**UNIVERSIDADE DO SAGRADO CORAÇÃO**

**GUSTAVO PRIMOLAN DE CARA**

**TÉCNICAS DE ATAQUES EM REDES SOCIAIS UTILIZANDO O MÉTODO PHISHING**

BAURU

2017

**GUSTAVO PRIMOLAN DE CARA**

**TÉCNICAS DE ATAQUES EM REDES SOCIAIS UTILIZANDO O MÉTODO PHISHING**

Monografia de iniciação científica do curso de Ciência da Computação apresentada ao Centro de Ciências Exatas da Universidade do Sagrado Coração, sob orientação do Prof. Me. Henrique Pachioni Martins.

BAURU

2017



**RESUMO DO PROJETO**

O ser humano é um animal político e apenas alcança sua plena realização na relação com o outro e as redes sociais são canais imprescindíveis para a concretização dos anseios humanos e completude das relações sociais, pois permitem contatos com quaisquer pessoas a elas interligadas, independente de espaço e tempo, mas exige controle e garantia de segurança das informações. No entanto as invasões da privacidade das informações tornam-se cada vez mais frequentes, com o surgimento de novos métodos de violação de dados e, a partir do estudo desta área de pesquisa, propõe-se a exemplificação de um método de roubo de informação, muito utilizado nas redes sociais, denominado como *phishing*. O trabalho visa demonstrar os pormenores do método *phishing* e as diversas ferramentas que são manipuladas na sua execução, destacando-se o sistema operacional *Kali Linux*, que facilita o trabalho dos hackers por já conter softwares específicos para intrusão, embora desenvolvido para testar a vulnerabilidade do sistema, visando sua segurança. Tem ainda o presente projeto o objetivo de alertar os usuários dos sistemas e redes sociais desse meio de intrusão e da necessidade de agir com cautela quando da suspeita de links maliciosos.

**Palavras-chave:** Redes sociais. Segurança da Informação. Método *phishing*.

**LISTA DE ILUSTRAÇÕES**

[Figura 1 - Xerox Alto (1973) 10](#_Toc494700949)

[Figura 2 – Comunicação de dados entre dispositivos 11](#_Toc494700950)

[Figura 3 - Exemplo de uma rede LAN 12](#_Toc494700951)

[Figura 4 - Exemplo de uma rede MAN 13](#_Toc494700952)

[Figura 5 - Exemplo de uma rede WAN 14](#_Toc494700953)

[Figura 6 - Segurança da Informação: Tríade CIA 16](#_Toc494700954)

[Figura 7 - Esquema do Pharming 20](#_Toc494700955)

[Figura 8 - Facebook 22](#_Toc494700956)

[Figura 9 - Twitter 23](#_Toc494700957)

[Figura 10 – LinkedIn 24](#_Toc494700958)

[Figura 11 - Estrutura de um Sistema Operacional 25](#_Toc494700959)

[Figura 12 - Configuração da Máquina Utilizada 27](#_Toc494700960)

[Figura 13 - Configuração Máquina Virtual 28](#_Toc494700961)

[Figura 14 - Setoolkit 29](#_Toc494700962)

[Figura 15 - Configuração SET 30](#_Toc494700963)

[Figura 16 - Configuração etter.dns 31](#_Toc494700964)

[Figura 17 - Dados capturados 32](#_Toc494700965)

SUMÁRIO

[1 INTRODUÇÃO 8](#_Toc497945763)

[2 OBJETIVOS 9](#_Toc497945764)

[2.1 OBJETIVO GERAL 9](#_Toc497945765)

[2.2 OBJETIVOS ESPECÍFICOS 9](#_Toc497945766)

[3 REDES DE COMPUTADORES 10](#_Toc497945767)

[3.1 LOCAL AREA NETWORK (LAN) 12](#_Toc497945768)

[3.2 METROPOLITAN AREA NETWORK (MAN) 12](#_Toc497945769)

[3.3 WIDE AREA NETWORK (WAN) 13](#_Toc497945770)

[3.4 WIRELESS LOCAL AREA NETWORK (WLAN) 14](#_Toc497945771)

[4 SEGURANÇA DA INFORMAÇÃO 16](#_Toc497945772)

[4.1 SEGURANÇA NA INTERNET 17](#_Toc497945773)

[5 GOLPES NA INTERNET 18](#_Toc497945774)

[5.1 PHISHING 18](#_Toc497945775)

[5.1.1 Pharming 19](#_Toc497945776)

[5.2 ENGENHARIA SOCIAL 20](#_Toc497945777)

[5.3 SPYWARE 20](#_Toc497945778)

[6 REDES SOCIAIS DIGITAIS 21](#_Toc497945779)

[6.1 FACEBOOK 21](#_Toc497945780)

[6.2 TWITTER 22](#_Toc497945781)

[6.3 LINKEDIN 23](#_Toc497945782)

[7 SISTEMAS OPERACIONAIS 24](#_Toc497945783)

[7.1 LINUX 25](#_Toc497945784)

[7.1.1 Kali Linux 26](#_Toc497945785)

[8 METODOLOGIA 26](#_Toc497945786)

[8.1 MÁQUINA UTILIZADA 27](#_Toc497945787)

[8.2 SOFTWARES UTILIZADOS 28](#_Toc497945788)

[8.2.1 Social-Engineer Toolkit (SET) 28](#_Toc497945789)

[8.2.2 Ettercap 29](#_Toc497945790)

[9 IMPLEMENTAÇÃO DO CENÁRIO 29](#_Toc497945791)

[10 CONSIDERAÇÕES FINAIS 32](#_Toc497945792)

[REFERÊNCIAS 33](#_Toc497945793)

# 

# INTRODUÇÃO

A informação tem sido de vital importância para o mundo moderno, devido à manutenção dos negócios e realização de novos empreendimentos entre pessoas, empresas e povos. (DANTAS, 2011). Tendo isso em mente é de vital importância à proteção da informação, surgindo então o termo denominado Segurança da Informação.

Uma boa informação abre verdadeiras oportunidades para quem sabe como utilizá-la (DANTAS, 2011), justificando medidas efetivas para conter as ações fraudulentas e invasivas da intimidade alheia. Uma das formas de como conseguir esses dados é pelo método *phishing*, que é uma técnica que se utiliza da engenharia social para criar vítimas, enganando-as com o intuito de obter informações pessoais (como números de cartões de créditos) para depois utilizá-las indevidamente (OLIVO, 2010).

