Carlos Daniel da Silveira Santos
Orientador: Prof. Fredison Muniz de Sousa

Avaliação do Uso das Redes Wi-fi na cidade de Valença do Piauí e Picos

Picos - PI
14 de agosto de 2023

Carlos Daniel da Silveira Santos
Orientador: Prof. Fredison Muniz de Sousa

Avaliação do Uso das Redes Wi-fi na cidade de Valença do Piauí e Picos

Monografia submetida ao Curso de Bacharelado em Sistemas de Informação como requisito parcial para obtenção de grau de Bacharel em Sistemas de Informação

Universidade Federal do Piauí
Campus Senador Heuvídio Nunes de Barros
Bacharelado em Sistemas de Informação

Picos - PI
14 de agosto de 2023

FICHA CATALOGRÁFICA
Serviço de Processamento Técnico da Universidade Federal do Piauí
Biblioteca José Albano de Macêdo

S237a Santos, Carlos Daniel da Silveira
Avaliação do uso das redes Wi-fi na cidade de Valença do Piauí e Picos [recurso eletrônico] / Carlos Daniel da Silveira Santos - 2023.
56 f.

1 Arquivo em PDF
Indexado no catálogo *online* da biblioteca José Albano de Macêdo-CSHNB
Aberto a pesquisadores, com restrições da Biblioteca

Trabalho de Conclusão de Curso (Graduação) – Universidade Federal do Piauí, Bacharelado em Sistemas de Informação, Picos, 2023.
"Orientador : Prof. Fredison Muniz de Sousa"

1. Wi-fi. 2. WPS. 3. Segurança em redes. 4. Protocolo de segurança. 5. Internet. I. Sousa, Fredison Muniz de. II. Título.

CDD 004.678

Emanuele Alves Araújo CRB 3/1290

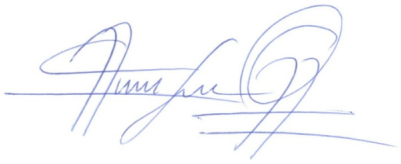
AVALIAÇÃO DO USO DAS REDES WI-FI NAS CIDADES DE VALENÇA DO PIAUÍ E PICOS - PI

CARLOS DANIEL DA SILVEIRA SANTOS

Monografia **APROVADA** como exigência parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Data de Aprovação

Picos – PI, 14 de Agosto de 2023



Prof. Fredison Muniz de Sousa

Prof. Leonardo Pereira de Sousa

Prof. Ismael de Holanda Leal

Agradecimentos

Agradeço a Deus pela saúde, disposição e por ter me dado força para continuar. À toda minha família, por todo o apoio, em especial a minha noiva Kemily de Jesus de Sousa Santos e também a minha mãe Maria Dineusa Silveira, por todo apoio e suporte necessário. À Universidade Federal do Piauí e a todos os Professores, pelas oportunidades, pela confiança e por sempre viabilizarem minha formação acadêmica e profissional. À todos os amigos que acompanharam de perto minha jornada na UFPI e que sem dúvida me impulsionam a ser um aluno melhor Gabriel Holanda, Lucas Vinicius, Lucas Sousa, Samuel Lelis, Pedro Azevedo, Saul Rocha, Jederilson, Gerson, Samuel Oliveira, Thaliane, Gabriell Oliveira, Marcos Paulo. A todos os que, direta ou indiretamente, contribuíram para a minha formação durante esta trajetória.

Divido com todos os méritos desta conquista.

Não temas, porque eu sou contigo; não te assombres, porque eu sou teu Deus; eu te fortaleço, e te ajudo, e te sustento com a destra da minha justiça.

Isaías 41:10

Resumo

O Wi-Fi Protected Setup (WPS) é um padrão estabelecido pela Wi-Fi AllianceTM para a segurança de redes sem fio. Introduzido em 2006, o WPS tinha como objetivo facilitar a configuração e substituir padrões obsoletos. No entanto, algumas vulnerabilidades foram identificadas no processo. Uma das falhas do WPS reside no fato de utilizar um PIN (Número de identificação pessoal) de apenas 8 dígitos, tornando-o vulnerável a ataques de força bruta. Essa limitação compromete a segurança das redes Wi-Fi, colocando em risco a privacidade e a integridade dos dados dos usuários. Este trabalho propõe um estudo das vulnerabilidades e falhas dos equipamentos de redes, com o objetivo de utilizar os recursos de maneira adequada e atender às necessidades dos usuários. A proposta é analisar a segurança das redes sem fio em Valença do Piauí e Picos, identificando pontos fracos como criptografia, uso do WPS assim apresentando soluções para fortalecer a proteção dessas redes. A pesquisa constatou um aumento significativo na segurança das redes Wi-Fi analisadas. Recomenda-se maior conscientização sobre problemas de segurança, adoção do método WPA2, desativação do WPS e atualização do firmware dos roteadores sem fio.

Palavras-chaves: Wi-Fi, WPS, Segurança, Internet, Protocolo.

Abstract

Wi-Fi Protected Setup (WPS) is a standard established by the Wi-Fi AllianceTM for securing wireless networks. Introduced in 2006, WPS was intended to ease configuration and replace obsolete standards. However, some vulnerabilities were identified in the process. One of the shortcomings of WPS lies in the fact that it uses a PIN (Personal Identification Number) of only 8 digits, making it vulnerable to brute force attacks. This limitation compromises the security of Wi-Fi networks, putting the privacy and integrity of users' data at risk. This work proposes a study of the vulnerabilities and failures of network equipment, with the objective of using resources properly and meeting the needs of users. The proposal is to analyze the security of wireless networks in Valença do Piauí and Picos, identifying weaknesses such as encryption, use of WPS, thus presenting solutions to strengthen the protection of these networks. The research found a significant increase in the security of the analyzed Wi-Fi networks. Increased awareness of security issues, adoption of the WPA2 method, disabling WPS, and updating the firmware of wireless routers is recommended.

Lista de ilustrações

Figura 1 – Princípio da comunicação na Internet através do modelo OSI 14

Figura 2 – Ataque com Rogue AP 35
Figura 3 – Fases de um teste de penetração 36

Figura 4 – Distribuição de pontos de acesso na zona comercial da cidade de Valença do Piauí 40
Figura 5 – Distribuição de pontos de acesso na zona comercial da cidade de Picos 41
Figura 6 – Uso de criptografia Wi-Fi em Valença do Piauí. 42
Figura 7 – Suporte WPS em Valença do Piauí. 43
Figura 8 – Frequência das Redes em Valença do Piauí. 43
Figura 9 – Canais de banda 2.4 GHz em Valença do Piauí. 44
Figura 10 –Canais de banda 5 GHz em Valença do Piauí. 45
Figura 11 –Uso de criptografia Wi-Fi em Picos Piauí. 46
Figura 12 –Suporte WPS em Picos Piauí. 47
Figura 13 –Frequência das Redes em Picos Piauí. 47
Figura 14 –Canais de banda 2.4 GHz em Picos Piauí. 48
Figura 15 –Canais de banda 5 GHz em Picos Piauí. 49

Lista de tabelas

Tabela 1 – Cronologia dos padrões 802.11 19
Tabela 3 – Taxonomia dos Rogue AP's 36

Tabela 4 – Principais Fabricantes de Dispositivos de Redes de Picos 51
Tabela 5 – Principais Fabricantes de Dispositivos de Redes de Valença do Piauí . 52

Lista de abreviaturas e siglas

WPS	*Wi-Fi Protected Setup*
IOT	*Internet of Things*
OSI	*Open Systems Interconnection*
WI-FI	*Wireless Fidelity*
WPA	*Wireless Protected Access*
WEP	*Wired Equivalent Privacy*
WPA2	*Wireless Protected Access II*
OMS	Organização Mundial da Saúde
PIN	*Personal Identification Number*
IRDA	*Infrared Data Association*
IEEE	*Institute of Electrical and Electronic Engineers*
TKIP	*Temporal Key Integrity Protocol*
KRACK	*Key Reinstallation Attacks*
NFC	*Near Field Communication*
WLAN	*Wireless Local Area Network*
FHSS	*Frequency Hopping Spread Spectrum*
DSSS	*Direct Sequence Spread Spectrum*
OFDM	*Orthogonal Frequency Division Multiplexing*
OFDMA	*Orthogonal Frequency Division Multiple Access*
LLC	*Logical Link Control*
MINO	*Multiple-Input Multiple-Output*
SISO	*Single-Input Single-Output*
MU-MIMO	*Multi-User MIMO*
IBSS	*Independent Basic Service Set*

