Análise e teste de vulnerabilidade de redes *Wireless* em instituições de ensino que utilizam o protocolo WPS

Gabriel Neris dos Santos[1], **Victor Hugo Lima Bauer**[2], **Carlos Alberto da Silva**[3]

[1]Curso de Bacharelado em Sistemas de Informação – Faculdade de Computação (FACOM)
Universidade Federal de Mato Grosso do Sul (UFMS).
Av. Costa e Silva, s/n. - Bairro Universitário - CEP 79070-900 - Campo Grande - MS.

{g.neris, victor.bauer, carlos.silva}@ufms.br

Abstract. *The article addresses wireless network technology and its vulnerabilities, with a focus on the threat posed by the Wi-Fi Protected Setup (WPS) protocol. The study highlights the need to assess the security of these networks to ensure the reliability of the connection and presents a comparative analysis of security test results for wireless networks in different educational institutions.*

Resumo. *Esta pesquisa aborda a tecnologia de redes wireless e suas vulnerabilidades, com foco nas ameaças ao protocolo WPS (Wi-fi Protected Setup). O estudo destaca a necessidade de avaliação continua da segurança dessas redes para garantir a confiabilidade e disponibilidade das conexões, e apresenta uma análise comparativa entre os resultados dos testes de segurança das redes wireless em diferentes instituições de ensino.*

1. Introdução

Com a popularização dos dispositivos móveis, organizações frequentemente implementam redes *wireless* para proporcionar acesso rápido e eficiente à internet a seus usuários. No entanto, essas redes possuem desvantagens no quesito de segurança [Gimenes 2005], já que diferentes das redes cabeadas, essas ficam expostas para indivíduos mal intencionados dentro de suas regiões de cobertura, que geralmente ultrapassam o perímetro da organização.

É recomendado que sejam utilizados procedimentos para mitigar os riscos de infecção por parte dos usuários da rede, como definir quais locais podem ser acessados, o que pode ser armazenado e qual o sistema de segurança deve estar operando nos dispositivos que estarão conectados. Isso faz com que as redes se tornem mais segura, porém é necessário investir em mais mecanismos de defesa focados para redes sem fio. Para minimizar os problemas de acesso indevido, [Rufino 2005] propõe que os pontos de acesso da rede sejam posicionados de forma estratégica, a fim de que a rede tenha alcance somente na área necessária.

Segundo [Duarte 2003], em uma rede deve haver equilíbrio entre os métodos de segurança e sua usabilidade, para que um usuário credenciado não tenha problemas para se conectar a rede e seja mantida a confidencialidade, disponibilidade, integridade e usabilidade da mesma.

A presente pesquisa tem como objetivo apresentar os protocolos de segurança WPS de redes sem fio, e realizar testes e análise da segurança em instituições de ensino, explorando as vulnerabilidades do protocolo WPS.

2. Fundamento Teórico

Nesta seção apresentamos a tecnologia das redes locais sem fio e os seus protocolos de segurança para conexão.

2.1. Redes locais sem fio

As redes locais sem fio surgiram como uma alternativa às redes cabeadas, sendo que possuem uma maior flexibilidade devido à capacidade de comunicação sem a necessidade de conexões físicas por meio de cabos. Essa característica permite a mobilidade dos dispositivos e facilita a implementação em ambientes diversos.

A tecnologia de redes sem fio IEEE 802.11, comumente chamada de Wi-Fi (*Wireless Fidelity*), é encontrada atualmente em locais de trabalho, residências, instituições educacionais e aeroportos, destacando-se como uma das tecnologias de acesso à *Internet* mais relevantes. [Kurose and Ross 2013]. Tal padrão foi desenvolvido pela IEEE (*Institute of Electrical and Electronics Engineers*) e publicado em 1999, sendo adotado como principal tecnologia de redes locais sem fio desde então.

