UNIVERSIDADE DO SAGRADO CORAÇÃO

PAULO HENRIQUE GAIOTTI DE OLIVEIRA

ANÁLISE DE VULNERABILIDADE UTILIZANDO TÉCNICAS DE ATAQUE PHISHING NA REDE SOCIAL FACEBOOK

BAURU
2016

PAULO HENRIQUE GAIOTTI DE OLIVEIRA

ANÁLISE DE VULNERABILIDADE UTILIZANDO TÉCNICAS DE ATAQUE PHISHING NA REDE SOCIAL FACEBOOK

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas da Universidade do Sagrado Coração, como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação, sob orientação do Prof. Me. Henrique Pachioni Martins.

BAURU
2016

PAULO HENRIQUE GAIOTTI DE OLIVEIRA

ANÁLISE DE VULNERABILIDADE UTILIZANDO TÉCNICAS DE ATAQUE PHISHING NA REDE SOCIAL FACEBOOK

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas da Universidade do Sagrado Coração, como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação, sob orientação do Prof. Me. Henrique Pachioni Martins.

Banca examinadora:

_____
Prof. Me. Henrique Pachioni Martins
Universidade do Sagrado Coração

_____
Prof. Me. Patrick Pedreira Silva
Universidade do Sagrado Coração

_____
Prof. Dr. Elvio Gilberto da Silva
Universidade do Sagrado Coração

Bauru, 25 de novembro de 2016.

AGRADECIMENTOS

Primeiramente quero agradecer a Deus por ter me dado saúde para estar aqui hoje, meus pais Isaura e Marcos que sempre fizeram de tudo para eu realizar meu sonho que é me formar em Ciência da Computação. Minhas irmãs Ana Carolina e Danieli que me toleraram e me ajudaram durante todo esse tempo e meu avô Armando Gaiotti, que sempre me deu ótimos conselhos. Pois em todos os momentos em que eu pensava que estava tudo perdido, eles sempre me reergueram, me apoiaram, incentivaram e me deram forças para que eu pudesse continuar em busca dos meus sonhos.

Agradeço e muito ao meu Orientador Prof. Me. Henrique Pachioni Martins, ao Prof. Me. Patrick Pedreira Silva e ao Prof. Dr. Elvio Gilberto da Silva, que me ajudaram em tudo que sempre precisei em toda minha carreira acadêmica, e além de serem ótimos professores, se tornaram meus amigos.

E por fim, agradeço a todos os professores que contribuíram com meus estudos tanto no ensino fundamental quanto no acadêmico para enfim, eu me tornar Bacharel em Ciência da Computação.

“Seu trabalho vai ocupar uma grande parte da sua vida, e a única maneira de estar verdadeiramente satisfeito é fazendo aquilo que você acredita ser um ótimo trabalho. E a única maneira de fazer um ótimo trabalho é fazendo o que você ama fazer. Se você ainda não encontrou, continue procurando.”
(Steve Jobs).

RESUMO

Devido ao grande avanço da tecnologia, surgiram também várias ameaças de vírus em computadores que são espalhados pela internet todos os dias. A grande ameaça e a mais utilizada nos dias de hoje é o Phishing, que pode ocorrer de diversas formas como conversas falsas de e-mails que pedem para clicar em links suspeitos, páginas para imitar sites de bancos, redes sociais e outras instituições, tendo como objetivo coletar informações e dados pessoais importantes de suas vítimas. A segurança na tecnologia é de extrema importância nos dias de hoje e para não cair em armadilhas como essa, o internauta precisa estar muito atento com os métodos Phishing. Por tal razão, este trabalho teve como objetivo realizar um estudo e a demonstração de ataques Phishing na rede social Facebook através de uma rede Wi-Fi, explorando as principais técnicas e ferramentas utilizadas para sua elaboração, a fim de mostrar as vulnerabilidades e reforçar ou adquirir novos conhecimentos para contribuir com a área de segurança da informação, demonstrando formas de prevenção à este tipo de ataque. A metodologia utilizada consistiu em pesquisas bibliográficas, projeto e na realização de ataques Phishing em um ambiente virtual criado, sendo executado com familiares e obtendo então, os resultados dos testes. Visto que não foi possível colocar a página clonada na rede compartilhada e esta só pôde ser acessada pelo IP utilizado na instalação, os objetivos deste trabalho não foram atingidos completamente, porém, pôde-se demonstrar a obtenção de dados de acesso pessoais sem permissão, denominado ataque Phishing.

Palavras-chave: Vulnerabilidade em redes sociais. Phishing. Segurança da informação. Phishing em rede social.

ABSTRACT

Due to the great advancement of technology, there have also appeared several virus threats on computers that are scattered over the internet every day. The biggest and most common threat these days is Phishing, which can occur in a variety of ways, such as fake e-mail conversations asking to click on suspicious links, pages to imitate banking sites, social networks and other institutions. Collect important information and personal data from their victims. Security in technology is of the utmost importance these days and not to fall into such traps, Internet users need to be very attentive to Phishing methods. For this reason, this work aimed to carry out a study and demonstration of Phishing attacks on the social network Facebook through a Wi-Fi network, exploring the main techniques and tools used for its elaboration, in order to show the vulnerabilities and strengthen or Acquire new knowledge to contribute to the area of information security, demonstrating ways to prevent this type of attack. The methodology used consisted of bibliographic research, design and the accomplishment of Phishing attacks in a created virtual environment, being executed with relatives and obtaining, then, the results of the tests. Since it was not possible to place a page in a shared network and this is an access point via IP used in the installation, the objectives of this work were not completely defined, however, it was possible to demonstrate a obtaining of access data without permission, called Phishing Attack.

Keywords: Vulnerability in social networks. Phishing. Information security. Phishing in social network.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AP - Access Point (Ponto de Acesso)

CRC - Cyclic Redundancy Check (Verificação de Redundância Cíclica)

IBGE - Instituto Brasileiro de Geografia e Estatística

IEEE - Institute of Electrical and Electronics Engineers

IP - Internet Protocol (Protocólo de Internet)

IV - Initialization Vector (Vector de Inicialização)

OSI - Open Systems Interconnection (Interconexão de Sistemas Abertos)

RAM - Random Access Memory (Memória de Acesso Aleatório)

SSID - Service Set Identifier (Identificador de Conjunto de Serviço)

URL - Uniform Resource Locator (Localizador Padrão de Recursos)

WEP - Wired Equivalent Privacy

SUMÁRIO

1 INTRODUÇÃO

Com o avanço da tecnologia, surgiram também várias ameaças de vírus em computadores que são espalhados pela internet todos os dias e uma grande e a mais utilizada ameaça nos dias de hoje é o Phishing, que tem o objetivo de coletar informações e dados pessoais importantes de suas vítimas.

O Phishing pode ocorrer de diversas formas como conversas falsas de e-mails que pedem para clicar em links suspeitos, páginas para imitar sites de bancos, redes sociais e outras instituições, sempre no intuito de roubar informações confidenciais de pessoas ou empresas, ou seja, com este tipo de ataque os invasores podem conseguir nomes de usuários e senhas de um site qualquer, como também podem obter dados de contas bancárias e cartões de crédito.

A segurança na tecnologia é de extrema importância e para não cair em armadilhas como essa, o internauta precisa estar muito atento com os métodos Phishing.

Entre os serviços mais acessados através da Internet, as redes sociais são um sucesso entre os internautas de todo o mundo, somando cada dia mais e mais usuários. O grande sucesso dos sites de relacionamento criou um novo espaço para compartilhamento de informações, consequentemente, formou um mural no qual usuários mal-intencionados garimpam e extraem informações privadas de usuários desprotegidos utilizando-se de técnicas psicológicas, a engenharia social.

Completando todos os campos pertencentes ao Profile, o usuário publicará informações valiosas para prática do Phishing ou roubo de identidade, isto é, nome, cidade, opção sexual, visão política, religiosidade, instituições de ensino e local de trabalho já formam um quadro completo a ser explorado por um indivíduo mal intencionado.

De acordo com a Kaspersky Lab, 22% dos golpes Phishing são direcionados para usuários do Facebook, sendo que o total de ataques é assustador, já que foram registrados mais de 600 milhões de tentativas de acesso indevido, detectado só com os usuários dos produtos da Kaspersky. A explicação do analista sênior de segurança da Kaspersky Lab, Fabio Assolini, é que este tipo de ataque funciona porque joga com a confiança das pessoas, ou seja, com a engenharia social. Os usuários tendem a confiar muito mais em mensagens que vêm de amigos do que as de pessoas estranhas (MANNARA, 2015).

Mannara (2015) ainda destaca que muitos usuários já caíram em armadilhas de cibercriminosos no Facebook, e que estes golpes são disseminados com a criação de sites falsos que imitam o Facebook para roubar dados, e-mails que pedem credenciais mas não passam de um golpe e mensagens que escondem vírus.

Nos dias de hoje, estes fatos não são nenhuma novidade devido às matérias que saem em jornais, revistas e outros meios de comunicação, de pessoas que foram vítimas do ataque Phishing, tendo suas contas invadidas, e seus dados pessoais como senhas de banco entre outras coletadas e até mesmo sua vida íntima divulgadas na internet.

Devido ao contexto deste grande número de pessoas que por algum motivo, ou até mesmo por desconhecerem as vulnerabilidades de seu computador, notebook ou celular caem neste tipo de ataque, foi definido o tema deste trabalho, com o intuito de realizar um ataque Phishing em uma rede Wi-Fi local e demonstrar como estes meios podem ser facilmente invadidos, descrevendo o funcionamento de uma das técnicas de ataque mais utilizadas, com o intuito de ao final, orientar como um usuário comum deve se conectar nas redes sociais em ambientes com redes sem fio, contribuindo assim, para uma maior segurança.

2 OBJETIVOS

Este trabalho tem como objetivo, realizar uma das técnicas de ataque mais utilizadas da engenharia social, o Phishing, em uma rede social.

2.1 OBJETIVO GERAL

Realizar um estudo e demonstração de ataques Phishing na rede social Fecebook através de uma rede wi-fi, explorando as principais técnicas e ferramentas utilizadas para sua elaboração, a fim de mostrar as vulnerabilidades, demonstrando formas de prevenção à este tipo de ataque.

2.2 OBJETIVOS ESPECÍFICOS

a) Efetuar um levantamento teórico das formas de ataque Phishing.
b) Elaborar estratégias para realização dos ataques.
c) Realizar tentativas de ataque na rede social Facebook, colocando em prática os métodos pesquisados.
d) Descrever todos os procedimentos de tentativas de ataque realizados.
e) Identificar as situações em que os usuários são mais vulneráveis ao ataque.
f) Apresentar os resultados obtidos de forma a contribuir para uma maior segurança do usuário.

3 REFERENCIAL TEÓRICO

Nesta seção serão discutidos os assuntos sobre redes de computadores, segurança da infraestrutura, criptografia, ataques, redes sociais, sistemas operacionais e os trabalhos correlatos.

3.1 REDES DE COMPUTADORES

A Internet é um amplo sistema de comunicação que conecta muitas redes de computadores, e existem várias formas e recursos de vários equipamentos que podem ser interligados e compartilhados, mediante meios de acesso, protocolos e requisitos de segurança (BOF, 2010).

