ANÁLISE DO USO E DO CONTEÚDO DA DISTRIBUIÇÃO KALI LINUX

Fernando Souza Rodrigues[1], Paulo Ferreira da Silva Júnior[1]

[1]Departamento de Ciência da Computação – Universidade Federal de Roraima (UFRR)
Av. Capitão Ene Garcez, 2413 - Bairro Aeroporto, Boa Vista - Roraima, RR.

fernando.rodrigues@ufrr.br, juniorrkcm@outlook.com

Abstract. *Kali Linux is a security-focused operating system that provides tools for penetration testing, forensic analysis, and security auditing [Hertzog et al, 2017]. It is widely used by companies and institutions to identify and remediate vulnerabilities. Kali Linux offers different versions and spin-offs, allowing for customization based on specific needs. It is a valuable tool for security professionals and ethical hackers due to its wide range of features and flexibility [Schultz e Perciaccante 2017].*

Resumo. *O Kali Linux é um sistema operacional focado em segurança da informação, oferecendo ferramentas de testes de penetração, análise forense e auditoria de segurança [Hertzog et al, 2017]. É amplamente utilizado por empresas e instituições para identificar e corrigir vulnerabilidades. Possui diferentes versões e spin-offs, permitindo personalização conforme necessidades específicas. O Kali Linux é uma ferramenta valiosa para profissionais de segurança e hackers éticos, devido à sua variedade de recursos e flexibilidade [Schultz e Perciaccante 2017].*

1. Introdução

A análise do uso e do conteúdo da distribuição Kali Linux é um estudo que examina minuciosamente todas as especificações possíveis dessa ferramenta, bem como seus softwares e suas devidas aplicabilidades. Essa distribuição, baseada no Debian, é amplamente empregada por profissionais de segurança cibernética e hackers éticos devido às suas ferramentas especializadas. A análise aborda o uso prático do Kali Linux e investiga o conteúdo das suas ferramentas e recursos, visando a identificação e correção de vulnerabilidades em sistemas e redes.

2. Trabalhos Relacionados

Durante os esforços de pesquisa foram identificados poucos trabalhos relacionados à distribuição Kali Linux, dentre os quais foi selecionado o trabalho de Hertzog [Hertzog et al, 2017]. Neste livro os autores apresentam o Kali como um sistema operacional multifuncional, mas projetado principalmente para auxílio em teste de penetração. A abordagem apresentada pelos autores tem o intuito de ajudar os usuários iniciantes do Linux, mas também usuários de longa data que desejam formalizar seu conhecimento apresentando temas que vão desde o Debian GNU/Linux até conceitos de avaliação de segurança.

Outro trabalho usado neste artigo foi o de Schultz e Perciaccante [Schultz e Perciaccante 2017] onde o foco dos autores é fornecer um conjunto mais aprofundado de receitas para aproveitar as ferramentas presentes no. Para isso, os autores abordam

aspectos do teste de penetração, juntamente com iniciativas sobre o uso da plataforma Kali Linux. A abordagem mais prática contida neste livro nos ajudará a entender alguns softwares contidos no referido S.O.

3. Kali Linux

A distribuição Kali Linux é o sucessor do sistema operacional BackTrack lançado em 2006, baseado no Debian e tinha foco em testes de segurança e testes de penetração [Hertzog et al, 2017]. Ele se destina, como o próprio site descreve, a testes avançados de penetração e auditoria de segurança [KALI 2022]. Mati Aharoni e Devo Kearns desenvolveram o Kali Linux que é mantido pela Offensive Security Ltd.

3.1 Breve Histórico do Kali

O projeto Kali Linux foi baseado no KNOPPIX, uma distribuição GNU/Linux baseado no Debian projetada para rodar diretamente em um CD/DVD, pendrive, e foi originalmente chamado Whoppix, que significa WhiteHat Knoppix. Whoppix tinha lançado de v2.0 para v2.7[Saive 2023].

Whoppix deu lugar ao WHAX, abreviação de WhiteHat Slax. A mudança de nome foi informada pela mudança no sistema operacional base de Knoppix para Slax, uma outra distribuição Linux baseada no Debian. WHAX começou na v3 e pegou de onde Whoppix parou[Saive 2023].