Contudo, em virtude das transmissões sem fio serem realizadas por radiodifusão, facilitando a recepção de pacotes de informações não solicitados por computadores vizinhos, emerge um significativo desafio de segurança [Tanenbaum and Wetherall 2011]. Devido a esse aspecto, foram desenvolvidos ao longo dos anos protocolos de segurança para o padrão 802.11, sendo estes o WEP, WPA e WPA2.

2.2. WEP - *Wired Equivalent Privacy*

Na década de 1990, o WEP (*Wired Equivalent Privacy*) foi criado para fornecer segurança em redes sem fio, visando equipará-las às redes com fio em termos de proteção. O WEP foi desenvolvido e fundamentado em três princípios de segurança: (i) Confidencialidade: garantindo a ininteligibilidade das mensagens interceptadas; (ii) Autenticidade: assegurando a legitimidade do usuário; (iii) e Integridade: garantindo a chegada das mensagens sem alterações. O mesmo utilizava o algoritmo RC4 para proteger redes sem fio. Um algoritmo de cifra de fluxo simétrica, rápido e relativamente simples, que era usado para criar chaves de criptografia que eram compartilhadas entre dispositivos conectados à rede. No entanto, o uso do RC4 pelo WEP foi comprometido devido a falhas de segurança graves, isso somado suas múltiplas vulnerabilidades e deficiências de implementação resultaram em seu comprometimento. A utilização de apenas 24 bits, de um total de 128 bits, no vetor de inicialização da chave de criptografia resultou em poucos bits para a chave, permitindo ataques de força bruta para sua descoberta. Devido a isso, o WEP tornou-se obsoleto, levando à sua atualização para WEP2, que corrigiu essa falha. No entanto, posteriormente, foi substituído pelo protocolo WPA. [Linhares and Gonçalves 2007].

2.3. WPA - *Wi-Fi Protected Access*

O WPA foi o protocolo criado com foco em corrigir as falhas de segurança que restavam no WEP sem que precisasse haver a troca de equipamentos. Uma das melhoria significativa foi a implementação do MIC (*Message Integrity Check*), um componente adicionado para verificar se os dados transmitidos mantiveram sua integridade durante a transmissão. No entanto, essa implementação também abriu a possibilidade de realização de ataques de negação de serviço. Através da exploração de uma vulnerabilidade em seu mecanismo de proteção contra ataques de força bruta, que verifica a ocorrência de erros de checagem e caso haja duas dentro de um minuto, a conexão do ponto de acesso é cancelada por 60 segundos. Dessa forma, sendo possível por meio de injeção de pacotes causar intencionalmente esses erros, e tornando a rede indisponível [Linhares and Gonçalves 2007].

O TKIP, que representa o Protocolo de Integridade de Chave Temporal (Temporal Key Integrity Protocol, em inglês), desempenha um papel crucial no WPA (Wi-Fi Protected Access) para a criptografia de mensagens transmitidas. Este protocolo utiliza o algoritmo RC4, similar ao WEP (Wired Equivalent Privacy), porém, adota medidas preventivas para mitigar possíveis ataques. Diferentemente do WEP, o TKIP evita o envio da chave secreta de forma não criptografada, implementando uma abordagem mais sofisticada na gestão dos vetores de inicialização. O funcionamento do WPA

baseia-se em uma chave secreta, comumente chamada de PMK (Pairwise Master Key), que possui um comprimento variando entre 32 e 512 bits. Essa chave PMK é responsável por gerar uma PTK (Pairwise Transient Key) durante a conexão, utilizando parâmetros específicos adquiridos nesse processo. A PTK, então, é compartilhada entre o dispositivo cliente e o ponto de acesso, fortalecendo a segurança da comunicação sem fio. Essa abordagem proporciona uma camada adicional de proteção ao estabelecer uma chave transitória única para cada par de dispositivos envolvidos na comunicação [Paim 2011].

Um mecanismo que vale a pena ser citado, é a criação de diferentes modos de funcionamento. Sendo o Personal, destinado às redes domésticas e o Enterprise destinado às corporações, por ser mais seguro permitindo que haja um servidor de autenticação centralizado.

