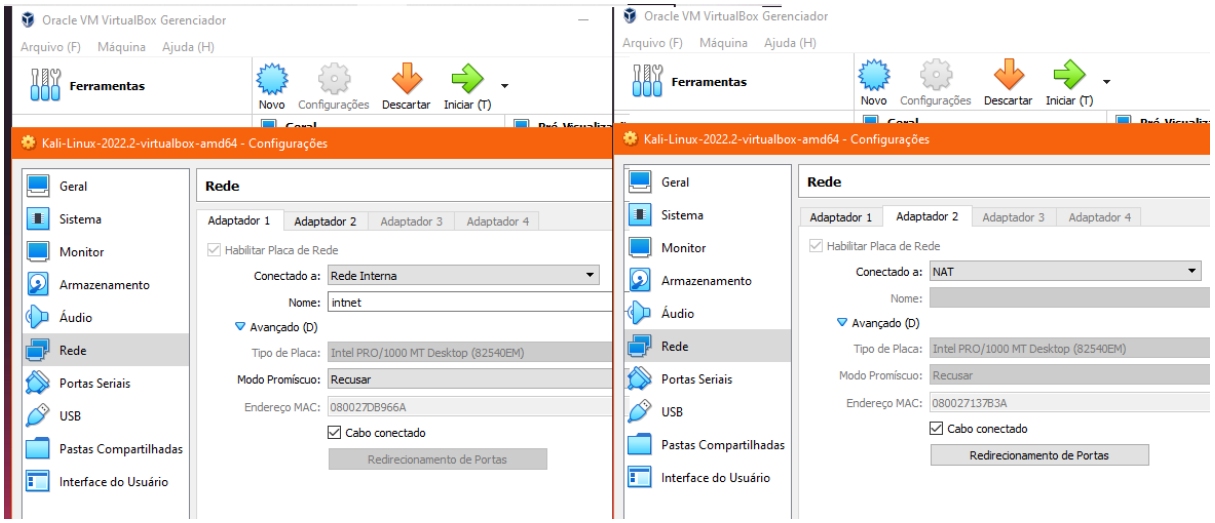

Figura 1: Configurações da placa de rede do *Kali Linux* - fonte: da autora

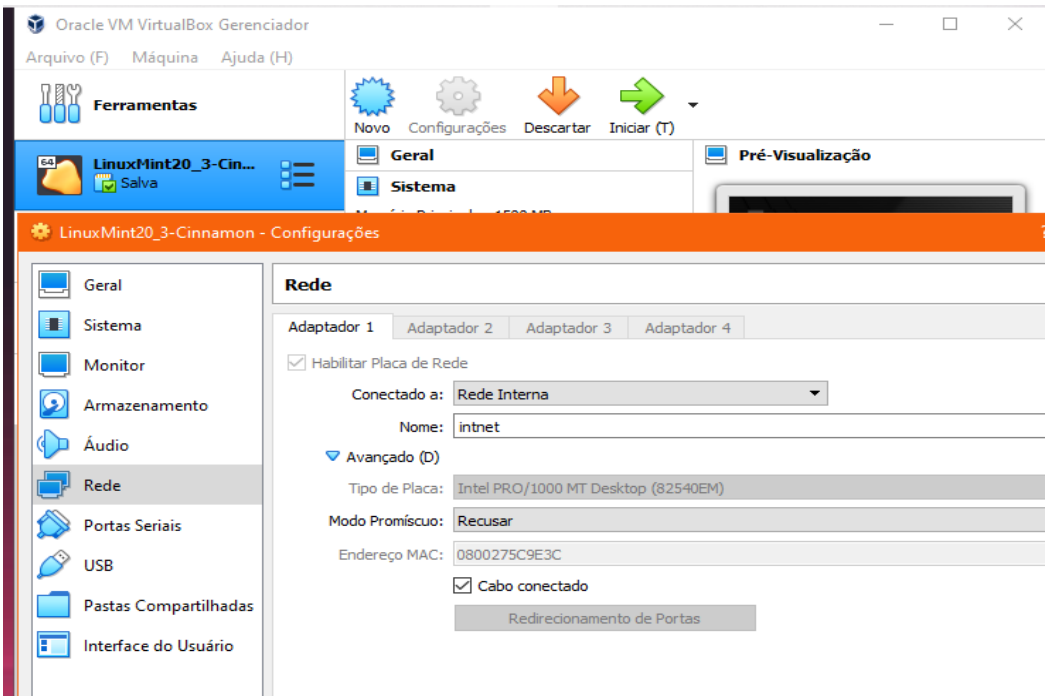

Figura 2: Configuração da placa de rede do *Linux Mint* - fonte: da autora

Como pode ser observado na Figura 1 e Figura 2, as placas de rede estão devidamente configuradas e prontas para iniciar o sistema. No tópico seguinte será demonstrado as configurações das interfaces de rede dos hosts Kali e *Mint* respectivamente.

5.1.2 Kali Linux

Antes do processo de configuração do *Kali* é preciso atualizar o sistema, dessa forma seus aplicativos e *frameworks* são atualizados, permitindo maior segurança como indicado nas recomendações da cartilha de segurança.