Na mesma época, o Auditor Security Collection, ou simplesmente Auditor, era um sistema operacional baseado em Linux com uma coleção de ferramentas baseadas em Linux que são muito úteis para auditar um sistema. Com esforços conjuntos entre Auditor, Knoppix e WHAX, nasceu o BackTrack. Foi baseado no Slackware, uma distro Linux muito utilizada para servidores de hospedagem web e FTP, de v1 para v3 e mais tarde mudou para o Ubuntu com v4 para v5[Saive 2023].

Kali Linux foi lançado oficialmente em 2013, substituindo o BackTrack. Ele começou a usar Debian estável antes de fazer a transição para o teste Debian quando Kali se tornou um sistema operacional contínuo[Saive 2023].

Aqui está um quadro completo da linha do tempo:

Tabela 1. Histórico de versões lançadas do Kali [Saive 2023]

Data	**Projeto Lançado**	**SO Base**
30th August 2004	Whoppix v2	Knoppix
17th July 2005	WHAX v3	Slax
26th May 2006	BackTrack v1	Slackware Live CD 10.2.0
06th March 2007	BackTrack v2	Slackware Live CD 11.0.0

19th June 2008	BackTrack v3	Slackware Live CD 12.0.0
9th Jan 2010	BackTrack v4 (Pwnsauce)	Ubuntu 8.10 (Intrepid Ibex)
10th May 2011	BackTrack v5 (Revolution)	Ubuntu 10.04 (Lucid Lynx)
13th March 2013	Kali Linux v1 (Moto)	Debian 7 (Wheezy)
11th August 2015	Kali Linux v2 (Sana)	Debian 8 (Jessie)
16th Jan 2016	Kali Linux Rolling	Debian Testing

3.2 Ambiente Gráfico

O ambiente gráfico padrão do Kali Linux é o GNOME. O Kali é uma distribuição Linux voltada para testes de segurança e auditoria de sistemas, e o ambiente GNOME é amplamente utilizado em várias distribuições Linux devido à sua interface amigável e recursos poderosos. No entanto, é importante mencionar que os ambientes gráficos podem ser facilmente alterados no Linux, incluindo o Kali Linux. Se você preferir usar outro ambiente gráfico, como KDE, LXDE, MATE ou qualquer outro, você pode instalá-lo e configurá-lo no Kali Linux de acordo com suas preferências.

Vantagens e facilidades do ambiente gráfico:

- Interface amigável: O GNOME é conhecido por sua interface limpa e intuitiva, o que torna a navegação e o uso do sistema mais fácil, especialmente para usuários iniciantes.
- Produtividade: O GNOME possui recursos e funcionalidades que visam melhorar a produtividade do usuário. Ele oferece uma organização eficiente de janelas, permitindo alternar entre aplicativos de forma rápida e fácil. Além disso, possui recursos de pesquisa rápida e acesso direto a aplicativos frequentemente utilizados, tornando o trabalho mais eficiente.
- Personalização: O GNOME permite personalizar a aparência e o comportamento do ambiente de acordo com as preferências individuais. É possível alterar temas, ícones, papéis de parede e ajustar as configurações de acordo com as necessidades do usuário.
- Acessibilidade: O GNOME tem um forte foco em acessibilidade, tornando-o adequado para usuários com necessidades especiais. Ele oferece recursos como suporte a leitores de tela, redimensionamento de fontes, ajuste de contraste e opções de teclado acessíveis, garantindo que pessoas com diferentes habilidades possam utilizar o sistema.
- Integração com aplicativos: O GNOME possui uma integração sólida com aplicativos populares, facilitando a execução de tarefas comuns. Ele se integra bem com suítes de escritório, navegadores da web, clientes de email e outros aplicativos amplamente utilizados.