Há muitas formas de se executar o *phishing*, como por exemplo, através de janelas pop-up no navegador, mensagens ou e-mails. Conforme Olivo (2010), com apenas um clique a vítima pode receber um pacote com algum tipo de malware (software mal intencionado), que pode acarretar no roubo de dados ou podendo até deixar um software que comprometa a máquina, deixando-a como um zumbi em uma *botnet* – máquina que será comandada remotamente para executar o que o seu utilizador quiser.

Considerando este contexto, este trabalho tem como objetivo o estudo de segurança nas redes sociais, propondo uma exemplificação das formas de como o *phishing* é utilizado por usuários mal intencionados e aconselhando maneiras de prevenir esses ataques.

# OBJETIVOS

Apresenta-se nos tópicos a seguir o objetivo geral e os objetivos específicos desta pesquisa.

## OBJETIVO GERAL

Esclarecer o método *phishing* em suas diversas formas de efetivação, inclusive utilizando exemplos práticos de ataque às redes sociais por tal método intrusivo.

## OBJETIVOS ESPECÍFICOS

1. Realizar uma investigação teórica sobre o método *phishing*;
2. Fazer a delimitação sobre quais argumentos serão utilizados para a exemplificação;
3. Escolher a melhor forma de representar o método, considerando o método *phishing*;
4. Estudar e definir de uma forma adequada à simulação proposta nesta investigação;
5. Promover a divulgação da experiência e resultados obtidos em eventos técnicos e científicos, publicações correlatas, e participar do Congresso Anual de Iniciação Científica e Desenvolvimento Tecnológico e Inovação da USC.

# REDES DE COMPUTADORES

Surgindo da necessidade de compartilhamento rápido e constante das informações, os modelos de comunicação em massa, como celulares e internet, são de grande utilização nos dias atuais. (AMARAL, 2012).

Amaral (2012) aborda que no início, as redes de computadores eram pequenas, possuindo poucos computadores e sendo utilizadas pelas companhias aéreas apenas para fins comerciais e tendo as soluções de tecnologias sendo pertencentes, normalmente, a um único fabricante.

Como fato histórico, na década de 1970 houve um movimento para padronizar as redes, através de fabricantes diferentes, dando direção à construção de protocolos abertos que poderiam servir a várias soluções; já na década de 1980, as empresas DEC, Intel e Xerox se uniram para criar o que conhecemos hoje como o padrão Ethernet. (AMARAL, 2012).

É possível observar na Figura 1 a primeira estação de trabalho da Xerox Alto e também a primeira a ser ligada em rede.

Figura - Xerox Alto (1973)

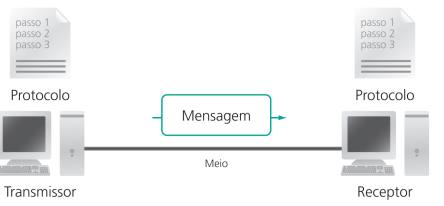


Fonte: Morimoto (2008, p. 15).

Constituindo-se de um conjunto de dois ou mais computadores interligados, as redes de computadores possuem o objetivo de compartilhar recursos e fornecer a troca de informações. (FRANCISCATTO; CRISTO; PERLIN, 2014).

A troca de informações entre dois dispositivos é feita através de algum meio de comunicação, tal como um par de fios, como pode ser observado na Figura 2 abaixo. (ALENCAR, 2010).

Figura – Comunicação de dados entre dispositivos



Fonte: Alencar (2010).

De acordo com Alencar (2010), um sistema básico com o objetivo de comunicação de dados entre eles, é constituído pelos cinco seguintes elementos:

1. Mensagem: Informação transmitida. Seu formato pode ser considerado como texto, números, figuras, vídeos e áudios;
2. Transmissor: Dispositivo responsável pelo envio da mensagem;
3. Receptor: Dispositivos responsável ao recebimento da mensagem;
4. Meio: Caminho físico pelo qual passará a mensagem;
5. Protocolo: Conjunto de regras para que a comunicação entre os dispositivos seja realizada.

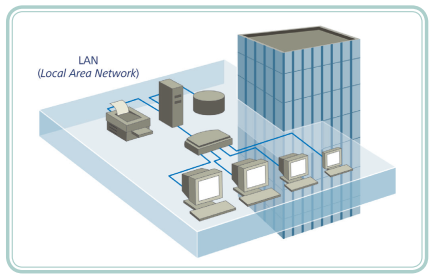
Franciscatto, Cristo e Perlin (2014), abordam que geralmente, as redes de computadores são classificadas de acordo com sua disposição geográfica e hierarquia.

Nos tópicos a seguir, são abordados as principais classificações das redes de acordo com suas disposições geográficas.

## LOCAL AREA NETWORK (LAN)

A rede do tipo LAN, ou também chamada de rede local, possui um espaço limitado quanto a extensão geográfica que pode atuar. (FRANCISCATTO; CRISTO; PERLIN, 2014). É possível notar um exemplo dessa rede através da Figura 3.

Figura - Exemplo de uma rede LAN



Fonte: Franciscatto, Cristo e Perlin (2014, p.17).

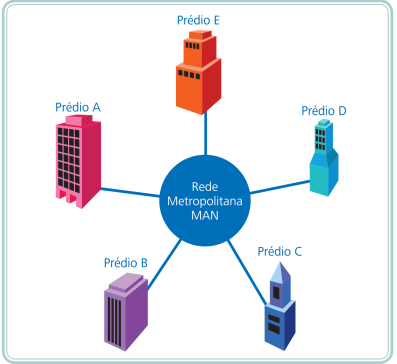
## METROPOLITAN AREA NETWORK (MAN)

Essa rede é caracterizada por possuir um espaço de média dimensão, podendo o mesmo ser uma região, cidade, campus e entre outros. (FRANCISCATTO; CRISTO; PERLIN, 2014).

Segundo Franciscatto, Cristo e Perlin (2014), uma MAN está sempre associada a conexão de várias redes local (LAN), sendo considerada uma parte menor de uma rede do tipo WAN, como é descrita no tópico abaixo.

A Figura 4 demonstra um exemplo da rede do tipo MAN.

Figura - Exemplo de uma rede MAN



Fonte: Franciscatto, Cristo e Perlin (2014, p.18).