2.4. WPA2 - *Wi-Fi Protected Access 2*

Como o WPA implementou apenas uma parte do novo padrão IEEE 802,11i, o WPA2 acabou se tornando o novo o protocolo para redes sem fio, já que implementou todos os pontos do novo padrão [Júnior 2008]. Esse protocolo trouxe uma melhoria considerável em sua criptografia, por utilizar o protocolo CCMP, baseado em AES (*Advanced Encryption Standard*), que é mais robusto e resistente contra ataques. Também trouxe um mecanismo de pré autenticação, dedicado a diminuir a latência na autenticação ao transitar de um ponto de acesso a outro [Linhares and Gonçalves 2007].

2.5. WPA3 -*Wi-Fi Protected Access 3*

O WPA3 introduz inovações significativas para aprimorar a segurança nas redes sem fio, simplificando procedimentos, fortalecendo a autenticação, aumentando a robustez criptográfica, especialmente em ambientes com dados altamente sensíveis, e preservando a resiliência em redes críticas. Todas as implementações do WPA3 incorporam as práticas mais avançadas em segurança, eliminam protocolos legados desatualizados e impõem a utilização de quadros de gerenciamento protegidos (PMF). Considerando as distintas finalidades e exigências de segurança, o WPA3 oferece recursos adicionais, adaptados tanto para ambientes pessoais quanto empresariais. Os usuários do WPA3-Personal desfrutam de uma camada adicional de proteção contra tentativas de adivinhação de senha, enquanto os usuários do WPA3-Enterprise podem agora empregar protocolos de segurança de alto nível, especialmente desenhados para garantir a integridade de redes que manipulam dados confidenciais. Essa abordagem personalizada destaca o compromisso do WPA3 em atender às diversas demandas de segurança nas redes sem fio modernas [Alliance 2019].

Este oferece proteção eficaz contra tentativas de adivinhação de senha offline, limitando o usuário a uma única tentativa e exigindo interação direta com o dispositivo s. Isso implica que o usuário deve estar fisicamente presente sempre que desejar tentar adivinhar a senha. Em contrapartida, o WPA2 carece de uma camada integrada de criptografia e privacidade em redes públicas abertas, tornando os ataques de força bruta uma ameaça significativa [Kaspersky 2023]. Tais proteções são implementadas através do protocolo *Simultaneos Authentication of Equals*(SAE).

No entanto, podem levar mais alguns anos para que seja comum encontrar dispositivos utilizando WPA3, já que para isso serão precisas atualizações de hardware e software nos dispositivos atuais para que possam ter compatibilidade com esse protocolo.

2.6. WPS - *Wi-fi Protected Setup*

O protocolo WPS (*Wi-fi Protected Setup*), conforme citado por [Singh 2017], foi desenvolvido para simplificar a configuração de um ponto de acesso seguro, especialmente para proprietários residenciais comuns. Embora tenha sido introduzido inicialmente em 2006 com esse propósito, em 2011 foi identificada uma falha significativa em seu design. [Moreno 2016] destaca que sua implementação representa uma ameaça significativa à segurança, pois permite que um atacante descubra o número PIN (utilizado como autenticação no WPS). Sem conhecer a senha, o atacante pode enviar o PIN via

WPS e obter todas as configurações da rede, incluindo a senha. Tal processo de descoberta pode ser efetuado por meio da execução de um ataque de força bruta.

O procedimento de força bruta para descobrir o número PIN é delineado da seguinte maneira: o PIN do roteador é composto por um conjunto de 8 dígitos, sendo o último um checksum dos sete anteriores. Assim, há um total de 10^7 combinações possíveis, ou seja, 10.000.000. Dentro desse valor total, as verificações para o número PIN são divididas em duas partes: caso os quatro primeiros números do PIN estejam corretos, apenas os três últimos são validados. Dessa forma, o cálculo correto é 10^4 somado a 10^3, acrescido do checksum, resultando em um total de 11.000 combinações.