Após a atualização do *Kali* foram executados os seguintes passos:

1. Entrar em modo super usuário para ter acesso a comandos especiais e permissão para alterar arquivos;
2. Verificação do *status* de interface de rede, como mostrado na Figura 3,. A placa de rede *eth0* está com acesso a rede interna, e a *eth1* está configurada para *Internet*, ambas já possuem endereços *IP*;

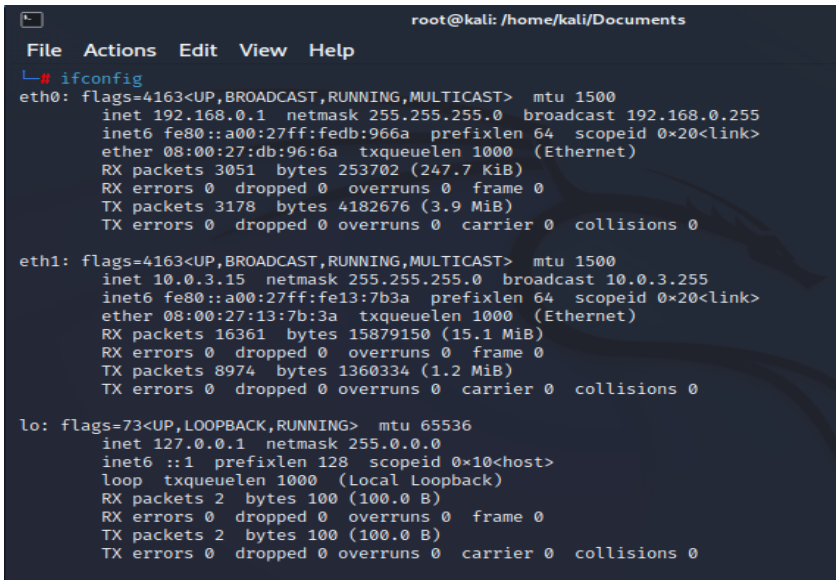

Figura 3: Status das interfaces de rede do *Kali* - fonte: da autora

3. Se no processo de verificação, houver algum problema e, não tiver um *IP* configurado, o arquivo de configuração de interface deve ser editado manualmente. O arquivo pode ser acessado por meio do comando: *"nano /etc/resolv.conf"*. No *Kali* o terminal deve ser semelhante a Figura 4.

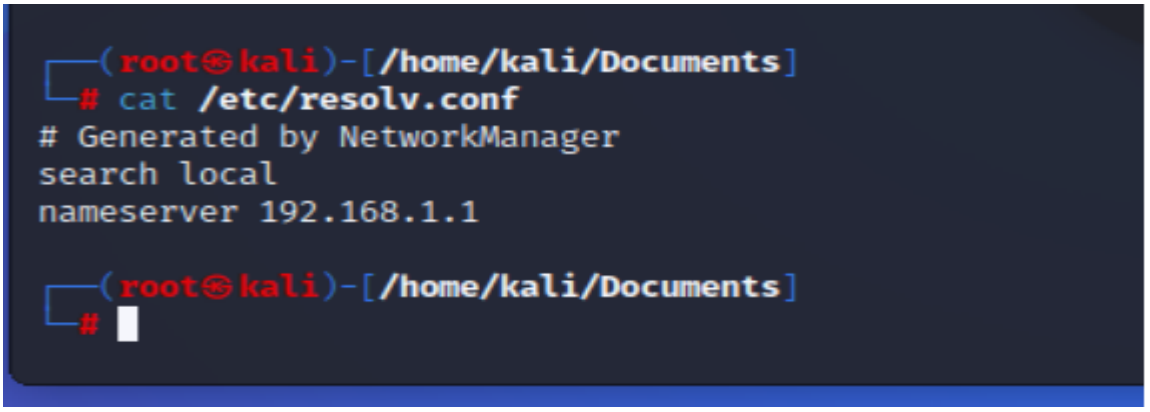

Figura 4: Arquivo de configuração da interface de rede - fonte: da autora

4. Para finalizar a configuração do *Kali* deve ser usado os comandos *"service apache2 restart"* e *"service apache2 status"*. Com o último comando o terminal exibirá uma tela, com *"active (running)"*, indicando que o serviço foi reiniciado com as novas configurações.

5.1.3 Linux Mint

O processo de instalação para o *Mint* não difere muito, assim que iniciado deve atualizar todos os seus componentes antes de começar as configurações. Em seguida será executados os passos:

1. Logar como super usuário para ter permissão de acesso e modificação dos arquivos;
2. Verificar a interface de rede, no *Mint* a placa é *enp0s3*, com o comando *ifconfig*. Para que o *Mint* possa se comunicar com o *Kali* é preciso que o endereço *IP* esteja como mostra na Figura 5;