BSS	*Basic Service Set*
ESS	*Extended Service Set*
WDS	*Wireless Distribution System*
Pre-RSN	*Robust Security Network*
MITM	*Man In The Middle*
PMF	*Protected Management Frames*
SRAP	*Smartphone Rogue AP*
ISSAF	*Information System Security Assessment Framework*
OSSTMM	*Open Source Security Testing Methodology Manual*

Sumário

1 Introdução 14
1.1 Objetivos 15
1.2 Organização 16

2 Referencial Teórico 17
2.1 Redes sem Fios 17
2.1.1 Padrão 802.11 17
2.1.2 Padrão 802.11a 18
2.1.3 Padrão 802.11b 19
2.1.4 Padrão 802.11g 20
2.1.5 Padrão 802.11n 20
2.1.6 Padrão 802.11ac 20
2.1.7 Padrão 802.11ax 21
2.1.8 WLAN (*Wireless Local Area Network*) 22
2.1.9 Mecanismos de autenticação, criptografia e integridade de dados para o padrão IEEE 802.11 23
2.1.9.1 Mecanismos de autenticação padrão IEEE 802.11 24
2.2 Protocolos de Segurança 25
2.2.1 Protocolo WEP (*Wired Equivalent Privacy*) 25
2.2.2 Protocolo WPA (Wi-Fi *Protected Access*) 25
2.2.3 Protocolo WPA2 (Wi-Fi *Protected Access2*) 27
2.2.4 Protocolo WPA3 (Wi-Fi *Protected Access3*) 28
2.2.5 Protocolo WPS 28
2.3 Classificação de ataques as redes WLAN (*Wireless Local Area Network)* . . 29
2.4 Ataques de Negação de Serviço 33
2.5 Ataques de AP falso 34
2.6 Teste de penetração (*Pentesting*) 36

3 Trabalhos Relacionados 38
3.1 Trabalhos que utilizam o WPS para exploração de Vulnerabilidades 38
3.2 Trabalhos que exploram vulnerabilidades em WPA e WPA2 38

4 Desenvolvimento do Trabalho 40
4.1 Resultados 41
4.1.1 Valença do Piauí 41
4.1.2 Picos 45

4.1.3 Fabricantes de Equipamentos de Redes e Segurança 49
4.1.3.1 A Importância de Identificar Fabricantes 50
4.1.3.2 Segurança Baseada no Fabricante 50
4.1.3.3 Atualizações e Patches 50
4.1.3.4 Avaliação de Riscos 50
4.1.3.5 Integração com Políticas de Segurança 50
4.1.3.6 Análise com OUI Lookup do Wireshark 51

5 Conclusão 54

Referências 55

1 Introdução

As redes de computadores são compostas por dispositivos capazes de se comunicar entre si. Essa conexão pode ocorrer por meio de diferentes meios, como fios de cobre, fibra óptica e ondas de rádio. Esses sistemas utilizam equipamentos concentradores, chamados de *switches*, para interligar os dispositivos da rede. Além disso, é adotada a estrutura cliente-servidor, na qual as tarefas são distribuídas entre os fornecedores de recursos (servidores) e os usuários que requerem os serviços (clientes) (TANENBAUM; WETHERALL, 2011).

A estrutura de uma rede possui um componente essencial para a comunicação: o protocolo de comunicação. Os protocolos consistem em conjuntos de regras que estabelecem a comunicação entre as diversas camadas do modelo OSI (Open Systems Interconnection). A representação das camadas do modelo OSI pode ser observada na figura 1. Esses protocolos desempenham um papel crucial no controle do formato e do significado das informações transmitidas (TANENBAUM; WETHERALL, 2011). No contexto das redes Wi-Fi (Wireless Fidelity), o Wi-Fi Protected Setup (WPS) é amplamente utilizado como um padrão de segurança. Seu objetivo principal é facilitar e agilizar a conexão entre dispositivos e redes sem fio. Essa tecnologia funciona por meio de uma senha criptografada, garantindo a segurança da conexão.

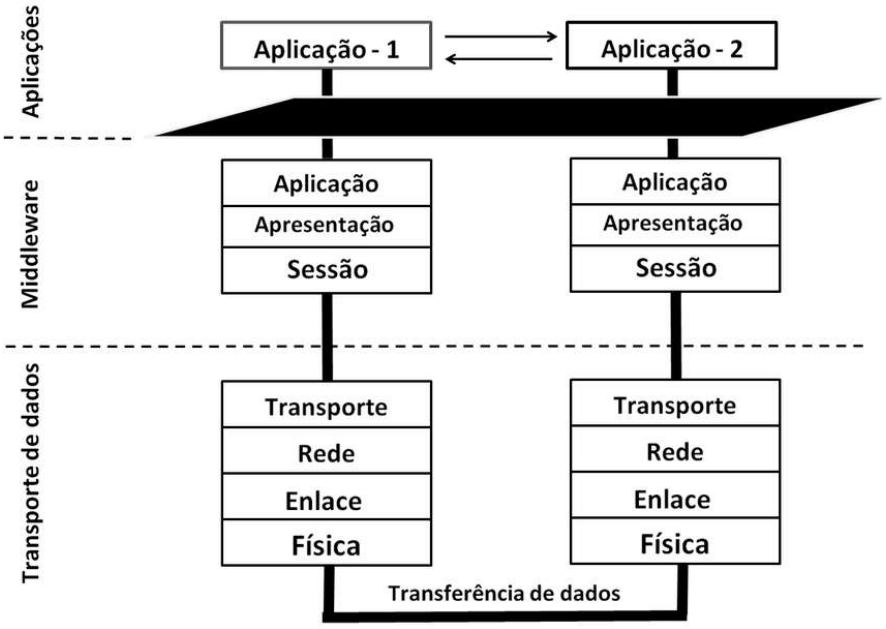


Figura 1 – Princípio da comunicação na Internet através do modelo OSI

Atualmente a rede Wi-Fi não se limita mais apenas a checar redes sociais ou e-mails, ela se tornou fundamental para viabilizar estudos híbridos ou remotos, bem como o trabalho

em Home Office. Ela precisa oferecer qualidade e estabilidade para enfrentar videoconferências e outras tarefas exigidas pelos novos tempos. Com o crescimento e a relevância das redes Wi-Fi, surge também a preocupação com a segurança dessas redes. Nunca antes estivemos tão constantemente compartilhando informações vulneráveis, e as redes sem fio apresentam desafios adicionais em comparação com as redes cabeadas. Suas ondas eletromagnéticas atravessam o ar, paredes e diversos obstáculos, o que pode aumentar as vulnerabilidades e os riscos. Caso a segurança da rede não seja cuidadosamente planejada, as redes sem fio podem se tornar alvos perfeitos para a captura de informações.

Existem diversas vulnerabilidades e ataques possíveis contra redes e dispositivos sem fio, especialmente quando o atacante possui acesso a informações sensíveis como o status da configuração do WPS (Wi-Fi Protected Setup) do ponto de acesso as redes preferenciais dos dispositivos IoT (Internet of Things) e os protocolos de segurança e criptografia da rede, como WPA (Wireless Protected Access), WEP (Wired Equivalent Privacy) e WPA2 (Wireless Protected Access II). Com o avanço e a popularização dos dispositivos IoT, a segurança da rede Wi-Fi tornou-se um ponto crítico na proteção desses dispositivos, já que a maioria deles depende exclusivamente da transmissão sem fio de dados. Por estarem principalmente conectados a redes locais, esses dispositivos muitas vezes possuem implementações de segurança frágeis. Consequentemente, qualquer comprometimento da segurança das redes sem fio coloca todos os dispositivos conectados a elas em risco.

Embora o WPS seja promovido como um método seguro para configurar dispositivos sem fio, é importante destacar que existem projetos e falhas de implementação que podem permitir que invasores obtenham acesso a redes protegidas (VIEHBÖCK, 2011). Há duas principais formas de atacar um dispositivo Wi-Fi com WPS. A primeira é por meio de um ataque de força bruta offline, que explora desequilíbrios no registro do protocolo. Embora exija alguma interação do usuário, esse tipo de ataque é considerado o mais eficiente em termos de sucesso. Já a segunda forma de ataque explora fraquezas na implementação do WPS e envolve a criação de um "evil twin"(rede falsa). É importante ressaltar que, mesmo desabilitando completamente o WPS nos roteadores, todas as vulnerabilidades não são eliminadas (MOHTADI; RAHIMI, 2015).