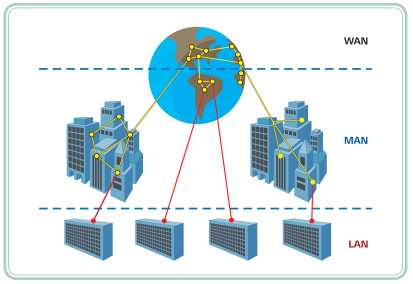
É interessante abordar um exemplo de MAN muito utilizada no dia a dia, que são as redes ISP (*Internet Service Provider*). As redes ISP podem ser conhecidas como os nossos provedores de serviço de internet do qual são contratados para que seja possível o acesso à internet em uma rede LAN. (FRANCISCATTO; CRISTO; PERLIN, 2014).

## WIDE AREA NETWORK (WAN)

Abrangendo uma grande área geográfica, a rede de longa distância (WAN), pode ser uma rede que faz parte de um país, continente e entre outros, permitindo a comunicação de longa distância, sempre interligando redes dentro da região que ela é encontrada.

Na Figura 5 é possível observar um exemplo de uma rede WAN.

Figura - Exemplo de uma rede WAN

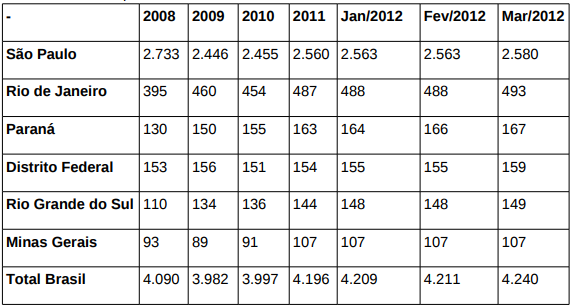


Fonte: Franciscatto, Cristo e Perlin (2014, p.19).

## WIRELESS LOCAL AREA NETWORK (WLAN)

Se tornando cada vez mais populares, as redes sem fio possuem sua instalação simples, como pode ser notado na Tabela 1. (REIS, 2012).

Tabela - Pontos de redes sem fio no Brasil



Fonte: Reis (2012, p. 8).

A WLAN permite disponibilizar a rede e acessos à *Internet* rapidamente a ambientes onde há grande demanda de mobilidade, quando a instalação de cabos tradicionais não é possível. (REIS, 2012).

Reis (2012), também comenta que, apensar dos grandes benefícios das redes sem fio, devemos analisar alguns fatores para que a escolha dessa tecnologia seja feita de forma correta, sendo esses fatores:

1. Verificar fontes que utilizam a mesma faixa de operação da rede sem fio, pois pode ocorrer de existir interferência.
2. Implementar a melhor configuração de segurança, pois diferentes das redes cabeadas, as WLAN são mais sensíveis a falhas.
3. Verificar compatibilidade com as aplicações existentes, pois a rede sem fio não possuí uma transmissão tão rápida em relação a cabeada.
4. Levantar os computadores que irão utilizar a rede sem fio, pois é necessário verificar custo, facilidade de instalação, performance e quantidade de pontos de acesso que serão necessários para a WLAN.

# SEGURANÇA DA INFORMAÇÃO

Alguns conceitos são importantes quando falamos de informação. Definições para dados, informação e conhecimento são necessárias para que possamos entender a importação da informação. (DANTAS, 2011).

Segundo Dantas (2011), a classe mais baixa da informação são os dados, tendo logo em seguida a informação propriamente dita, que nada além do que os dados que passam por algum tipo de processamento para serem utilizados de uma inteligível. A informação da qual a relevância, confiabilidade e importância foram avaliadas é nomeada de conhecimento e sendo sempre obtido pela interpretação e integração de dados e informações para se construir uma situação. (DANTAS, 2011).

Uma forma de garantir a autenticidade da informação é inserir medidas de segurança que preservem a confidencialidade, integridade e disponibilidade das informações (Figura 6). (SILVA; CARVALHO; TORRES, 2003).

Figura - Segurança da Informação: Tríade CIA



Fonte: Abreu (2011, p. 14).

A base para que uma empresa tenha novas oportunidades e maior liberdade de negócios é a segurança. Sempre dependentes da tecnologia, os negócios dependentes que a mesma consiga proporcionar os princípios básicos para que seja garantido a segurança. (LAUREANO, 2005).

De acordo com Laureano (2005), os princípios mais básicos para garantir a segurança da informação são:

1. Confidencialidade: Informação apenas acessada por pessoas autorizadas. Tem a intenção de impedir que pessoas não autorizadas possuam informações que não as convêm;
2. Disponibilidade: Informação sempre disponível quando requisitada;
3. Integridade: Informação não pode ser modificada no momento que foi armazenada.

Aumentar a produtividade dos usuários através de um ambiente mais organizado é também, um dos intuitos da segurança. Sempre proporcionar um maior controle sobre todos os recursos digitais.

## SEGURANÇA NA INTERNET

Sempre presente no cotidiano das pessoas, a Internet traz muita facilidade e oportunidades, sendo difícil imaginar uma vida sem a utilização dela. (CERT.br, 2012).

Além das vantagens, a Internet também traz alguns riscos, que de acordo com o Cert.br (2012), alguns destes riscos são:

1. Contato com pessoas mal-intencionadas;
2. Furto de identidade;
3. Furto e perda de dados;
4. Invasão de privacidade;
5. Divulgação de boatos;
6. Dificuldade de exclusão;

Cert.br (2012) também comenta que,

Um problema de segurança em seu computador pode torna-lo indisponível e colocar em risco a confidencialidade e a integridade dos dados nele armazenados. Além disto, ao ser comprometido, o seu computador pode ser usado para a prática de atividades maliciosas como, por exemplo, servir de repositório para dados fraudulentos, lançar ataques contra outros computadores (e assim esconder a real identidade e localização do atacante).

Portanto, com tudo o que foi dito, nota-se que para reduzir os riscos, é necessário que seja adotado uma postura preventiva e que exista uma atenção com à segurança independentemente da tecnologia utilizada ou local.

# GOLPES NA INTERNET

De acordo com CERT.br (2012),

Normalmente, não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial, e por este motivo, golpistas vêm concentrando esforços na exploração de fragilidades dos usuários.

Sempre fazendo a utilização de técnicas de engenharia social, os atacantes possuem o objetivo de enganar e persuadir as pessoas que podem ser potenciais vítimas a fornecerem informações sigilosas. (CERT.br, 2012).

Contendo a passo dos dados de algum indivíduo, os golpistas possuem a liberdade de efetuar transações financeiras, acessar sites, enviar mensagens eletrônicas, abrir empresas fantasmas e até mesmo criar contas bancárias ilegítimas. (CERT.br, 2012)

Nos subtópicos apresentados em seguida, são exemplificados alguns golpes que ocorrem com maior frequência na internet.