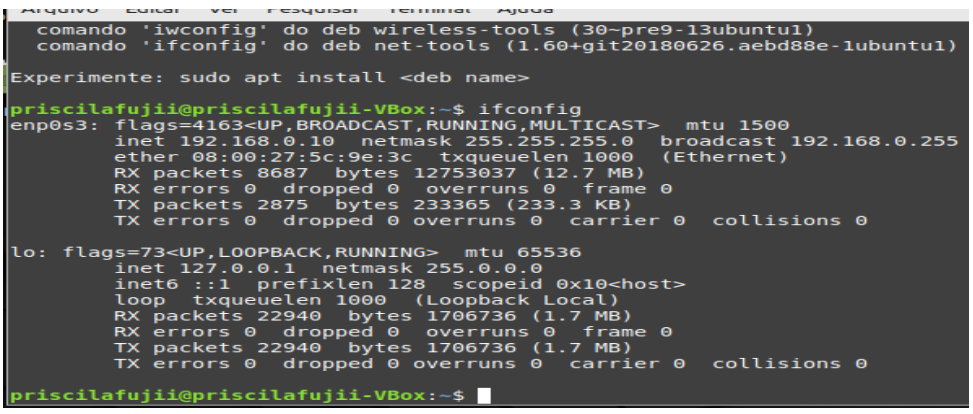

Figura 5: Status da interface de rede do *Mint* - fonte: da autora

3. Além da configuração de endereço *IP* é necessário definir o *gateway* padrão e outros itens, como é mostrado na Figura 6;

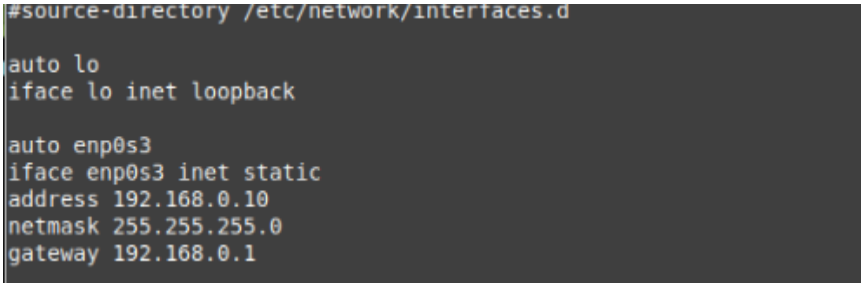

Figura 6: Arquivo de configuração da interface de rede do *Mint* - fonte: da autora

4. Reinicie a máquina *Mint* para que as alterações sejam devidamente instaladas;

Finalizado o processo de configuração de ambas as máquinas convidadas, é necessário testar a comunicação entre elas. Para esse teste será usado o comando *ping*, quando digitado deve ser seguido pelo endereço *IP* da máquina a qual busca comunicação. Por exemplo, no terminal do *Mint* o usuário deve digitar *ping* 192.168.0.1 seguido de Enter, e no *Kali* será *ping* 192.168.0.10. A Figura 7 pode mostrar que o teste de comunicação, de *Mint* para *Kali*, foi bem-sucedido.

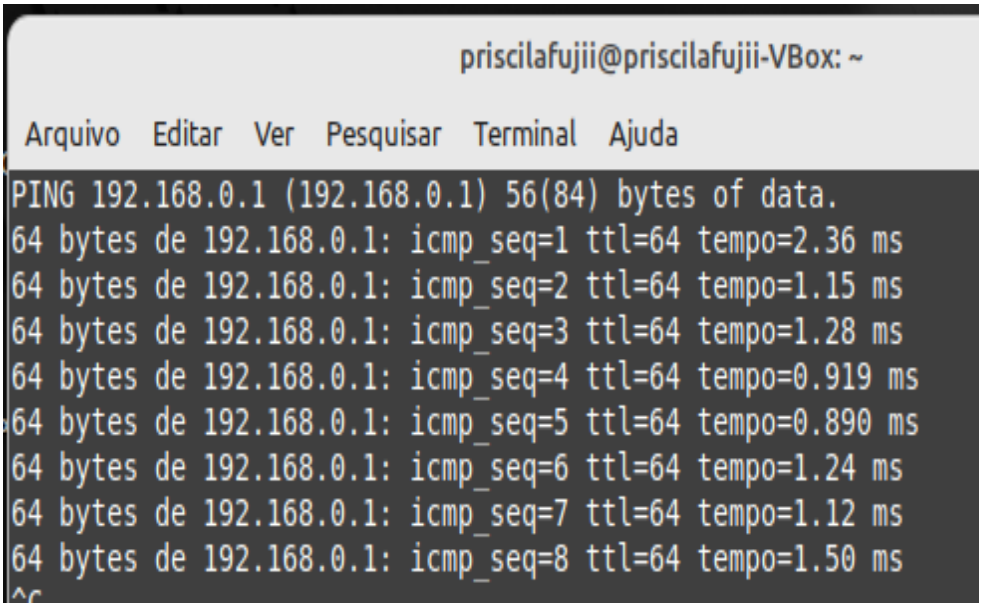

Figura 7: Ping de *Mint* para *Kali* - fonte: da autora

Para que o *ping* funcione a máquina na mesma rede deve estar ligada, caso contrário aparecerá uma mensagem de inalcançável.

5.2 TESTE DE VULNERABILIDADE COM *PHISHING*

Para efetuar o teste de vulnerabilidade, proposto neste trabalho, foi utilizado a ferramenta *SET (Social Engineering Toolkit)*, que contém vários fatores de ataques que usam engenharia social. Para iniciá-lo é preciso estar logado como super usuário no sistema do *Kali*, em seguida digitar o comando *"setoolkit"* e logo aparecerá a interface do *software*.