Este mesmo autor define uma rede de computadores como sendo dois ou mais computadores e outros dispositivos conectados entre si, de modo a poderem compartilhar seus serviços, podendo ser: mensagens (e-mails), dados, impressoras, etc.

Similarmente, para Forouzan e Mosharraf (2013), uma rede é a interligação de um conjunto de dispositivos capazes de se comunicar, sendo que nesta definição, um dispositivo pode ser um host (ou um sistema final, como as vezes é chamado), tal como um grande computador, desktop, estação de trabalho, telefone celular ou sistema de segurança ou também pode ser um dispositivo de conexão, tal como um roteador, que liga um rede a outras redes, um switch (ou computador) que liga dispositivos entre si, um modem (modulador-demodulador) que altera a forma dos dados, e assim por diante, sendo que estes dispositivos em uma rede são conectados usando meios de transmissão com ou sem fio, como cabo ou ar.

3.1.1 Redes sem fio

As Redes sem fio ou wireless (WLANs, Wireless Local Area Network) surgiram assim como muitas outras tecnologias, no meio militar, devido a necessidade de implementação de um método simples e seguro para troca de informações em ambiente de combate. O tempo passou e a tecnologia evoluiu, deixando de ser restrito ao meio militar e se tornou acessível a empresas, faculdades e ao usuário doméstico (FARIAS, 2005).

Uma rede sem fio se refere a uma rede de computadores sem a necessidade do uso de cabos, sendo que a ligação é feita por meio de equipamentos que usam radiofrequência (comunicação via ondas de rádio) ou comunicação via infravermelho, e o uso desta tecnologia vai desde transceptores de rádio até satélites no espaço, sendo que seu uso mais comum é em redes de computadores, servindo como meio de acesso à Internet, através de locais remotos como um escritório, um restaurante ou até mesmo em casa (BOF, 2010).

De acordo com Rufino (2005), as redes sem fio possuem dois tipos de funcionamento: o modo de Infraestrutura, que possui um concentrador que é um equipamento central de uma rede que possibilita, para essa topologia, uma melhor administração e concentração de todos os dispositivos clientes em um só ponto, sendo que tal funcionalidade permite controlar todos os dispositivos e políticas de segurança como autorização, autenticação, controle de banda, filtros de pacote, criptografias em um único ponto e também possibilita a interligação com redes cabeadas ou com a Internet, já que em geral, os concentradores também desempenham o papel de gateway ou ponte de acesso.

Ainda de acordo com este autor, no modo de operação Ad-Hoc, em que o funcionamento é baseado em redes ponto-a-ponto nas quais os computadores e dispositivos sem fio conversam diretamente entre si sem a necessidade de um ponto de acesso. Esse tipo de modo de operação possui vantagens de simplificação na troca de arquivos sem necessidade de mão de obra especializada, porém, disponibiliza um elevado índice de falta de segurança na comunicação entre os dispositivos sem fio.

3.2 SEGURANÇA DA INFRAESTRUTURA

A segurança física de uma rede sem fio, muitas vezes não é lembrada e nem levada em consideração em muitos casos de implementação. Em uma rede cabeada, é um ponto importante e de necessária preocupação, e na rede sem fio, onde a área de abrangência “física” aumenta substancialmente, não é diferente.

Na rede cabeada, a segurança é feita configurando-se uma porta de entrada para a rede (um servidor de autenticação), e há necessidade de um ponto de acesso físico para conectar um equipamento (notebook, computador pessoal, e outros) (RUFINO, 2005).

Para Ferreira (2013), o posicionamento dos pontos de acesso deve ser minuciosamente estudado, pois é possível que venha a colidir com necessidades essenciais: a velocidade e o desempenho da rede. Um ponto de acesso posicionado em um ponto alto terá um desempenho melhor, pois o sinal ficará mais limpo, possivelmente livre de interferências. Por consequência sua abrangência será maior, abrindo assim possibilidades de interceptações no sinal, facilitando o acesso não autorizado e sofrendo possíveis ataques.

Sendo assim, a segurança da infraestrutura consiste na provisão e políticas adotadas pelo administrador de rede para prevenir e monitorar o acesso não autorizado, uso incorreto, modificação ou negação da rede de computadores e dos seus recursos associados, visto que segurança de rede envolve a autorização de acesso aos dados de uma rede, os quais são controlados pelo administrador de rede.

3.2.1 Segurança em redes sem fio

Segundo Ferreira (2013), as redes sem fio apresentam uma série de vulnerabilidades que têm sua origem na concepção dos padrões adotados. Ao contrário das redes cabeadas, as redes sem fios são de transmissão não guiada num meio comum e acessível a todos, dentro do raio de ação das antenas. Sendo assim, caso a rede não possua mecanismos mínimos de segurança configurados, o acesso à essa rede fica imediatamente disponível a quem esteja dentro do raio de ação dos APs (Acess Points), com um terminal compatível com a tecnologia utilizada.

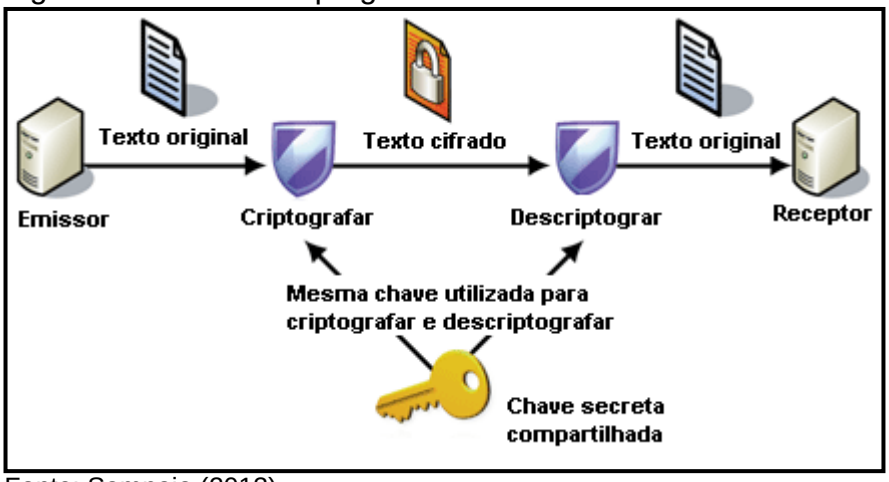
Ainda para o autor citado anteriormente, os ataques mais comuns em redes sem fio referem-se à obtenção de informações sem autorização, acesso indevido à rede e ataques de negação de serviço. Estes ataques possuem graus de dificuldade dependentes das características de implantação da rede, o que significa dizer que, para que uma rede sem fio possua as mesmas características de segurança de uma rede com fios, existe a necessidade de inclusão de mecanismos de autenticação de dispositivos e confidencialidade de dados.

3.3 CRIPTOGRAFIA

A criptografia é um meio de aprimorar a segurança de uma mensagem ou arquivo embaralhando o conteúdo, de modo que ele só possa ser lido por quem tenha a chave de criptografia correta para desembaralhá-lo. A criptografia é também uma ferramenta fundamental para prover segurança, pois por meio dela, é possível atender a todos os requisitos clássicos de segurança, sendo que a maioria dos ataques à redes poderia ser solucionada pela utilização de um mecanismo criptográfico seguro.

Segundo Fernandes et al. (2013), tradicionalmente, a criptografia é separada em dois ramos: simétrica e assimétrica, sendo a primeira, caracterizada pela existência de um segredo, chamado de chave secreta, compartilhado entre os nós que desejam se comunicar. Esta chave é utilizada em operações que alteram os dados a transportar, enviando um texto criptografado ao invés de um texto em aberto, como demonstra a Figura 1.

Figura 1 - Fluxo de criptografia simétrica



Fonte: Sampaio (2013).

As principais operações realizadas pelos algoritmos simétricos são o ou-exclusivo, a troca de colunas, a troca de linhas, a permutação, a rotação e a expansão, que são operações de baixo custo computacional, e apesar de serem simples, as combinações dessas operações devem ser capazes de tornar difícil a descoberta da mensagem para quem não possui a chave secreta. Sendo assim, a eficiência desses algoritmos é medida pelo seu custo computacional, e pela capacidade de modificar a saída dada uma pequena mudança na entrada (FERNANDES et al., 2013).

Ainda na definição do mesmo autor, na criptografia assimétrica existem duas chaves, a chave pública e a privada, em que a chave pública deve ser distribuída aos membros da rede, enquanto que a privada deve ser mantida em segredo pelo nó, como mostra a Figura 2.

Figura 2 - Fluxo da criptografia assimétrica

Fonte: Andrade (2013).

Esse tipo de criptografia possui maior custo computacional que a simétrica, por fazer uso de operações como o logaritmo discreto, curva elíptica e fatoração de inteiros, aliadas as considerações de segurança da Teoria dos Números, tendo como objetivo principal, que a partir de uma das chaves, não seja possível encontrar a outra, o que é obtido quando se usa para o cálculo de funções que são simples de calcular, mas quase impossíveis de se reverter computacionalmente. Existem outras funcionalidades e possibilidades com o uso da criptografia assimétrica, como a distribuição de chaves de forma segura e a assinatura de mensagens (FERNANDES et al., 2013).

A National Research Council (NRC) cita que a criptografia hoje é, provavelmente, o aspecto mais importante da segurança de comunicações, e tem se tornado cada vez mais importante como um componente básico para a segurança do computador.

> A palavra criptografia é originária dos termos gregos kryptós, que quer dizer oculto, e graph, escrever. Em dicionários da língua portuguesa, pode-se encontrar a seguinte definição para palavra criptografia: escrita secreta por meio de abreviaturas ou de sinais convencionados de modo a preservar a confidencialidade da informação (AQUINO JUNIOR et al., 2008, p. 13).

A criptografia é feita através de algoritmos matemáticos, que faz o estudo de princípios e técnicas pelas quais uma informação clara pode ser transformada em uma informação ilegível, ou seja, o chamado texto cifrado, e que apenas através de uma “chave” pode passar pelo processo reverso, tendo como objetivo de que apenas emissor e o receptor da mensagem possam ter acesso à informação original.

Stallings (2008) enfatiza que a ferramenta automatizada mais importante para a segurança da rede e das comunicações é a criptografia, e que duas formas de criptografia são usadas normalmente: a criptografia convencional (simétrica) e a por chave pública (assimétrica).

3.4 ATAQUES

De acordo com Fernandes et al. (2013), os ataques à redes ad hoc móveis podem ser divididos em passivos ou ativos. Os ataques passivos não afetam a operação da rede, sendo caracterizados pela espionagem dos dados sem alterá-los, isto é, o atacante não interfere no funcionamento da rede, mas pode escutá-la e analisar o seu tráfego. Ele tem acesso à informação, porém não a altera ou destrói. Este tipo de ataque são de difícil detecção por não influírem no comportamento da rede.