Além disso o Kali disponibiliza outras formas de personalização da interface gráfica como, por exemplo:

- Wallpapers: O Kali Linux geralmente inclui uma variedade de wallpapers, que podem variar entre imagens relacionadas à segurança, arte abstrata ou fotografias. Esses wallpapers são fornecidos pela equipe do Kali Linux e podem ser encontrados nas configurações de aparência do sistema.
- Ícones: Os ícones padrão do Kali Linux são geralmente derivados do conjunto de ícones do GNOME. Isso inclui ícones para aplicativos, pastas, dispositivos e outros elementos do sistema. No entanto, é possível personalizar os ícones no Kali Linux, seja alterando-os individualmente ou instalando pacotes de ícones de terceiros.
- Esquemas de cores: O Kali Linux normalmente adota um esquema de cores escuro e contrastante para fornecer uma aparência adequada ao foco em segurança. Esses esquemas de cores são aplicados aos elementos da interface do usuário, como barras de título, botões e menus. Novamente, é possível personalizar os esquemas de cores no Kali Linux por meio das configurações do sistema ou usando temas personalizados.

3.3 Vantagens e facilidades

A seguir apresentamos algumas vantagens e facilidades verificadas na distribuição Kali Linux, como:

1. Ferramentas pré-instaladas - O Kali Linux vem com uma ampla gama de ferramentas de segurança pré-instaladas, como scanners de vulnerabilidades (Nikto, Burp Suite, SQLMap, etc.[ACERVO LIMA 2022]), frameworks de testes de penetração (BeEF, Lynis, Aircrack-ng, etc.[Ribeiro 2022]), ferramentas de análise forense (Binwalk, Bulk Extrator, etc.[ACERVO LIMA 2022]), ferramentas de recuperação de dados (Foremost[Santos 2018]), etc.
2. Documentação abrangente - O Kali Linux oferece documentação detalhada e abrangente, incluindo manuais, tutoriais e uma base de conhecimento online disponível em kali.org/docs.
3. Comunidade ativa - Através de fóruns (forums.kali.org/), blogs (kali.org), grupos de discussão (discord.kali.org/) e outras plataformas, os usuários, tanto especialistas em segurança e desenvolvedores, podem obter suporte, compartilhar conhecimento, colaborar em projetos e ficar atualizados sobre as últimas tendências em segurança da informação.
4. Portabilidade - O Kali Linux é uma distribuição baseada em Debian e, portanto, possui suporte para uma ampla gama de hardware e arquiteturas. Ele pode ser instalado em computadores pessoais[Gonzalez 2022], laptops[Tomas 2018], servidores[Brown 2022] e até mesmo em dispositivos embarcados[Klimaszewski 2023], permitindo que os usuários realizem testes de segurança em diferentes ambientes.

3.4 Softwares presentes na distribuição

O kali Linux apresenta uma grande variedade de softwares, tornando inviável a descrição de cada um neste relatório. Assim apresentamos apenas os principais presentes na distro, tais como:

- **Nmap:** Uma poderosa ferramenta de mapeamento de rede usada para descobrir hosts e serviços na rede, verificar portas abertas e realizar varreduras de segurança [KALI 2022].
- **Wireshark:** Uma ferramenta de análise de tráfego de rede que permite capturar e analisar pacotes de dados em tempo real. É usado para diagnosticar problemas de rede e realizar análises forenses de tráfego [KALI 2022].
- **Metasploit Framework:** Uma plataforma de teste de penetração que permite a identificação de vulnerabilidades e a execução de ataques controlados para testar a segurança dos sistemas [KALI 2022].
- **Burp Suite:** Uma plataforma de testes de segurança de aplicativos web que oferece recursos como análise de vulnerabilidades, exploração de falhas, interceptação de tráfego e injeção de payloads [KALI 2022].
- **Maltego:** Uma ferramenta de análise de inteligência que permite coletar, analisar e visualizar informações sobre alvos específicos para auxiliar em investigações de segurança [KALI 2022].
- **Hydra:** Uma ferramenta de força bruta que permite realizar ataques de login automatizados, testando combinações de nomes de usuário e senhas em diversos serviços [KALI 2022].