De início será fornecido opções como *"fast-track penetration"* (penetração rápida), "*third party modules"* (módulos de terceiros) e *"Social Engineering Attacks"* (ataques de engenharia social). Como pode ser observado na Figura 8.

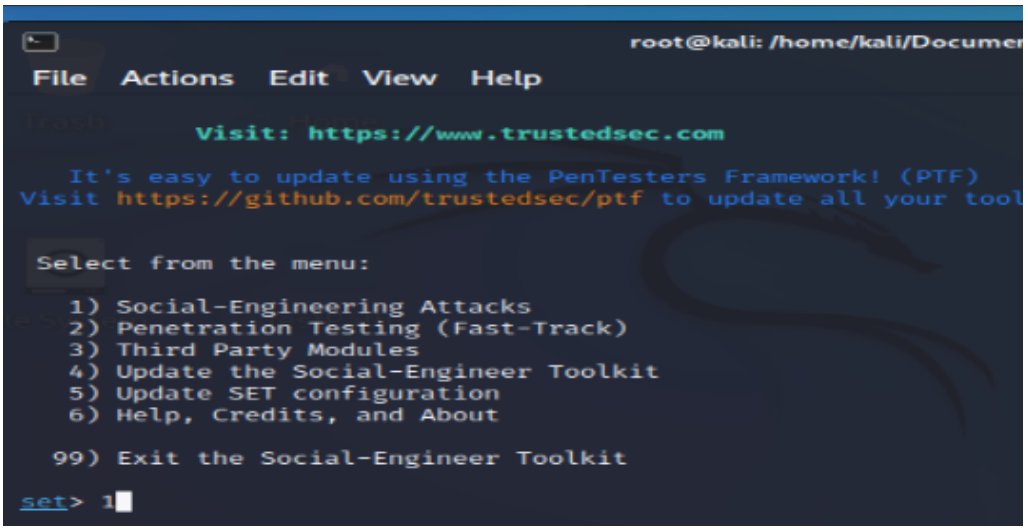

Figura 8: Primeiro menu do *SET* - fonte: da autora

Após escolher a primeira opção, será mostrado outro menu com opções de ataques a sites, desta vez a escolha será o segundo item *"website attack vectors"* (vetor de ataque ao site), como mostrado na Figura 9.

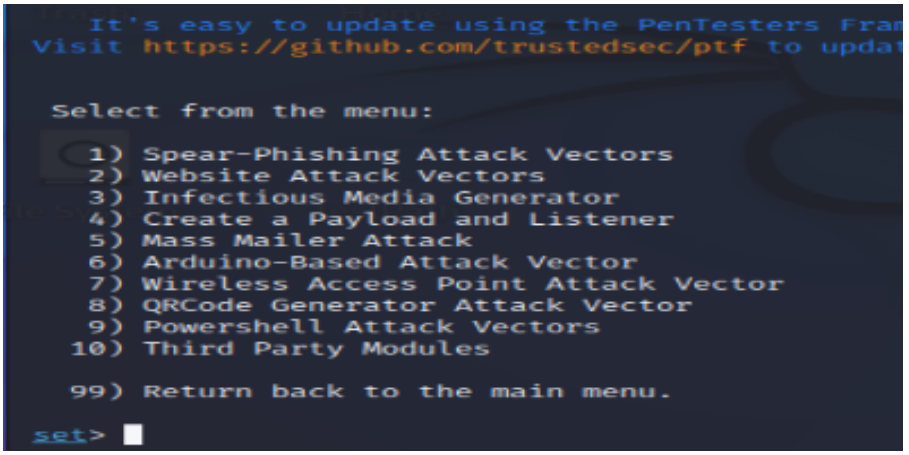

Figura 9: Segundo menu de opções - fonte: da autora

Novamente o *SET* fornecerá mais 7 opções para métodos de ataque, como por exemplo *"Java Applet Attack Method"* (método de ataque ao applet[5] Java), *"Metasploit Browser Exploit Method"* (método de exploração do navegador metasploit) e, a opção escolhida, *"Credencial Harvester Attack Method"* (método de ataque do coletor de credenciais), como pode demonstrado na Figura 10.

