UNIVERSIDADE FEDERAL DO PARÁ
CAMPUS UNIVERSITÁRIO DE CASTANHAL
FACULDADE DE COMPUTAÇÃO

MÁCIO LEANDRO MOTA DE OLIVEIRA

KALI LINUX: ANÁLISE TEÓRICA DO SEU EMPREGO NA SEGURANÇA DA INFORMAÇÃO

Castanhal – PA

2023

MÁCIO LEANDRO MOTA DE OLIVEIRA

KALI LINUX: ANÁLISE TEÓRICA DO SEU EMPREGO NA SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso, apresentado a Faculdade de Computação da Universidade Federal do Pará, como parte das exigências para obtenção do título de Bacharel em Sistemas de Informação.

Orientador: José Jailton H. F. Junior

Castanhal – PA

2023

MÁCIO LEANDRO MOTA DE OLIVEIRA

KALI LINUX: ANÁLISE TEÓRICA DO SEU EMPREGO NA SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso, apresentado a Faculdade de Computação da Universidade Federal do Pará, como parte das exigências para obtenção do título de Bacharel em Sistemas de Informação.

APROVADO EM:

_____
Prof.
Orientador

_____
Prof.
Co-Orientador

_____
Membro: Prof.

A minha família, que sempre me apoiou,
aos meus Professores, que me guiaram
nessa jornada pelas sendas do
conhecimento e aos meus amigos. A todos,
dedico esse trabalho de coração sincero.

AGRADECIMENTOS

Dedico este trabalho a Deus, por ter me presenteado com o dom da vida, a minha esposa Jayane, que me apoiou desde o início se alegrou e se preocupou junto a mim, aos meus filhos Mácio Jr, José Miguel e Maya, que foram meu combustível para continuar na busca pelo conhecimento, foram noites que deixei de estar ao lado deles, para seguir direto do trabalho ao campus da universidade, valorizo muito a confiança e o apoio que me deram para continuar.

Aos meus pais Manoel e Lucilete, por terem plantado em mim a semente do desejo por aprender, minha mãe que dedicou horas para tentar me ensinar português, eu sendo ainda apenas uma criança, que preferia brincar a estar ali sentado estudando, mais tarde pude entender o motivo dessa dedicação e dessa insistência para que me tornasse um bom cidadão através dos estudos, meu pai que dedicou seu tempo entre trabalho e atenção a nós, meu irmão Alex, obrigado por seguir a minha frente como um bom exemplo mais velho no qual me espelhava a ser, pois era elogiados pelos seus professores por sua dedicação aos estudos.

Por fim, agredeço aos meus professores, em especial ao meu Orientador José Jailton Júnior, que não me deixou desamparado nos momentos mais difíceis, sempre me auxiliou para que chegasse até ao final deste trabalho, aos meus colegas de curso, que contribuíram para o meu aperfeiçoamento como aluno e como pessoa também, meu muito obrigado.

A persistência é o caminho do êxito (Charles Chaplin)

RESUMO

A constante evolução tecnológica proporcionada pela revolução da microcomputação e o advento da internet permitiram grande avanço nas relações sociais, de produção e nas comunicações humanas. Contudo, apesar de seus incontáveis benefícios, tal avanço tecnológico traz também novas formas de ameaça, tornando vulneráveis dados tão importantes quanto sigilosos. Assim, desponta o ramo das Ciências Computacionais da Segurança da Informação. Esse ramo do Conhecimento Computacional ocupa-se de prover a segurança dos dados, através da segurança de redes, *softwares* e *hardwares*, fazendo uso de um vasto leque de ferramentas e técnicas para tanto. Entre essas ferramentas e técnicas está o emprego do Kali Linux, uma distribuição do Sistema Operacional Linux desenvolvida especificamente para a Segurança da Informação, com ferramentas para testes de intrusão, detecção de vulnerabilidades diversas e monitoramento do tráfico de rede. Assim, o tema do presente trabalho é: “Kali Linux: análise teórica do seu emprego na segurança da informação”. Seu objetivo geral foi compreender as técnicas e ferramentas do Kali Linux para a Segurança da Informação. Para tanto, uma pesquisa exploratória, embasada em uma revisão de literatura. Entre suas principais considerações finais o presente trabalho aponta a eficiência do Kali Linux enquanto ferramenta da Segurança da Informação.

Palavras-chave: Segurança da Informação, Kali Linux, Detecção de Intrusão em Redes Computacionais.

ABSTRACT

The constant technological evolution brought about by the microcomputing revolution and the advent of the internet has allowed for significant advancements in social relations, production, and human communications. However, despite its countless benefits, this technological progress also brings new forms of threats, making data that is as important as it is confidential vulnerable. Thus, the field of Computer Science in Information Security emerges. This branch of Computational Knowledge is concerned with providing data security through network security, software and hardware security, using a wide range of tools and techniques for this purpose. Among these tools and techniques is the use of Kali Linux, a distribution of the Linux operating system specifically developed for Information Security, with tools for penetration testing, detection of various vulnerabilities, and network traffic monitoring. Therefore, the topic of this work is: "Kali Linux: theoretical analysis of its application in information security". Its overall objective was to understand the techniques and tools of Kali Linux for Information Security, through an exploratory research based on a literature review. One of the main final considerations of this work is the efficiency of Kali Linux as a tool for Information Security.

Keywords: Information Security, Kali Linux, Computer Network Intrusion Detection.

SUMÁRIO

1. INTRODUÇÃO

O mundo vive a era denominada pelo sociólogo Manuel Castells (2005) como a “Era da Sociedade em Rede”. Nessa era, a Internet assumiu papel fundamental na comunicação humana, causando profundas mudanças tecnológicas e socioculturais em nosso mundo.

Nesse contexto, não apenas a sociedade sofreu transformações, mas as corporações foram, também, profundamente modificadas. Assim, a troca de dados, entre plantas remotas de uma mesma corporação ou entre corporações tornou-se, independente da distância geográfica, instantânea. Consequentemente tornou-se possível o gerenciamento de uma unidade remota, localizada a milhares de quilômetros de sua matriz.

Contudo, a disponibilidade de dados e informações diversas na rede traz riscos à segurança desses. Outra mudança cultural surgida com o advento da internet foi a possibilidade de diversos tipos de ameaças e crimes virtuais, o que traz grande importância para a segurança da informação. Diversas ferramentas têm sido criadas para aplicação específica na segurança da informação, com finalidades como monitorar portas abertas, detectar intrusos na rede ou atuar como *firewall*. Uma dessas ferramentas é o Kali Linux, bastante empregado por analistas e auditores de segurança, *pentesters* e *hackers* para avançados testes de invasão e *pentest*.

Assim, o presente trabalho tem como seu tema: “Kali Linux: análise teórica do seu emprego na segurança da informação”.

1.1 OBJETIVOS GERAIS

O objetivo geral do presente trabalho é compreender as técnicas e ferramentas do Kali Linux para a Segurança da Informação.

1.2 OBJETIVOS ESPECÍFICOS

Conceituar a evolução da internet; descrever a segurança da informação e suas ferramentas e conceituar o Kali Linux.

1.3 MOTIVAÇÃO

A pergunta problema que norteia o presente trabalho é: como o Kali Linux pode ser usado para incrementar a segurança da rede?

O estágio atual da Sociedade em Rede, no qual os dados estão amplamente dispersos online, tornando-se passíveis de diversas ameaças, torna necessário que se expanda o conhecimento sobre a segurança da informação, justificando assim a realização do presente trabalho.

O presente trabalho é de natureza aplicada, devido ao seu caráter prático. Este objetiva gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos. Envolve verdades e interesses locais. (GERHARDT, 2009). A abordagem do trabalho é qualitativa, pois lida com aspectos em termos de características. (MARCONI; LAKATOS, 2002).

Como método, essa pesquisa se classifica em nível exploratório, pois o principal objetivo de uma pesquisa exploratória é desenvolver, transparecer e alterar conceitos, em busca da identificação de problemas ou possibilidades pesquisáveis para estudos e, a pesquisa exploratória, proporciona a necessária visão geral do tema a ser estudado. (GIL, 2012).

Os níveis de pesquisas podem ser classificados em relação ao fim e ao meio. Com relação à finalidade, a pesquisa pode ter um caráter exploratório quando o sistema a ser pesquisado não possuir nenhum tipo de pesquisa já relacionada. Quanto ao meio, pode possuir caráter descritivo em relação aos tipos de pesquisas existentes, como por exemplo, a revisão bibliográfica. (VERGARA, 2000).

Como procedimento é realizada uma revisão bibliográfica, que consiste em um levantamento bibliográfico detalhado do objeto de pesquisa. (GIL, 2012). A revisão bibliográfica deve ser utilizada quando questões referentes ao “como” e “porque” fazem parte do contexto da pesquisa. A revisão bibliográfica relata todos os aspectos envolvidos no contexto, é uma análise aprofundada do sujeito de pesquisa. (YIN, 2005). A principal característica da revisão bibliográfica é a intensidade do estudo. Para utilizar essa metodologia, devem-se destacar algumas considerações, como: a compreensão do estudo; a investigação de todo o objeto; a possibilidade de descobertas de outras relações de acordo com o aprofundamento do estudo. (FACHIN, 2003).

A etapa inicial do trabalho, que ocupou-se da construção de referencial teórico para a compreensão de própria internet, da evolução computacional, dos

princípios de segurança da informação, do Linux e do Kali Linux. A figura 1 mostra a estruturação utilizada no trabalho.