## PHISHING

Uma das mais populares técnicas relacionadas às fraudes online, o *phishing* é, na realidade, uma analogia ao termo “*fishing*”que tem o seu significado do inglês como pesca ou pescaria. (JORGE, 2007).

O CERT.br (2012) define o *phishing* como o tipo de fraude por meio do qual o golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

### Pharming

O tipo de ataque *pharming*, visa modificar a relação que existe entre um endereço eletrônico de um *site* e seu servidor web correspondente. (JORGE, 2007).

De acordo com Jorge (2007), “o termo surgiu em analogia à *farming* um outro termo utilizado na indústria farmacêutica e agrícola, que trata da modificação genética de hospedeiros para incrementar a produção de drogas medicinais”.

Para o CERT.br (2012), o *pharming*, envolve o redirecionamento da navegação do usuário para *sites* falsos, alterando o serviço do *Domain Name Service* (DNS). Assim, quando o indivíduo tenta acessar o *site* legítmo, o seu navegador faz o redirecionamento para o *site* do modificador do servidor. Esse redirecionamento pode ocorrer pelos seguintes motivos:

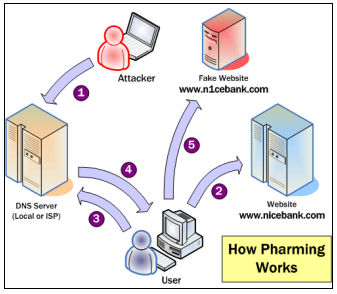
1. Comprometimento do serviço de DNS do provedor que você utiliza;
2. Códigos maliciosos projetados para alterar as configurações do serviço de DNS do seu computador;
3. Ação direta de um invasor, tendo acesso às configurações do serviço de DNS do seu computador ou *modem* de banda larga.

Simon (2007), afirma que o nome do ataque se origina da semelhança com a técnica, pois também é feita uma modificação no “hospedeiro” que contém as informações para o funcionamento da rede. Os “hospedeiros” são conhecidos como Servidores de Nome de Domínio (DNS).

Outras técnicas maliciosas estão relacionadas ao *pharming*, podendo haver desde uma instalação de um *spyware* para propaganda e publicidade nocivas, como também a junção com a técnica de *phishing,* redirecionando para um *site* bancário falso, com o foco em roubar os dados de um indivíduo. (JORGE, 2007).

De acordo com Jorge (2007), o ataque funciona em servidores DNS, explorando as falhas de segurança, programação ou má configuração, permitindo modificar a memória temporária (cache) do sistema atacado. Feito isso, o atacando tem a possibilidade de manipular e alterar as configurações no servidor, fazendo atribuições de “nomes de domínio” a IP’s controlados pelo mesmo. Na Figura 7 é possível ver uma representação do ataque.

Figura - Esquema do Pharming



Fonte: Jorge (2007, p. 47).

## ENGENHARIA SOCIAL

Com o objetivo de explorar a ingenuidade ou confiança do usuário, a engenharia social é uma técnica que visa apresentar histórias e situações que levam o executor da mesma receber dados sigilosos e posteriormente usa-los para obter acesso não autorizado a computadores ou informações. (JORGE, 2007).

Jorge (2007) também comenta que “as técnicas de engenharia social podem ser usadas em contatos pessoas, por telefone, e-mail ou chats”.

Mitnick e Simon (2003), definem a engenharia social como a influência e a persuasão para enganar as pessoas, com o intuito de convencê-las que o engenheiro social é alguém que na verdade ele não é, tendo como o objetivo principal, se aproveitar das pessoas para obter informações com ou sem o uso da tecnologia.

## SPYWARE

De acordo com Honeycutt (2004 citador por JORGE, 2007), um *Spyware* é um software que tem como seu principal objetivo enviar informações pessoais de um indivíduo para um terceiro, sem o consentimento do mesmo, incluindo informações sobre sites acessados ou até mesmo algo mais sensível, como dados de usuário e senhas.

Para Jorge (2007), o *Spyware* sempre permanece despercebido, ocultando-se de tal forma que o usuário não consiga reconhecer.

# REDES SOCIAIS DIGITAIS

Composta por indivíduos, organizações, associações, empresas ou outras entidades sociais, as redes sociais são designadas por atores, estando relacionados por um ou vários tipos de relações, como por exemplo, amizade, familiares, comerciais e entre outros. (FERREIRA, 2011).

Circulando diversos fluxos de informação, definimos as redes sociais de informação como um conjunto de pessoas que possuem algum padrão de contatos ou interações. (FERREIRA, 2011).

Ferreira (2011) também comenta que nos últimos anos, a expressão redes sociais tem sido associava, a quase que exclusivamente a tecnologias da informação e que na atualidade, a grande maioria das redes sociais existem independentemente da tecnologia.

Como esse trabalho abordará as redes sociais vinculadas a tecnologia, é possível observar, nos próximos subtópicos, as redes sociais digitais mais utilizadas da atualidade.

## FACEBOOK

De acordo com Moreira e Correia (2014), o Facebook, em sua página, define-se ser um produto/serviço que possui o objetivo de oferecer às pessoas o poder de partilhar e tornar o mundo mais interligado.

O Facebook interliga páginas de perfil dos seus utilizadores, sendo nessas páginas que os mesmos interligam seus perfis uns com os outros. (MOREIRA; CORREIA, 2014).

De acordo com Recuero (2009), originalmente chamado de *thefacebook*, o Facebook é um sistema criado pelo americano Mark Zuckerberg enquanto era aluno de Harvard. Sua principal ideia era focar alunos que estavam saindo do secundário (atual ensino médio, de acordo com o ensino brasileiro) e aqueles que estavam entrando em universidades.

É possível observar, na Figura 8, o *layout* atual da página inicial do Facebook.

Figura - Facebook



Fonte: Elaborada pelo autor.