1.1 Objetivos

O objetivo geral deste trabalho é levantar dados que mostrem o atual cenário do nível de segurança das redes Wi-Fi no município de Valença do Piauí e Picos localizado no estado do Pauí. Os objetivos específicos deste trabalho são:

- Identificar o perfil das redes Wi-Fi da cidade Valença do Piauí e Picos;
- Demonstrar o atual nível de segurança das redes identificadas;
- Determinar a porcentagem de uso do WPS nas redes sem fio.

1.2 Organização

O restante deste trabalho está organizado da seguinte forma: O capítulo 2 apresenta conceitos para a compreensão deste trabalho. O capítulo 3 apresenta os trabalhos relacionados, comparando-os com nossa proposta. O capítulo 4 demonstra como foi realizado o presente trabalho. Finalmente, o capítulo 5 apresenta a conclusão e trabalhos futuros.

2 Referencial Teórico

Este capítulo descreve conceitos fundamentais para a compreensão deste trabalho. As seções incluem conceitos sobre os principais protocolos, suas vulnerabilidades e métodos de ataques.

2.1 Redes sem Fios

A tecnologia *wireless*, possibilita a transmissão de conexão entre pontos distantes sem precisar utilizar fios, como telefones sem fio, rádios ou o seu celular (CANCELA et al.,). Essa tecnologia engloba uma série de outras, sendo a mais comum delas a Wi-Fi. Podem ser consideradas tecnologias *wireless*, como o IrDA (*Infrared Data Association*), que transmite através de um adaptador infravermelho. Há também o *bluetooth*, muito utilizado em *smartphones*, porém sua distância é relativamente curta, dentre outros (ENGST; FLEISHMAN, 2005).

O *Institute of Electrical and Electronic Engineers* (IEEE) constituiu um grupo de pesquisa para criar padrões abertos que pudessem tornar a tecnologia sem fio cada vez mais realidade. Seu objetivo era desenvolver padrões técnicos que fossem adotados por diferentes fabricantes, definindo a comunicação entre fabricante e cliente de rede. Ao longo do tempo, foram desenvolvidos diversos padrões, sendo o padrão 802.11, conhecido como Wi-Fi, aquele que se destacou e foi melhor desenvolvido (RUFINO, 2019).

O comitê apresentou o padrão IEEE 802.11, que foi inicialmente definido como uma especificação de nível físico e de *enlace* do modelo OSI para redes locais sem fio WLAN. A WLAN funcionava a 1 Mbps (megabits por segundo) ou 2 Mbps (TANENBAUM, 2003). Com o passar do tempo, outros padrões foram criados de acordo com a necessidade do mercado. O último padrão apresentado é o 802.11ax, que foi ratificado no segundo semestre de 2019, com o objetivo de fornecer um desempenho mais previsível para aplicações avançadas, como vídeo 4K ou 8K (LÓPEZ-PÉREZ et al., 2019).

O IEEE desenvolveu diversos padrões e subpadrões para a tecnologia de WLAN. Entre eles, destacam-se os subpadrões 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac e 802.11ax. Esses padrões diferem em relação à frequência de operação, taxa de transmissão, largura de banda, modulação utilizada para transmissão dos dados e recursos de segurança suportados.

2.1.1 Padrão 802.11

O padrão IEEE 802.11 trabalha com as determinações das camadas 1 e 2 do modelo de referência OSI (Open Systems Interconnection). Isso significa que essa especificação

abrange a Camada Física (1) e a Camada de Enlace (2). O padrão 802.11, aprovado pelo IEEE em 1997, é um membro da família 802. Ele traz definições para a camada 1 e também para a subcamada MAC (Controle de Acesso ao Meio) na camada 2. Para a função de controle de link lógico LLC da subcamada 2, o 802.11 adota o padrão 802.2. Na camada física, o 802.11 define uma série de padrões de transmissão e de codificação para comunicações sem fio, sendo eles: FHSS (*Frequency Hopping Spread Spectrum*), DSSS (*Direct Sequence Spread Spectrum*), OFDM (*Orthogonal Frequency Division Multiplexing*), suas funções são:

- Codificação e decodificação de sinais;
- Geração/remoção de parâmetros para sincronização;
- Recepção e transmissão de bits;
- Especificação do meio de transmissão.

Na camada de enlace do modelo OSI, o padrão 802 define duas subcamadas: o LLC (*Logical Link Control*) e o MAC (*Media Access Control*). Entretanto, o padrão 802.11 define funções somente para a subcamada MAC, que tem as seguintes atribuições:

- Aspectos de transmissão: reunião de dados dentro de um pacote com endereços e campos de detecção de erro;
- Aspectos de recepção: abertura de pacote e execução de reconhecimento de endereços e detecção de erros;
- Controle de acesso ao meio de transmissão LAN.

Essas funções garantem o adequado funcionamento da comunicação sem fio, coordenando o acesso ao meio compartilhado de forma eficiente e possibilitando a troca de informações entre os dispositivos conectados à rede WLAN.

Já as funções de provimento de ligação para camadas superiores e execução de controle de fluxo e erro de pacotes da camada LLC são herdados do padrão 802.2 e incorporados ao 802.11. Uma síntese cronológica dos padrões 802.11 usuais é apresentada na tabela 1.

2.1.2 Padrão 802.11a

O padrão 802.11a, criado pelo IEEE em paralelo ao 802.11b, é uma extensão do padrão original e opera na frequência de 5 GHz, permitindo uma taxa de transmissão de dados de até 54 Mbps. Essa frequência mais elevada reduz a interferência de dispositivos como telefones sem fio e fornos micro-ondas. No entanto, o alcance das redes 802.11a é limitado devido à sua frequência mais alta, tornando o sinal menos eficaz na penetração de obstáculos físicos.

Padrão	**Ano**	**Frequência de Operação GHz**	**Taxa máxima de transmissão Mbit/s**	**Largura de Banda MHz**	**Modulação**
802.11	1997	2.4	2	22	DSSS, FHSS
802.11a	1999	5	54	20	OFDM
802.11b	1999	2.4	11	22	DSSS
802.11g	2003	2.4	54	20	OFDM, DSSS
802.11n	2009	2.4 / 5	600	20 - 40	OFDM
802.11ac	2013	5 - 5.8	6930	20 - 40 - 80 - 160	OFDM
802.11ax	2019	2,4 / 5	1200	80 - 160	OFDM, OFDMA

Tabela 1 – Cronologia dos padrões 802.11

Em ambientes corporativos com alta demanda por largura de banda, o 802.11a foi amplamente adotado, mas seu custo mais elevado em comparação com o 802.11b limitou sua adoção em ambientes domésticos e pequenas empresas. Com o avanço da tecnologia, o 802.11a foi substituído por padrões mais recentes, como o 802.11n, 802.11ac e 802.11ax (Wi-Fi 6 e Wi-Fi 6E), que oferecem maior velocidade, alcance e eficiência. No entanto, o legado do 802.11a ainda é relevante em contextos específicos que requerem altas taxas de transferência de dados e enfrentam problemas de interferência em ambientes com muitos dispositivos sem fio próximos (SCARFONE et al., 2008a).

2.1.3 Padrão 802.11b

O padrão 802.11b, ao ser introduzido em 1999, trouxe uma significativa melhoria em relação ao seu antecessor, o 802.11 original. A possibilidade de alcançar uma taxa máxima de transmissão de 11 Mbps representou um avanço considerável na velocidade de transferência de dados em redes sem fio. Além disso, a escolha da faixa de frequência de 2,4 GHz permitiu uma compatibilidade com dispositivos já existentes que operavam nessa mesma faixa. Essa compatibilidade contribuiu para uma rápida adoção do 802.11b em ambientes domésticos e escritórios, tornando-o o padrão mais utilizado na época.

No entanto, apesar das vantagens, o 802.11b também apresentou algumas limitações, especialmente relacionadas à sua faixa de frequência. O uso do espectro de 2,4 GHz o tornou mais suscetível a interferências provenientes de dispositivos que operavam na mesma frequência, como telefones sem fio e fornos micro-ondas. Essa interferência poderia afetar o desempenho e a estabilidade da conexão em redes Wi-Fi baseadas em 802.11b, especialmente em ambientes com muitos dispositivos sem fio próximos.