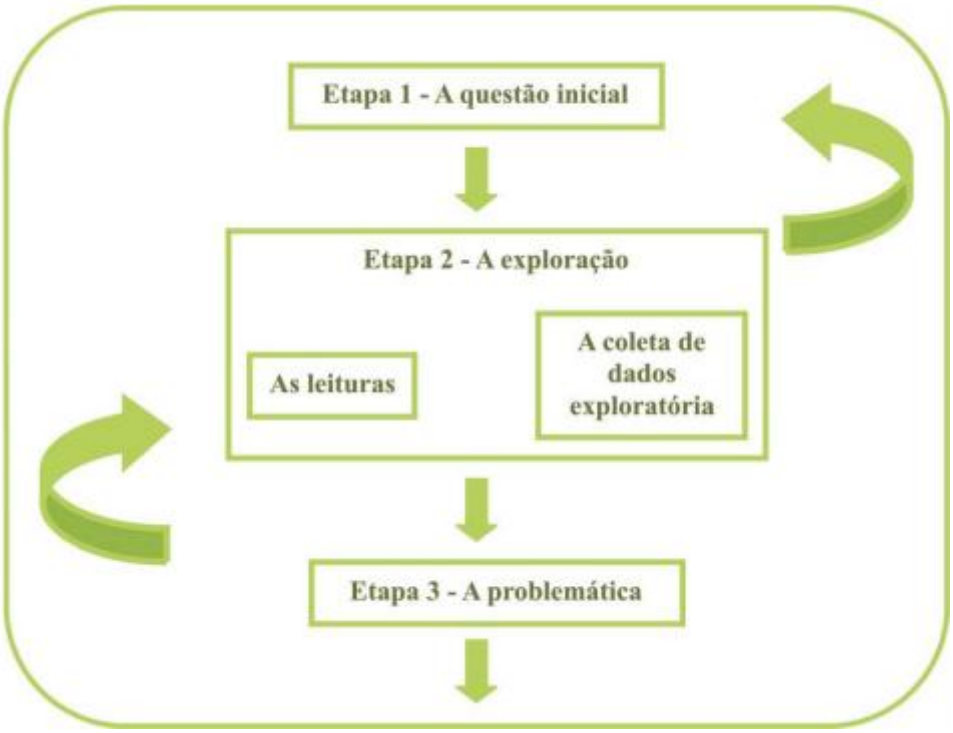

Figura 1 – Estruturação da base de referências
Fonte:

Assim, a definição da questão inicial, norteadora, permite o estabelecimento da problemática, e essa, leva a pesquisa bibliográfica e a sua exploração. À medida que as leituras e a exploração avançam, estas levam a modificações na formulação da pergunta inicial e da problemática, até que essas atinjam sua forma final.

A seguir, passa-se a fase de análise, que permite analisar estes, a fim de compreender a realidade do tema estudado, buscando responder a pergunta inicial e a problemática do trabalho. A etapa de análise é mostrada na figura 2.

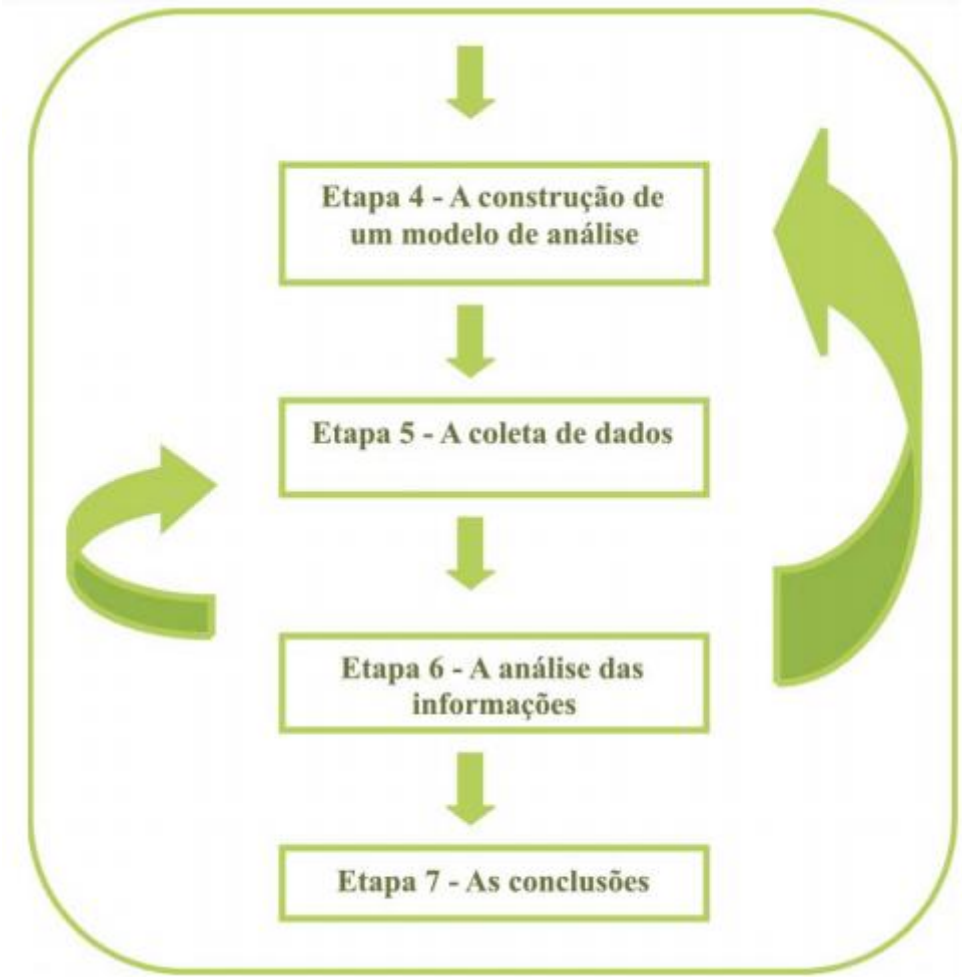

Figura 2 – Fase de campo do trabalho
Fonte:

Para a coleta dos dados é construído um modelo de análise, que para o presente trabalho é o estudo dos dados colhidos através da revisão bibliográfica. Tais dados são analisados e compilados, extraindo-se deles os elementos essenciais para a compreensão de todos os aspectos envolvidos na temática, permitindo assim, a discussão dos dados analisados e a produção de conclusões sobre estes

2. A EVOLUÇÃO COMPUTACIONAL E A INTERNET

Há séculos, a humanidade buscava formas de facilitar cálculos matemáticos, através de dispositivos que auxiliassem na realização ou realizassem os cálculos. No século XVIII, o matemático francês Blaise Pascal criou a "pascalina", criou a primeira máquina de calcular funcional. (WHITE, 2018)

Houve lento, porém contínuo progresso das máquinas de calcular, com invenções importantes, como a máquina de computação de dados através, de Hermann Hollerith, até a eclosão da Segunda Guerra Mundial (1939 – 1945). Nesse conflito, duas necessidades bélicas levaram engenheiros civis a desenvolver os primeiros protocomputadores[1]: a necessidade de orientar projéteis de artilharia e de decifrar os códigos nazistas. Assim, os norte-americanos construíram o *Mark I* para orientar a artilharia, enquanto os ingleses criaram o *Colossus*, capaz de decifrar os códigos das complexas codificadoras Enigma nazistas. (WHITE, 2018)

Nos anos do pós guerra, a continuação das pesquisas, aliada ao desenvolvimento de transistores[2] e materiais supercondutores[3], impulsionaram o desenvolvimento da Ciência Computacional. (WHITE, 2018)

Nos anos 1970, o advento das linguagens de programação de alto nível, como a linguagem C[4], que compreendem sintaxes e instruções próximas da linguagem humana, em substituição aos complicados comandos da linguagem *Assembly*[5], que utiliza comandos binários e hexadecimais para construir seus códigos de programa, permitiu que o computador pudesse realizar cálculos avançadas, além de construções gráficas das representações numéricas, o que

---

1 Computadores eletro-mecânicos, que empregavam válvulas eletrônicas e meios de cálculo e armazenamento de dados mecânicos. Caracterizavam-se por seu grande tamanho físico e pouca funcionalidade. Apresentavam ainda pequeno Tempo Médio entre Falhas, uma vez que as válvulas, que eram utilizadas até o limite de sua capacidade, não sobreviviam por mais do que 36 horas de operação. (WHITE, 2018)

2 Transistor ou Resistor de Transferência. Originado do termo inglês *Transfer Resistor*, foi desenvolvido nos laboratórios Bell em 1947. É utilizado, em eletro-eletrônica para amplificar ou trocar sinais eletrônicos ou potência elétrica. Passou a ser largamente empregado, em todo tipo de dispositivo elétrico, desde amplificadores de áudio e televisores até em satélites e supercomputadores. (WHITE, 2018)

3 Materiais, metálicos ou cerâmicos, capazes de conduzir energia elétrica com valores de resistência próximos de zero. Esses materiais tornaram possível a fabricação de componentes eletrônicos cada vez menores e mais leves, essenciais para o estado atual da tecnologia. Os transistores são feitos com materiais semicondutores. (WHITE, 2018)

4 Linguagem de Programação C. Linguagem, em computação, significa o programa, cuja formulação de código é conhecida como linguagem, empregado para escrever *software*, tanto para computadores, quanto para outras aplicações, como o gerenciamento de robôs. (WHITE, 2018)

5 Linguagem binária, que traduz as instruções do *software* para o *hardware*, permitindo que o computador compreenda os comandos dados pelo operador e devolva a esse os dados processados na tela, em forma inteligível. (WHITE, 2018)

possibilitou a expansão dos computadores para um grande número de ramos de atividade. (LIBERTY e JONES, 2005)