3.5 Gerenciador de Pacotes

O gerenciador de pacotes padrão do Kali é o APT (Advanced Package Tool) que facilita a instalação, atualização, remoção e gerenciamento de pacotes de software [Kumar 2022]. Além do APT, o Kali Linux também suporta o uso de outros gerenciadores de pacotes, como o dpkg (que é a ferramenta de baixo nível subjacente ao APT) e o aptitude[Adams 2022]. Os tipos de pacotes padrão aceitos pelo APT são .deb, extensão padrão dos sistemas derivados do Debian [Andrade 2021].

3.6 Lista Usuários

Red Teams de empresas, equipes que simulam ataques contra uma empresa, utilizam o Kali para realizar testes de penetração, como, por exemplo, Rapid7[RAPID7 (2022)]. Além disso, este sistema operacional é muito utilizado por administradores de segurança e hackers Black Hat. Um é responsável por detectar e prevenir violações de segurança, enquanto o outro é responsável por identificar e talvez explorar violações de segurança[JAVATPOINT 2021].

3.7 Kernel linux do Kali

A versão de kernel Linux utilizada é a 6.1[Rudra 2023], a primeira a ter suporte inicial à linguagem Rust no Kernel principal para melhor segurança[Arindam 2022]. Uma das principais características é a ativação do Intel Meteor Lake que oferece suporte inicial

para os próximos chips Meteor Lake, suporte inicial para placas de vídeo AMD RDNA 3, otimizações para PCs AMD, além de suporte aprimorado a SoC ARM[Rudra 2022].

3.8 Documentação

A documentação oficial da distro Kali Linux pode ser encontrada em seu próprio site que detém uma ampla documentação sobre o sistema operacional, indo desde a instalação do S.O. até a recompilação do kernel.

3.9 Segurança da Distribuição Linux

Em termos de segurança técnica, o Kali Linux possui várias medidas para fornecer uma plataforma segura para testes de segurança. Algumas características incluem:

- Ferramentas de segurança: O Kali Linux é embalado com uma ampla variedade de ferramentas de segurança e testes de penetração. Essas ferramentas são projetadas para identificar vulnerabilidades e testar a segurança de sistemas e redes, ajudando a identificar e corrigir possíveis pontos fracos.
- Atualizações de segurança: A equipe por trás do Kali Linux fornece atualizações de segurança regulares para garantir que as vulnerabilidades conhecidas sejam corrigidas e que o sistema esteja protegido contra ameaças conhecidas.
- Comunidade ativa: O Kali Linux possui uma comunidade de usuários e desenvolvedores ativos, o que permite a rápida detecção e correção de problemas de segurança. Além disso, a comunidade também fornece suporte e compartilha conhecimento relacionado à segurança cibernética.

3.10 Hardware Mínimo e GPU

A configuração de hardware mínima recomendada para a instalação e uso do Kali Linux pode variar dependendo da versão específica e dos recursos que serão utilizados. As especificações mínimas gerais que comumente são recomendadas [KALI 2022]:

1. Processador: Processador de 1 GHz ou mais rápido.
2. Memória RAM: 2 GB de RAM ou mais. Recomenda-se 4 GB ou mais para um desempenho mais suave.
3. Espaço em disco: 20 GB de espaço livre no disco rígido.
4. Placa de vídeo: Placa de vídeo compatível com resolução de 1024x768 ou superior.
5. Conectividade: Placa de rede compatível com Ethernet para acesso à internet.
6. Porta USB: Pelo menos uma porta USB para instalação e uso de dispositivos externos, como pendrives de inicialização ou adaptadores de rede.

O Kali Linux é compatível com uma ampla variedade de placas de GPU, pois é baseado no kernel Linux e possui suporte para uma extensa lista de drivers gráficos. Isso inclui tanto placas de GPU da NVIDIA quanto da AMD, além de outras placas gráficas compatíveis com os drivers de código aberto disponíveis no kernel Linux [KALI 2022].