Mesmo com a introdução de padrões mais recentes e avançados, o legado do 802.11b ainda era visível em muitos dispositivos e infraestruturas de rede. A compatibilidade com esse padrão tornou-se uma consideração importante para garantir que dispositivos mais antigos pudessem continuar a se conectar a redes Wi-Fi modernas. A evolução contínua

do Wi-Fi trouxe consigo melhorias significativas em termos de velocidade, alcance e segurança, mas o 802.11b permaneceu parte da história da tecnologia sem fio, representando um marco importante no desenvolvimento e popularização das redes Wi-Fi em todo o mundo (CAÇADOR, 2014).

2.1.4 Padrão 802.11g

O padrão 802.11g trouxe melhorias em velocidade, alcance e segurança para as redes sem fio. Com a implementação do conjunto de protocolos de segurança Wi-Fi Protected Access (WPA), as redes Wi-Fi se tornaram mais seguras contra ataques e interceptação de dados. O WPA substituiu o antigo padrão de segurança WEP, proporcionando mecanismos mais robustos de criptografia e autenticação.

Essa adoção do WPA foi essencial para proteger as redes Wi-Fi contra ameaças emergentes, garantindo a privacidade das informações transmitidas e impedindo o acesso não autorizado. Além disso, o 802.11g desempenhou um papel importante na popularização das redes sem fio em todo o mundo, sendo compatível com dispositivos baseados em 802.11b e incentivando a adoção mais ampla em ambientes domésticos e corporativos. Embora tenha sido substituído por padrões mais recentes, como o 802.11n, 802.11ac e 802.11ax (Wi-Fi 6 e Wi-Fi 6E), o legado do 802.11g permanece presente em muitos dispositivos e infraestruturas de rede, contribuindo significativamente para a evolução e disseminação das redes Wi-Fi no início do século XXI (GAST, 2005).

2.1.5 Padrão 802.11n

Com uma demanda crescente por redes Wi-Fi de melhor desempenho, maximizar a taxa de transmissão foi o principal motivador para a criação do padrão 802.11n. Essas novas determinações melhoram a largura de banda suportada pela utilização de múltiplos sinais de entrada e saída e antenas MINO (*Multiple-Input Multiple-Output*).

O conjunto de padrões 802.11n foi homologado pelo IEEE em 2009, com especificações que preveem até 600 Mbit/s de taxa de transmissão, oferecendo também maior alcance do sinal e maior resistência a interferências. Além disso, é retrocompatível com dispositivos 802.11b/g. No entanto, dispositivos mais antigos que utilizam o padrão SISO (*Single-Input Single-Output*) não se beneficiam das novas melhorias (CAÇADOR, 2014).

2.1.6 Padrão 802.11ac

O padrão 802.11ac representou uma significativa evolução nas redes Wi-Fi, trazendo melhorias na transferência de dados e eficiência das conexões sem fio. Operando na faixa de 5 GHz, evitou interferências e congestionamentos, garantindo um ambiente mais adequado para redes sem fio. Uma das principais inovações foi a tecnologia MU-MIMO,

permitindo o envio simultâneo de dados para vários dispositivos, melhorando o desempenho em ambientes movimentados. Além disso, sua compatibilidade com a frequência de 2,4 GHz e a taxa de transmissão de até 6930 Mbit/s trouxeram maior flexibilidade e velocidade para os usuários.

O 802.11ac tornou-se o padrão Wi-Fi mais avançado na época de sua homologação, impulsionando sua adoção em residências, empresas e espaços públicos. Embora tenha sido sucedido por padrões ainda mais avançados, como o 802.11ax (Wi-Fi 6) e 802.11ax (Wi-Fi 6E), o legado do 802.11ac deixou um impacto duradouro na busca contínua por redes Wi-Fi mais rápidas, seguras e eficientes (CAÇADOR, 2014).

2.1.7 Padrão 802.11ax

O IEEE 802.11ax foi lançado em maio de 2014 com o objetivo de melhorar a taxa de transferência por área em cenários de alta densidade e vem sendo chamado de Wi-Fi 6, representando a nova geração de Wi-Fi. O Wi-Fi 6 traz como vantagens maior rapidez, aumento de eficiência e melhores taxas na transferência de dados, além de possibilitar melhor comunicação com múltiplos dispositivos que realizam solicitações simultâneas de dados quando comparado às gerações anteriores do Wi-Fi.

O Wi-Fi 6 é capaz de atingir uma largura de banda de 1,2 gigabits por fluxo, sendo capaz de entregar até 8 fluxos por dispositivo e se conectar às frequências de 2.4GHz e 5GHz, além de usar OFDMA para aumentar a eficiência para uploads e downloads (SILVA, 2017). O Wi-Fi 6 apresenta várias melhorias que reforçam a segurança das redes Wi-Fi, ajudando a proteger contra ameaças e garantir a privacidade das comunicações. Trazendo suporte nativo ao WPA3 (Wi-Fi Protected Access 3), que é a versão mais recente do protocolo de segurança Wi-Fi, o WPA3 substitui o antigo WPA2 e oferece maior proteção contra ataques de força bruta, tornando mais difícil para os invasores obterem acesso não autorizado à rede.

Uma característica importante do Wi-Fi 6 é a capacidade de criar segmentos de rede virtuais, conhecidos como VLANs (Virtual LANs). Essa funcionalidade permite que diferentes dispositivos sejam isolados em redes separadas, melhorando a segurança ao evitar que dispositivos não autorizados acessem partes sensíveis da rede. O Wi-Fi 6 suporta métodos de autenticação mais fortes, como autenticação baseada em certificados. Isso torna mais difícil para invasores falsificarem a identidade de um dispositivo e ganharem acesso indevido à rede. Além das melhorias em segurança, o Wi-Fi 6 também oferece outros benefícios significativos, como maior velocidade, capacidade para suportar mais dispositivos simultaneamente e maior eficiência energética.

2.1.8 WLAN (*Wireless Local Area Network*)

Definido pelo IEEE (1997), as formas de os elementos se comunicarem e trocarem informações em uma infraestrutura WLAN podem ser várias em diferentes arquiteturas. As três principais formas para um enlace são:

- IBSS (*Independent Basic Service Set*), também referenciada com Ad-Hoc;
- BSS (*Basic Service Set*);
- ESS (*Extended Service Set*).

Para o enlace BSS, existe a necessidade de um equipamento concentrador, um ponto de acesso ou AP (*Access Point*). Também chamada de rede infraestruturada, os elementos móveis participantes dessa rede devem se conectar ao elemento AP que está em seu raio de alcance. Atuando como um elemento da camada 1 (Física) do modelo OSI, o AP é semelhante ao Hub em uma rede cabeada. Ele recebe o sinal de um dispositivo e propaga o sinal pelo espaço para todos os elementos de sua área de cobertura em busca do receptor. Essa característica já demonstra uma vulnerabilidade marcante dos ambientes Wi-Fi, pois cada um dos dispositivos participantes daquela rede pode receber a comunicação uns dos outros, mesmo não sendo o nó receptor da transmissão.

Na arquitetura BSS, o AP pode atuar como uma ponte (*bridge*) entre a rede LAN e a WLAN. Dessa forma, os equipamentos sem fio (Wi-Fi) e cabeados (Ethernet) podem se comunicar, formando uma mesma rede lógica. Um ponto de vulnerabilidade pode ser observado nessa ligação das redes cabeadas e das redes sem fio. Essa característica pode promover o acesso de um dispositivo sem fio à rede cabeada. Na arquitetura IBSS ou Ad-Hoc, os elementos participantes dessa rede se comunicam diretamente uns com os outros, não existindo a necessidade de um elemento concentrador, e os equipamentos devem estar na mesma área de cobertura de sinal entre eles. Esse tipo de comunicação é restrita a poucos equipamentos e normalmente é de uso doméstico.

As redes BSS são limitadas a um único elemento concentrador. Para resolver essa limitação, um enlace ESS estende o crescimento de uma WLAN por meio da ligação de várias BSS, possibilitando maior abrangência e área de cobertura. Nesse cenário de múltiplas BSS, o protocolo WDS (*Wireless Distribution System*) compartilha as informações entre os APs, possibilitando que os dispositivos troquem de BSS sem desconectar-se e permitindo a criação de várias células para atendimento de grandes áreas geográficas, tais como universidades, fábricas, parques, praças, shoppings e até pequenas cidades.