Porém, o maior obstáculo a generalização do uso dos computadores residia em seu tamanho físico: até o final dos anos 1970, o computador consistia, com poucas exceções, de diversos terminais, ligados via rede a um *mainframe*, sua unidade central de processamento, que possuía algumas dezenas de metros quadrados de tamanho. (GONÇALVES, 2015)

Uma das poucas exceções era um produto direto de um dos episódios da Guerra Fria: A Corrida Espacial. Nessa corrida, EUA e URSS disputavam, em sucessivas metas, a conquista do espaço. Embora, os soviéticos tenham, sem o emprego de tecnologia computacional ou eletrônica avançada, em 12 de abril de 1961, sido os primeiros a colocar um homem, o cosmonauta Iuri Gagarin, na órbita terrestre; os EUA venceram a Corrida Espacial, em 20 de julho de 1969, ao enviar o módulo de pouso *Eagle*, parte da missão *Apollo* 11, à superfície lunar. A bordo do módulo *Eagle*, além de dois astronautas, iam também alguns microcomputadores, responsáveis pela navegação e controle do pouso, decolagem e motores. (BROWN, 2019)

Essa tecnologia, que foi desenvolvida por civis trabalhando para o governo norte-americano, não ficou limitada à Corrida Espacial. Antes mesmo que as naves do programa *Apollo* realizassem sua alunissagem, microcomputadores bastante semelhantes plotavam o curso ou calculavam a trajetória da queda das bombas das aeronaves F-4 *Phantom* II e A-6 *Intruder* que operavam nos céus do Sudeste Asiático, durante a Guerra do Vietnam (1955-1975). (BROWN, 2019)

O início dos anos 1980 assistiu outra revolução civil: o advento do microcomputador. Em 1977 Ted Hoff da empresa Intel Corporation criou o microprocessador[6], item que seria essencial para a existência do Microcomputador. Com o uso do microprocessador (ou *microchip*), dois jovens, Steve Jobs e Steve Wozniak construíram o primeiro microcomputador (chamado também de computador pessoal, PC, derivado do inglês *personal computer*), que recebeu o nome de Apple I. (WHITE, 2018)

---

6 Microprocessador. Constituído por milhares de transistores, é a unidade responsável pelo controle lógico dos dispositivos computacionais. Operando em uma linguagem binária, sua operação se dá pelo acionamento (1) e desligamento (0), de microchaves, instaladas no interior dos transistores, e que permitem que as operações lógicas necessárias ao funcionamento do computador e ao gerenciamento e tratamento da informação sejam realizadas. (WHITE, 2018)

Jobs e Wozniak fundaram então a empresa Apple, e lançaram seu segundo modelo, o Apple II, que tornou-se um grande sucesso de vendas, pressionando, em 1980, a gigante IBM a entrar no nascente mercado de microcomputadores, tornando assim, a computação acessível à milhares de pessoas, em todo o mundo. (WHITE, 2018)

Porém, a revolução dos microcomputadores não se limitou a levar a ciência computacional para dentro dos lares. Empresas que antes não podiam contar com o apoio de computadores para realizar suas atividades, passaram, finalmente, a utilizá-lo. Cálculos antes complexos, como a folha de pagamento ou o balanço mensal da empresa, passaram a ser realizados de forma automática e simples. Na indústria, os engenheiros rapidamente se aliaram aos cientistas computacionais para transformar o microcomputador em uma máquina capaz de gerar projetos técnicos de diversas áreas, como a mecânica e a eletrônica, além de desenvolver programas que permitiam a esses dispositivos controlarem máquinas na linha de produção. (WHITE, 2018)

Outra revolução, acontecida na comunicação, seria vital para a expansão tecnológica humana.

2.1 A INTERNET

Desde o final dos anos 1970, a Informática passa por um processo acelerado de desenvolvimento, no qual as novas tecnologias sucedessem-se rapidamente, tornando-se seus avanços dispersos por todas as áreas do conhecimento humano (CERQUEIRA, 2004; OLIVEIRA, ROCHA e BITTENCOURT, 2004).

Para suas operações de tratamento automatizado dos dados, a Informática se vale do computador. Tecnicamente, o computador é definido como uma máquina, composta de partes eletrônicas e eletromecânicas, que possui a capacidade de recepção, armazenamento, tratamento e produção de informações, de forma automática, com rapidez e precisão (OLIVEIRA, ROCHA e BITTENCOURT, 2004).

Na década de 1990, o Departamento de Defesa dos EUA, substituiu a ARPANET pela NSFNET, de uso público, embora Universidades e empresas já utilizassem a ARPANET.

Para a expansão mundial da internet foram essenciais a criação da *World Wide Web (www)*, uma integração de redes mundiais e protocolos de comunicação,

criada pelos engenheiros do Centre Européen pour la Recherche Nucléaire (CERN), Robert Caillau e Tim Berns-Lee; o surgimento da Hyper Text Markup Language (HTML), a linguagem universal na qual são escritos os sites e o surgimento dos *browsers* ou navegadores de internet. O primeiro *browser*, o LYNX permitia apenas a transferência de texto entre os usuários, porém, o segundo navegador, o MOSAIC, já permitia o compartilhamento de imagens entre os usuários, e que se popularizou pelo mundo com o nome de internet (FERREIRA, 2017).

Assim, o advento do microcomputador, e a queda nos seus valores de comercialização, possibilitaram o alcance universal da informática, que passou a fazer parte do dia a dia da sociedade humana.

Estava iniciada a Era da Sociedade em Rede, como denominou o sociólogo Manuel Castells (2005): uma sociedade onde o limite geográfico já não é mais empecilho ao contato, nem há necessidade de horas ou dias para que se propague uma notícia. Nessa sociedade, os negócios são feitos instantaneamente, entre partes fisicamente distantes, sem a necessidade de qualquer meio de transporte. Mesmo as maiores distâncias geográficas do globo podem, na sociedade em rede, ser vencidas em alguns milissegundos. Dentro desse conceito, surgiriam ainda, pequenas revoluções na forma de comunicação e contato social: o advento das redes sociais e dos serviços de *streaming*.

Contudo, o advento da internet trouxe consigo outras inovações, além da constituição da Sociedade em Rede, de Manuel Castells (2005). A internet permitiu a integração remota de sensores, a transferência de dados entre servidores, bem como sua manipulação e visualização em aplicações remotas, que não se limitam mais ao computador pessoal, podendo ser acessadas da tela de um celular ou de outros tipos de dispositivos, como máquinas de cartão de crédito, robôs, dispositivos de telemetria, câmeras remotas e uma infinidade de outros, dando origem a IoT.

Porém, tal evolução e expansão das redes computacionais trouxeram consigo novos contextos, paradigmas, tecnologias e preocupações com a segurança.

3. REDES, SEGURANÇA DE REDES, SISTEMAS E DADOS

Uma rede de computadores pode ser definida como uma interligação, através do uso de protocolos de comunicação, transmitidos através de cabos ou tecnologias de transmissão sem fio; que permite a troca de dados entre as máquinas conectadas, em um ou ambos os sentidos. A mais notória evolução no ramo da comunicação por meio de redes computacionais foi o advento da internet. (LOUREIRO, NOGUEIRA, et al., 2017)

O advento da internet alterou permanentemente a estrutura social humana. Aliada ao avanço da microcomputação e das nanotecnologias, a internet permitiu novas formas de interação humana, como o compartilhamento instantâneo de notícias, independente de distâncias geográficas, o contato com pessoas de locais distantes e o comércio online, que permite ao cliente adquirir mercadorias a partir de um computador pessoal (PC) ou mesmo um *smartphone*, de qualquer lugar do globo, sem estar fisicamente na loja vendedora do produto, criando assim a prática que ficou conhecida como comércio online ou *e-commerce*. (MITSHASHI, 2011)

As primeiras transmissões de dados computacionais ocorrem por volta de 1940, com o uso de teletipos conectando calculadoras. Eram apenas experimentos, como o realizado por Petilson, que transmitiu as instruções de um problema, da faculdade de Dartmouth, New Hampshire, para uma calculadora programável, localizada em New York, usando um teletipo Model K, e recebeu, pelo mesmo meio, os resultados. (ESPIRIDIÃO, 2016)

O desenvolvimento das redes ganharia maior impulso nos anos 1960, devido a necessidade de comunicação computacional dos laboratórios universitários que estavam a serviço do *Department of Defense* (DoD). Esses laboratórios compunham a *Advanced Research Projects Agency* (ARPA). (MITSHASHI, 2011)

Na ARPA, a ligação de saídas computacionais a aparelhos de teletipo era um assunto de extremo interesse, havendo muita pesquisa e experimentação para aprimorar os processos de transmissão de dados através de redes computacionais. (FREITAS, 2017)

Essas pesquisas levaram ao desenvolvimento da rede experimental *Intergalatic Network*, precursora da mais avançada e geograficamente mais abrangente ARPANET. (LOUREIRO, NOGUEIRA, et al., 2017)

Outro passo importante para a evolução das redes de computadores. Foi dado em 1964, quando estudantes do MIT, apoiados por engenheiros e técnicos da Bell e da General Eletrics, utilizaram um computador DEC's PDP-8 para rotear e gerenciar conexões telefônicas. (ESPIRIDIÃO, 2016)

Finalmente, em 1969, utilizando circuitos de 50 kbits/s, a Universidade da California – Los Angeles (UCLA), a Universidade de Stanford, a Universidade da California em Santa Barbara e a Universidade de Utah, foram conectadas pela ARPANET. (MITSHASHI, 2011)