Por outro lado, os ataques ativos são aqueles em que o atacante cria, altera, descarta ou inviabiliza o uso dados em trânsito. Estes tipos de são os mais numerosos, podendo atuar em diferentes camadas do modelo OSI. Os atacantes podem ser classificados como internos ou externos, sendo que os internos são aqueles que conseguem de alguma forma se passar por membros da rede, enquanto que os externos são aqueles que influenciam, mas não participam da rede. Este tipo de ataque em sua maior parte, têm como alvo a vulnerabilidade de alguma camada específica do modelo OSI (FERNANDES et al., 2013).

De fato, a eficiência e as possibilidades de ataques variam de acordo com o acesso que o atacante tem à rede. Se de alguma forma ele conseguir obter chaves, ou for incluído na lista de vizinhos válidos, passando a ser um atacante interno, poderá causar mais problemas.

3.4.1 Invasões

De acordo com Rufino (2005) e Bof (2010), com tantas possibilidades de invasão facilitadas através de softwares, ou até mesmo sem nenhum conhecimento, muitos indivíduos obtêm acessos à rede sem fio sem autorização, comprometendo assim a confiabilidade e a integridade das informações que circulam pela rede sem fio.

Indo mais a fundo, o invasor pode ter quatro comportamentos estratégicos diferentes em relação ao processo de invasão de redes sem fio:

a) **Interrupção:** Procedimento no qual o invasor influi em interromper as passagens de dados de um ponto para outro;
b) **Interseção:** Procedimento no qual o invasor realiza coleta de informações para saber o que se passa dentro da rede e por fim ter acesso a ela futuramente;
c) **Modificação:** Nesse procedimento o invasor não apenas escuta o tráfego da rede, mas também modifica e compromete os dados para depois enviá-los para o dispositivo a que está sendo atacado, sendo que o objetivo é que este se torne um dispositivo zumbi e o invasor tenha total controle os dispositivos;
d) **Fabricação:** Nesse caso, o invasor desenvolve os dados a serem enviados para um determinado destino com intuito de se obter acesso a rede sem fio (RUFINO, 2005 e BOF, 2010).

Quando um invasor descobre uma rede sem fio completamente mal configurada, ele pode utilizar softwares maliciosos (Scanners) que capturam os pacotes de dados com o intuito de se obter o SSID e a chave de acesso. Existe a possibilidade do atacante se passar por um membro da rede sem fio, e assim os dispositivos dão a permissão para executar tarefas como se fosse um usuário normal (RUFINO, 2005).

3.4.2 Técnicas de ataque

Segundo Peres (2003), os ataques mais comuns em redes sem fio referem-se à obtenção de informações sem autorização, acesso indevido à rede e ataques de negação de serviço, sendo que estes ataques possuem graus de dificuldade dependentes das características de implantação da rede.

A principal preocupação em relação à segurança em redes sem fio diz respeito a forma de funcionamento padrão destas redes ser do tipo Open System, pois significa que um usuário desavisado, ao instalar a rede pela primeira vez, possibilita acesso a todos os dados da rede sem proteção alguma.

Sendo assim, este mesmo autor define que todos os sistemas computacionais em execução nesta rede que não possuem criptografia estarão disponíveis a qualquer dispositivo dentro da área de abrangência do AP. Os usuários que optam por este tipo de sistema, não possuem qualquer forma de confidencialidade, nem de autenticação de dispositivos, tendo como problemas imediatos:

a) **Ataque passivo para captura legível de informações da rede**, caracterizado pela possibilidade de um atacante obter todas as informações que trafegam na rede sem criptografia. Entre os diversos programas que não utilizam qualquer forma de cifragem estão as aplicações de e-mail, telnet e ftp, disponibilizando nomes de usuários e senhas. O atacante não interfere no funcionamento da rede e, nos casos das redes sem fio, pode facilmente mascarar-se sem ser detectado.
b) **Ataque ativo durante a comunicação**, no qual um atacante pode passar por um AP da rede. Com isto, os dispositivos passam a confiar informações sensíveis diretamente ao atacante e como não existe autenticação, não existe forma de se garantir que o AP com quem um dispositivo está associado é realmente um equipamento autorizado. Neste ataque, conhecido como “man-in-the-middle”, o atacante deve alterar o funcionamento normal da rede para conseguir passar-se por um dispositivo. Também á possível que um atacante simplesmente autentique seu dispositivo móvel na rede através de um AP e a partir deste momento, conforme as permissões da rede, terá o mesmo acesso que um usuário autorizado.

Nas redes que utilizam a autenticação Shared Key juntamente com o protocolo de segurança WEP, os mesmos ataques podem ser realizados, aumentando-se a complexidade. Tendo em vista o mecanismo de cifragem do WEP, se um atacante altera um bit do texto cifrado, este mesmo bit será alterado na mensagem original. Ou seja, o atacante consegue alterar um bit específico na mensagem cifrada, mesmo sem conhecer seu conteúdo, o segredo compartilhado,

ou a chave. Os ataques mais comuns em redes que utilizam o WEP, geralmente são:

a) **Ataques Estatísticos**, que são ataques passivos, onde o objetivo é descobrir o significado de textos cifrados, sendo que uma forma de realizar este tipo de ataque é a de obter uma série de pacotes cifrados com a mesma chave.
b) **Ataques de injeção de tráfego,** supõe-se que o atacante possua conhecimento completo do conteúdo de uma mensagem cifrada, basta que construa uma nova mensagem, calcule o novo CRC e altere os bits da mensagem original (dados e CRC) para que seja aceita pelo AP.
c) **Ataques de redirecionamento de mensagens,** o atacante pode alterar informações como endereço de destino, e fazer com que um pacote seja direcionado para internet, possuindo conhecimento sobre os cabeçalhos dos pacotes. Ao direcionar o pacote a um endereço IP destino em uma máquina a qual possui controle, o atacante faz com que o AP decifre a mensagem antes de enviá-la. Na máquina destino, o atacante recupera o texto original, enquanto monitorando a rede sem fio obtém a mesma mensagem cifrada. Assim, além de obter o conteúdo da mensagem, o atacante toma conhecimento de mais uma chave gerada a partir de um IV.
d) **Construção de tabelas de decifragem,** O pequeno número de IVs possibilita que um atacante, realizando um conjunto de ataques à rede, possa montar uma tabela contendo uma série (ou todas) as chaves utilizadas com os respectivos IVs, sendo que uma vez construída esta tabela, é possível decifrar todas as mensagens que possuem as chaves com IVs conhecidos.
e) **Obtenção do segredo compartilhado,** o algoritmo utilizado nas redes sem fio apresenta fraquezas que dizem respeito a um grande número de chaves fracas geradas pelo WEP, e pela possibilidade de descobrir bits da chave a partir da análise/conhecimento dos primeiros bits da mensagem (pelo fato do IEEE 802.11 utilizar os dados encapsulados pelo LLC – Logical Link Control os primeiros bits dos quadros são

sempre os mesmos). Ao obter o segredo compartilhado, a privacidade da rede fica completamente vulnerável.

3.4.3 Phishing

Segundo Reinaldo Filho (2014), palavra phishing, uma corruptela do verbo inglês fishing (pescar, em português), é utilizada para designar alguns tipos de condutas fraudulentas que são cometidas na rede, sendo as mais comuns: mensagens eletrônicas (e-mails) onde são feitas propaganda de pechinchas comerciais, são solicitados renovações de cadastro, são feitos convites para visualização de sites, são ofertadas gratuitamente soluções técnicas para vírus, entre outras, onde assim, as pessoas mal informadas e desatentas acabam clicando para verificar o conteúdo do site onde pedem informações pessoais, e é assim que muitas pessoas caem neste tipo de ataque.

Este é um tipo de ameaça da Internet, que é aplicada através de comunicação em programas de instant messaging, telefone e como uma mensagem de e-mail, onde nessa mensagem está pedindo para clicar em um link que o encaminhará automaticamente para um anexo que será baixado automaticamente e vem um vírus junto, como demonstra a Figura 3, ou também por uns sites falsos muito parecidos graficamente com os sites verdadeiros, como na Figura 4, e que pedem informações pessoais como por exemplo: confirmar a senha do cartão de crédito de um determinado banco, e assim que a pessoa digita o número, a pessoa maliciosa que enviou o e-mail está pronto para pegar esses dados e aplicar o golpe imediatamente.

A categoria delituosa em questão consiste exatamente nisso: em “pescar” ou “fisgar” qualquer pessoa desavisada, não acostumada com esse tipo de fraude. O Phishing, portanto, é uma modalidade de spam, em que a mensagem além de indesejada é também fraudulenta. Assim o phisherman pode ter como alvo os dados de um usuário, e respectivos números da conta e senhas bancárias, para serem utilizados em sites de Internet banking, ou pode coletar dados de cartão de crédito e senhas utilizadas em sites de comércio eletrônico ou de leilão e de sistemas de pagamento online (REINALDO FILHO, 2014).

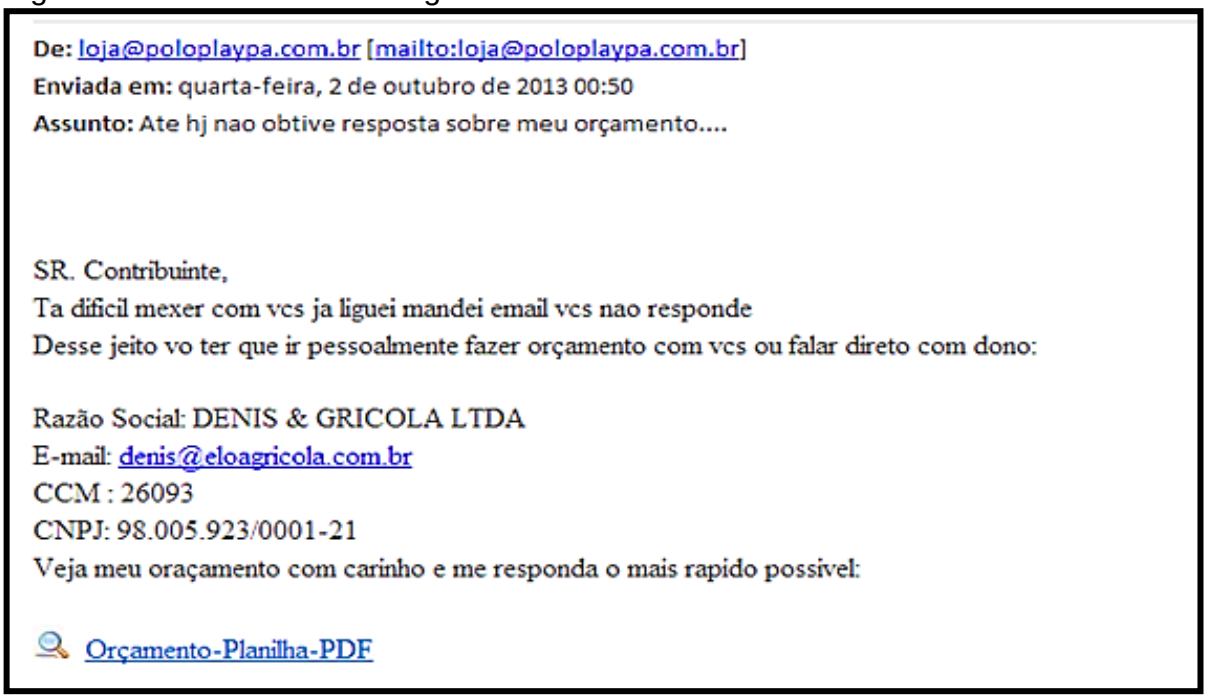
Similarmente, para Rafael (2013), o Phishing pode ser traduzido como “pescaria” ou “e-mail falso”, e compreendem e-mails manipulados e enviados a

organizações e pessoas com o intuito de aguçar algum sentimento que faça com que o usuário aceite o e-mail e realize as operações solicitadas.