3.11 TPM2, SecureBoot e descriptografia de armazenamento automatizado

Kali Linux tem suporte para o TPM 2.0 (Trusted Platform Module 2.0) que é um processador de criptografia instalado nas placas-mãe que oferece segurança durante a inicialização do sistema operacional [Zaino 2021]. Também oferece suporte ao Secure Boot pois o Kali é assinado, ou seja, possui assinatura criptografada que assegura a origem do fornecedor, para seguir com o boot sem problemas[OFFSEC 2016].

Kali Linux, por padrão, não possui uma funcionalidade de descriptografia de armazenamento automatizado. O Kali Linux é uma distribuição voltada para segurança e testes de penetração, e muitas vezes é utilizado em ambientes em que a criptografia de armazenamento é altamente recomendada ou obrigatória. Portanto, a criptografia é geralmente mantida ativa para garantir a segurança dos dados, exigindo que o usuário insira uma senha ou chave de criptografia durante o processo de inicialização para desbloquear o armazenamento e acessar o sistema.

No entanto, é possível configurar manualmente uma solução de descriptografia de armazenamento automatizado no Kali Linux, utilizando ferramentas e técnicas específicas. Por exemplo, é possível configurar o uso do LUKS (Linux Unified Key Setup) ou outras ferramentas de criptografia para permitir a descriptografia automática durante o processo de inicialização.

3.12 Daemons Padrões

Por ser baseado no Debian muitas das daemons padrões do dela são incluídas por padrão no Kali Linux. Alguns exemplos de daemons comuns que são normalmente encontrados no Kali Linux:

- **Apache2 (httpd):** O servidor web hospedar e servir páginas web. Ele permite executar aplicativos e serviços web no sistema Kali [KALI 2022].
- **Openssh (sshd):** O daemon SSH permite que os usuários se conectem remotamente ao sistema usando o protocolo SSH (Secure Shell) [KALI 2022].
- **cron:** O daemon cron é responsável pela execução de tarefas agendadas em horários específicos. Ele permite agendar a execução automática de scripts, comandos ou programas em momentos pré-determinados [KALI 2022].

É possível visualizar os daemons em execução no sistema usando comandos como “systemctl list-units --type=service” ou “service --status-all”.

3.13 Interpretador de Comandos

O interpretador de comandos padrão (shell) do Kali Linux é o Bash (Bourne Again SHell). O Bash é uma variante avançada do shell Bourne original e é amplamente utilizado em sistemas Linux e Unix. Ele fornece uma interface de linha de comando interativa, onde os usuários podem digitar comandos e interagir com o sistema operacional [KALI 2022].

3.14 Edições e Spin-Offs

O Kali Linux possui algumas edições e spin-offs desenvolvidos por terceiros, que adaptam o sistema operacional para atender a necessidades específicas. Aqui estão algumas das edições e spin-offs conhecidos do Kali Linux:

1. **Kali Linux Light:** Uma versão mais leve do Kali Linux que apresenta uma interface de usuário mínima e um conjunto reduzido de pacotes. É projetado para sistemas com recursos limitados ou para aqueles que desejam uma distribuição mais enxuta[Logan 2023].
2. **Kali Linux VMware:** Uma versão do Kali Linux otimizada para uso em máquinas virtuais VMware. É fornecido como uma imagem pronta para uso com

configurações e drivers adequados para ambientes de virtualização VMware[Palmer 2021].

3. **Parrot Security:** é uma distribuição de Linux baseada no Debian, projetada para testes de segurança, análise forense digital, privacidade e anonimato online. Ele possui uma interface amigável, uma ampla variedade de ferramentas de segurança pré-instaladas e suporte a recursos avançados, como navegação segura na rede Tor e VPNs. É uma escolha popular entre profissionais de segurança cibernética e entusiastas, oferecendo atualizações frequentes e suporte ativo da comunidade [PARROTSEC 2023].
4. **BackBox:** é uma distribuição de Linux baseada no Ubuntu, focada em segurança cibernética e testes de penetração. Possui uma ampla gama de ferramentas de segurança pré-instaladas, uma interface amigável e é usado por profissionais da área para avaliar e proteger sistemas e redes. É uma opção confiável e estável, com suporte da comunidade e atualizações regulares [BACKBOX 2022].