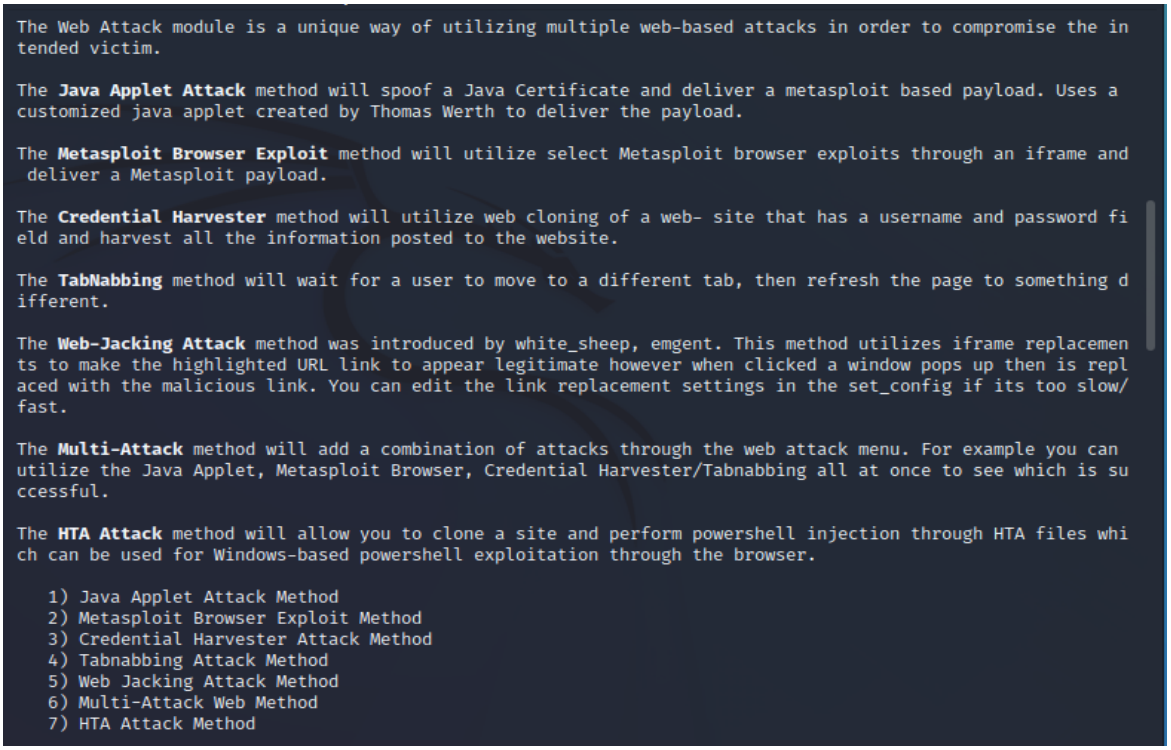

Figura 10: Terceiro menu de opções - fonte: da autora

[5] Pequenos programas que executam tarefas específicas numa *webpage*. Costumam ser embutidos no sistema operacional ou aplicativos.

Por fim, as últimas três opções fornecidas pelo SET, observando a Figura 11, as opções começando dos primeiros modelos web, segundo clonagem de site e importação personalizada. A opção escolhida será a segunda.

Figura 11: Último menu de opções - fonte: da autora

Depois da escolha, a ferramenta SET solicitará o endereço IP onde o site falso deve ser disponibilizado e apertar Enter, neste momento o atacante deve colocar o IP da própria máquina, o IP respectivo da interface “eth0”, como foi ilustrado na Figura 3. Em seguida o SET solicitará que o usuário forneça o link URL do site que deseja clonar. Quando o terminal apresentar a tela como a Figura 12, a clonagem estará realizada, apenas aguardando a vítima acessar o site clonado.

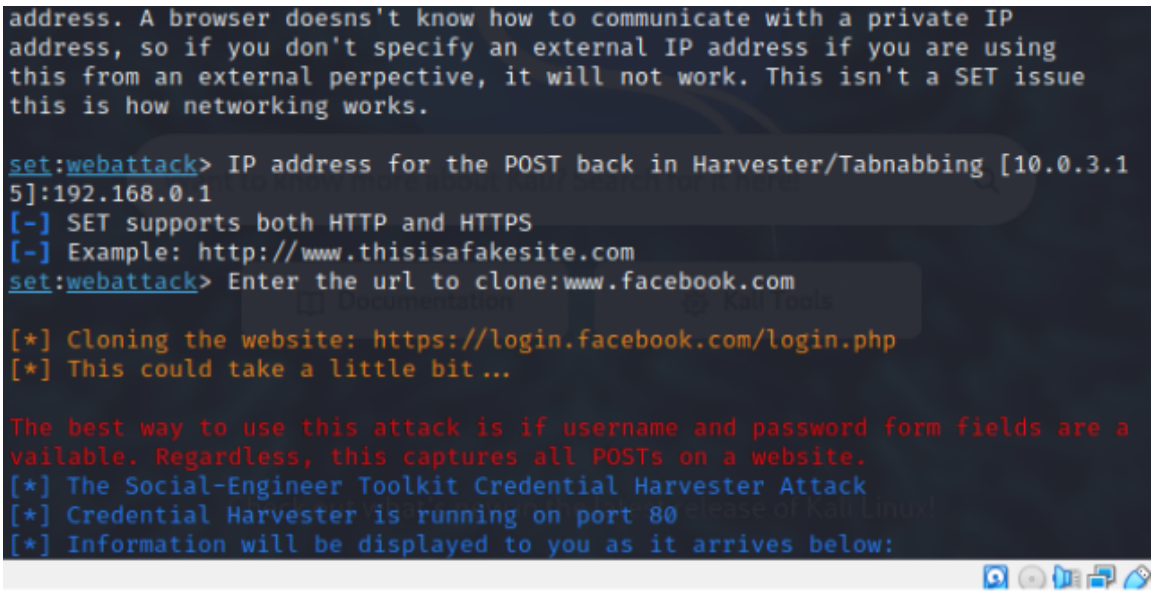

Figura 12: *Kali* **aguardando** o acesso da vítima - *fonte: da autora*

Como foi configurado anteriormente, a rede do Mint é voltada para comunicação somente com outras máquinas na mesma rede interna, sendo incapaz de acessar o google ou firefox e fazer uma pesquisa. Neste ataque, a vítima (Mint) não terá outra opção a não ser o site falso com phishing esperando. A máquina atacante (Kali) consegue acessar a Internet e, isso permite sua clonagem dos sites, o clone é disponibilizado na rede interna. Quando a vítima acessar o navegador e digitar o endereço IP da máquina atacante, o SET irá detectar uma tentativa de acesso e mostrará ao atacante as informações como IP de origem da vítima, tipo de acesso e a data e hora do acesso, como mostra a Figura 13.