Este procedimento inicial envolve as etapas como autenticação, associação e certificados digitais na comunicação do roteador com um possível usuário da rede (configuração de segurança). Subsequentemente, o Ponto de Acesso (AP) inicia o processo enviando a mensagem M1, seguida pela resposta do atacante com a mensagem M2, e, por fim, o AP envia a mensagem M3. Em seguida, o atacante transmite a mensagem M4. Caso a resposta seja um NACK, sinaliza-se que a primeira metade do número está incorreta, demandando um incremento (por exemplo, de 0001000 para 0002000, 0003000, e assim por diante), repetindo o processo até localizar a primeira metade correta. Uma vez identificada a metade correta, é encaminhada ao roteador uma mensagem M4 contendo a primeira metade do PIN correto. Dado que a primeira metade está correta, a mensagem NACK não é enviada, e o roteador responde com a mensagem M5. O atacante recebe o M5 e envia a mensagem M6. Em caso de recebimento de um NACK, indica-se que a segunda metade do número está incorreta, devendo ser incrementada. Se a mensagem M7 for recebida, considera-se que o número PIN está correto. Com o número PIN correto, o roteador compartilha a configuração da rede com o atacante, incluindo a senha [Moreno 2016].

3. Metodologia

No curso do desenvolvimento desta pesquisa, optamos por empregar o sistema operacional Kali Linux [Kali 2023] como plataforma principal, e para a execução dos testes de intrusão em redes sem fio, adotamos a ferramenta Wifite2 [derv82 2018], que serão descritos a seguir.

3.1. Kali Linux

O Kali Linux é uma distribuição de código aberto fundamentada no Sistema Operacional Debian, sendo uma solução multiplataforma, acessível e gratuita para profissionais e estudantes da área de segurança da informação. Segundo [Kali 2023], este é especificamente projetado para realizar testes de penetração e auditorias de segurança, contando com uma extensa variedade de mais de 600 ferramentas incorporadas. Em virtude destas particularidades, e considerando que as ferramentas que serão apresentadas foram otimizadas para execução no Kali Linux, optamos por empregar este sistema operacional como plataforma principal para a execução dos testes.

3.2. Wifite2

O Wifite2 é a segunda versão da ferramenta de automatização de ataques *wireless* "Wifite", desenvolvida para sistemas operacionais baseados em Linux. Segundo [derv82 2018], a ferramenta é projetada especificamente para a versão mais recente do Kali Linux, sendo suportado também pela distribuição Parrot Security OS [ParrotSecurity 2023].

Este possui em sua composição outras ferramentas de auditoria de redes sem fio, como por exemplo, a suíte "Aircrack-ng" [Aircrack-ng 2023], que foi desenvolvida para empregar métodos conhecidos de obtenção da senha de um ponto de acesso sem fio. Esses métodos englobam:

- WPS: The Offline Pixie-Dust attack.
- WPS: The Online Brute-Force PIN attack.
- WPA: The WPA Handshake Capture.
- WPA: The PMKID Hash Capture.

- WEP: Vários ataques incluindo fragmentação, chop-chop, aireplay, etc.

Para que haja êxito em sua utilização, é essencial que o dispositivo no qual o Wifite2 será executado, e esteja equipado com uma placa de rede sem fio que suporte os modos de monitoramento e injeção de pacotes. Ao ser executada, a ferramenta escaneia as redes *wireless* próximas, permitindo que o usuário realize seleção de alvos dentro do alcance. A partir das informações capturadas da rede, o *script* escolhe a melhor estratégia para cada um dos alvos, e inicia o processo de teste de penetração, porém é possível selecionar novas estratégia através de parâmetros. Sua execução pode ser iniciada a partir do comando:

```
sudo wifite
```

O Wifite2 não realiza ataques em redes com criptografia WPA2 *Enterprise*, e sua funcionalidade abrange exclusivamente redes com criptografia WEP, WPA e WPA2 *Personal*. Considerando que o escopo desta pesquisa visa explorar a vulnerabilidade presente no protocolo WPS, optamos por empregar a abordagem do ataque *Pixie Dust* para os testes de penetração.