3.15 Repositório e Instalação

Disponibilizamos um repositório no GitHub com o material para ajudar na instalação do distrito Kali Linux, assim como uma apresentação que resume alguns pontos até aqui apresentados. Ele está acessível a qualquer pessoa através do link <https://github.com/juniorrkcm/Paulo-Fernando_dist_os_rr_2023>.

4. Resultados

A distribuição Kali Linux oferece várias interfaces gráficas, incluindo o ambiente de desktop GNOME e o Xfce. A escolha da interface gráfica depende das preferências do usuário e dos requisitos de hardware. O ambiente de desktop GNOME oferece uma experiência mais rica em recursos, enquanto o Xfce é mais leve e consome menos recursos do sistema.

O kernel do Linux é o coração do sistema operacional e fornece a interface entre o hardware e o software. O Kali Linux usa o kernel Linux padrão, que é atualizado regularmente para garantir a estabilidade, segurança e compatibilidade com o hardware mais recente.

O Kali Linux também oferece um console de linha de comando, que é amplamente utilizado por profissionais de segurança cibernética e testadores de penetração. Através do console, é possível executar comandos e utilizar ferramentas específicas para análise de segurança e testes de penetração.

Em relação ao uso de memória RAM e memória de armazenamento, o Kali Linux tem requisitos mínimos de hardware, mas é recomendável ter pelo menos 2 GB de RAM e 20 GB de espaço de armazenamento para uma experiência de uso adequada.

No entanto, dependendo das ferramentas e processos em execução, pode ser necessário mais recursos, especialmente para tarefas intensivas em CPU ou de análise de grandes conjuntos de dados.

5. Conclusão

Em conclusão, a análise do uso e do conteúdo da distribuição Kali Linux desempenha um papel fundamental no campo da segurança da informação. Essa análise permite entender como essa distro de segurança funciona e como hackers éticos utilizam essa poderosa ferramenta em testes de penetração, auditorias de segurança e pesquisa de vulnerabilidades. Ao investigar o conteúdo do Kali Linux, é possível explorar as ferramentas e recursos disponíveis, garantindo uma abordagem ética e responsável. A análise do uso e do conteúdo do Kali Linux é essencial para identificar e corrigir vulnerabilidades em sistemas e redes, bem como para adquirir uma maior compreensão, contribuindo para aprimorar a segurança cibernética e proteger informações sensíveis.

6. Referências

ACERVO LIMA (2022). "Kali Linux - Ferramentas De Análise De Vulnerabilidade". Disponível em: <https://acervolima.com/kali-linux-ferramentas-de-analise-de-vulnerabilidade/>. Acesso em: 09 de junho de 2023.

Adams, D., (2022). "Debian Package Managers: dpkg, apt and Aptitude Explained". Disponível em: <https://linuxhint.com/https-linuxhint-com-debian_package_managers/>. Acesso em: 09 de junho de 2023.

Andrade, E., (2021). "Gerenciador de pacotes DPKG do Debian e derivados". Disponível em: <https://www.erickandrade.com.br/gerenciador-de-pacotes-dpkg-do-debian-e-derivados/>. Acesso em: 12 de junho de 2023.

Arindam, (2022). "Linux Kernel 6.1 is out with Initial Rust Support. This is What's New". Disponível em: <https://www.debugpoint.com/linux-kernel-6-1/#:~:text=Linus%20Torvalds%20released%20Linux%20Kernel,reasons%2C%20this%20release%20is%20important.> Acesso em: 09 de junho de 2023.

BACKBOX (2022). BackBox Software. Disponível em: https://backbox.com/. Acesso em: 09 de junho de 2023.

Brown, K., (2022). "Kali http server setup". Disponível em: <https://linuxconfig.org/kali-http-server-setup>. Acesso em: 09 de junho de 2023.

Gonzalez, D. G., (2022). "Como Instalar o Kali Linux". Disponível em: <https://www.linuxadictos.com/pt/como-instalar-kali-linux.html>. Acesso em: 09 de junho de 2023.