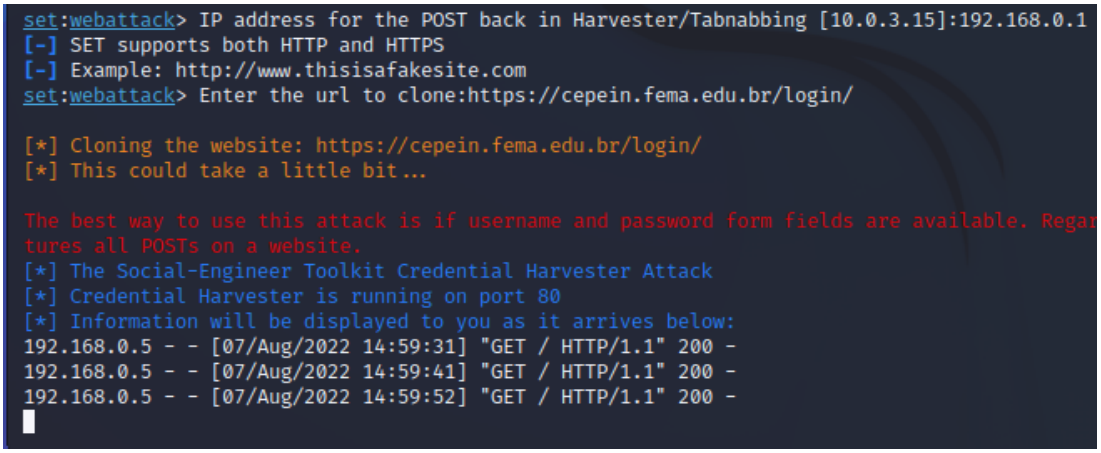

Figura 13: Acesso ao *site* falso detectado - *fonte: da autora*

Neste caso, o *site* clonado foi o Facebook, quando a vítima digitar o endereço *IP*, supondo que foi fornecido pelo atacante, será apresentado uma página de *login* do Facebook solicitando o e-mail e senha. Como ilustra a Figura 14.

Figura 14: *Site* clonado do Facebook - fonte: da autora

Quando o formulário de *login* for preenchido e clicar Enter a página recarregará, mas não apresenta nada após isso. Enquanto isso, no terminal do atacante (*Kali*) aparecerá as credenciais digitadas pela vítima, e caso a vítima não desconfie do ataque e recarregue a página para uma nova tentativa o *SET* estará pronto para uma nova captura. Como ilustra a Figura 15.

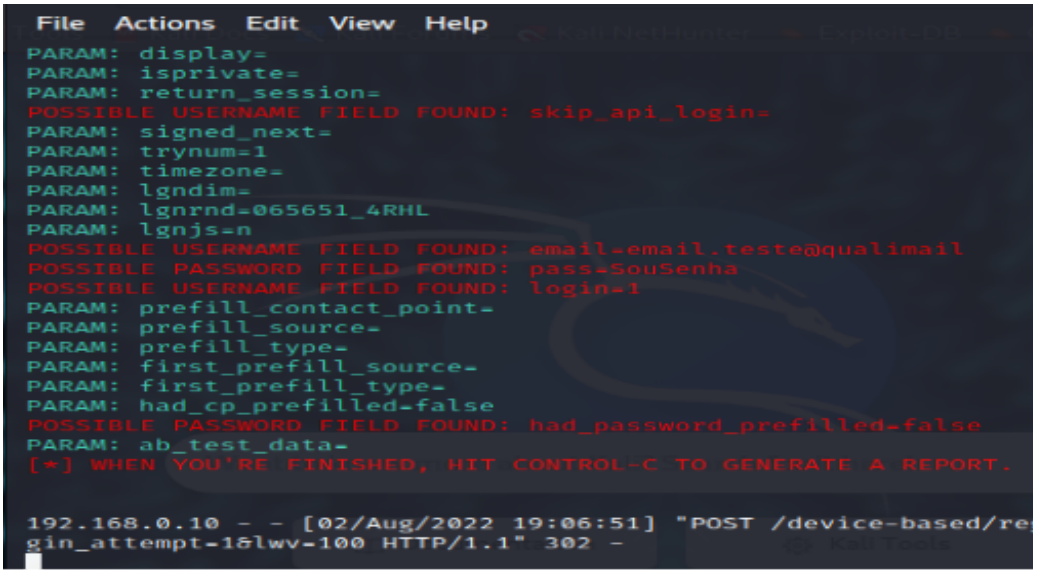

Figura 15: Credenciais obtidas da vítima, nas três linhas vermelhas - fonte: da autora

5.3 RESULTADOS E DISCUSSÃO

Na simulação apresentada observou-se que a ferramenta *SET* foi muito eficiente no que se refere a esse tipo de teste de vulnerabilidade, uma vez que, obteve informações de uma máquina vítima, contudo, é possível escalar uma quantidade maior de dispositivos na rede interna para captar os dados sensíveis como login e senha.