O conhecimento da topologia de uma WLAN é essencial para a estruturação das ações do teste proposto na etapa experimental da presente pesquisa. Scarfone et al. (2008b) define os dispositivos que compõem a topologia desse tipo de rede, suas funções na rede e limitações relacionadas às topologias existentes.

2.1.9 Mecanismos de autenticação, criptografia e integridade de dados para o padrão IEEE 802.11

A disseminação e o crescimento da demanda das redes locais sem fio aconteceram em diversos segmentos, como empresas, escritórios, residências, instituições de ensino, shoppings, praças e restaurantes. Essa expansão levou ao desenvolvimento do padrão 802.11-1997 original, passando por diversos processos evolutivos. Essas evoluções ocorreram tanto em relação à velocidade e largura de banda, quanto, principalmente, nos aspectos relacionados à segurança da informação (FENG, 2012).

Os mecanismos precursores da segurança do padrão IEEE 802.11-1997 se mostraram ineficientes e deficitários em relação aos processos de comunicação e conexão segura dos clientes e equipamentos às WLAN. Esse padrão inicial apresentava frágeis garantias aos preceitos básicos da segurança da informação (confidencialidade, integridade e disponibilidade) e aos usuários e equipamentos membros da rede sem fio (TEWS; BECK, 2009).

A partir da data de sua criação (1997) até 2004, os mecanismos de segurança fornecidos pelo protocolo de segurança WEP (*Wired Equivalent Privacy*) foram amplamente analisados e testados. Eles se mostraram com um grande número de vulnerabilidades, além de problemas significativos na segurança do padrão 802.11 em sua versão original de 1997. Dentre os principais problemas que podem ser destacados estão o tamanho das chaves criptográficas, o mecanismo de cifragem e checagem de dados ineficientes, a fragilidade no processo de autenticação e a manipulação dos quadros de controle.

Diante dessas preocupantes constatações, o protocolo WEP foi substituído pelo protocolo WPA (Wi-Fi Protected Access). O WPA, que significa Wi-Fi de Acesso Protegido, foi desenvolvido e publicado em 2003 pela Wi-Fi Alliance com o objetivo de aprimorar a segurança e corrigir as falhas apresentadas pelo WEP (SARI; KARAY et al., 2015).

Esse novo padrão foi lançado de forma emergencial, sendo considerado uma versão preliminar (rascunho) para o padrão oficial da IEEE, o IEEE 802.11i, popularmente conhecido como WPA2 (Wi-Fi Protected Access 2). No ano de 2004, o padrão oficial IEEE 802.11i / WPA2 foi finalizado, mantendo a compatibilidade com o WPA. Em 2007, o WPA foi incorporado à norma IEEE 802.11-2007, tornando-se a referência máxima para a segurança de redes WLAN. De acordo com o IEEE (2007), a nova arquitetura WPA2 consegue implementar autenticação, integridade e confidencialidade ao ambiente de rede e à comunicação de forma consistente e eficiente.

Com a evolução na proteção das WLAN, os mecanismos de segurança desenvolvidos e incorporados ao padrão 802.11 seguiram uma cronologia. A ligação entre os mecanismos de segurança fornecidos pelos protocolos (WEP, WPA/WPA2) e os preceitos fundamentais da segurança da informação busca garantir a confidencialidade, integridade e disponibilidade dos ativos da informação (pessoas, tecnologia, ambiente físico). O experimento realizado nesta pesquisa, em suas etapas iniciais, teve como objetivo detectar o tipo de mecanismo adotado pelas redes Wi-Fi pesquisadas, para determinar quais pontos

da segurança seriam testados e avaliados.

2.1.9.1 Mecanismos de autenticação padrão IEEE 802.11

Conforme o IEEE (1997), o padrão 802.11 especifica dois mecanismos de autenticação conhecidos como Autenticação Pre-RSN (Robust Security Network). São eles: Sistema Aberto (Open System Authentication) e Chave Compartilhada (Shared Key Authentication).

Na autenticação *Open System*, apenas uma autenticação/associação básica é necessária entre o ponto de acesso (AP) e os dispositivos clientes (STAs). O processo ocorre em três estágios para que os dispositivos possam se integrar ao canal de comunicação. Esse mecanismo é simples e não implementa nenhuma autenticação que solicite usuário e senha, criptografia ou controle de acesso. Nele, apenas frames de controle do cabeçalho 802.11 são trocados entre os dispositivos (LINHARES; GONÇALVES, 2009).

Para a autenticação *Shared Key*, o mecanismo de privacidade WEP (Wired Equivalent Privacy) deve ser obrigatoriamente implementado. Nas topologias WLAN infraestruturadas (BSS) do padrão 802.11, o primeiro estágio do processo de autenticação de uma estação cliente (STA) é descobrir a existência de uma rede disponível ou presente em seu raio de alcance. Essa descoberta da infraestrutura pode ocorrer de forma ativa ou passiva.

No modo passivo, o STA escuta os frames de gerenciamento (*Beacon*) enviados pelo ponto de acesso (AP), nos quais o AP anuncia sua existência e oferta de conexão. Já no modo ativo, o anúncio acontece de forma inversa, em que a estação envia aos canais os frames de gerenciamento (Probe Request) com o objetivo de receber do AP a resposta por meio de um frame (*Probe Response*).

O sucesso no processo de descoberta de uma infraestrutura leva ao segundo estágio, que é a autenticação da STA no AP. A STA envia um frame de gerenciamento para solicitar ao AP sua autenticação (*Authentication Request*). Ao receber essa mensagem, o AP envia sua resposta por meio de um frame (*Authentication Response*). No entanto, apenas a autenticação no AP não garante à estação a troca de dados na rede. O processo de autenticação bem-sucedido requer ainda o terceiro estágio, que é a Associação.

Como nos estágios anteriores, a associação também ocorre por meio de trocas de frames de gerenciamento. A estação autenticada envia frames de associação (*Association Request*) ao ponto de acesso, que responde de forma satisfatória ou não à STA com um pedido de associação (*Association Response*).

Com o cumprimento dos três estágios (Descoberta, Autenticação e Associação), a estação pode enviar e receber dados para as demais STAs que participam da mesma WLAN (BSS ou ESS). Uma representação gráfica dos três estágios possíveis de conexão de uma STA é apresentada. Em arquiteturas ESS, migrações (*roaming*) de estações de um AP para outro AP podem ocorrer. Essa migração está diretamente relacionada à qualidade e potência do sinal entre a STA e o AP.

Dado que uma STA pode se autenticar em vários APs, mas só pode estar associada a um AP por vez, um mecanismo de desassociação e reassociação é utilizado para essa movimentação. Frames de gerenciamento (*Disassociation Request / Reassociation Request*) são enviados pela STA para desassociar do antigo AP e se associar ao novo AP (CAÇADOR, 2014).

2.2 Protocolos de Segurança

Todas as atividades na Internet que envolvem duas ou mais entidades remotas comunicantes são governadas por um protocolo. Por exemplo, protocolos executados no hardware de dois computadores conectados fisicamente controlam o fluxo de bits no "cabo"entre as duas placas de interface de rede. Protocolos de controle de congestionamento em sistemas finais controlam a taxa com que os pacotes são transmitidos entre a origem e o destino. Além disso, protocolos em roteadores determinam o caminho de um pacote da origem ao destino (KUROSE; ROSS; ZUCCHI, 2007).

2.2.1 Protocolo WEP (*Wired Equivalent Privacy*)

O protocolo IEEE 802.11 WEP foi criado em 1997 para fornecer autenticação e criptografia de dados entre um hospedeiro e um ponto de acesso sem fio (ou seja, a estação-base) usando uma técnica de chave compartilhada simétrica. A WEP não especifica um algoritmo de gerenciamento de chave, então supomos que o hospedeiro e o ponto de acesso sem fio de alguma forma concordam sobre a chave através de um método fora da banda (KUROSE; ROSS; ZUCCHI, 2007).

O WEP trabalha com chaves simétricas, o que significa que a mesma chave é sempre usada para criptografar e descriptografar as informações que serão transmitidas na rede. No entanto, o WEP apresenta uma série de problemas e sua incapacidade de garantir a confidencialidade dos dados foi comprovada em um estudo (FLUHRER; MANTIN; SHAMIR, 2001). O WEP pode ser quebrado por meio de ataques probabilísticos, que foram otimizados em diversos programas específicos, como o software *WEPCrack* e *Airsnort*. Para realizar o ataque, o invasor precisa capturar alguns milhares de pacotes e executar análises usando o software para obter o segredo compartilhado. Em resumo, o WEP não oferece um nível adequado de segurança e pode ser facilmente comprometido por meio desses ataques.