3.3. Ataque *Pixie Dust*

O *Pixie Dust* é um ataque de força bruta *offline* que tem como objetivo descobrir o PIN de oito dígitos da tecnologia WPS. Este método é conduzido de forma *offline* devido às contramedidas implementadas pelos fabricantes de equipamentos *wireless* após a divulgação da vulnerabilidade no WPS, que passaram a limitar o número de tentativas para inserção do PIN. Nesse contexto, o ataque se concentra na exploração da vulnerabilidade presente na mensagem M3 (Descrita no item 2.5) do processo de comunicação do WPS. Durante a execução do *Pixie Dust*, a análise é direcionada à etapa em que duas chaves de 128 bits (E-S1 e E-S2) são empregadas para a criptografia da primeira e segunda metade do PIN, respectivamente. Essa abordagem possibilita a descoberta do número PIN mediante a análise e manipulação dessas chaves de forma *offline*, evitando a necessidade de realizar múltiplas tentativas de inserção do PIN [Moreno 2016].

Tal tipo de ataque pode ser realizado utilizando a ferramenta ”Pixiewps” [wiire a 2020]. O Wifite2 incorpora o Pixiewps em seu código e automaticamente executa esse método em sua sequência de testes padrão, mas também pode executá-la de forma independente por meio do comando:

```
sudo wifite --pixie
```

3.4. Ambiente de teste

Foram selecionadas oito instituições de ensino como locais para aplicação dos testes, abrangendo diversos níveis educacionais, incluindo tanto instituições públicas quanto privadas. Em respeito à segurança dessas entidades, considerando as vulnerabilidades apresentadas, elas permanecerão anônimas e serão representadas por letras do alfabeto, como apresentado na Tabela 1.

Tabela 1. Instituições de Ensino investigadas

Instituição	Nível	Tipo
A	Superior	Pública
B	Infantil/Fundamental	Privada
C	Médio	Privada
D	Fundamental/Médio	Pública
E	Infantil	Privada
F	Infantil/Fundamental/Médio	Privada
G	Superior	Privada
H	Infantil	Privada

4. Resultados Obtidos

A realização bem-sucedida dos testes descritos nesta pesquisa no ambiente de teste definido é evidenciada pelos resultados apresentados na Tabela 2 e Figura 1. Entre todos os locais testados, observou-se

êxito no ataque, indicando que foi possível obter o PIN WPS e consequentemente acesso à senha da rede sem fio por meio da vulnerabilidade do protocolo WPS, em metade dos casos. Cabe ressaltar que em todas as instituições, ao menos uma rede utiliza o método de criptografia WPA *Personal*, com o protocolo WPS ativado, o que torna o ambiente inseguro visto que se trata de uma instituição de ensino com diversos dados sensíveis.

Tabela 2. Resultado dos teste de penetração

Instituição	Redes Escaneadas	Redes WPA-P	Redes WPS Ativo	Ataques bem sucedidos
A	16	4	1	1
B	5	5	1	0
C	2	2	2	2
D	1	1	1	0
E	2	2	1	0
F	2	2	2	2
G	1	1	1	0
H	2	2	1	1

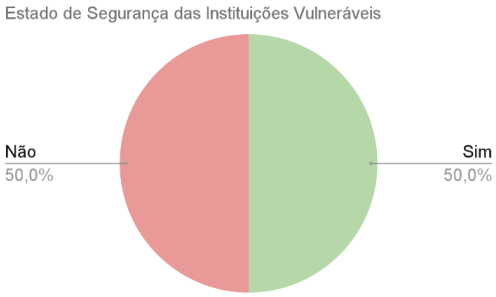

Figura 1. Gráfico de porcentagem de sucesso

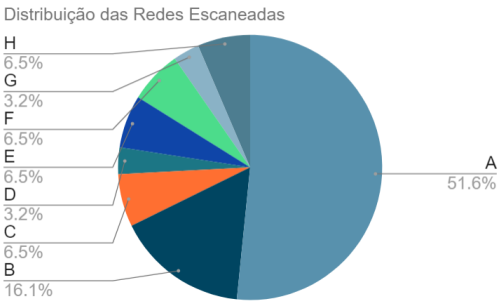

Figura 2. Gráfico de distribuição dos ataques

Também, houveram casos, como das instituições B, D e E, onde foi possível observar que mesmo com a utilização do WPS, não foi possível obter o PIN. Acreditamos que isso se deve, a distancia dos pontos de acesso do local onde era possível testar e/ou a configurações dos dispositivos que não permitiram a realização do ataque.