## TWITTER

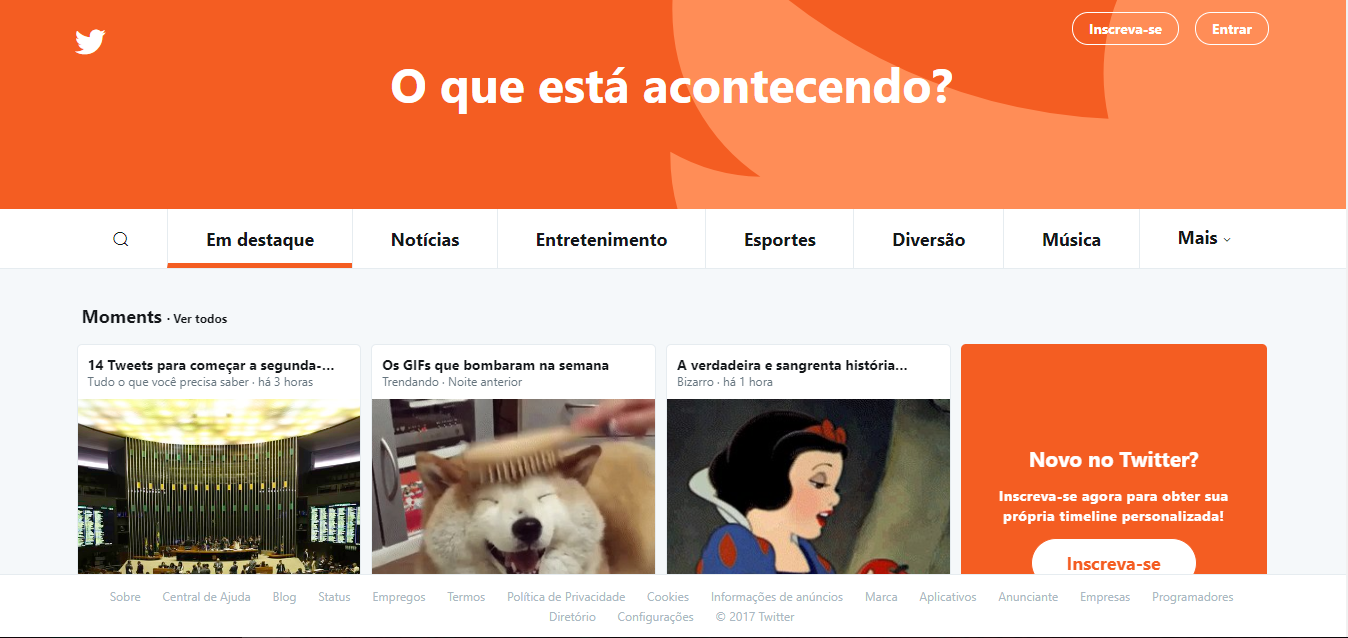
Incialmente, o Twitter tinha como objetivo atender a necessidade de comunicação interna da empresa Americana Obvious Corp, sendo de propriedade de Jack Dorsey. (BERTI, 2009).

De acordo com Berti (2009), em agosto de 2006, o Twitter se tornou público e possibilitou a criação de perfis, fazendo parecer muito com outras redes sociais da época, como o Facebook ou o inativo Orkut.

Recuero (2009) comenta que o Twitter “é construído enquanto microblogging porque permite que sejam escritos pequenos textos de até 140 caracteres”.

É possível acompanhar pela Figura 9, o layout atual do Twitter.

Figura - Twitter



Fonte: Elaborada pelo autor.

## LINKEDIN

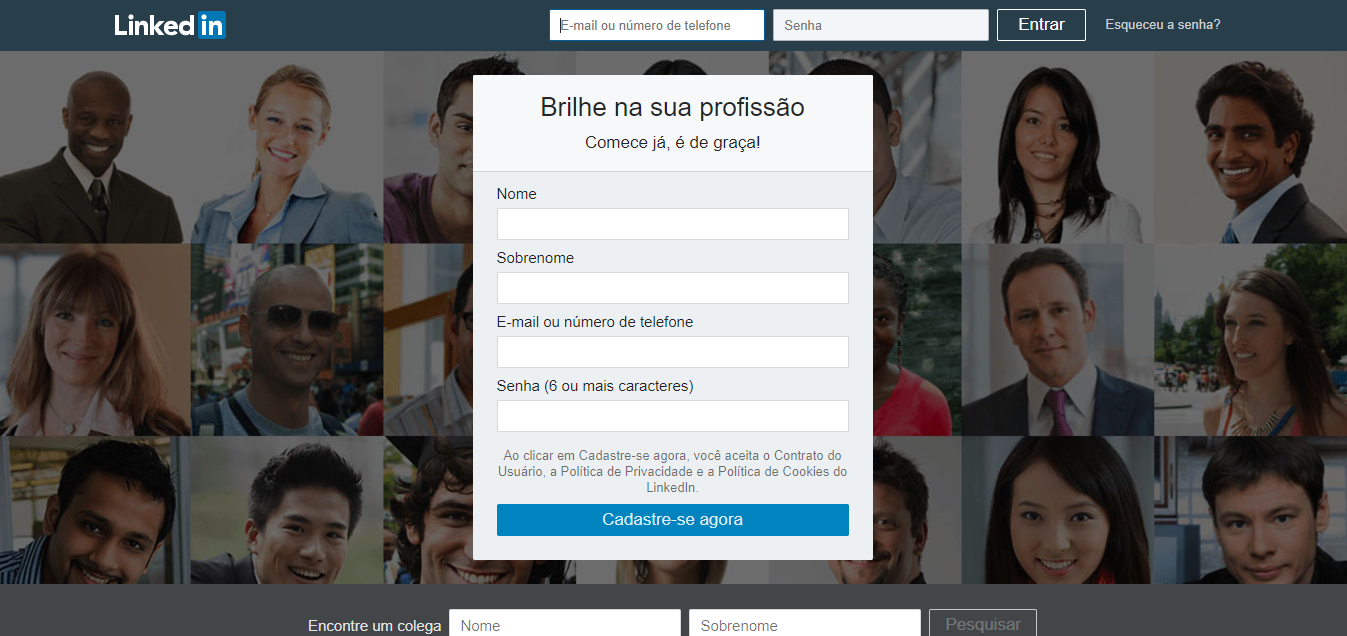
Lançada no início de 2003, o LinkedIn é uma rede de negócio e está localizado no estado da Califórnia. Parecido com outras redes sociais, o LinkedIn permite a criação de perfis, entretanto voltado para a carreira profissional. (OLIVEIRA, 2011).

Além disso, o LinkedIn possibilita que o usuário crie uma relação com empresas, profissionais, além de ser possível a elaboração de um currículo online, permitindo a procura por empregos. (OLIVEIRA, 2011).

De acordo com Oliveira (2011), é por essas características que o LinkedIn se intitula ser uma rede de negócios, trazendo sempre o relacionamento profissional e usado para encontrar empregos, anunciar vagas, além de outras funções.