2.2.2 Protocolo WPA (Wi-Fi *Protected Access*)

Para corrigir as vulnerabilidades apontadas no WEP, foi criado o WPA, um protocolo de criptografia mais robusto do que o anterior. O foco da criação do WPA era manter a compatibilidade com o WEP, mas ampliando suas características de segurança. Além

de fornecer criptografia de dados forte para corrigir os pontos fracos do WEP, o WPA também adiciona autenticação do usuário, que estava ausente no WEP (ALLIANCE, 2003).

Com o WPA, foi apresentada uma nova tecnologia de chave denominada TKIP (Temporal Key Integrity Protocol), na qual a chave de criptografia é trocada periodicamente. A autenticação é realizada por meio de trocas de chaves dinâmicas, o que previne ataques de retransmissão de pacotes. Apesar dessas melhorias em relação ao WEP, ainda é possível realizar um ataque de força bruta se um atacante obtiver os quadros trocados durante o processo de autenticação (FLEISHMAN; MOSKOWITZ, 2003).

o número de vulnerabilidades exploráveis ainda é considerável para redes que adotam o WPA como medida de segurança. Alguns dos principais pontos de falhas incluem:

- Ataque de Dicionário em Senhas PSK: Neste tipo de ataque, o invasor utiliza um dicionário pré-construído de palavras e frases para tentar descobrir a chave PSK, assumindo que ela esteja presente no dicionário. Se a chave PSK for derivada de palavras comuns, há uma boa chance de sucesso nesse tipo de ataque.

- Captura de informações durante a autenticação de handshake de 4 vias: O processo de autenticação de quatro vias envolve a troca de informações em texto não criptografado, o que pode ser capturado e utilizado em ataques de dicionário e processos de cracking PSK.

- Possibilidade de Negação de Serviço após a detecção de erros de MIC: O mecanismo de detecção de erros WPA pode levar a uma Negação de Serviço quando dois ou mais erros de pacote são detectados em menos de um minuto. Isso pode ser explorado por um invasor para gerar pacotes maliciosos e causar múltiplas desconexões, resultando em interrupção do serviço.

- Vulnerabilidades no algoritmo de Michael e no TKIP: Pesquisas revelaram vulnerabilidades no algoritmo de Michael, responsável pela integridade dos dados, e no TKIP, que lida com a criptografia de dados. Isso pode permitir a um invasor descriptografar pacotes e realizar ataques de *Man In The Middle* (MITM), nos quais os hackers podem roubar informações da rede.

- Falta de proteção contra estruturas de gerenciamento e negação de serviço: O WPA não fornece proteção ou criptografia para quadros de gerenciamento e controle, deixando a rede vulnerável a ataques similares aos problemas encontrados no WEP.

Devido a essas vulnerabilidades, é sempre recomendado que as redes avancem para protocolos mais seguros, como o WPA2 ou o mais recente WPA3, para garantir uma melhor proteção contra ameaças de segurança.

2.2.3 Protocolo WPA2 (Wi-Fi *Protected Access2*)

O protocolo WPA2 foi desenvolvido para oferecer um nível de segurança ainda maior do que o padrão WPA, e para isso, substituiu o método criptográfico utilizado no WPA (STANGARLIN; FILHO, 2017). O WPA2 introduz um novo algoritmo criptográfico que é considerado completamente seguro, porém, isso pode resultar em incompatibilidade com algumas interfaces de rede mais antigas. Apesar desse inconveniente, o WPA2 é amplamente considerado o padrão de segurança Wi-Fi mais seguro, pois apresenta componentes cruciais para a segurança da rede sem fio, como autenticação, cifragem e integridade (KUMAR; GAMBHIR, 2014).

Apesar de ser considerado o padrão de segurança mais seguro, o WPA2 não está livre de falhas. Uma vulnerabilidade conhecida como KRACK (Key Reinstallation Attacks) foi descoberta e afetou quase todas as redes wireless. Esse ataque consiste em enganar a criptografia da rede, permitindo que os dados sejam interceptados pelo atacante. Felizmente, para que esse tipo de ataque aconteça, o atacante deve estar dentro do alcance da rede, o que torna o cenário um pouco menos provável em determinadas ocasiões (VANHOEF; PIESSENS, 2017). No entanto, é importante estar ciente dessas vulnerabilidades e tomar medidas para mitigar os riscos. Manter o software e firmware atualizados e implementar medidas de segurança adicionais, como o uso de VPNs (Redes Privadas Virtuais) em redes públicas, pode ajudar a proteger as redes wireless contra possíveis ataques. O monitoramento contínuo e a adoção de boas práticas de segurança são fundamentais para garantir a segurança das redes wireless.

O WPA2 é considerado o padrão de segurança Wi-Fi mais seguro. No entanto, esse sistema ainda apresenta algumas vulnerabilidades que podem ser exploradas. São elas:

- Ataques de dicionário para Passphrase PSK: As possibilidades de exploração da Passphrase PSK no WPA2 por meio de ataque de dicionário continuam presentes, assim como no WPA.

- Falsificação de endereços e dados no uso do GTK (Group Temporal Key): Para STAs já autenticadas na rede, é possível explorar uma deficiência na especificação de segurança do WPA2. A norma 802.11-2007 não fornece suporte para chave pairwise contra falsificação de endereços e dados forjados no GTK. Ou seja, um usuário Insider (usuário interno mal intencionado), que tenha sido autenticado e seja membro da rede, pode falsificar mensagens multicast protegidas pela chave GTK one-way. O ataque chamado de Hole 1965 explora essa falha e permite falsificação de ARP (ARP Spoofing). Assim, um ataque MITM entre as STAs, o Insider e o AP pode capturar todo o tráfego das estações.

- Falta de proteção dos quadros de gerenciamento e negação de serviço: A estrutura de segurança do WPA2 também não prevê nenhum mecanismo de proteção dos frames

de gestão como no WPA. Os mesmos tipos de problemas do WEP e WPA estão presentes aqui.

- Ataques de negação de serviço (DoS): Como no WEP e WPA, os ataques de DoS por injeção de frames forjados dos tipos *De-Authentication*, *Disassociation*, *Beacon*, entre outros, ainda persistem, permanecendo como um ponto fraco do WPA2.

- Interferência por radiofrequência (*Jamming*): Essa vulnerabilidade está associada diretamente à camada 1 (física), onde um ou mais rádios emitem sinal de mesma frequência com potência alta. Essa interferência causa uma negação de serviço nos APs próximos ao atacante. O *jamming* é um ataque simples e de grande impacto na rede. Quando bem-sucedido, consegue poluir o espectro de frequência consumindo toda a banda de rede WLAN. Como os mecanismos WEP, WPA e WPA2 atuam na camada 2 (link de dados), os mecanismos de segurança são ineficazes a essa vulnerabilidade.

2.2.4 Protocolo WPA3 (Wi-Fi *Protected Access3*)

Após o ataque KRACK (*Key Reinstallation AttaCK*) no WPA2 no outono de 2017, a Wi-Fi Alliance começou a desenvolver o WPA3, que foi anunciado em 2018. O WPA3 é uma certificação que adiciona mecanismos de proteção ao seu antecessor, o WPA2. Ele oferece resistência a ataques de dicionário, proteção dos quadros de gerenciamento e sigilo de encaminhamento (LOUNIS; ZULKERNINE, 2019).

O WPA3 oferece uma conectividade mais fácil para dispositivos que não possuem uma configuração de interface visual, devido à expansão da IoT e dispositivos modernos que permitem a conexão com Wi-Fi. Este é o protocolo mais avançado para proteger as redes. Uma das principais melhorias de segurança é a proteção contra ataques de dicionário, que representavam um grande problema para redes que utilizavam o WPA e o WPA2. O ataque de dicionário consistia em adivinhar a senha, onde o invasor tentava diversas combinações de frases ou palavras para acertar a senha, já que o WPA e o WPA2 permitiam múltiplas tentativas de inserção de senha. Além disso, o novo protocolo adiciona criptografia para a troca de dados, mesmo em redes sem proteção por senha.