É possível observar na Figura 2 a representação das instituições em relação a quantidade de redes analisadas, sendo a instituição A a com a maior número de redes analisadas.

5. Trabalhos Relacionados

Um estudo relevante para análise foi conduzido por [Lima and Silva 2021], que realiza testes de penetração usando ferramentas de intrusão para não autenticar dispositivos, capturar o *handshake* da rede e tenta quebrar a senha com o auxílio de *wordlists* geradas pela ferramenta ”Crunch”.

[Carranza et al. 2017] conduziram testes automatizados em sua pesquisa, semelhantes aos realizados neste estudo, utilizando a ferramenta *wifite*. Eles empregaram o ataque ”Pixie-Dust” para obter acesso à senha por meio do código PIN, seguido pela análise de tráfego HTTP com o auxílio do ”Wireshark”, destacando o potencial risco associado à vulnerabilidade do código PIN.

Outro estudo relevante é o conduzido por [Lu and Yu 2021], no qual foram realizados testes de penetração em redes *wireless* explorando a vulnerabilidade do protocolo WPS. No entanto, eles utilizaram a ferramenta ”Reaver” de forma independente, além de empregar outras técnicas, como a falsificação de AP.

6. Conclusão e Trabalhos Futuros

Dada a crescente facilidade de acesso a equipamentos e ferramentas facilitadores de ataques a redes sem fio, torna-se evidente a necessidade de realizar monitoramento contínuo das vulnerabilidades

nos protocolos de segurança. Como destacado nesta pesquisa, algumas instituições ainda apresentam vulnerabilidades relacionadas ao WPS em suas redes, o que pode acarretar sérias consequências para a organização. Uma vez que um invasor não autorizado ganhe acesso à rede da instituição, ele pode iniciar uma série de ataques, tais como a interceptação de pacotes, exposição de dados de usuários, ataque a outras instituições por meio da rede invadida, e, dependendo da configuração da rede, realizar varreduras em dispositivos conectados utilizando softwares específicos. Diante desse cenário, reforça-se a importância do monitoramento constante para mitigar riscos e fortalecer a segurança das redes corporativas.

Segundo [SYNNEX 2023] é recomendado que corporações utilizem WPA2 Enterprise, por desabilitar recursos de WPS e trazer um nível maior de segurança à rede. No entanto, caso não possa aderir ao WPA2 Enterprise, é recomendado que o WPS seja desativado quando possível. Em cenários onde é realmente necessário o uso do WPS mesmo mediante dos riscos apresentados, orientamos que pelo menos seja desabilitado o uso do PIN como método de autenticação, impossibilitando a descoberta da senha através desse recurso.

Dos desafios vencidos, podemos citar a dificuldade para obter alcance de algumas redes devido ao limite de acesso, onde foi preciso encontrar locais onde havia potência de sinal suficiente para realizar o teste.

Como trabalhos futuros, pretendemos considerar testes de penetração dedicados a redes sem fio que adotam o protocolo WPA2 *Enterprise*. Este protocolo é amplamente recomendado no ambiente de grande corporações, devido à sua robustez e habilidade de fornecer uma camada adicional de segurança. A análise destas redes pode aprimorar nossa compreensão sobre a eficácia do WPA2 *Enterprise* no ambiente corporativo e institucional.

Referências

[Aircrack-ng 2023] Aircrack-ng (2023). Aircrack-ng. `https://www.aircrack-ng.org/`. Acessado em 17 de Novembro de 2023.