O sucesso da ARPANET inspirou as primeiras redes comerciais, que utilizam o primitivo protocolo x.25, que serviu de base ao TCP/IP. (ESPIRIDIÃO, 2016)

Em 1976, John Murphy, da Datapoint Corporation implementou o sistema de token para a transferência confiável de pacotes de dados, representando outra evolução na tecnologia das redes computacionais. (LOUREIRO, NOGUEIRA, et al., 2017)

Nos anos 1990, acordos entre o DoD e diversos centros acadêmicos no mundo inteiro levaram a decisão de tornar a ARPANET aberta, permitindo o acesso a usuários no mundo todo, dando origem à internet como conhecemos hoje. Ainda nos anos 1990, a velocidade de comunicação Ethernet foi aumentada, primeiro para 10 mbit/s e, posteriormente, para 100 mbit/s. (MITSHASHI, 2011)

Foram estabelecidas, entre o final dos anos 1980 e o meio dos anos 1990, as topologias comum de rede: em estrela (na qual todos os usuários se comunicam com um nó central); em Barramento ou BUS (topologia multiponto, na qual não há enlace ponto a ponto, ficando todos os nós conectados ao mesmo meio de transmissão) e topologia em Anel (topologia circular, teoricamente capaz de enviar e transmitir dados em qualquer direção, embora seja mais comumente encontrada operando unidirecionalmente. (ESPIRIDIÃO, 2016)

Cabe ainda lembrar que a topologia das redes pode ser física (a aparência real dessa) ou lógica (a forma de transmissão dos dados nessa). (MITSHASHI, 2011)

Os meio de interconexão mais comuns nas redes de computadores são os modems, os roteadores (com ou sem capacidade *WiFi*), os switches e os HUBs. (FREITAS, 2017)

Outro item essencial a comunicação são os cabos. Embora já tenham sido usados cabos coaxiais, esses hoje, encontram apenas empregos específicos, tendo sido quase que completamente substituídos pelos cabos de oito vias, com conectores RJ 45. Esses podem apresentar o padrão EIA/TIA 568 A ou B, ou ainda,

serem cabos Crossover (usados para a comunicação direta entre duas máquinas). (ESPIRIDIÃO, 2016)

Essencial, notadamente às redes corporativas, é o acesso remoto, realizado por aplicações como a Área de Trabalho Remota ou o Terminal Client, que permitem aos usuários acessarem de qualquer parte do globo, os dados e aplicações necessárias à realização de suas funções. (MITSHASHI, 2011)

3.1 GERENCIAMENTO DE REDES

Uma rede de computadores pode ser definida como uma forma de comunicação entre computadores, que permite a troca de dados entre esses, simplificando a execução de diversas tarefas e expandindo o leque de empregos possíveis para dispositivos computacionais. É, por exemplo, muito comum, o uso de aplicações do tipo cliente – servidor em ambientes corporativos, para as quais, a rede é um elemento fundamental. (ESPIRIDIÃO, 2016)

O gerenciamento de rede pode ser definido como uma disciplina dentro das ciências computacionais, cujo objetivo é a operação, gerenciamento e monitoramento de redes de dados e voz. Nas ciências computacionais a grande diferença entre os termos gestão e administração de redes.A figura do último é responsável por disponibilizar serviços e aplicações para a rede (serviços de diretório, sistemas de arquivos, cotas de disco, gerenciamento de serviços como a pilha de impressão e o DHCP, entre outros) enquanto a do primeiro é responsável monitoramento da rede, preocupado com questões como o desempenho dessa, a estabilidade e a segurança. (MITSHASHI, 2011)

São, portanto, atividades comuns do gestor de redes: obter informações extraídas dessa; estabelecer os critérios para o acionamento de alarmes; detectar e diagnosticar ocorrências de falhas; registrar a ocorrência de eventos; garantir a segurança; conhecer e controlar alterações em equipamentos associados à rede; acompanhar o desempenho da rede e dos recursos e inventariar os recursos disponíveis na rede e a sua forma mais comum de uso. (ESPIRIDIÃO, 2016)

Reconhece-se cinco áreas distintas dentro do gerenciamento de rede:

- Gerenciamento de Falhas
- Gerenciamento da Configuração

- Gerenciamento de Contas (Administração)
- Gerenciamento de Desempenho
- Gerenciamento de Segurança (ESPIRIDIÃO, 2016)

O gerenciamento de redes emprega, por seu turno, um conjunto de aplicações, nas quais processos gerenciais monitoram a rede, com o fito de aumentar sua produtividade, eficiência, segurança e desempenho. (LOUREIRO, NOGUEIRA, et al., 2017)

O processo agente consulta uma base de dados administrativos (MIB), onde as informações da rede ficam armazenadas em uma estrutura em forma de árvore hierárquica (baseado na visão orientada a objeto), permitindo que esse possa, baseado na comparação de dados, aferir e analisar a eficiência da rede. (MITSHASHI, 2011)

Os modelos para gerenciamento de rede podem ser:

- Modelo Internet: nesse modelo, de abordagem gerente/agente, as informações de desempenho são mantidas do lado agente, sendo enviadas com o gerente as solicita;
- Modelo OSI: esse modelo, pertencente a ISO, baseia-se no modelo de orientação a objeto. Os recursos geridos nesse modelo são representados na forma de objetos lógicos, chamados de objetos gerenciados.

Existem cinco área funcionais no gerenciamento num ambiente OSI:

- Gerência de configuração (estado da rede)
- Gerência de desempenho (vazão e taxa de erros)
- Gerência de falhas (comportamento anormal)
- Gerência de contabilidade (consumo de recursos)
- Gerência de segurança (acesso) (ESPIRIDIÃO, 2016)

Os principais softwares de gerenciamento de rede no mercado são:

Nagios: Possui recursos como o log de rede, o analisador de rede e o mapeadores de rede em tempo real. Desenvolvido originalmente para Linux, pode ser, mediando ajustes, instalado em servidores Windows. (ESPIRIDIÃO, 2016)

Zabbix: *software* open source, muito empregado no gerenciamento de redes. Desenvolvido em linguagem C, pode, sem necessidade de adaptação, rodar em qualquer sistema operacional existente hoje. (MITSHASHI, 2011)

PRTG: Desenvolvido em linguagem C especialmente para uso no Windows, possui ferramentas para a monitoração de todos os dispositivos, operações de dados, sistemas e dispositivos em uma estrutura de TI. (ESPIRIDIÃO, 2016)

3.2 ADMINISTRAÇÃO DE SERVIDORES WINDOWS E LINUX

O servidor é um elemento chave para as modernas redes e aplicações corporativas. Notadamente com o advento da internet, que levou ao surgimento de grande número de aplicações online, o desenvolvimento de aplicações do tipo cliente – servidor cresceu exponencialmente, aumentando ainda mais a importância dessas máquinas.

A definição mais elemento de servidor descreve esses elementos essenciais às ciências computacionais como computadores (ou *softwares*) que fornecem serviços aos computadores – clientes, em uma rede computacional ou aplicação específica. Tais serviços podem ser de diversas naturezas, como serviços de email, proteção (firewall), gerenciamento de impressão ou armazenamento. Esse tipo de arquitetura computacional é denominado de cliente – servidor.

Um servidor pode servir a vários clientes, mas, embora seja raro, pode também servir a apenas um cliente, que necessita de elevados recursos computacionais. Um mesmo cliente pode se conectar a diversos servidores, e um mesmo serviço pode ser acessado por diversos clientes simultaneamente.

O emprego do termo servidor nas ciências computacionais teve seu início na década de 1950, na mesma época em que se desenvolvia a Teoria das Filas, estando a origem desse verbete intimamente associada com essa teoria.

No final dos anos 1960, a expressão “Server” aparecia frequentemente na documentação da ARPANET, sendo descrito como “server-host”. O desenvolvimento do termo servidor, bem como o desenvolvimento do própria servidor está intimamente relacionado com o desenvolvimento das redes computacionais e da ARPANET. Pode-se afirmar que o servidor é elementar para a existência das redes de dados complexas, assim como as redes de dados complexas são elementares para a existência do servidor.

O desenvolvimento das necessidades computacionais levou ao surgimento de uma grande gama de finalidades específicas para os servidores. As mais comuns são:

- Servidor de arquivos: responsável pelo armazenamento de arquivos. Possui discos rígidos de grande capacidade, e pode gerenciar um grupo de unidades de armazenamento externas ou em nuvem.
- Servidor web: armazena as páginas de um site ou aplicação online.
- Servidor de email: armazena os serviços de email, possuindo recursos para a filtragem e controle desse serviço.
- Servidor de impressão: direciona os pedidos do *spooler* de impressão dos clientes para as impressoras corretas.
- Servidor de Banco de Dados: essencial para as aplicações do tipo cliente – servidor, tanto locais quanto remotas; armazena o banco de dados e, em alguns casos, também o SGBD. Possui backups redundantes e regras de segurança elevadas, para garantir a segurança dos dados.
- Servidor DNS: responsável pela resolução do DNS (tradução do nome do domínio para o IP e vice-versa).
- Servidor Proxy: servidor responsável pelo serviço de Proxy, que atua como controlador e otimizador da navegação na internet.
- Servidor FTP: utilizado para o upload e download de arquivos online
- Servidor de Virtualização: hospeda máquinas virtuais, usadas tanto para aumento da capacidade computacional quanto para a prototipagem de software e testes de segurança.
- Servidor de aplicação: também chamado de middleware, esse servidor disponibiliza um ambiente para a instalação de determinadas aplicações, possibilitando o uso de thin clients, que possuem apenas a capacidade de acesso à rede e ao servidor, diminuindo os custos com aquisição e manutenção de hardware, além de simplificar o processo de manutenção.
- Servidor de Imagem: servidor especializado no armazenamento de imagens. É utilizado em empresas relacionadas à comunicação, como Jornais, Agências de Fotografia e Marketing.
- Servidor de Fax: comum no começo da internet, hoje está em desuso. Sua função é gerenciar o envio de Fax pela internet.