O atacante pode ativar o *site fake* e enviar seu *link* para outros usuários por meio de email, entretanto, para aqueles que desconfiam de um *link* como “http://192.168.0.1”, existe uma ferramenta que disfarça o *IP* para um conjunto alfabético de *string*, denominada encurtador de *URL*. No entanto, este pequeno truque funciona para os usuários distraídos e apressados. Antes de clicar no *link*, o usuário deve colocar o cursor do *mouse* em cima do *link*, com isso aparecerá o verdadeiro *link* no canto inferior esquerdo para onde o usuário será direcionado, permitindo a visualização. No caso de inconsistência, o usuário nunca deve clicar no *link* enviado.

Supondo que seja enviado um *link* para baixar um aplicativo nessa rede interna, quantos usuários não seriam afetados pela instalação de um Tróia sem perceber. Nesta rede interna podem ter várias máquinas, mas basta uma ser hackeada para causar danos. Mesmo que o usuário tenha dúvidas em relação ao *link* falso, o atacante pode reavaliar o perfil do usuário para mudar a tática de abordagem, e é nesse ponto que entra os princípios da engenharia social.

6. CONSIDERAÇÕES FINAIS

Apesar de estarmos no ano 2022, no tempo das tecnologias modernas, existem as pessoas que ainda sentem dificuldade em lidar com dispositivos modernos ou a própria Internet. Por esse motivo, as pessoas acabam sendo ignorantes quanto à segurança da informação, principalmente as pessoas que acreditam na ilusão da segurança cibernética e se esquecem que por trás das telas ainda existem pessoas capazes de aplicar golpes. Este trabalho teve como propósito informar ao leitor dos riscos relacionados à informação, que existem ao utilizar a Internet de forma descuidada. No entanto, a Internet não é o único meio de comunicação, ainda sucedem casos de golpes por telefone ou pessoalmente. Por mais que as tecnologias sejam desenvolvidas com a finalidade de proporcionar melhor segurança, o fator humano não acompanha esse ritmo. Essa questão não é recente, ataques cibernéticos podem ser recorrentes caso as pessoas não tomem consciência do risco e não sejam treinadas adequadamente, como foi citado no capítulo de métodos de proteção.

Para que o usuário possa compreender como é possível acontecer um ataque através das vulnerabilidades, definiu-se objetivos específicos que consistem na conscientização dos riscos cibernéticos como a instalação de *malwares*, negligência nas configurações de segurança do sistema e as técnicas de persuasão dos engenheiros sociais. Em relação às vulnerabilidades cibernéticas foi conclusivo que efetuar atualizações, do sistema e aplicativos, regularmente é indispensável, pois a cada versão atualizada são corrigidos brechas ou erros das versões anteriores. Isso vale para a proteção contra instalação de *malwares* no sistema, porém a atualização e configuração do navegador não pode ser deixada de lado. Como foi observado no capítulo de materiais e métodos, o ataque de *phishing* foi executado sem problemas e o navegador não bloqueou, ou sequer notificou algo de errado. Para o ataque de *phishing* é conclusivo que a melhor medida é a instalação de extensões capazes de detectar o *phishing*, ou verificar o direcionamento do *link* com o cursor do *mouse*. No que diz respeito a engenharia social foi abordada a questão das técnicas utilizadas para conquistar a confiança de outra pessoa, e como isso pode alcançar e afetar a segurança local, já que o fator humano é um potencial agente de vulnerabilidade. Nenhum sistema de segurança consegue superar o fornecimento espontâneo de informações. A análise permitiu concluir que o fator humano pode deixar de ser um risco, ou no mínimo mitigar, se implementado um treinamento correto e conscientização constante.

Dessa forma, o objetivo proposto neste trabalho de informar, e conscientizar, o usuário pôde ser atingido visto que não é possível eliminar completamente os riscos e vulnerabilidade, mas minimizá-los. Seguindo as recomendações propostas no capítulo 4 é plenamente viável se proteger contra os riscos da Internet e melhorar a proteção contra a engenharia social. Relembrando que por mais tentador que seja o *link*, ele nunca deve ser aberto sem ser verificado antes, ou reforce a proteção do navegador com extensões adicionais. Em caso de mais pessoas utilizarem o mesmo dispositivo é preciso separar a área de trabalho criando contas individuais. Isso é responsabilidade básica esperada do usuário.

As ferramentas utilizadas neste trabalho permitiram uma análise detalhada do ataque de *phishing* e, com isso, facilitar o entendimento do usuário de como a coleta de informações como credenciais, ou qualquer informação que seja preenchida no falso formulário, pode ser bem fácil e imperceptível.

Em pesquisas futuras é estimado a melhoria da segurança da informação, e paralelamente à essa melhoria é esperado o aperfeiçoamento dos riscos e vulnerabilidades. É esperado que este trabalho sirva de referência para conscientização das vulnerabilidades associadas à informação, sejam elas cibernéticas ou sociais.