2.2.5 Protocolo WPS

O WPS é um programa de certificação opcional, projetado para facilitar a tarefa de instalar e configurar a segurança em redes locais sem fio (VIEHBÖCK, 2011). Introduzido no início de 2007, o programa fornece um conjunto de soluções de configuração de rede. A principal e única vantagem do uso desse recurso é a eliminação da necessidade de utilizar e memorizar senhas. O WPS pode ser implementado nos roteadores de três formas diferentes:

- PIN: Neste método, um número de identificação pessoal (*Personal Identification Number* - PIN) é configurado no concentrador e utilizado no momento da conexão inicial. Esse número é, em muitos casos, informado em uma etiqueta colada ao concentrador. A autenticação via PIN no WPS é feita através da troca de mensagens entre o cliente e o concentrador sem fio. Nessa fase, são trocadas oito mensagens.

- Botão WPS: Neste método, o usuário tem que pressionar um botão (físico ou lógico) no concentrador e iniciar a procura no cliente. Alguns clientes podem vir com um botão WPS também.

- NFC (*Near Field Communication*): Funciona por uma aproximação mínima de 10 centímetros de distância entre os dispositivos. Pelo fato da transmissão de informações via NFC ser instantânea, não é necessária a inserção de senhas ou códigos de acesso. O contato entre os dois dispositivos deve ser bastante próximo para evitar o envio ou recebimento acidental de dados. Após posicionados bem próximos, a conexão é estabelecida.

De fato, o WPS é considerado uma técnica de autenticação fraca, pois tem sido alvo de diversos ataques bem-sucedidos ao longo do tempo. Um sistema que utilize a autenticação WPS por meio de PIN pode ser facilmente quebrado por um ataque de força bruta, mesmo que esteja sendo usado em conjunto com os padrões WPA ou WPA2 e uma senha forte (SILVA, 2014). Dessa forma, uma das melhores opções para garantir a segurança das redes sem fio é desabilitar a função WPS nos roteadores. Isso ajuda a evitar possíveis vulnerabilidades e protege a rede contra ataques que exploram essa falha de segurança. Além disso, é importante manter sempre atualizado o firmware do roteador e adotar outras práticas de segurança, como o uso de senhas fortes e a troca periódica das mesmas.

2.3 Classificação de ataques as redes WLAN (*Wireless Local Area Network)*

De acordo com o IEEE (1997), o padrão 802.11 trabalha nas camadas 1 e 2 do modelo OSI, identificadas respectivamente como camadas Física (PHY) e camada de Enlace (*Data Link*), sendo a segunda especificamente na subcamada MAC (controle de acesso ao meio). Devido a essas características específicas, esse protocolo apresenta ameaças e vulnerabilidades particulares.

Pesquisadores seguem diferentes abordagens para classificar e tipificar os ataques: Uma primeira linha de pesquisadores agrupa os ataques de acordo com sua natureza e características fundamentais de exploração das vulnerabilidades. Isso inclui ataques aos mecanismos criptográficos, ataques de negação de serviço, ataques de APs falsos, ataques de escuta de rede, ataques de injeção de pacotes, ataques de interferência em radiofrequência

e ataques de engenharia social. A segunda linha busca classificar a exploração dos ataques alinhada aos pilares da segurança da informação, que são: ataques contra confidencialidade, ataques contra integridade, ataques contra disponibilidade, ataques contra controle de acesso e ataques contra autenticação. Dessa forma, os ataques são agrupados de acordo com o aspecto específico da segurança da informação que eles visam comprometer. Essa abordagem permite uma compreensão mais abrangente das vulnerabilidades e riscos associados ao protocolo 802.11. Ama terceira linha de classificação divide os ataques em duas categorias com base nas ações do atacante na rede: ataques passivos e ataques ativos. Segundo Milliken (2012), essa gama de ataques pode ser agrupada em três macrocategorias: ataques aos mecanismos criptográficos e de autenticação (*Encryption Bypass attacks*), ataques de negação de serviço (*Denial of Service attacks*) e ataques de falsificação de APs (*AP Masquerading attacks* ou *Rogue Access point attacks* - RAP). Outro estudo realizado por Liu (2007) também apresenta duas macrocategorias de tipos de ataques nas WLAN: os *Crypt Attacks* e os *DoS Attacks*. Essas diferentes classificações permitem uma análise mais abrangente das ameaças e vulnerabilidades que podem afetar as redes sem fio e auxiliam na definição de estratégias de segurança mais eficazes.

As principais ameaças e ataques em redes sem fio incluem escaneamento e quebra de senha, ataques do tipo MITM (*Man In The Middle*) e captura de pacotes (*Sniffing*), utilização de pontos de acesso falsos (*Rogue Access Point - RAP*), ataques de negação de serviço (*Denial of Service - DoS*) e, por fim, a própria engenharia social (*Social Engineering*). Esses ataques podem ser categorizados de acordo com a *CIA triad* (Confidencialidade, Integridade e Disponibilidade), bem como incluindo os aspectos de Controle de Acesso e Autenticação. A compreensão dessas ameaças é essencial para a implementação de medidas efetivas de segurança em redes Wi-Fi:

- Ataques à Confidencialidade (*Confidentiality Attacks*): Esses ataques visam violar os controles que garantem o sigilo das informações, permitindo que pessoas não autorizadas interceptem dados enviados em texto claro ou criptografados.

- Ataques à Integridade (*Integrity Attacks*): Nesse tipo de ataque, o objetivo é contornar os controles que asseguram a integridade dos dados, ou seja, garantir que os dados não sejam modificados, apagados ou adicionados de maneira não autorizada. Isso pode causar erros ou facilitar outros tipos de ataques.

- Ataques à Disponibilidade (*Availability Attacks*): Os ataques de disponibilidade têm como alvo os controles que garantem o acesso total a dados ou recursos por sistemas ou usuários autorizados. Os atacantes buscam degradar ou negar o acesso aos recursos da WLAN para usuários autorizados ou forçá-los a desconectar voluntariamente.

- Ataques ao Controle de Acesso (*Access Control Attacks*): Nesse tipo de ataque, os atacantes tentam burlar os controles, filtros e ferramentas que garantem o acesso

à rede. Isso pode incluir a falsificação de endereços de um usuário autorizado na WLAN.

- Ataques à Autenticação (*Authentication Attacks*): Os ataques à autenticação têm como objetivo burlar os controles implementados para validar a identidade de usuários, como senhas ou credenciais. Os atacantes procuram descobrir, roubar ou falsificar as credenciais de um usuário autorizado da WLAN.

A diversidade de classificações e métodos de ataques é possível nas redes 802.11. Alguns autores classificam os ataques de acordo com o foco (Criptografia, Negação de Serviço ou AP Falso), enquanto outros os agrupam por manipulação da rede (Passivo ou Ativo). Os ataques são organizados em relação às possíveis perdas dessas garantias, como sintetizado na Tabela 2.3:

Categoria do Ataque	**Método do Ataque**	**Descrição do método de Ataque**
Ataques a Confidencialidade	*Eavesdropping*	Captura e decodificação do tráfego para obter informações confidenciais
	WEP Key Cracking	Captura de frames WEP para descoberta da chave
	AP Phinsing	Criação um AP malicioso para roubo de credenciais de acesso
	Man-in-the-Middle	Ataques para interceptar as conexões dos usuários e ter acesso ao conteúdo trafegado
	Evil Twin AP	AP malicioso configurado com mesmo SSID para enganar usuários da rede
Ataques a Integridade	Session Hijacking	Tomada de uma sessão autenticada e autorizada de um usuário legítimoda rede
	802.11 Frame Injection	Forjar quadro 802.11 e envia na rede com o objetivo de ganhar acesso ou manipular ações dos componentes darede
	EAP Injection	Forjar quadro 802.1X/EAP e envia na rede com o objetivo de ganhar acesso ou manipular ações dos componentes da rede
	Response Poisoning	Interceptação e manipulação de pacotes forjados para usar contra AP, STA‘s ou servidor RADIUS
	ARP Replay	Forçar alteração da tabela ARP do AP ou das STA‘s da rede
	RF Jamming	Congestiona a frequência WLAN com um sinal de rádio mais forte