Os principais Sistemas Operacionais (SO) encontrados em servidores são o Linux (em diversas distribuições) e o Windows Server.

O Linux é bastante empregado em servidores de Firewall, destinados a proteção de uma rede interna contra ameaças e invasores externos.

O Windows é usado para a gerência de usuários e permissões (Active Directory – AD), e para diversos serviços, como servidores de impressão, de armazenamento e de email.

Os servidores Linux destacam-se ainda por seu baixo custo, robustez e versatilidade das ferramentas de gerenciamento. Uma delas, o Squid, é bastante empregado no rastreamento de acesso a sites indevidos ou não seguros por colaboradores, além de permitir funções complexas de inteligência corporativa, como o rastreio de vestígios de espionagem industrial, através do acesso a FTPs e outras formas de armazenamento em nuvem suspeitos. Esse serviço, aliado à triagem de email, tem sido amplamente empregado pelos serviços de inteligência corporativa.

Outra importante vertente da Segurança da Informação, é a Segurança de Sistemas.

3.3 SEGURANÇA DE SISTEMAS

O conceito de segurança existe nas sociedades humanas desde que essas começaram a se organizar como tal. Inicialmente, esse conceito previa apenas a defesa dos grupos humanos contra predadores e contra o ataque de outros grupos, em disputas por territórios de caça. Contudo, já havia, muito embora, sem qualquer noção teórica, conceitos como segurança preventiva, como o fogo aceso a noite e os vigias e de segurança e a segurança proativa, representada, nesses grupos, pela prática, retratada em pinturas rupestres, de atacar os grupos que se aproximavam das áreas de caça. (NEVES, 2002)

A evolução sociocultural e tecnológica humana trouxe consigo o amadurecimento dos conceitos de segurança, bem como o surgimento de ramificações específicas dessa. A medida que o conhecimento e a tecnologia humana aumentavam, surgiam ramos específicos da segurança, como a segurança no mar, a segurança de voo, a segurança privada, a segurança do trabalho e, mais recentemente, a segurança da informação. Embora com atuações e visões

diferentes, essencialmente, todas as formas de segurança consistem em prover a integridade e o bem estar física e mental de pessoas, bem como, a preservação de seu patrimônio. (NEVES, 2002)

A segurança da informação pode ser definida como a proteção de um conjunto de dados, evitando preventivamente qualquer ameaça a esses, e agindo rapidamente para restabelecer a segurança, caso as medidas preventivas falhem. (ALVES, 2015)

Ao contrário do que possa parecer inicialmente, a segurança da informação não está relacionada apenas com sistemas computacionais, informações digitais ou armazenamento dessas, aplicando-se a todos os aspectos das ciências computacionais, como redes de dados e sensores, celulares e *smartphones* e outros. Mesmo meios físicos de armazenamento de dados, como cartões perfurados, têm sua proteção regida pela segurança da informação. (ESPIRIDIÃO, 2016)

Há quatro propriedades definidas na segurança da informação:

- Confidencialidade: propriedade que limita o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação;
- Integridade: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (Corrente, intermediária e permanente). O ciclo de vida da informação orgânica - criada em ambiente organizacional - segue as três fases do ciclo de vida dos documentos de arquivos; conforme preceitua os canadenses da Universidade do Quebec (Canadá): Carol Couture e Jean Yves Rousseau, no livro Os Fundamentos da Disciplina Arquivística;
- Disponibilidade: propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação;
- Autenticidade: propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo. (MITSHASHI, 2011)

A segurança da informação é regulamentada pela norma ISO/IEC 17799:2005, baseada no padrão britânico BS 7799. No Brasil, a regulamentação da segurança da informação é dada pela ABNT NBR ISO/IEC 27002:2013. (ESPIRIDIÃO, 2016)

Há vários mecanismos para o controle da segurança da informação, que podem ser físicos (restringem fisicamente o acesso a informação, como portas e controles de acesso) ou lógicos (implementados através de softwares). (MITSHASHI, 2011)

Os principais meios lógicos são:

- Mecanismos de encriptação: criptografam os dados, sendo reversível apenas pela outra ponta da conexão, que possui a chave criptográfica;
- Certificados digitais: conjunto de dados criptografados que permite a autenticação de transações de dados, funcionando como uma chave digital e verificador de autenticidade dos dados;
- Autenticação e autorização: usadas no gerenciamento de login, permitem o acesso a dados específicos, bem como o privilégio para manipulá-los.
- ID: permite identificar o usuário que realizou dada transação, sendo essencial haver uma ID válida em dado sistema, para que se possa ter acesso aos dados em questão;
- Chaves pública e privada: forma de autenticação, garantem a fidedignidade a dado acesso ou transação, permitindo o rastreio desse e controlando os privilégios de acesso;
- Protocolos seguros: são protocolos de comunicação, que permitem o acesso a ambientes online seguros, nos quais os dados podem ser acessados e manipulados de forma confiável;
- VPN: rede privada, cujo acesso é restrito aos usuários que possuam a permissão. Se vale de chaves específicas para permitir ou negar o acesso de usuários. (ESPIRIDIÃO, 2016; MITSHASHI, 2011)

Normalmente, a segurança da rede se baseia no estabelecimento de um *firewall*, fazendo uso de um servidor, baseado em Linux, estabelecido atrás de uma DMZ. Esse servidor, além das próprias diretivas de rede do Linux, que permitem amplo gerenciamento e grande segurança aos demais servidores, possui algumas ferramentas, como o detector de intrusão à rede e *sniffers*, que “farejam” todo o

tráfico de rede, permitindo saber as transações realizadas nessas, com sua origem e destino. Há ainda, um controle de MAC Adress e de IPs, que impede que dispositivos não autorizados tenham acesso á rede. (ESPIRIDIÃO, 2016)

4. O USO DO KALI LINUX NA SEGURANÇA DA INFORMAÇÃO

Os constantes avanços nas ameaças existentes a segurança da informação levam, também ao desenvolvimento de contramedidas igualmente avançadas. Muitas dessas são baseadas no SO Linux, em suas diversas distribuições.

4.1 LINUX

O termo Linux é comercialmente utilizado para fazer referência ao conjunto de SO (chamados de distribuição) que tem como base o Kernel Linux, criado pelo finlandês Linus Torvalds, baseado no sistema Minix. Esse, criado em 1987 por Andrew S. Tanenbaum, em Amsterdã, era um protótipo didático de sistema operacional, com baixos requerimentos de memória física e uso de disco, possuindo Kernel, gestor de memória e sistema de arquivo, em sua versão 1.0, compatíveis com o Unix, em sua versão 7. (NEGUS e BRESNAHAN, 2014)

Os primeiros usos e versões do Linux foram promovidos por entusiastas das ciências computacionais, como uma alternativa de SO de código aberto, porém, dada a capacidade de múltiplos empregos e a, praticamente, infinita, gama de modificações possíveis, rapidamente gigantes do mercado de informática, como a IBM, a Sun Microsystems, a HP e a Red Hat, se interessaram pelo Linux, desenvolvendo distribuições próprias ou produtos para uso comercial nesse SO, notadamente, na área de firewall e segurança da informação. (LEITE, 2014)

Atualmente, uma contenda entre os membros da Free Software Foundation (FSS) e diversos membros das comunidades de *softwares* de código aberto, levou a FSS a sugerir o nome GNU/Linux para designação das distribuições do Linux. (NEGUS e BRESNAHAN, 2014)

O Linux é um descendente do Unix original, sendo este criado pela AT&T Bell Laboratories, nos EUA, pelos cientistas computacionais Ken Thompson, Dennis Ritchie, Douglas McIlroy e Joe Ossana. Escrito totalmente em linguagem *Assembly*, bastante comum à época, sua primeira distribuição comercial surgiu em 1971. O código foi migrado para a mais moderna Linguagem C, por Dennis Ritchie, em 1971. (LEITE, 2014)

É interessante notar que a lei antitruste norte-americana impediu a AT&T de licenciar o UNIX, tornando assim, sua distribuição aberta. (SOUZA e GOMES, 2013)

Simultaneamente ao desenvolvimento do Linux por Linus Torvalds, Richard Stallman, pesquisador do núcleo de inteligência artificial do Massachusetts Institute of Technology (MIT), iniciou o desenvolvimento de seu projeto GNU. Assim, em 1992, o GNU estava quase completo, restando apenas a criação de um Kernel, capaz de integrar e controlar todas as parte do GNU. Esse problema foi resolvido, ainda em 1992, quando Linus tornou aberta a licença de seu recém desenvolvido Kernel. (NEGUS e BRESNAHAN, 2014)

Nascia assim o Linux, o primeiro SO completo de licença aberta distribuído desde o fechamento da licença do Unix. O nome Linux foi criado por Ari Lemmke, que deu esse nome ao diretório do FTP onde estavam os arquivos originais do código fonte do Linux. O nome original concebido por Linus Torvalds era Freax; sendo Linux a junção de Linus e Unix. (LEITE, 2014)

Há hoje dezenas de distribuições do Linux, com diversas aplicações, desde os destinados a distribuição de um SO de código aberto para o Usuário Final (normalmente, utilizando uma interface gráfica), até distribuições com finalidades específicas, como o emprego didático, o gerenciamento de bancos de dados ou desenvolvimento de *software* e *hardware*. Uma das mais bem sucedidas distribuições do Linux é o Ubuntu, cuja interface é apresentada na figura 5.