Ainda para este autor, sem dúvidas, esta é a técnica mais utilizada para conseguir um acesso na rede alvo, sendo que os casos mais comuns de Phishing são desde e-mails recebidos de supostos bancos, da Receita Federal informando que seu CPF está irregular ou que o Imposto de Renda apresentou erros, e que para regularizar consta um link, até as situações mais absurdas que muitas pessoas ainda caem por falta de conhecimento, tais como, e-mail informando supostas traições, e para ver as fotos consta um link ou anexo, ou que as fotos do churrasco já estão disponíveis no link, entre outros, sendo que a maioria dos Phishings possuem algum anexo ou links dentro do e-mail que direcionam para a situação que o Cracker deseja.

Segundo Ouch (2013), o Phishing é uma técnica que usa engenharia social, que será explicada posteriormente, onde o atacante tenta persuadi-lo a tomar uma ação.

Figura 3 - E-mail com Phishing



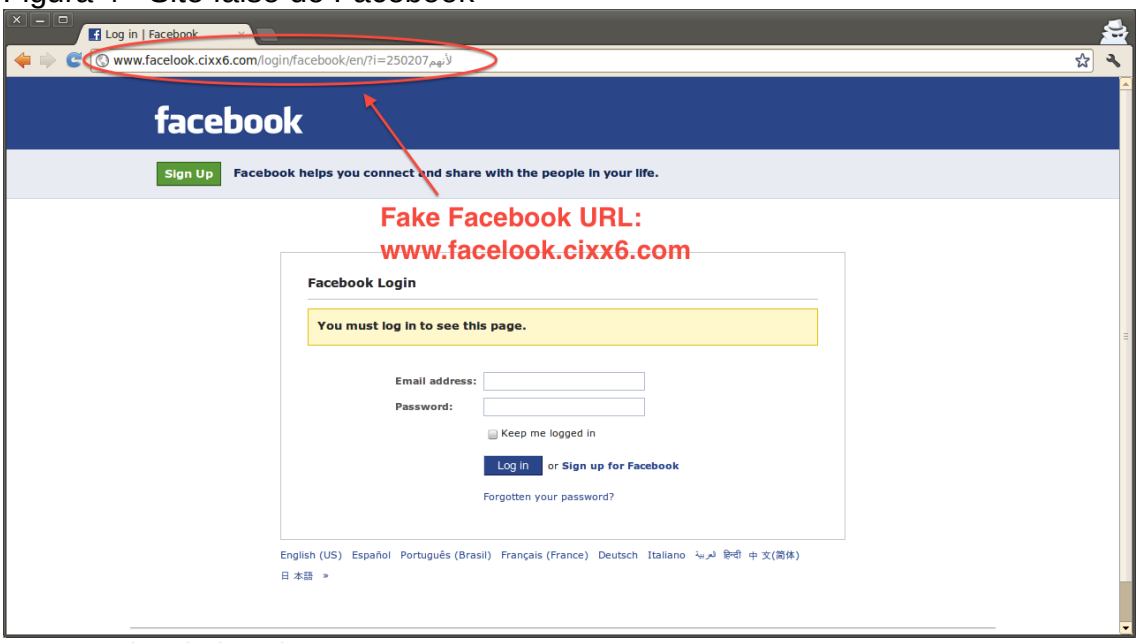
Fonte: Profissionaisti (2013).

A Figura 3 demonstra o meio usado para fazer o ataque Phishing em uma mensagem de e-mail. Como descrito anteriormente, o link no canto inferior desta figura refere-se ao arquivo com vírus e os erros na escrita alertam o usuário de um

possível ataque Phishing, visto que Mannara (2015) relata que erros ortográficos, solicitação de informações pessoais, redirecionamento automático à sites, entre outros, são sinais claros de falsificação nestes e-mails e um provável ataque Phishing.

Já a Figura 4 demonstra o site falso que imita o Facebook para roubar dados.

Figura 4 - Site falso do Facebook



Fonte: TechTudo (2015).

Como se pode ver, o layout do site falso é muito similar ao verdadeiro, havendo como única diferença para o usuário inexperiente ou desatento, a extensão da URL destacada na Figura 3. Esses sites falsos imitam o Facebook para roubar dados, e-mails e credenciais, mas não passam de um golpe, em que as mensagens escondem vírus e fazem com que estes ataques sejam disseminados.

3.4.4 Engenharia social

A engenharia social é definida como a arte de manipular uma pessoa para que esta faça uma ação que pode ou não ser de seu interesse, sendo que este ato visa obter uma informação, acesso à ambiente restrito ou conseguir que a “vítima” realize certa ação (CORTELA, 2013).

Ainda de acordo com este autor, a engenharia social explora diversas características humanas a fim de atingir seu objetivo, que consistem na exploração

de confiança, autoconfiança, amizade e persuasão como técnicas comuns deste framework que não existe apenas no mundo digital.

O Phishing, como dito anteriormente, é uma técnica que usa engenharia social na qual frequentemente esses ataques começam com um e-mail fingindo ser de alguém ou de uma fonte em que você confia, como um amigo, seu banco ou sua loja de Internet favorita, e esses e-mails então tentam seduzí-lo a tomar uma ação como clicar em um link, abrir um anexo ou responder uma mensagem. Os criminosos cibernéticos montam esses e-mails para parecerem convincentes, enviando-os a milhões de pessoas ao redor do mundo, sem um alvo específico em mente, ou seja, na verdade nem sabem exatamente quem será sua vítima. O que sabem é apenas que quanto mais e-mails enviarem, mais pessoas poderão enganar (OUCH, 2013). Deste modo, não podemos contar com um software capaz de inibir esta ação (CORTELA, 2013).

3.5 REDES SOCIAIS

A rede social é composta por pessoas ou organizações, conectadas por um ou vários tipos de relações, compartilhando valores e objetivos comuns.

Mata (2012) define a rede social como uma modalidade de site criado com o objetivo que criar uma rede de amizades criando um vínculo remoto e digital, sendo um organismo em mutação e constante desenvolvimento dentro da internet, se adequando à realidade e se transformando à medida que detecta necessidade de oferecer mais e atender uma demanda que a obriga a se reinventar quase que o tempo todo.

As redes sociais virtuais permitem compartilhar dados e informações, tornando-se um instrumento poderoso utilizado no contexto mundial para disseminar ideias através de textos, arquivos, imagens fotos, vídeos, criação de comunidades, etc.

É indiscutível que as redes sociais fazem parte hoje do cotidiano e estimulam a venda de produtos digitais, mas é importante ressaltar os danos causados pelas redes sociais como o terrorismo, ação de bandidos, guerra de torcidas, Bullyng, pedofilia, discriminação, a ação dos hackers, enfim, uma gama de usos negativos de seus recursos (MATA, 2012).

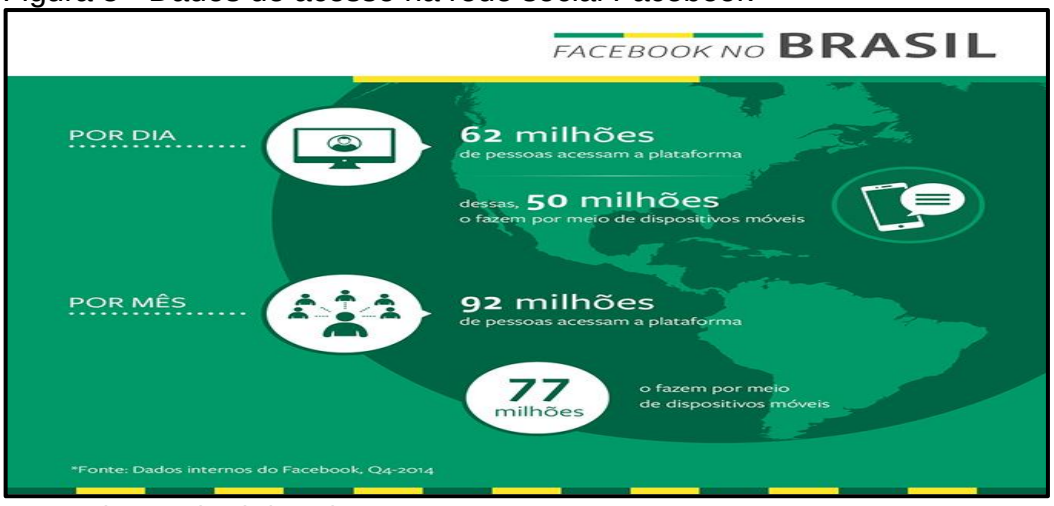
3.5.1 Facebook

O Facebook surgiu em 2004, fundado por Mark Zuckerberg, ex-estudante de Harvard contando com o apoio de Andrew McCollum e Eduardo Saverin, sendo que a intenção inicial do Facebook era que fosse só para estudantes da universidade de Harvard, mas posteriormente foi estendida ao Instituto de Tecnologia de Massachusetts (MIT), à Universidade de Boston, ao Boston College e a todas as escolas Ivy League, e somente no ano de 2006 o Facebook iniciou-se sua abrangência. Depois disso o crescimento foi rápido e passou a admitir estudantes de outras universidades da região de Boston (Boston College, Boston University, Northeastern University, Tufts 21 University), e também de Rochester, Stanford, Columbia, Yale, NYU e Northwestern (MATA, 2012).

Segundo Kirkpatrick (2011), em setembro de 2005, a empresa tornou-se oficialmente Facebook e já atingia 85% dos estudantes americanos do ensino superior e aos poucos, a plataforma foi se abrindo para outros públicos, como estudantes do ensino médio, no final de 2005 e, em 2006, para qualquer pessoa convidada pelos usuários (desde que tivessem mais de 13 anos). Antes do registro aberto, entravam 20 mil novos usuários por dia, na segunda semana de outubro, após a abertura, o número havia crescido para 50 mil.

O levantamento mais recente, segundo o próprio site, foi realizado no último trimestre de 2014, e mostra que a presença de brasileiros no Facebook não para de crescer. A Figura 5 mostra os acessos ao Facebook por dia e mês, além da divisão entre computadores e dispositivos móveis.

Figura 5 - Dados de acesso na rede social Facebook



Fonte: Site Facebook (2016).

De acordo com a Figura 5, disponibilizada no próprio site, 62 milhões de pessoas acessam diariamente esta rede social e hoje, 92 milhões de pessoas acessam esta plataforma todos os meses – o que corresponde a 45% de toda a população brasileira, segundo o IBGE (FACEBOOK, 2016), justificando então, a importância deste estudo de vulnerabilidade nesta rede social.