Na Figura 10, é possível analisar o *layout* atual da rede social.

Figura – LinkedIn



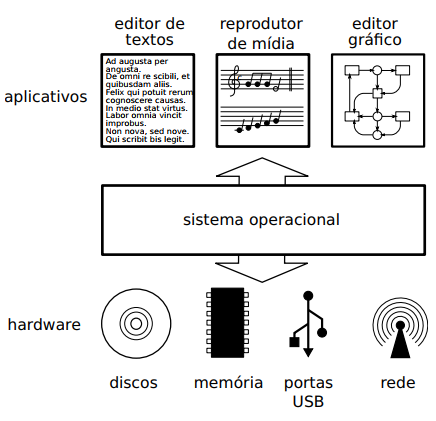
Fonte: Elaborada pelo autor.

# SISTEMAS OPERACIONAIS

Maziero (2017), comenta que a camada de software que opera entre os aplicativos voltados ao usuário final, o hardware e sendo uma estrutura de software ampla e muitas vezes de alta complexidade, com a capacidade de incorporar aspectos de baixo nível (como gerência de memória física) e de alto nível (como programas voltados ao usuário) é chamado de sistema operacional.

Na Figura 9 é possível observar a estrutura e o objetivo de um sistema operacional.

Figura - Estrutura de um Sistema Operacional



Fonte: Maziero (2017, p. 13).

## LINUX

Desenvolvido por um programador finlandês chamado Linus Torvalds e inspirado no sistema operacional Minix, o conhecido Linux é um termo popular utilizado para fazer referência a sistemas operacionais que utilizam o núcleo Linux. (ALENCAR, 2015).

Segundo Alencar (2015), o código fonte do sistema operacional é disponível sob a licença GPL em sua segunda versão, para que se possa utilizar, estudar, modificar e fazer destruição do mesmo com ampla liberdade, de acordo com os termos da licença.

Por conta de sua licença, outros sistemas operacionais baseados no Linux foram criados e desenvolvidos distribuições do mesmo.

Esse trabalho abordará a utilização do sistema operacional Kali Linux, que é uma avançada distribuição Linux especializada em Testes de Intrusão e Auditoria de Segurança. (OFFENSIVE SECURITY, 2013).

### Kali Linux

O Kali Linux é uma distribuição Linux, baseada em Debian, com o objetivo de ser utilizado para auditoria de segurança, destinando-se a profissionais de segurança e administradores de TI, permitindo-lhes realizar testes avançados de penetração, análise forense e auditoria de segurança. (HERTZOG; GORMAN; AHARONI, 2017).

O projeto do Kali Linux teve seu início em 2012, quando a *Offensive Security* decidiu que queriam substituir o projeto Linux *Backtrack*. (HERTZOG; GORMAN; AHARONI, 2017).

Uma vez com o Kali Linux inicializado, é possível descobrir rapidamente vários tipos de ferramentas disponíveis para testes de penetração e aquisição de informação. (HERTZOG; GORMAN; AHARONI, 2017).

Por conta dessas características, o Kali Linux foi o sistema operacional escolhido para a implementação do ambiente controlado com a finalidade de testes e demonstrações que o trabalho propõe a fazer.

# METODOLOGIA

Este trabalho foi desenvolvido em duas fases distintas: uma fase de investigação dos aspectos teóricos e uma etapa de amostragem da implementação do método *phishing*. Na primeira fase foi feito um estudo teórico dos diversos assuntos relacionados com o escopo do trabalho. Portanto, um levantamento bibliográfico foi o primeiro passo para a construção da pesquisa, avaliando bibliografias em livros, artigos científicos, buscando um aprofundamento maior no método *phishing*, para a compreensão do processo de simulação, com testes para validar os conceitos.

Nesta etapa foi realizada uma análise do método *phishing*, de forma a fazer um recorte referente à quais técnicas serão aplicadas a amostragem.

Na segunda fase, foi realizada a implementação do cenário proposto e dos métodos e os testes necessários. Tais testes foram modelados conforme o conjunto de informação definidos na fase anterior. No fim deste processo, os dados foram coletados e analisados a fim de fornecer os subsídios necessários para avaliação da proposta desta investigação.

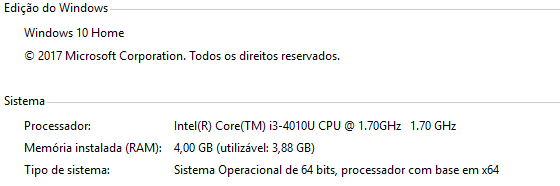
Algumas ferramentas foram utilizadas na etapa da implementação do cenário. É possível acompanhar tais ferramentas (*hardware* e *software*) nos tópicos abaixo.

## MÁQUINA UTILIZADA

A máquina que utilizada para a implementação do cenário é um Notebook Acer com 4 GB de memória RAM, Sistema Operacional Windows 10 Home 64 bits, processador *Intel* *Core* i3-4010U (Quarta geração) 1.70GHz.

É possível acompanhar a configuração da máquina através da Figura 12.

Figura - Configuração da Máquina Utilizada

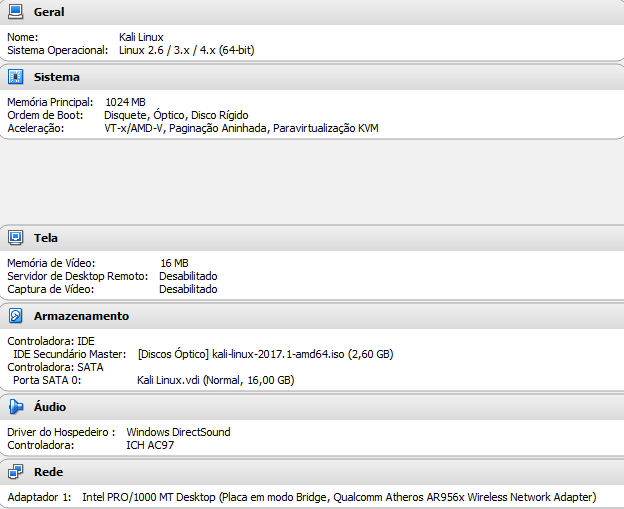


Fonte: Elaborada pelo autor.

Nesta máquina, foi configura uma Máquina Virtual (VM) utilizando o software oferecido gratuitamente pela *Oracle*, o *Oracle VitualBox*.