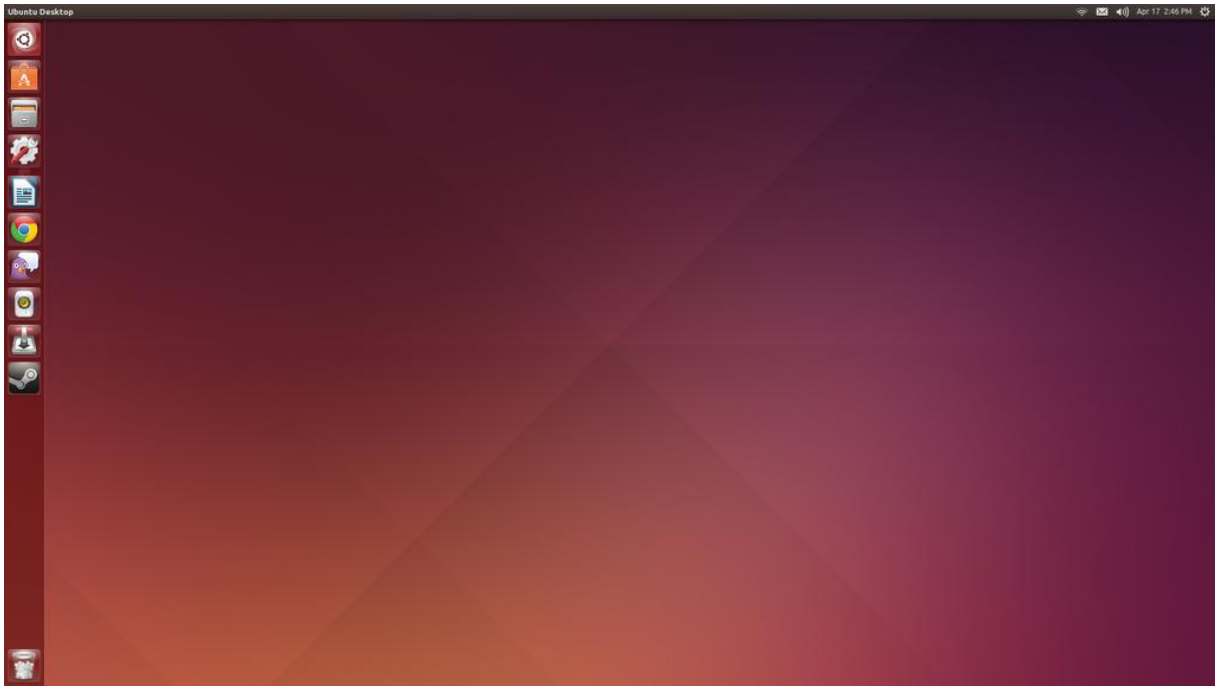

Figura 5 – Interface gráfica da distribuição Ubuntu do Linux
Fonte: Autoria Própria (2020)

Algumas dos mais importantes empregos do Linux ocorrem na área de segurança da informação, tanto no teste de segurança de *softwares*, *hardwares* e segurança de redes, quanto na construção de complexos *firewalls* e servidores de *Proxy*, capazes de neutralizar ou detectar prontamente quase todas as ameaças existentes. (ESPIRIDIÃO, 2016)

Uma das distribuições Linux mais empregadas para testes de segurança e intrusão é o Kali Linux, um SO projetado especificamente para essa função.

4.2 KALI LINUX

O Kali Linux é uma das mais avançadas e complexas distribuições Linux existentes atualmente. Destinada a funções específicas, como a auditoria de segurança e testes de intrusão, essa distribuição possui uma grande gama de ferramentas especializadas nativas. Foi desenvolvido e é mantido pela Offensive Security Ltd, possuindo distribuição "rolling-release"[7]. Sua instalação pode ocorrer por um *Live-CD* ou através de *pendrive Live-USB*. (SANTOS, 2015) A logomarca oficial do Kali Linux é apresentada na figura 6.

7Rolling-release: termo comercial para *softwares* em contínuo desenvolvimento.

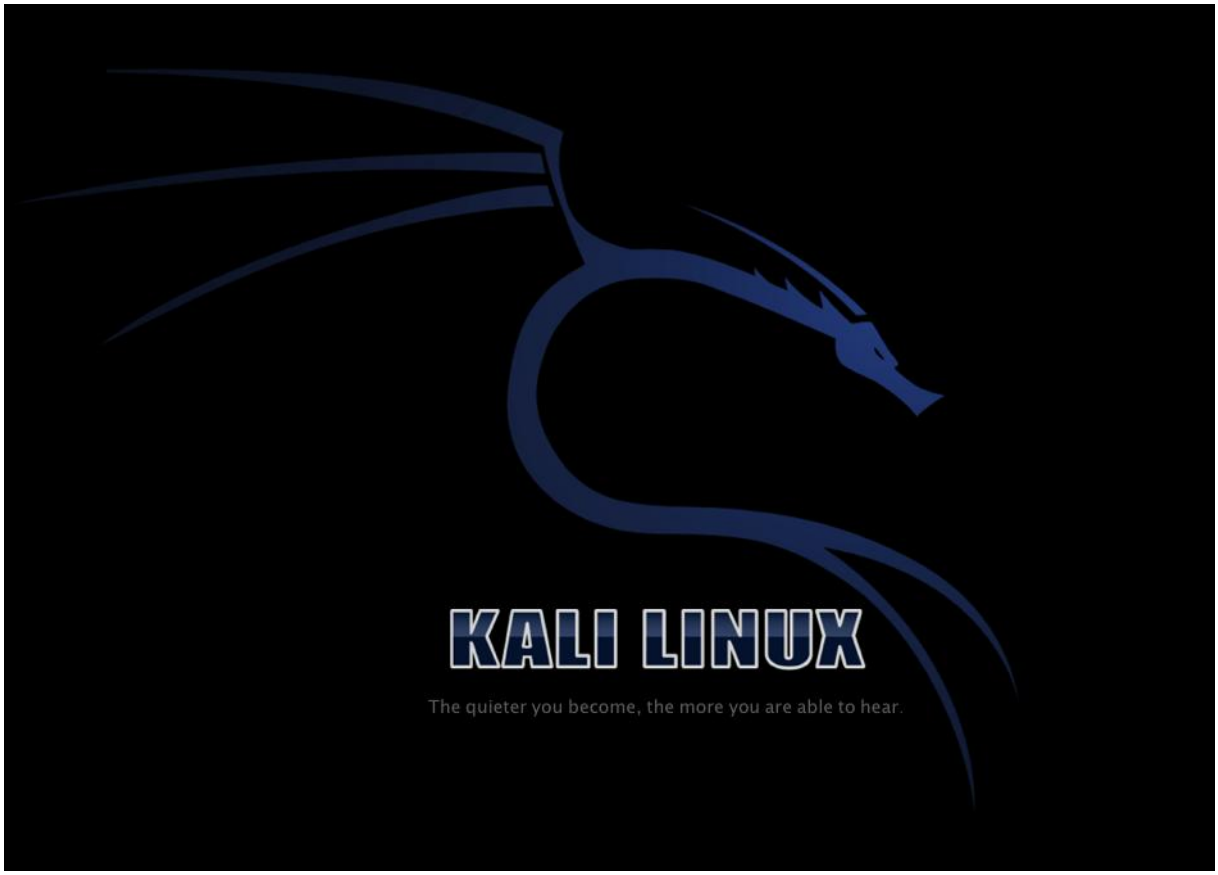

Figura 6 – Logomarca do Kali Linux
Fonte: (BENESCIUTT e MARTIMIANO, 2018)

Entre as ferramentas mais comuns estão o Whireshark, um analisador de tráfego de rede (*sniffer*), com interface gráfica, e grande número de informações disponível; o Nmap, um *port scan* que permite a criação e monitoração de mapas precisos de uma rede ou computador, indicando portas abertas e serviços que as utilizem; John the Ripper, um *software* de quebra de senhas, através de *force attack* (ataque de força bruta) e o Aircrak-ng, um completo *software* para uso em redes *Wi-Fi* no padrão 802.11, que utiliza uma placa *wireless* com um *driver* de modo de monitoramento bruto para detecção de redes, quebra de senhas WEP, e *sniffer* de pacote e análise de tráfego em redes *Wi-Fi*. (ASSUNÇÃO, 2014; BENESCIUTT e MARTIMIANO, 2018) O Kali Linux possui uma interface gráfica, além do modo console, para otimizar seu emprego. Essa interface é apresentada na figura 7.