3.6 SISTEMAS OPERACIONAIS

Um sistema operacional pode ser definido como um conjunto de programas especialmente feitos para a execução de várias tarefas, assim como servir de intermediário entre o utilizador e o computador, e gerir todos os periféricos de um computador, ou seja, podemos dizer que o sistema operacional é o programa mais importante do computador, sendo que o sistema operacional mais conhecido é o MS-DOS (Microsoft Disk Operating System).

Uma das atribuições do sistema operacional é carregar na memória e providenciar a execução dos programas que o usuário solicita. Mesmo quando um programa qualquer está sendo executado, o sistema operacional pode continuar trabalhando, ou seja, todos os acessos ao teclado, vídeo e impressora, assim como acessos ao disco para ler e gravar arquivos são realizados pelo sistema operacional, que fica o tempo todo ativo, prestando serviços aos programas que estão sendo executados.

O sistema operacional também faz um gerenciamento dos recursos do computador, para evitar que os programas entrem em conflito, funcionando como um "maestro", providenciando para que todos os programas e todos os componentes do computador funcionem de forma harmônica (SILBERCHATZ; GALVIN, 2000).

3.6.1 Linux

Campos (2006) define o Linux como um kernel e um sistema operacional que roda sobre ele (dependendo do contexto de alguns autores), que foi desenvolvido por Linus Torvalds tendo como base o código fonte do sistema Minix, que é uma versão simplificada do sistema operacional Unix. O Linux adota uma licença livre onde todos podem usá-lo e distribuí-lo, fazendo com que seja um sistema bastante maduro, pois uma comunidade inteira de desenvolvedores acaba por contribuir e

ajudar no seu desenvolvimento, reportando falhas, dando opiniões, ou até mesmo participando do desenvolvendo direto ou indireto do código fonte do sistema. Por se tratar de um sistema bem confiável e seguro, o Linux é usado por padrão em diversas empresas, principalmente nos quesitos servidores, onde é crucial que não haja falhas nem paradas dos serviços oferecidos.

Atualmente há diversas distribuições Linux no mercado e na internet, com características e usabilidades próprias, sendo que um site para verificar as diversas distribuições existentes é o Distrowatch[1].

3.6.1.1 Kali Linux

De acordo com Oliveira (2015), o Kali Linux atualmente é considerado uma das maiores e mais avançadas distribuições Linux de testes de penetração, sendo uma continuação do famoso backtrack, que adotava antes esse título. Ele é mantido e financiado pela Offensive Security, empresa fornecedora de treinamentos de segurança da informação e serviços de teste de penetração conhecida mundialmente, e por padrão, essa distribuição é pré configurada e moldada especificamente para testes e auditorias de segurança, vindo com muitas ferramentas instaladas específicas para isso.

3.6.2 Windows

O Windows é o sistema operacional da empresa Microsoft, que é mundialmente conhecida se tratando de sistemas operacionais para usuários. Ele possui várias versões, e como ele é mais voltado para um público menos experiente e à atividades usuais de escritório, ou seja, usuários que geralmente possuem um nível de conhecimento mais básico de tecnologia, ele possui um número elevado de usuários que o utilizam e consequentemente, aparecem diversas vulnerabilidades para o sistema da Microsoft. Com isso, existem diversos métodos e exploits utilizados para explorar as vulnerabilidades de algumas versões do Windows (OLIVEIRA, 2015).

[1] (http://distrowatch.com/index.php?language=PT).

3.6.3 Máquinas Virtuais

No estudo de Laureano et al. (2003 citado por POPEK e GOLGBERG, 1974), uma máquina virtual (Virtual Machine - VM) é definida como “uma duplicata eficiente e isolada de uma máquina real”, sendo que em uma máquina real, uma camada de software de baixo nível (por exemplo, a BIOS dos sistemas PC) fornece acesso aos vários recursos do hardware para o sistema operacional, que os disponibiliza de forma abstrata às aplicações, e quando o sistema operacional acessa os dispositivos de hardware, ele faz uso dos device drivers respectivos, que interagem diretamente com a memória e os dispositivos de E/S da máquina.

Para este mesmo autor, uma máquina virtual é o intermediário entre uma máquina real e um emulador, sendo que este último é o oposto da máquina real, ou seja, implementa todas as instruções realizadas pela máquina real em um ambiente abstrato, possibilitando executar um aplicativo de uma plataforma em outra, por exemplo, um aplicativo do Windows executando no Linux, portanto, a funcionalidade e o nível de abstração de uma máquina virtual encontra-se entre uma máquina real e um emulador, na medida em que abstrai somente os recursos de hardware e de controle usados pelas aplicações.

Uma máquina virtual é um ambiente criado por um monitor de máquinas virtuais (Virtual Machine Monitor – VMM), também denominado “sistema operacional para sistemas operacionais”, no qual o VMM pode criar uma ou mais máquinas virtuais sobre uma única máquina real. A vantagem da VMM em relação à um emulador, é que enquanto um emulador fornece uma camada de abstração completa entre o sistema em execução e o hardware, um VMM abstrai o hardware subjacente e controla uma ou mais máquinas virtuais (LAUREANO et al, 2003).

Existem basicamente dois tipos de abordagens para a construção de máquinas virtuais: no primeiro, o monitor de máquinas virtuais é implementado entre o hardware e os sistemas convidados e no segundo, onde o monitor é implementado como um processo de um sistema operacional real subjacente, denominado sistema anfitrião. Neste caso, visto que o sistema operacional convidado o e ambiente de execução na máquina virtual são idênticos ao da máquina real, é possível usar os softwares já construídos para a máquina real dentro das máquinas virtuais, e essa transparência evita ter de construir novas aplicações ou adaptar as já existentes (LAUREANO et al, 2003).

3.7 TRABALHOS CORRELATOS

Como atualmente grande parte das aplicações são online, é possível encontrar estudos de privacidade sobre diversos enfoques envolvendo as redes sociais e também os ataques Phishing.

Carvalho et al. (2013) desenvolveram um estudo da vulnerabilidade nessas aplicações web, no qual realizaram pesquisas na área e analisaram as mais conhecidas vulnerabilidades, trazendo maiores detalhes sobre suas consequências e possíveis correções, assim como algumas ferramentas que podem auxiliar na segurança através de um escaneamento completo da aplicação e identificação das vulnerabilidades encontradas.

Neste estudo, concluíram que um ataque bem sucedido em uma aplicação pode trazer grandes prejuízos, físicos ou morais aos usuários e as empresas, já que a gravidade desse ataque depende especialmente da experiência do atacante, e as ferramentas mostraram-se bastante eficientes, sendo possível definir a melhor ferramenta, levando em consideração os recursos oferecidos, a flexibilidade, a facilidade, e os resultados obtidos no escaneamento (CARVALHO et al., 2013).

Capistrano (2013) em seu estudo das redes sociais virtuais como ambiente de exposição de dados pessoais para a engenharia social, realizou uma pesquisa qualitativa com trinta pessoas de um universo específico através de questionário, entrevistas e análise das respectivas páginas sociais no Facebook. A atitude e o comportamento destas pessoas na rede social foram confrontados com técnicas da engenharia social e o resultado da análise mostrou que a grande maioria das pessoas acaba colocando sua segurança em risco em virtude de um comportamento inadequado na rede social.

Cortela (2013) estudou a engenharia social no Facebook visando mapear o problema em questão e propor uma solução para este tipo de ameaça que se aproveita não da tecnologia, mas sim da mente humana, tendo como foco principal deste estudo, a privacidade e como usuários leigos do Facebook publicam informações privadas, que podem ser garimpadas e posteriormente utilizadas por um engenheiro social. Ele ainda destacou que estas “soluções” sugeridas, impediriam o uso prático da rede e por isso talvez ainda não tenham sido implantados, visto que o número de usuários para um site de relacionamentos é o

seu lucro e é por isso que a facilidade de uso da plataforma sempre estará em primeiro plano.

Silva et al. (2012) fizeram em seu estudo, uma análise de vulnerabilidade de usuários no Facebook, com o objetivo de avaliar o risco de privacidade e o nível de exposição de cada usuário, apresentando e definindo após a análise de mais de 75 mil perfis de usuários do Facebook e suas redes de amizades, um indicador de vulnerabilidade que pode ser incorporado à interface do Facebook para permitir que cada usuário conheça o seu nível de exposição e o nível de exposição de cada integrante de sua rede de amigos.

Com este estudo, concluíram que este indicador proposto possui caráter qualitativo, sendo gerado a partir do chamado índice de exposição, que avalia a exposição quantitativa do usuário e após o cálculo dos índices de exposição para um grupo de usuários, puderam atribuir o indicador de vulnerabilidade de acordo com a classificação deste usuário dentro do grupo. Apresentaram também a classificação de todos os usuários da amostra em termos de seu índice de exposição e indicador de vulnerabilidade, permitindo uma maior compreensão do nível de risco assumido pelos usuários do Facebook.

4 METODOLOGIA

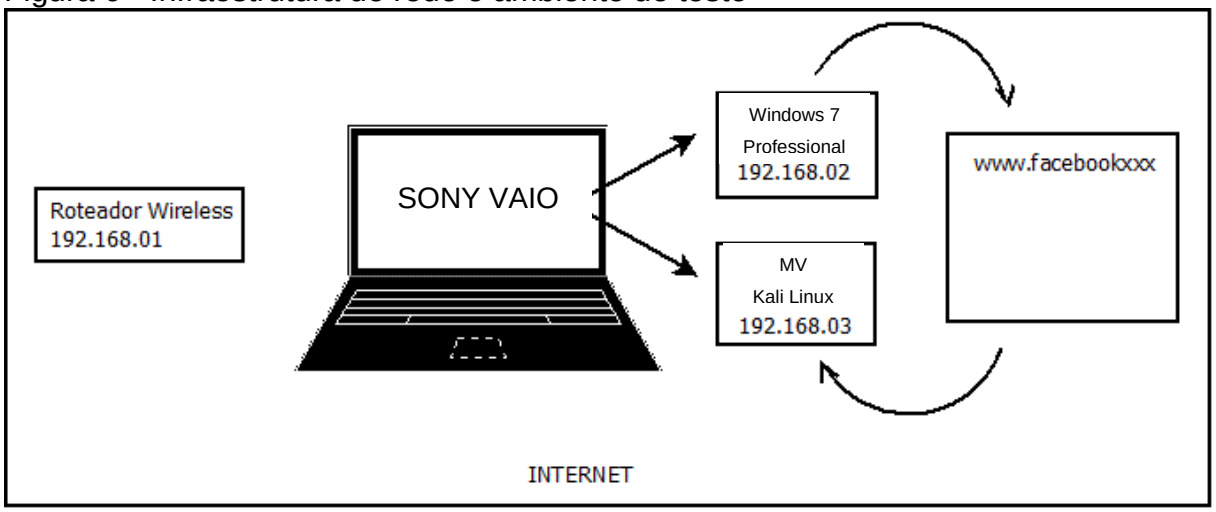
Este trabalho foi desenvolvido em três partes, sendo que na primeira parte foi realizada uma pesquisa bibliográfica em livros, artigos de jornais e revistas entre outros com o intuito de reunir conceitos sobre os temas abordados, para que em um segundo momento, fosse demonstrado na prática tudo o que foi aprendido na teoria.