Henrique, D. (2022). "Tudo o que você precisa saber sobre o Kali Linux". Disponível em: <https://diolinux.com.br/tecnologia/kali-linux.html>. Acesso em: 09 de Junho de 2023.

Hertzog, R., O'Gorman, J., Aharoni, M., (2017). Kali Linux Revealed: Mastering the Penetration Testing Distribution. 2017, Offsec Press, 1ª edição.

JAVATPOINT (2021). “Use of Kali Linux”. Disponível em: <https://www.javatpoint.com/use-of-kali-linux>. Acesso em: 09 de junho de 2023.

KALI (2022) OffSec Services Limited. Disponível em: <https://www.kali.org/docs/introduction/what-is-kali-linux/>. Acesso em: 09 de Junho de 2023.

Klimaszewski, S. (2023). “Raspberry Pi 4”. Disponível em: <https://www.kali.org/docs/arm/raspberry-pi-4/>. Acesso em: 09 de junho de 2023.

Kumar, V. (2022). “How to use Kali Linux Package manager to install packages or apps”. Disponível em: <https://www.cyberpratibha.com/blog/apt-package-handling-utility/#:~:text=The%20APT%20is%20a%20Kali,packages%20along%20with%20their%20dependencies>. Acesso em: 09 de junho de 2023.

Logan, (2023). “The Difference Between “Kali Linux” and “Kali Linux Lite””. Disponível em: <https://allthedifferences.com/the-difference-between-kali-linux-and-kali-linux-lite/>. Acesso em: 09 de junho de 2023.

Palmer, M., (2021). “Kali Linux VMware – The Complete 2021 Guide”. Disponível em: <https://vmiss.net/kali-linux-vmware/>. Acesso em: 09 de junho de 2023.

PARROTSEC (2023). The operating system. Disponível em: <https://www.parrotsec.org/>. Acesso em: 09 de junho de 2023.

RAPID7 (2022) Rapid7. Disponível em: <https://www.kali.org/docs/introduction/what-is-kali-linux/>. Acesso em: 09 de Junho de 2023.

Ribeiro, U. (2022). “As 7 Principais Ferramentas no Kali Linux para Pentest”. Disponível em: <https://www.certificacaolinux.com.br/ferramentas-kali-linux/>. Acesso em: 09 de Junho de 2023.

Rudra, S., (2022). “Linux Kernel 6.1 Released With Initial Rust Code”. Disponível em: <https://news.itsfoss.com/linux-kernel-6-1-release/>. Acesso em: 09 de de junho de 2023.

Rudra, S., (2023). “Kali Linux 2023.2 Release Adds a New Hyper-V Image and PipeWire to XFCE Variant”. Disponível em: <https://news.itsfoss.com/kali-linux-2023-2-release/>. Acesso em: 09 de junho de 2023.

Saive, R., (2023). “The History of Kali Linux Distribution”. Disponível em: <https://www.linuxshelltips.com/kali-linux-history/>. Acesso em: 09 de junho de 2023.

Santos, L., (2018). “Como recuperar arquivos excluídos no Kali Linux?”. Disponível em: <https://recoverit.wondershare.com.br/harddrive-recovery/kali-linux-data-recovery.ht

ml#:~:text=Foremost%20%C3%A9%20uma%20ferramenta%20de,rodap%C3%A9s%20e%20estruturas%20de%20dados.>. Acesso em: 09 de junho de 2023.

Schultz, C. P., Perciaccante B (2017). Kali Linux Cookbook: Effective penetration testing solutions. 2ª edição, Packt Publishing, 2017.

Tomas, C., (2018). “Kali Linux on your Pocket with the GPD 7 mini-laptop”. Disponível em: <https://medium.com/hackernoon/kali-linux-2018-2-on-your-pocket-with-the-gpd-7-\mini-laptop-77b0d59dec40>. Acesso em: 09 de junho de 2023.

Zaino, P. F., (2021). “Linux: Configure and use your TPM 2.0 module on Linux”. Disponível em: <https://paolozaino.wordpress.com/2021/02/21/linux-configure-and-use-your-tpm-2-0-module-on-linux/>. Acesso em: 09 de junho de 2023.