O sistema operacional que foi instalado nessa máquina foi o Kali Linux, como relatado nos tópicos anteriores. É possível acompanhar as configurações da máquina virtual na Figura 13.

Figura - Configuração Máquina Virtual



Fonte: Elaborada pelo autor.

## SOFTWARES UTILIZADOS

Nos próximos tópicos são exemplificados os principais softwares que foram utilizados no Kali Linux.

### Social-Engineer Toolkit (SET)

Os ataques construídos por esse software (que é um conjunto de ferramentas) tem o foco em uma pessoa ou uma organização. Sua utilização é durante testes de penetração. (KENNEDY, 2017).

O SET sendo uma ferramenta *hacker*, possui um menu com várias opções.

### Ettercap

O Ettercap foi desenvolvido com um objetivo de ser um sniffer (software que rastreia pacotes que são transportados pela rede) para redes locais (LAN) mas, durante o processo de desenvolvimento, ganhou cada vez mais recursos que mudaram para uma ferramenta poderosa e flexível para ataques de *Man In The Middle*. (ORNAGHI; VALLERI, 2017).

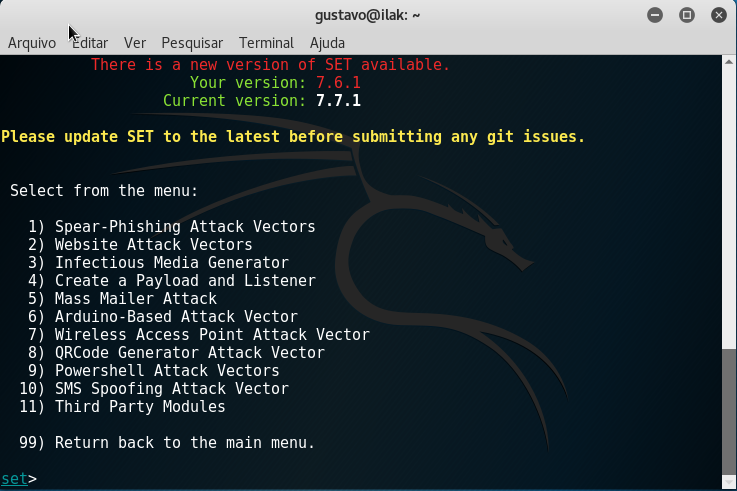
De acordo com Ornaghi e Valleri (2017) o Ettercap suporta a detecção de muitos protocolos (inclusive criptografados) e inclui muitos recursos para análise de rede.

# IMPLEMENTAÇÃO DO CENÁRIO

Foi utilizado o SET, como comentado nos tópicos acima, para clonar o Facebook.

Como o Kali Linux é um sistema operacional voltado para testes de penetração, não há a necessário de fazer o download do SET, apenas escreva no terminal o comando “*setoolkit”* e uma tela similar com a Figura 14 surgirá.

Figura - Setoolkit



Fonte: Elaborada pelo autor.

A opção escolhida será a 1, pois será um ataque de engenharia social.

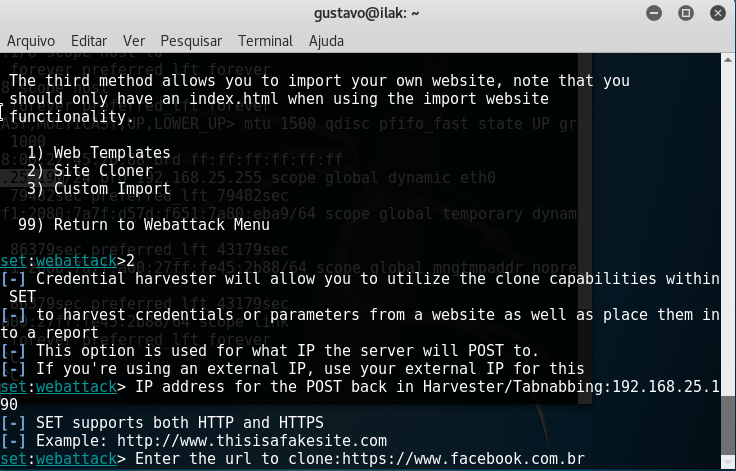
Logo em seguida será necessário escolher a opção 2, de Website Attack Vectors.

Após a etapa anterior a opção 3 é a escolhida, que é o método de ataque para a coleta de dados (*Credencial Harvester Attack Method*).

Por último a opção 2, para que possibilitará a clonagem do site.

Será necessário informar para o SET, o IP da máquina da qual será hospedado o site, no ambiente foi inserido o IP da máquina virtual, como pode ser notado na Figura 15 e então só precisará entrar com o site que será clonado, no caso do ambiente criado, a rede social digital Facebook foi escolhida.

Figura - Configuração SET



Fonte: Elaborada pelo autor.

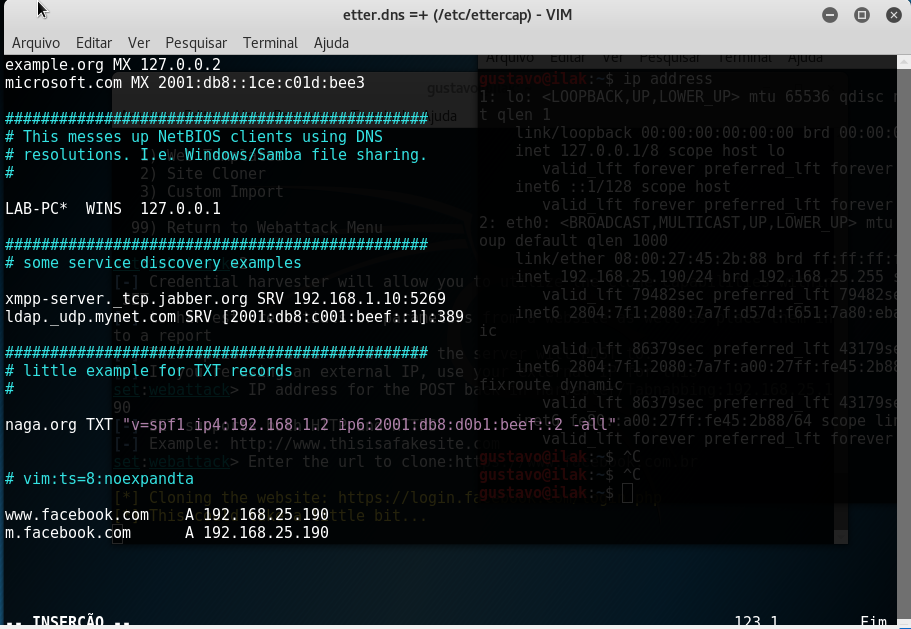
O site é clonado e movido para o diretório */var/www/html da máquina virtual*. O arquivo que mostrará as credenciais da vítima também será salvo nesse diretório.