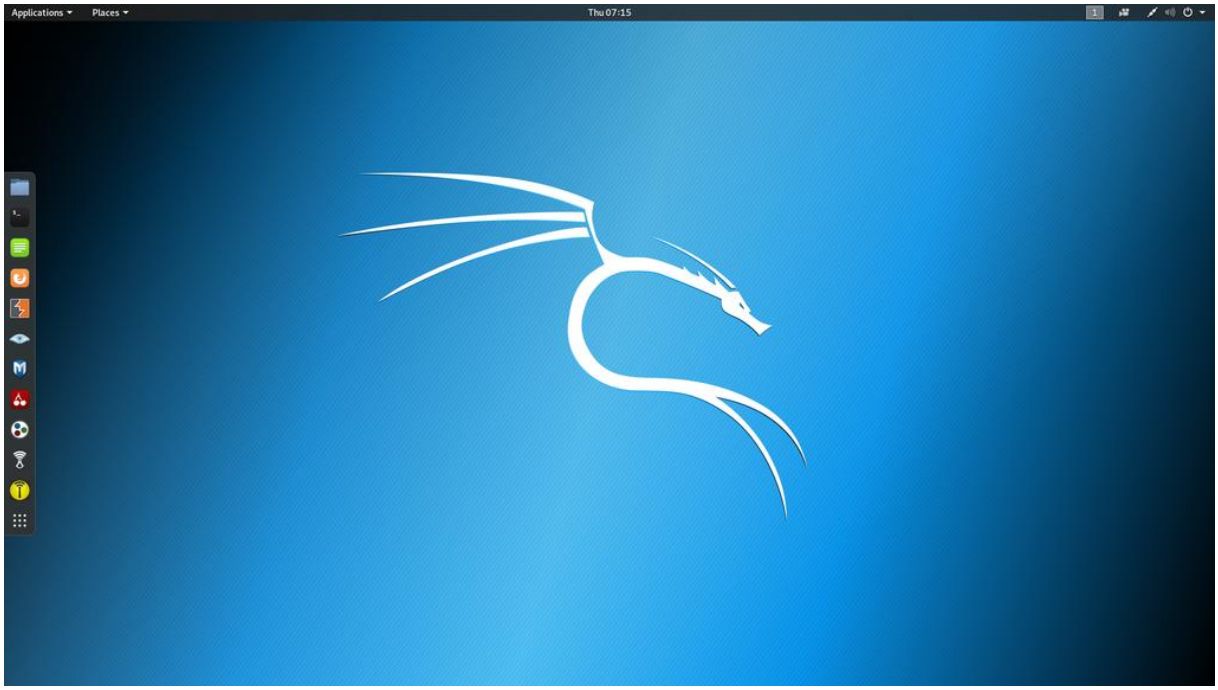

Figura 7 – Interface gráfica do Kali Linux
Fonte: Autoria Própria (2020)

Derivado da distribuição Back Track Linux, que possuía empregos semelhantes, porém com menos funcionalidades, o Kali Linux tornou-se o SO mais empregado para testes de segurança da informação, sendo suas ferramentas responsáveis pela descoberta de diversas vulnerabilidades importantes, em sites, *softwares* e *hardwares*, protegendo assim, os dados de empresas e pessoas ao redor do mundo.

4.3. RECURSOS TÉCNICOS EMPREGADOS NO KALI LINUX

O Kali Linux permite, apenas com suas ferramentas nativas, a realização de mais de 300 testes, entre *pentests*, testes de intrusão, de vulnerabilidade de senhas e outros. (SANTOS, 2018)

As ferramentas de teste do Kali Linux podem ser agrupadas, conforme sua função, conforme é apresentado no quadro 1.

Função	Descrição
Coleta de informações e análise de vulnerabilidade (Information Gathering and Vulnerability Analysis	Procura por *backdoors* e outras vulnerabilidades em *softwares*, que possam servir de prota de entrada para invasores, ou ser exploradas internamente por *softwares* de código malicioso
Aplicações *web*	Destina-se a localizar falhas e brechas exploráveis por invasores e amaeças em aplicações rodando *web*
Violação de Senhas (*Password Attack*)	Também chamadas de análise de senhas ou análise de vulnerabilidade de senhas, destinam-se a testas a resistência de senhas da rede e logins diversos contra ataques de força bruta ou por dicionário de senhas
Engenharia Reversa (Reverse Engineering)	Detecta, através do processo de engenharia reversa (a descontrução, até a separação total dos elementos componentes de um *hardware* ou *software*), em busca de vulnerabilidades
Wireless Attack	Sua função é detectar vulnerabilidades em redes WiFi e de sensores sem fio
Network Sniffer and IP Spoofing	Dedicam-se a analisar o tráfego de dados pela rede em busca de vulnerabiidade, bem como detectar e mapear os endereços IPs que estão conectados a esta
Relatórios	Produzem relatórios, para facilitar a análise dos dados gerados em outras ferramentas
Forense	Aplicações dedicas, utilizadas por peritos para elucidar crimes cibernéticos ou que utilizem recursos computacionais (como redes sociais) para sua realização

Quadro 1 – Tipos de ferramentas disponíveis no Kali Linux
Fonte: Autoria Própria (2020)

A análise do quadro 1 mostra a grande versatilidade de aplicações para o Kali Linux, uma vez que suas ferramentas permitem a realização de testes em qualquer área de segurança da informação.

Nas últimas décadas, tem tido destaque a área das aplicações forenses, uma vez que, além do aumento dos crimes cibernéticos, como o seqüestro de informações e roubo de dados bancários; a quantidade de crimes que envolvem o uso de meios computacionais em seu planejamento ou coordenação da execução aumenta cada vez mais, como é possível verificar nas constantes trocas de mensagens entre traficantes e quadrilhas especializadas em tipos específicos de roubos. (BENESCIUTT e MARTIMIANO, 2018)

4.3.1 John the Ripper

Ao analisar o *software* John the Ripper (JTR), a primeira consideração é feita sobre seu nome, que além de criativo, foi premiado em diversos eventos de *software* e de *marketing* ao redor do mundo. (ASSUNÇÃO, 2014) Também a logomarca do JTR foi premiada. Tal logomarca é apresentada na figura 8.

Figura 8 – Logomarca do John the Ripper
Fonte: Under Linux (2013)

O JTR destina-se a análise de senhas (*password cracking*), possuindo funções baseada em ataque de força bruta e em dicionários de senhas. Essa

ferramenta atua em ataques online e *offline*, possuindo versões gratuitas e pagas (JTR Pro). (BENESCIUTT e MARTIMIANO, 2018)

É considerada a mais versátil ferramenta de análise de senhas disponível para o Kali Linux. (SANTOS, 2015) A figura 9 mostra a tela de ajuda para as opções de quebra de senha presentes no JTR.

Figura 9 – Tela de ajuda para as opções de quebra de senha do JTR
Fonte: Autoria Própria (2020)

O JTR possui uma grande variedade de funções e modos operacionais, sendo os principais:

- Dicionário (*Wordlist*): Utiliza um banco de dados de palavras, verificando sua correspondência com a senha alvo ou partes dessa. É o modo de operação mais simples do JTR.

- Quebra Simples (*Single Crack*): Possui velocidade de processamento de informações mais rápida do que o modo Dicionário, utilizando dados do usuário, obtidos através de *mangling*, além de informações como o nome do usuário e do diretório desse, para obter possíveis combinações que levem a quebra da senha.
- Incremental: testa a senha caractere a caractere, aceitando parâmetros imputados pelo operador para agilizar o tempo de quebra. É o método mais robusto e com maior índice de eficiência do JTR.
- Externo (External): Considerado o método mais complexo de operação do JTR. Utiliza regras pré-programadas, salvas em um arquivo interno do JTR, que são utilizadas como parâmetros de teste para a quebra das senhas. Permite o uso de diversos arquivos, aumentando as regras de teste possíveis e sua eficiência. (SANTOS, 2018)

4.3.2 Nmap

Desenvolvido por Gordon Lyon, que utiliza o pseudônimo Fyodor, em suas ações como *Hacker* e *Pentester*, o Nmap é o *port scan* mais empregado na segurança da informação, possuindo uma *Console User Interface* (CUI – Interface de usuário em console) que pode ser substituída por uma *Graphical User Interface* (GUI – interface gráfica de usuário), que simplifica sua operação, tornando mais lógicos os comandos necessários ao monitoramento de portas em um computador ou rede. Escrito em C++, o Nmap surgiu em 1997, com seu código publicado por Fyodor na revista Phrack. (ASSUNÇÃO, 2014)

A interface mais comum para o Nmap é o console, apresentado na figura 10

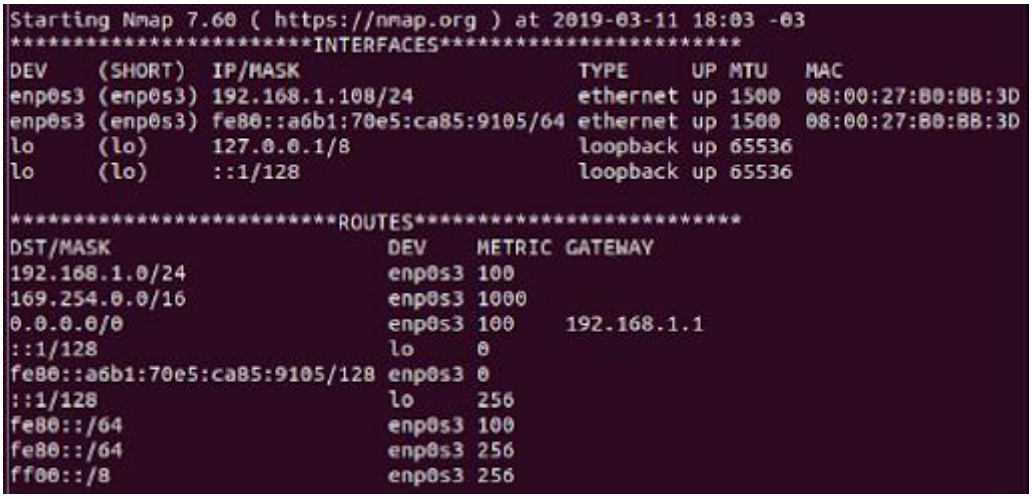

Figura 10 – Interface console do Nmap
Fonte: Autoria Própria (2019)

Há, contudo, interfaces gráficas, que simplificam o uso do Nmap. A mais comum delas é o ZeNmap, mostrado na figura 11.