[Alliance 2019] Alliance, W.-f. O. (2019). Wifi alliance. `https://www.wi-fi.org/discover-wi-fi/security`. Acessado em 30 de Novembro de 2023.

[Carranza et al. 2017] Carranza, A., Magallanes, J., Decusatis, and Espinal, J. (2017). Automated wireless network penetration testing using wifite and reaver. *15th LACCEI International Multi-Conference for Engineering, Education, and Technology: "Global Partnerships for Development and Engineering Education"*.

[derv82 2018] derv82 (2018). Wifite2. `https://github.com/derv82/wifite`. Acessado em 17 de Novembro de 2023.

[Duarte 2003] Duarte, L. O. (2003). Análise de vulnerabilidades e ataques inerentes a redes sem fio 802.11x. *IBILCE - Universidade Estadual Paulista*.

[Gimenes 2005] Gimenes, E. C. (2005). Segurança de redes wireless. *Trabalho de Conclusão do Curso de Tecnólogo em Informática com ênfase em Gestão de Negócios - FATEC SP*.

[Júnior 2008] Júnior, M. A. C. C. (2008). Evolução da segurança em redes sem fio. *Universidade Federal de Pernambuco (UFPE) - Centro de Informática (CIn)*.

[Kali 2023] Kali (2023). Kali linux. `https://www.kali.org/`. Acessado em 12 de Novembro de 2023.

[Kaspersky 2023] Kaspersky (2023). Wep, wpa, wpa2 e wpa3: Diferenças e explicação. `https://www.kaspersky.com.br/resource-center/definitions/wep-vs-wpa`. Acessado em 30 de Novembro de 2023.

[Kurose and Ross 2013] Kurose, J. F. and Ross, K. W. (2013). *Redes de Computadores e a internnet: uma abordagem top-down*. Pearson Education do Brasil Ltda, São Paulo, SP, 6st edition.

[Lima and Silva 2021] Lima, I. V. d. and Silva, J. A. d. (2021). AnÁlise de vulnerabilidades e contramedidas em relaÇÃo a ataques em redes sem fio. *UFAL - Campus de Arapiraca*.

[Linhares and Gonçalves 2007] Linhares, A. G. and Gonçalves, P. A. D. (2007). Uma análise dos mecanismos de segurança de redes ieee 802.11:wep, wpa, wpa2 e ieee 802.11w*. *Universidade Federal de Pernambuco (UFPE) - Centro de Informática (CIn)*.

[Lu and Yu 2021] Lu, H.-J. and Yu, Y. (2021). Research on wifi penetration testing with kali linux. *Complexity*.

[Moreno 2016] Moreno, D. (2016). *Pentest em Redes Sem Fio*. Novatec Editora Ltda, São Paulo, SP, 1st edition.

[Paim 2011] Paim, R. R. (2011). Wep, wpa e eap. *UFRJ - Universidade Federal do Rio de Janeiro*.

[ParrotSecurity 2023] ParrotSecurity (2023). Parrot security os. `https://www.parrotsec.org/`. Acessado em 17 de Novembro de 2023.

[Rufino 2005] Rufino, N. M. d. O. (2005). *Segurança de Redes Sem Fio*. Novatec Editora Ltda, São Paulo, SP, 1st edition.

[Singh 2017] Singh, H. (2017). *Kali Linux Wireless Pentesting and Security for Beginners*. rootsh3ll.com, 1st edition.

[SYNNEX 2023] SYNNEX, T. (2023). 5 vulnerabilidades na rede wi-fi que as empresas precisam combater. `https://blog-pt.lac.tdsynnex.com/5-vulnerabilidades-na-rede-wi-fi-que-as-empresas-precisam-combater`. Acessado em 18 de Novembro de 2023.

[Tanenbaum and Wetherall 2011] Tanenbaum, A. and Wetherall, D. (2011). *Redes de computadores*. Pearson Education do Brasil Ltda, São Paulo, SP, 5st edition.

[wiire a 2020] wiire a (2020). Pixiewps. `https://github.com/wiire-a/pixiewps`. Acessado em 18 de Novembro de 2023.