REFERÊNCIAS

ALEXANDRIA, João C. **Gestão da Segurança da Informação - Uma proposta para potencializar a Efetividade da Segurança da Informação em Ambiente de Pesquisa Científica**. 2009. p.183. Tese (Doutorado) - Área de tecnologia nuclear - Universidade de São Paulo, 2009.

ALMEIDA, Maurício B.; SOUZA, Renato R.; COELHO, Kátia C. Uma proposta de ontologia de domínio para segurança da informação em organizações: descrição do estágio terminológico. **Informação & Sociedade: Estudos**, v.20, n.1, jan/abr, 2010. p. 1-20.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT ISO/IEC 17799: 2001**. Disponível em <https://tororodeideias.files.wordpress.com/2012/03/nbr-iso-iec-17799.pdf> Acesso em 1 de Setembro. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT ISO/IEC 27001: 2006**. Disponível em <https://jkolb.com.br/wp-content/uploads/2016/09/ABNT-NBRISOIEC27001-20060331Ed1.pdf> Acesso em 1 de Setembro. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT ISO/IEC 27001: 2013**. Disponível em: <https://www.normas.com.br/visualizar/abnt-nbr-nm/25074/abnt-nbriso-iec27001-tecnologia-da-informacao-tecnicas-de-seguranca-sistemas-de-gestao-da-seguranca-da-informacao-requisitos>. Acesso em 31 de Agosto. 2022.

BELCIC, Ivan. **As melhores extensões para privacidade e segurança**. Disponível em: <https://www.avast.com/pt-br/c-best-security-and-privacy-extensions-for-google-chrome#:~:text=Uma%20das%20melhores%20extens%C3%B5es%20antiv%C3%ADrus,(isso%20se%20chama%20pharming).>. Acesso em 29 de Setembro.

BROSTOFF, Alexander. **Improving password system effectiveness**. 2005. p.263. Tese (Doutorado) - Departamento de informática - UCL (instituição de ensino superior em Londres). Londres, Londres, 2005.

CIALDINI, Robert. Influence. **Influencia** (publicação original da editora Collins, Traduzido para espanhol por Laya). 26 de Setembro. 2006.

CIALDINI, Robert. **The Science of Persu**. Digitalwellbeing.org. Disponível em: <https://digitalwellbeing.org/downloads/CialdiniSciAmerican.pdf>. Acesso em: 15 de Setembro. 2022.

GARFINKEL, Simson; SPAFFORD, Gene; SCHWARTZ, Alan. **Practical Unix & internet security**. 3. ed. Editora: O'Reilly Media, 2003.

LEFEBVRE, Clement; VERMEULEN, Vincent; OSCAR. **Sobre Linux Mint**. linuxmint. Disponível em: <https://www.linuxmint.com/about.php>. Acesso em: 30 Setembro. 2022.

MITNICK, Kevin; SIMON, William. A Arte de Enganar. Tradução de Kátia A. Roque. São Paulo: Pearson Education, 2002.

MOSIN, Nilesh Prajapati, Safvan Vohara. Case study on social engineering techniques for persuasion. **International journal on applications of graph theory in wireless ad hoc networks and sensor networks**, v.2, n.2, Junho 2010.

NASCIMENTO, Anderson; YUGE, Claudio. **O que é Phishing**. Canaltech. Disponível em: <https://canaltech.com.br/seguranca/o-que-e-phishing/>. Acesso em 26 de Set.

NIC.br (Núcleo de Informação e Coordenação do Ponto BR); CGI.br (Comitê Gestor da Internet no Brasil). CERT.br (Centro de Estudos e Tratamento de Incidentes de Segurança do Brasil). **Cartilha de segurança para Internet ver 4.0**. 2. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012.

ORACLE. **Manual do Usuário**. Oracle® VM VirtualBox®. Disponível em: <https://www.virtualbox.org/manual/UserManual.html#features-overview>. Acesso em: 26 set. 2022

PAIS, Ricardo; MOREIRA, Fernando; VARJÃO João. Engenharia social (ou o carneiro que afinal era um lobo). In: PEDRO CAMPOS E PEDRO QUELHAS DE BRITO (eds.) NOVAS TENDÊNCIAS EM MARKETING INTELLIGENCE, 2013. Porto, Portugal. **Resumos**. Porto, Escola de Gestão de Porto, 2013. Res. 171-187.

RODRIGUES, Renato. **Brasileiros são principais alvos de ataques de phishing no mundo**. Kaspersky Daily. Disponível em: <https://www.kaspersky.com.br/blog/brasileiros-maiores-alvos-phishing-mundo/17045/>. Acesso em 16 de set. 2022.

STANCIK, Peter. **USB Thief, um nuevo malware que rouba dados de dispositivos extraíbles**. We Live Security. Disponível em: <https://www.welivesecurity.com/la-es/2016/03/24/usb-thief-roba-datos-dispositivos-extraibles/>. Acesso em: 5 de out. 2022.

VELASCO, Ariana; SALUTES, Bruno. **O que é Segurança da informação?** Canaltech. Disponível em <https://canaltech.com.br/seguranca/seguranca-da-informacao-o-que-e-158375/>. Acesso em 4 de out. 2022.

WILSON, Ben. **O que é Kali Linux?** Documentação Kali. Disponível em: <https://www.kali.org/docs/introduction/what-is-kali-linux/>. Acesso em 25 set. 2022.