Agora será necessário fazer a configuração do Ettercap, para que seja possível o redirecionamento das vítimas que tentarão acessar o Facebook original para o clone do Facebook na máquina virtual.

O documento que será necessário ser feito a edição se encontra no diretório “*/etc/ettercap”*, sendo o arquivo “*etter.dns”*.

A configuração do arquivo deverá ser feita conforme a Figura 16.

Figura - Configuração etter.dns



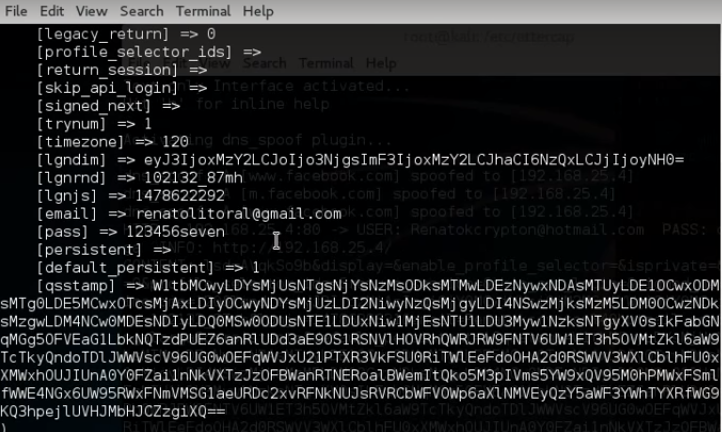
Fonte: Elaborada pelo autor.

Após tudo concluído, será executado o seguinte comando: *ettercap -T -q -i wlan0 -M arp -P dns\_spoof ///*.

Configurações feitas, só aguardar a vítima tentar acessar a rede social e será redirecionada para o site clonado, após tentar inserir seu usuário e senha ela será redirecionada para o site original, tendo que inserir novamente as suas credenciais.

A Figura 17 mostra o último teste feito, mostrando como as informações serão mostradas quando a vítima acessar o site clonado.

Figura - Dados capturados



Fonte: Elaborada pelo autor.

Com isso a implementação do cenário é finalizada. O tópico a seguir mostra algumas considerações em relação ao projeto.

# CONSIDERAÇÕES FINAIS

A pesquisa teve como objetivo principal a demonstração e implementação da técnica para um ataque *Phishing* em uma rede social, onde qualquer indivíduo conectado em uma rede pública conseguiria executar esse ataque.

É notório que o ataque é completamente possível e por conta disso é importante a cautela e o cuidado no momento em que usuários desavisados acessarem um rede pública.

Portanto, este projeto atingiu seus objetivos com o intuito de contribuir para uma maior segurança do sistema, adquirindo e transmitindo conhecimento com as técnicas demonstradas e concluindo-se, os resultados que a maior vulnerabilidade de usuários comuns que acessam redes sociais estão no fato de fazerem uma conexão 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.

# REFERÊNCIAS

ABREU, L. F. S. **A Segurança da Informação nas Redes Sociais.** 2011.

ALENCAR, M. S. **A História do Linux.** 2015.

ALENCAR, M. A. S. **Fundamentos de Redes de Computadores.** 2010.

AMARAL, A. F. F. **Redes de Computadores.** 2012.

BERTI, O. M. C. et al. **A história do Twitter no Piauí – de simples microblogging a instrumento de utilização jornalística.** 2009.

CERT.br. **Cartilha de Segurança para Internet.** 2012.

CORREIA, P. M. A. R; MOREIRA, M. F. R. **Novas Formas de Comunicação: História do Facebook – Uma história necessariamente breve.** 2014.

DANTAS, M. **Segurança da Informação: Uma Abordagem Focada em Gestão de Riscos**. 2011.

FERREIRA, G. C. **Redes Sociais de Informação: Uma História e um Estudo de Caso.** 2011.

FRANCISCATTO, R.; CRISTO, F.; PERLIN, T. **Redes de Computadores.** 2014.

HERTZOG, R.; GORMAN, J.; AHARONI, M. **Kali Linux Revealed.** 2017.

JORGE, P. G. A. **Fraudes na Internet: Uma proposta de identificação e prevenção.** 2007.

KENNEDY, D. **SET User Manual Made for SET 6.0.** 2017.

LAUREANO, M. A. P. **Gestão de Segurança da Informação.** 2005.

MAZIERO, C. A. **Sistemas Operacionais: Conceitos e Mecanismos.** 2017.

MITNICK, K. D; SIMON W. L. **A Arte de Enganar. Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação.** 2003.

SIMON, C. A. P. **Scam, phishing e pharming: as fraudes praticadas no ambiente Internet Banking e sua recepção no Brasil.** 2007. Disponível em: <http://www.egov.ufsc.br:8080/portal/conteudo/scam-phishing-e-pharming-fraudes-praticadas-no-ambiente-internet-banking-e-sua-recep%C3%A7%C3%A3o-no-> . Acesso em: 13 de Agosto de 2017.

MORIMOTO, C. E. **História das redes. Guia do Hardware.** Disponível em: <http://www.guiadohardware.net/tutoriais/historia-redes/pagina3.html>. Acesso em: 18 de julho de 2017.

OFFENSIVE SECURITY. **Official Kali Linux Documentation.** 2013.

OLIVEIRA, A. **O que é o LinkedIn? Conheça essa ferramenta online para encontrar empregos.**  2011. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2011/05/o-que-e-o-linkedin-conheca-essa-ferramenta-online-para-encontrar-empregos.html>. Acessado em 19 de maio de 2017.

OLIVO, C. **Avaliação de Características para Detecção de Phishing de Email**. 2010.

ORNAGHI, A.; VALLERI, M. **Manual Reference Pages – ETTERCAP.** 2017. Disponível em: <http://www.irongeek.com/i.php?page=backtrack-3-man/ettercap>. Acessado em 27 de agosto de 2017.

RECUERO, R. **Redes Sociais na Internet.** 2009.

REIS, G. H. R. **Redes Sem Fio.** 2012.

SILVA, P. T.; CARVALHO, H.; TORRES, C. B. **Segurança dos Sistemas de Informação. Gestão Estratégica da Segurança Empresarial.** 2003.