Para realização da segunda parte deste trabalho, ou seja, para o desenvolvimento do procedimento experimental, foi utilizado um Notebook Sony Vaio com 4GB de memória RAM, Sistema Operacional Windows 7 Professional 64 Bits e um roteador wireless Vivo, modelo ANATEL com segurança WPA2-Personal, Criptografia AES e Chave de Segurança de Rede.

Neste notebook, foi instalada uma máquina virtual Kali Linux, dividindo a memória RAM entre o SO Windows 7 e a MV Kali Linux.

A Figura 6 representa a infraestrutura de rede, demonstrando o ambiente de teste.

Figura 6 - Infraestrutura de rede e ambiente de teste



Fonte: Elaborada pelo autor.

A terceira parte deste trabalho consistiu na realização de ataques Phishing neste ambiente virtual criado. Após tudo instalado e configurado como demonstrado na Figura 6, foram utilizadas ferramentas de ataques do Kali Linux já fornecidas por este próprio SO, onde foi clonada a página da rede social Facebook.

Com o intuito de simular os testes realizados por crackers para esta engenharia social, utilizou-se uma rede Wi-Fi local, com a permissão da responsável pela mesma.

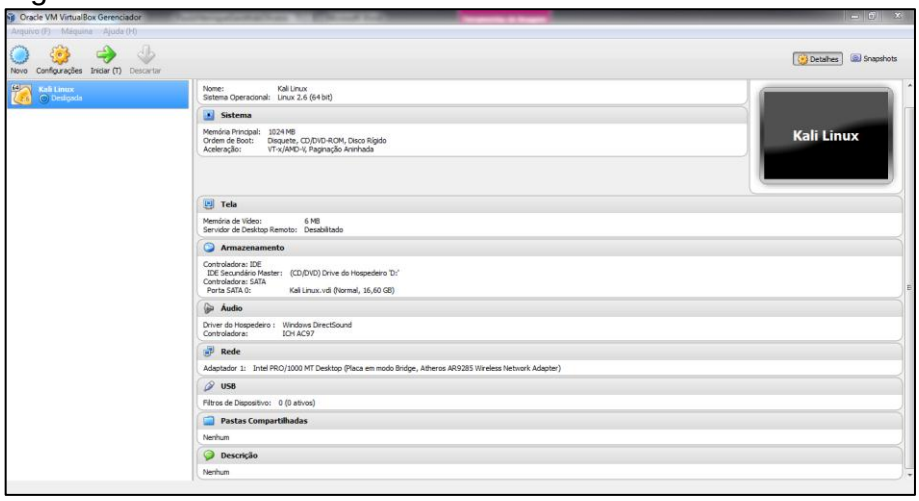
Esta página clonada do Facebook foi acessada primeiramente por um e-mail teste e após esta checagem, foram realizados testes com os usuários para obter os dados de acesso sem que soubessem.

Este programa foi deixado aberto por um dia e os dados obtidos dos usuários que caíram no ataque Phishing foram salvos.

5 RESULTADOS E DISCUSSÃO

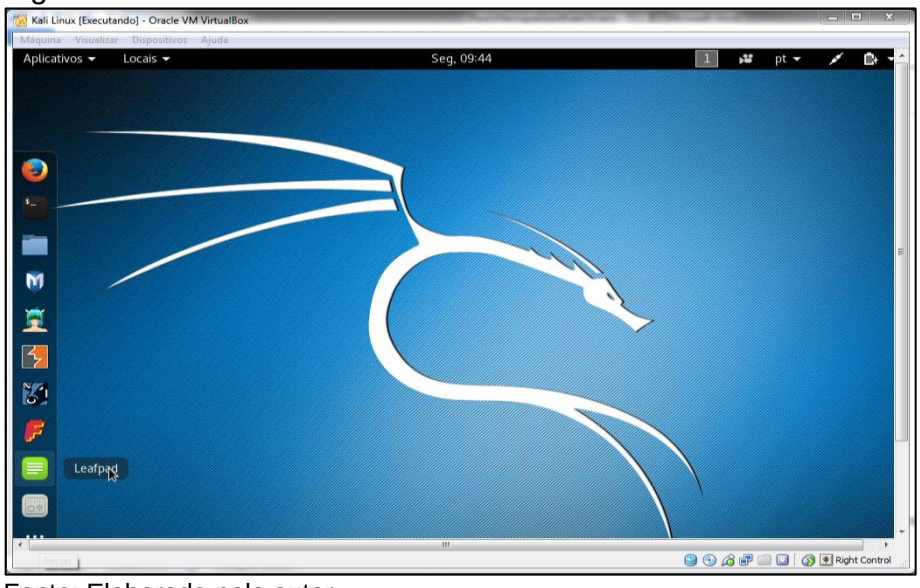
Para criar a infraestrutura de rede e o ambiente teste, primeiramente foi instalada a MV utilizando a ferramenta Virtual Box, ferramenta esta gratuita disponibilizada no site www.virtualbox.org. Nesta MV, foi instalado o SO Kali Linux, também gratuita e disponível no site www.kali.org. A versão do SO Linux instalado foi a Linux 2.6 (64 bit), dividindo a memória RAM do computador, destinando 1GB de memória RAM para o Kali Linux, criou-se um disco rígido virtual de 16GB para armazenamento dos dados e a rede configurada neste SO foi no modo Bridge, como mostra a Figura 7 e a interface desta versão instalada é mostrada na Figura 8.

Figura 7 - Infraestrutura da MV Kali Linux



Fonte: Elaborada pelo autor.

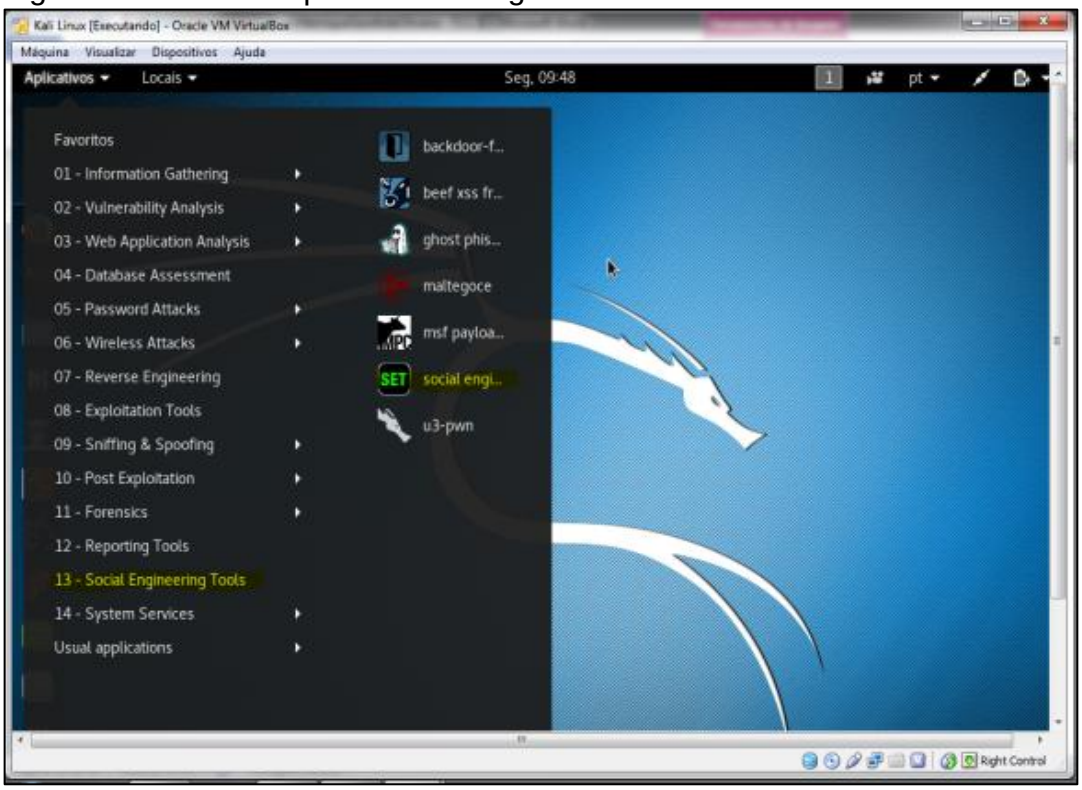
Figura 8 - Interface do Kali Linux



Fonte: Elaborada pelo autor.

Após a instalação do Kali Linux, usou-se o aplicativo disponibilizado por este próprio SO, de engenharia social, para clonar a página de login do Facebook, como mostra a Figura 9.

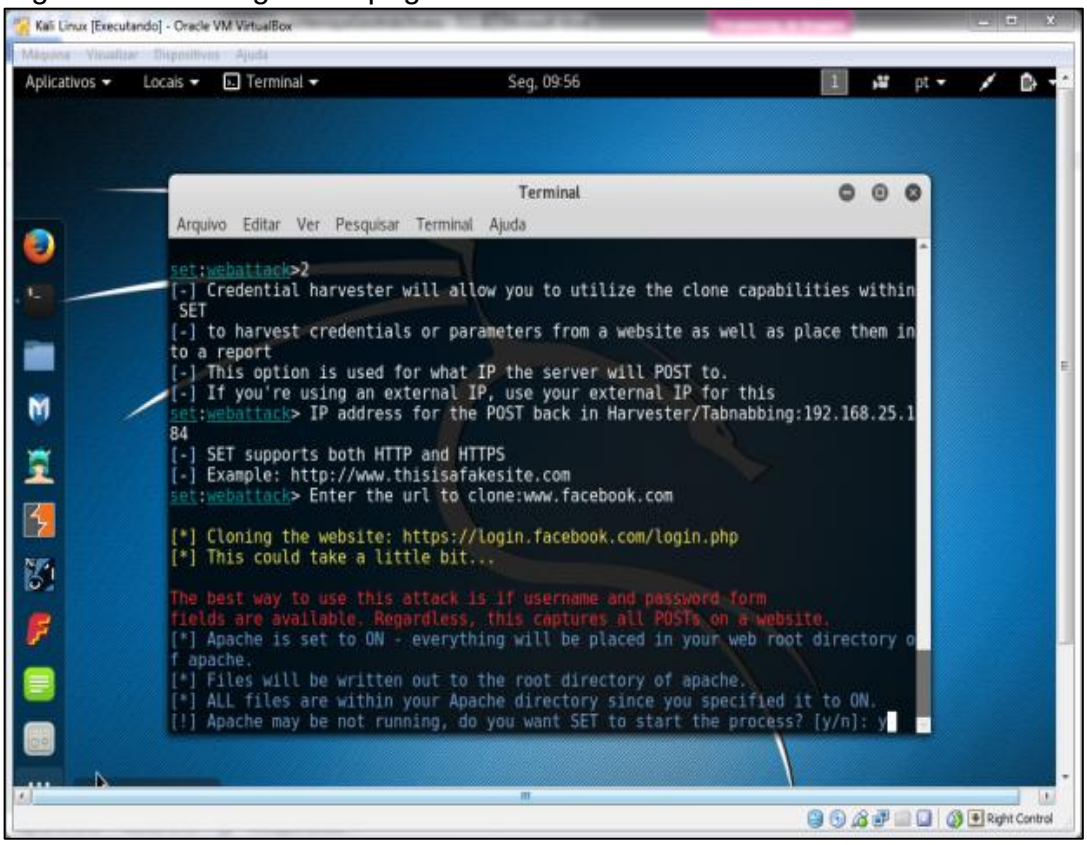
Figura 9 - Iniciando aplicativo de engenharia social do Kali Linux



Fonte: Elaborada pelo autor.