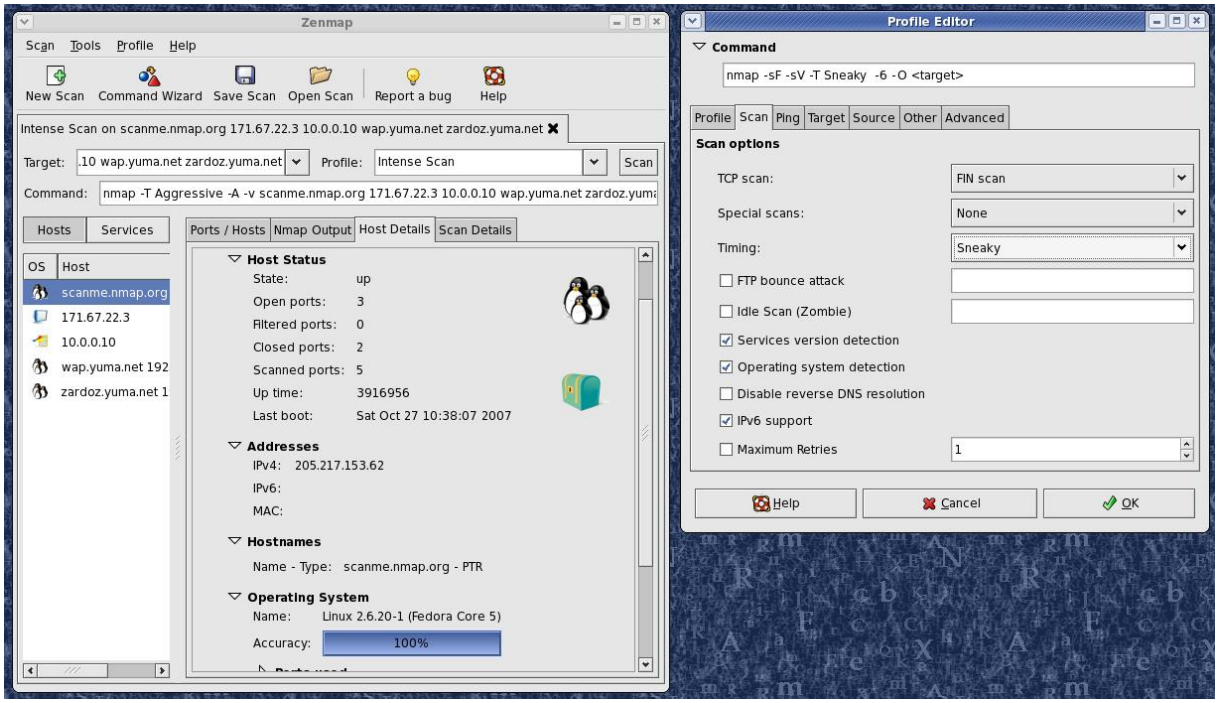

Figura 11 – Interface gráfica ZeNmap para o Nmap
Fonte: Autoria Própria (2020)

Os principais recursos do Nmap são:

- Descoberta de Hosts: detecta Hosts conectados a rede na qual o *scan* é executado, através de *ping* ou varredura de portas.

- Scanner de Portas: função mais popular do Nmap; permite a detecção de portas abertas na rede, indicando quais serviços ou aplicações fazem uso delas.
- Detecção de Versão: interroga serviços de rede, obtendo seu número de versão e aplicação vinculada.
- Detecção de SO: interroga o *Host*, detectando seu SO e versão.
- Interação *Script*/Alvo: utiliza componentes específicos para detectar o comportamento de determinado *script* em um alvo (*Host,* SO, serviço ou aplicação) na rede.

O Nmap e o JTR são duas das mais conhecidas e utilizadas ferramentas do Kali Linux, tendo, em dezenas de casos, sua eficiência comprovada, detectando vulnerabilidades e garantindo a segurança de redes e sistemas nos quais foram executados.

5. CONSIDERAÇÕES FINAIS

A constante evolução da tecnologia computacional molda a sociedade humana, transformando suas relações sociais, de produção, a forma como utiliza serviços e executa tarefas cotidianas.

Contudo, a forma como crimes e outras ameaças ocorrem também acompanha tal evolução tecnológica, levando a constante necessidade de evolução nas contramedidas de segurança, bem como na tecnologia envolvida nestas, a fim de que essa esteja constantemente atualizada com as novas ameaças.

Nesse cenário, a distribuição Kali do Linux surge como uma ferramenta extremamente versátil, permitindo a detecção de falhas na segurança de uma rede, além da mensuração das reais dimensões dessas e do planejamento e execução de suas correções.

Com o uso de suas ferramentas, como o JTR e o Nmap, o Kali Linux é uma completa suíte de detecção de vulnerabilidades e ameaças, permitindo aos especialistas em Segurança da Informação a simulação de cenários diversos, garantindo assim a segurança dos dados ante qualquer ameaça do mundo cibernético.

REFERÊNCIAS

ALVES, W. P. **C++ Builder**. Rio Claro: Erica, 2015.

ASSUNÇÃO, M. F. A. **Análise de eficiência na detecção de vulnerabilidade em ambientes web com o uso de ferramentas open source**. Belo Horizonte: FUMEC, 2014.

BENESCIUTT, M. Y.; MARTIMIANO, L. A. F. **Uso de teste de invasão para avaliar a segurança dos serviços Web da Universidade Estadual de Maringá**. 27º Encontro Anual de Iniciação Científitifca. Maringá: UEM. 2018.

BROWN, B. R. **The Apollo Chronicles:** Engineering America's First Moon Missions. Los Angeles - EUA: Oxford University Press, 2019.

CARMONA, T. **Administração de Redes**. São Paulo: Linux New Media, 2007.

CERQUEIRA, D. A. **A evolução da Informática:** desde os séculos passados até os dias de hoje. Sorocaba: ETE "Rubens de Faria e Souza", 2004.

ESPIRIDIÃO, H. **Introdução a Segurança em redes**. São Paulo: USP, 2016.

FACHIN, O. **Fundamentos de metodologia**. 4ª Edição. ed. São Paulo: Saraiva, 2003.

FERREIRA, C. **Breve História da Internet**. Porto: Universidade do Porto, 2017.

FREITAS, A. E. **Redes Wireless, Wifi:** WLANs. Belo Horizonte: UFMG, 2017.

GERHARDT, T. E.; SILVEIRA, D. T. **Métodos de pesquisa**. Porto Alegre: UFRGS, 2009.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 8ª Edição. ed. São Paulo: Atlas, 2012.

GONÇALVES, L. G. C. **A Revolução em Assuntos Militares no Contexto da Guerra de Secessão Americana (1861-1865)**. Franca: UNESP, 2015.

HUNECKE, M. **Windows Server**. Ribeirão Preto: Madras, 2015.

LEITE, G. F. **Introdução ao LINUX**. Rio de Janeiro: UFRJ, 2014.

LIBERTY, J.; JONES, B. **Teach Yourself C++ in 21 days**. 5ª Edição. ed. Indianapolis - EUA: Sams Publishing, 2005.

LOUREIRO, A. A. F. et al. **Redes de Sensores Sem Fio**. Belo Horizonte: UFMG, 2017.

MARCONI, M.; LAKATOS, E. M. **Técnicas de Pesquisa**. 6ª Edição. ed. São Paulo: Atlas, 2012.

MENEZES, A. F. et al. **Linux:** Administração de Redes. São Paulo: USP, 2018.

MITSHASHI, R. A. **Segurança de Redes**. São Paulo: USP, 2011.

MORIMOTO, C. E. **Servidores Linux, guia prático guia prático**. 3ª Edição. ed. Porto ALegre: Sul Editores, 2017.

NEGUS, C.; BRESNAHAN, C. **Linux:** A Bíblia. 8ª Edição. ed. Rio de Janeiro: Alta Books, 2014.

NEVES, W. A. **E no príncipio, era o macaco:** estudos avançados em antropologia. São Paulo: [s.n.], 2002.

NOGUEIRA, M. L. M. **Guia prático de redes Windows para novos administradores de rede**. Limeira: CESET - UNICAMP, 2013.

OLIVEIRA, L. A. H. G.; ROCHA, K. K. F.; BITTENCOURT, V. G. **Introdução à Informática:** Histórico e Evolução. Natal: UFRN, 2004.

SANTOS, A. A. **Análise de vulnerabilidade em rede, com teste de intrusão, utilizando a distribuição Kali Linux**. Petrolina: IF Sertão PE, 2015.

SANTOS, R. E. C. **Laboratório virtual para pentest na análise de vulnerabilidade**. Brasília: UNICEUB, 2018.

SOUZA, J.; GOMES, L. **Apostila de Linux**. São Carlos: UFSCAR, 2013.

UNDER LINUX. Disponível John the Ripper 1.8.0. **Under Linux**, 2013. Disponivel em: <https://under-linux.org/content.php?r=6697>. Acesso em: 03 fev 2020.

VERGARA, S. C. **Projetos e relatórios de pesquisa em administração**. São Paulo: Atlas, 2000.

WHITE, R. **Como funciona o computador**. 11ª Edição. ed. São Paulo: PC Computing, 2018.

YIN, R. K. **Estudo de caso:** planejamento e métodos. 3ª Ed. ed. Porto Alegre: Bookman, 200