Como mostra a Figura 9, foi aberto o aplicativo SET através do menu: Aplicativos > Social Engineering Tools > set-social engineering. Após selecionado este modo de engenharia social; o aplicativo abre um terminal para iniciar alguns comandos: 1) Social-Engineering Attacks (Ataque de Engenharia Social); 2) Website Attack Vectors; 3) Credential Harvester Attack Method; 2) Site Cloner; e em seguida abriu-se outro terminal com o comando ifconfig para identificar o IP a ser digitado na clonagem da página. Feitas todas estas etapas, foi solicitado a URL da página que deseja-se clonar, neste caso, www.facebook.com e após escrever este comando, parte-se para a etapa demonstrada na Figura 10.

Figura 10 - Clonagem da página www.facebook.com

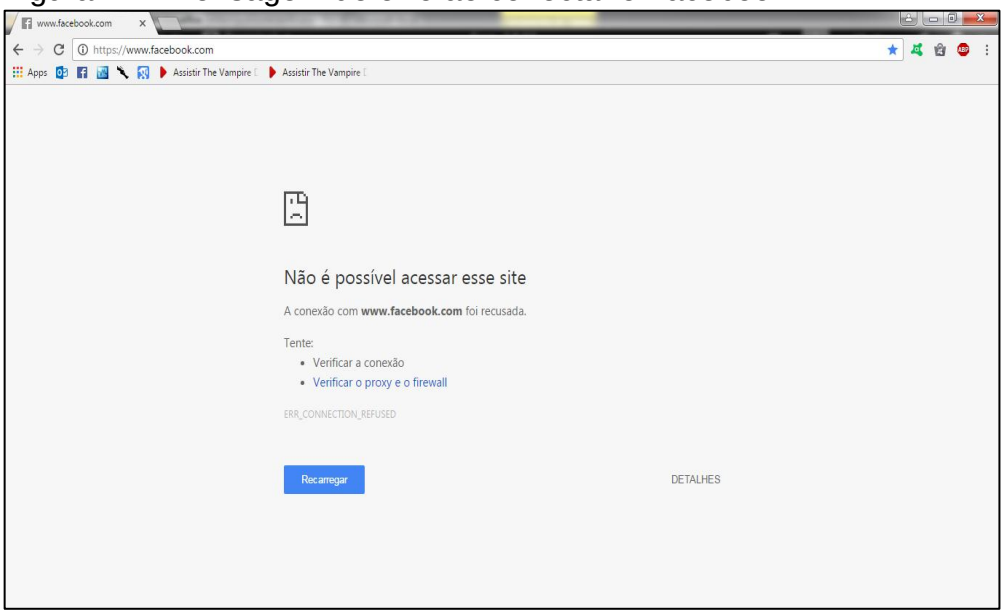


Fonte: Elaborada pelo autor.

A Figura 10 mostra a finalização da primeira etapa deste processo de clonagem. Foi aberto outro terminal para localizar e abrir o arquivo etter.dns para adicionar o novo destino da URL`www.facebook.com. Foram inseridas as novas linhas com seu respectivo IP e em seguida, os comandos para salvar e fechar. Foi aberto outro terminal e inserido o comando para ativar o plugin, e a partir deste momento, a ferramenta encontrava-se pronta para salvar os dados dos usuários que conectassem a página clonada.

Com o aplicativo para os ataques configurados, foram iniciados os testes, sendo que para isto, este programa instalado manteve-se aberto por 24 horas. Ao acessar o navegador por este mesmo notebook no SO Windows para realizar um teste inicial com a URL www.facebook.com, obteve-se uma mensagem de erro, mostrada na Figura 11.

Figura 11 - Mensagem de erro ao conectar o Facebook

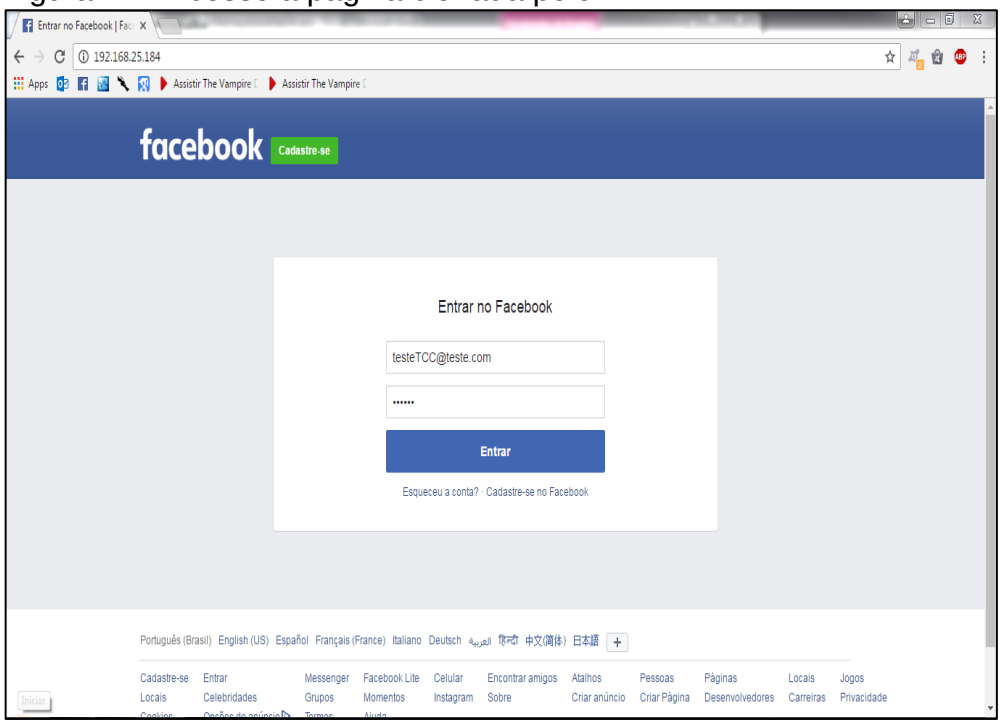


Fonte: Elaborada pelo autor.

Esta mensagem foi relatada por todos os usuários que compartilhavam a conexão Wi-Fi nesta residência.

Ao encontrar este erro, testou-se o acesso colocando na URL o IP configurado na instalação deste programa e percebeu-se que ao colocar este IP, redirecionava o usuário à página clonada, como mostra a Figura 12.

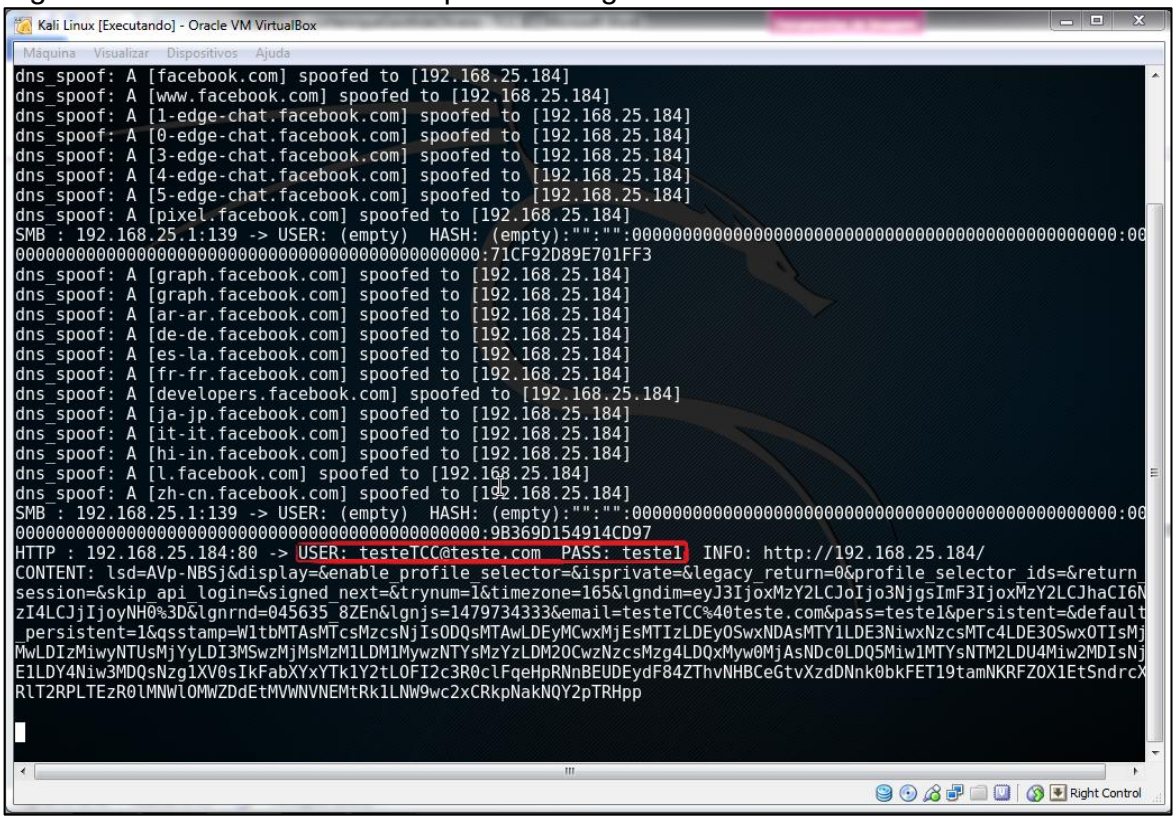
Figura 12 - Acesso à página clonada pelo IP



Fonte: Elaborada pelo autor.

Para testar se os procedimentos realizados estavam aptos à crackear os dados dos usuários e verificar o funcionamento do programa instalado para os ataques Phishing, entrou-se pelo SO Windows deste ambiente configurado para os testes no site facebook.com e com o e-mail testeTCC@teste.com obteve-se o primeiro resultado dos ataques, visto que o terminal registrou esta tentativa de acesso, roubando então, a senha deste usuário teste, como mostrado na Figura 13.

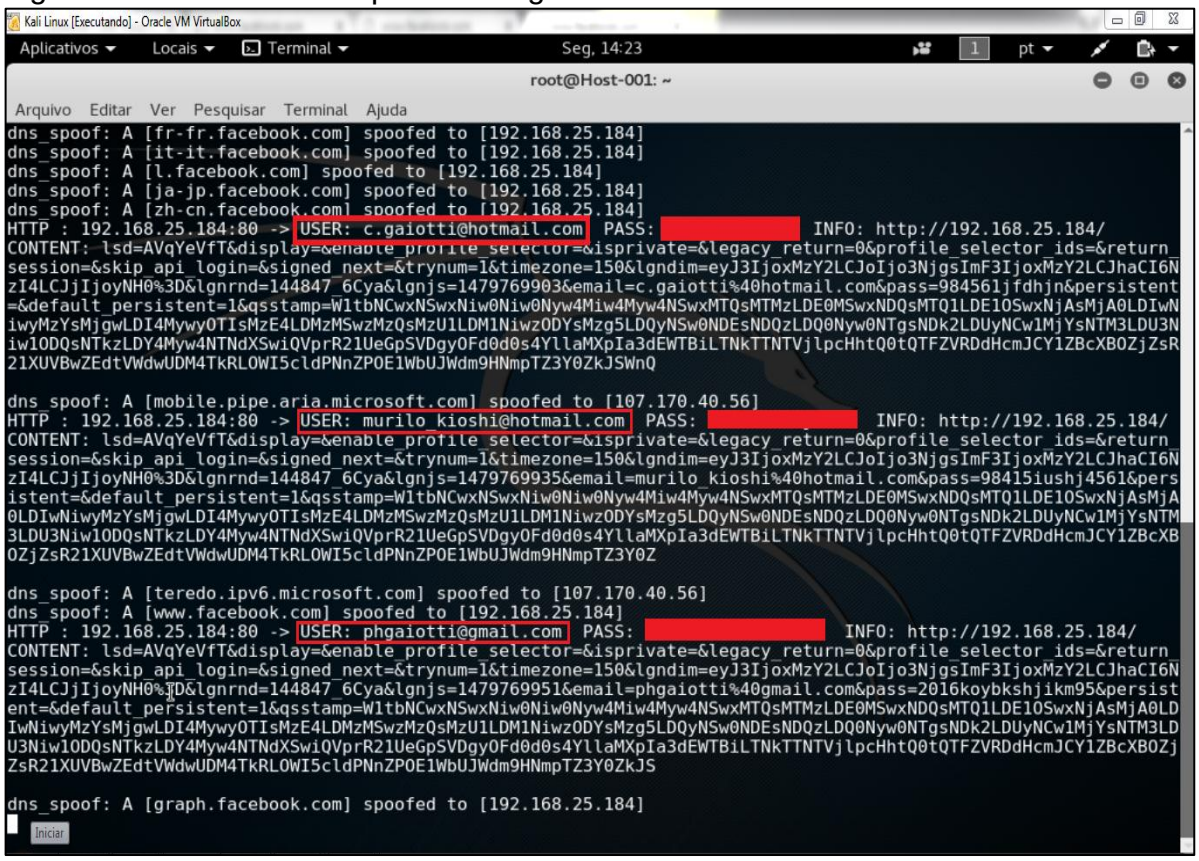
Figura 13 - Teste inicial do ataque Phishing



Fonte: Elaborada pelo autor.

Este primeiro teste realizado, mostra a eficácia do programa para roubar os dados de usuários fornecidos ao realizarem o login na página clonada. Ao comprovar o funcionamento deste programa e visto que não foi possível configurá-lo na rede Wi-Fi, foi solicitado à alguns usuários desta rede social presentes na casa, que acessassem a página colocando o IP na URL, visto que fazendo isto, o usuário era direcionado automaticamente à pagina clonada e estes resultados foram demonstrados na Figura 14, tendo um total de dados de três usuários, sendo que as senhas foram rasuradas para respeitar a privacidade destes.

Figura 14 - Testes do ataque Phishing



Fonte: Elaborada pelo autor.

Para finalizar os testes de ataque, este terminal foi fechado e os resultados foram salvos.

6 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo principal a demonstração da técnica de ataque Phishing para demonstrar a vulnerabilidade dos usuários de uma rede social ao acessarem suas contas por uma rede Wi-Fi.

Com o programa instalado para a realização deste ataque de engenharia social, iniciaram-se os testes, porém, nota-se que não foi possível colocar a página clonada na rede compartilhada e esta só pôde ser acessada pelo IP utilizado na instalação.

Este problema encontrado que impossibilitou atingir completamente os objetivos, pode ser que tenha ocorrido pelo fato de que durante a clonagem da página quando solicitado o IP, que neste caso, deve-se usar o IP wlan0, para que a página clonada fique disponível à todos que acessarem a internet local pela rede Wi-Fi, este não encontrava-se visível e nesta etapa, foi colocado o IP eth0 da conexão à cabo, impossibilitando talvez que a página clonada fosse acessada pelos usuários da casa e consequentemente, impedindo o ataque para obter os dados pessoais.

Entretanto, pode-se dizer que mesmo com este contratempo, a eficácia do programa que rouba os dados pessoais instalado foi comprovada, visto que se um indivíduo mal intencionado usa da engenharia social para que um usuário coloque os números deste IP cadastrado na URL como no caso deste trabalho, que redireciona automaticamente para a página clonada, este, chamado cracker, consegue todas as informações de login, mesmo sem ter colocado no Wi-Fi.

Sendo assim, este trabalho atinge seus objetivos com o intuito de contribuir para uma maior segurança do sistema, adquirindo e transmitindo conhecimento com as técnicas demonstradas e conclui-se após estes estudos e resultados que as maiores vulnerabilidades dos usuários da rede social estão no fato de acessarem uma conexão Wi-Fi não confiável, assim como no fato da engenharia social realizada para que cliquem em links que também redirecionarão estes usuários à páginas clonadas que roubam todos os seus dados.

Para trabalhos futuros, pode-se utilizar de diversos meios de continuação realizando a implementação em um ambiente mais próximo do real para obter resultados mais precisos e confirma-los em situações reais.

REFERÊNCIAS

ANDRADE, Eder. **História da Criptografia**. Disponível em: <http://www.dsc.ufcg.edu.br/~pet/jornal/abril2014/materias/historia_da_computacao.html>. Acesso em: 10 abr. 2016.

BOF, E. **Segurança em redes Wireless.** UCL - FACULDADE DO CENTRO LESTE, Serra, 2010.

CAMPOS, Augusto. **O que é Linux**. BR-Linux. Florianópolis, março de 2006. Disponível em <http://br-linux.org/faq-linux>. Acesso em: 4 abr. 2016.

CAPISTRANO, R. S.: **Redes sociais virtuais como ambiente de exposição de dados pessoais para a engenharia social** 2013. Disponível em: <http://www.repositoriobib.ufc.br/000012/00001226.pdf>. Acesso em: 2 maio 2016.

CARVALHO, F. R. et al.: **Vulnerabilidade em Aplicações Web.** Disponível em: <http://revistas.unifenas.br/index.php/RE3C/article/view/60>. Acesso em: 2 maio 2016.

CORTELA, J. J. C: **Engenharia Social no Facebook**. Dissertação de Mestrado, Universidade Estadual de Londrina, 2013.

FACEBOOK. **45% da população brasileira acessa o Facebook mensalmente.** Disponível em: <https://www.facebook.com/business/news/BR-45-da-populacao-brasileira-acessa-o-Facebook-pelo-menos-uma-vez-ao-mes>. Acesso em: 20 abr. 2016.

FARIAS, P. C. B.: **Rede Wireless**. 2005, Disponível em: <http://www.juliobattisti.com.br/tutoriais/paulocfarias/redeswireless001.asp>. Acesso em: 10 abr. 2016.

FERREIRA, J. L. M.: **Segurança em Redes sem Fio**. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

FOROUZAN, A.; MOSHARRAF, F.: **Rede de computadores:** uma abordagem Top-down. Editora AMGH, 2013.

FRANÇA, M. C. **Redes de Computadores**. Florianópolis: IF-SC, 2010.

LAUREANO, M. A. P.; et al.: **Detecção de intrusão em máquinas virtuais.** Anais do 5º SSI – Simpósio de Segurança em Informática – São José dos Campos – SP, 2003.

MANNARA, B.: **Sete conselhos para evitar ataques de phishing no seu perfil do Facebook.** 2015 Disponível em: <http://www.techtudo.com.br/listas/noticia/2015/06/sete-conselhos-para-evitar-ataques-de-phishing-no-seu-perfil-do-facebook.html>. Acesso em: 15 abr. 2016.

MATA, F. D.; **O Impacto das Redes Sociais na Sociedade Digital**. FATECSP - FACULDADE DE TECNOLOGIA DE SÃO PAULO, 2012.

MITINICK, K. D. et al. **A arte de enganar:** Ataques de Hackers: Controlando o Fator humano na Segurança da Informação. 4 ed. São Paulo: Pearson Makron Books 2003.

OLIVEIRA, N. L.: **Fases e etapas de um pentest:** análise e auditoria da estrutura de segurança em redes, sistemas e aplicações. Universidade Sagrado Coração. Bauru, 2015.

OUCH: **Ataques de phishing.** 2013. Disponível em: <https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201302_pt.pdf>. Acesso em: 20 abr. 2016.

PEIXOTO, Mário. **Segurança da Informação:** Vale muito aplicar a ISO 27002, 2012. Disponível em : <http://www.pouniasselvi.com.br/artigos/rev03-05.pdf> . Acesso em: 27 mar. 2016.

RAFAEL, G. C.: **ENGENHARIA SOCIAL:** AS TÉCNICAS DE ATAQUES MAIS UTILIZADAS. Disponível em: <https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/>. Acesso em: 20 abr. 2016.

RAFAEL, G. C.: **ENGENHARIA SOCIAL:** ENTENDENDO A TÉCNICA “PHISHING”. Disponível em: <https://www.profissionaisti.com.br/2013/11/engenharia-social-entendendo-a-tecnica-phishing/>. Acesso em: 20 abr. 2016.

REINALDO FILHO, D.; **A Responsabilidade dos Bancos pelos Prejuízos Resultantes do Phishing.** 2014 Disponível em: <HTTP://dialnet.unirioja.es/servlet/articulo?codigo=2857931>. Acesso em: 28 mar. 2016.

SAMPAIO, E. **Criptografia: Conceito e Aplicações**. 2013. Disponível em: <http://www.devmedia.com.br/criptografia-conceito-e-aplicacoes-revista-easy-net-magazine-27/26761>. Acesso em: 3 abr. 2016.

SILBERCHATZ, A.; GALVIN, P. B.: **Sistemas Operacionais: Conceitos**. Prentice Hall, 2000. São Paulo – SP.

SILVA, C. et al.: **Uma Análise de Vulnerabilidade de Usuários no Facebook.** Disponível em: <http://dl.acm.org/citation.cfm?id=2382707>. Acesso em: 4 maio 2016.

SILVA FILHO, A. M., **Entendendo e Evitando a Engenharia Social: Protegendo Sistemas e Informações.** 2004. Disponível em: <http://www.espacoacademico.com.br/043/43amsf.htm>. Acesso em: 27 mar. 2016.

STALLINGS, W. **Criptografia e Segurança de Redes**. São Paulo: Pearson Prentice Hall, 2008.

UFF: **Sistemas Operacionais.** Disponível em: <http://www2.ic.uff.br/~aconci/SistemasOperacionais.html>. Acesso em: 10 abr. 2016.