Ataques a Disponibilidade	*Beacon Flood*	Dificultar para as STAs a descoberta do AP legítimo por meio da geração excessiva de Frames Beacon
	Deauth Flood	Envio de pacotes de de-autenticação para um STA ou toda rede forçando as STA a saírem da rede
	DoS Frame Controls	Envio de um grande número de quadros de controle na rede gerando congestionamentos
	Fake SSID	Envio para rede grande quantidade de quadros SSID falsos dificultando o acesso das STA‘s
	EAP of Death	Envio de uma resposta 802.1X EAP de identificação incorreta levando a paralisação do AP
Ataques ao Controle de Acesso	*MAC Spoofing*	Modificação do Endereço MAC para burlar o controle por MAC
	Fake Auth	Associação à rede sem o estágio de autenticação
	WarDriving	Busca de informações da rede de foram geral (SSID, Probe Request, Security Method)
	Rogue AP	Ativação de um AP malicioso para roubo de credencias de acesso de usuários legítimos
Ataques a Autenticação	*Shared Key Guessing*	Descoberta da chave compartilhada WEP
	802.1X Identity Theft	Captura dos pacotes de resposta de identidade 802.1X. E ataque de força bruta para recuperar as identidades dos usuários
	PSK Cracking	Captura do frame 4 way handshake WPA-PSK e ataque de dicionário recuperar a chave WPA-PSK
	WEP Cracking	Criptoanálise e descoberta do protocolo WEP
	LEAP Cracking	Captura de quadros 802.1X/LEAP, e ataque de dicionário, a fim de recuperar as credenciais do usuário
	Password Capture	Repetidas tentativas de adivinhar a senha utilizando a identidade do usuário capturado
	VPN Login Cracking	Ataque de Força Bruta sobre o protocolo de autenticação VPN como o protocolo PPTP (point to point tunnelling protocol)

Categorias e métodos de ataque contra 802.11.

Waliullah e Gan (2014) classifica os ataques em dois tipos: ataques passivos e ataques ativos. Nos ataques passivos, um atacante tenta obter informações da rede apenas observando/coletando o tráfego que passa pela WLAN. Nesse tipo, o invasor não produz nem modifica dados da rede. Os dois tipos mais comuns são:

- Análise de Trafego (*Traffic Analysis*);
- Espionagem (*Eavesdropping*).

Já nos ataques ativos, o invasor escuta, gera e modifica informações/dados da rede atacada. Uma quantidade maior de ataques se enquadra nessa classificação, como:

- Negação de Serviço (*Denial of Service*);
- Injeção de Pacote (*Replay Attack*);
- Sequestro de Sessão (*Session Highjacking*);
- Pontos de Acesso Maliciosos (*Rogue Access Point*);
- Intermediação de conexão (*Main in the Middle*);
- Acesso não Autorizado (*Unauthorized Access*).

2.4 Ataques de Negação de Serviço

Diversos são os problemas, procedimentos e métodos aplicados aos ataques de negação de serviço em redes Wi-Fi. Os ataques de negação são divididos em quatro tipos de ataque, relacionando-os às camadas da arquitetura TCP/IP. Os quatro tipos são: ataques à camada de aplicação, ataques à camada de rede e transporte, ataques à camada MAC e ataques à camada física (SHARMA; BARWAL; NOIDA, 2014).

Em redes 802.11, os ataques DoS têm seu foco de ação nas camadas física e na subcamada MAC do nível de enlace. Na subcamada MAC, o endereçamento da placa de rede (MAC Address) é uma informação vital para o processo de comunicação e gerenciamento dos dispositivos e APs que participam da WLAN. Há uma confiança grande na integridade do endereço MAC de origem. Esses endereços MAC são tratados como identificadores únicos, utilizados para distinguir um dispositivo do outro. No entanto, não há nenhum mecanismo de validação desses endereços. Um invasor pode clonar o endereço de qualquer cliente ou AP facilmente.

Um atacante pode transmitir pacotes usando um endereço MAC de origem clonado de um AP. O destinatário desses quadros falsificados não tem nenhum meio de identificar se

os pacotes possuem endereço MAC legítimo ou forjado. Essa capacidade de enviar quadros de gerenciamento falsificados possibilita a realização de diversos ataques de negação na subcamada MAC.

Dois desses ataques à subcamada MAC são os ataques de inundação de autenticação/associação (*Authentication/Association flood attack*) e os ataques de inundação de desautenticação/desassociação (*Deauthentication/Disassociation flood attacks*) (COMPTON; HORNAT, 2007).

Durante um ataque de inundação de autenticação/associação, um atacante usa um endereço MAC falso para realizar repetidas tentativas de autenticação/associação com um AP de destino. O atacante visa exaurir a capacidade de memória e processamento do AP, deixando os clientes com pouca ou nenhuma chance de conexão com a rede Wi-Fi. Os ataques de negação de serviço aplicados à camada física de redes sem fio buscam causar obstrução e interferência nas frequências de transmissão. Os ataques de interferência (*Jamming Attacks*) são aplicados e discutidos há muitos anos, desde a Segunda Guerra Mundial. O congestionamento de uma rede WLAN com sinais de ruído pode degradar o rendimento da rede. A interferência com outros transmissores de rádio que utilizam a mesma frequência e potência maior pode prejudicar o desempenho de uma rede Wi-Fi (SHARMA; BARWAL; NOIDA, 2014).

Demonstrou-se nas pesquisas e literaturas que a implementação de mecanismos de proteção dos quadros de controle e gerenciamento ainda é um problema grave para a segurança do padrão 802.11. Apesar de a emenda 802.11w de 2009 ter implementado essas melhorias no padrão, somente em 2014 a Wi-Fi Alliance passou a certificar produtos com as especificações de segurança PMF (*Protected Management Frames*). Até 2015, apenas quatro produtos indicados no site da Wi-Fi Alliance haviam obtido o certificado. Os trabalhos pesquisados nesse tópico discutiram a efetividade dos ataques de Negação de Serviço às WLAN e os severos danos à rede causados por esses ataques.

2.5 Ataques de AP falso

Com base nas pesquisas e literatura disponível, constatou-se que a implementação de mecanismos de proteção para os quadros de controle e gerenciamento ainda é uma questão crítica para a segurança do padrão 802.11. Embora a emenda 802.11w de 2009 tenha incorporado melhorias nesse sentido, somente em 2014 a Wi-Fi Alliance começou a certificar produtos com as especificações de segurança PMF (*Protected Management Frames*). Até 2015, apenas quatro produtos listados no site da Wi-Fi Alliance haviam obtido essa certificação. As pesquisas abordadas nesse tópico discutiram a efetividade dos ataques de Negação de Serviço às WLAN e os graves danos causados por esses ataques à rede.

Os APs maliciosos podem ser divididos em dois grupos principais: os *Fake Access*

Point e os *Rogue Access Point*. O Fake AP é criado ou instalado por um atacante mal-intencionado que não faz parte do grupo de usuários da rede. Seu principal objetivo é realizar ataques MITM e DoS para roubo de informações e espionagem. Por outro lado, os Rogue APs podem ter caráter malicioso ou serem implementados por um usuário da própria rede que deseja conectar uma rede Wi-Fi própria à rede cabeada da empresa/instituição. Essa conexão é feita com o objetivo de utilizar os recursos e infraestrutura já disponíveis na rede local (LAN), conforme ilustrado na figura 2 (COMPTON; HORNAT, 2007).

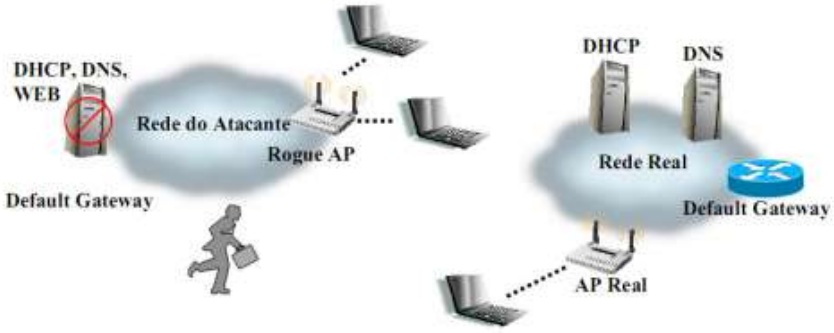


Figura 2 – Ataque com Rogue AP

Atacar uma STA (cliente da rede) para obter informações ou acesso às credenciais da rede Wi-Fi, em alguns casos, pode ser possível e até mais simples do que atacar o AP ou servidor de autenticação. Essa facilidade é proporcionada por meio da manipulação ou implementação de APs maliciosos, o que facilita bastante essas ações. Apenas uma STA era avaliada quanto à possibilidade de se associar ao AP malicioso, e nenhum dado do usuário ou da STA era registrado ou armazenado.

Ma et al. (2007) propõem uma taxonomia para os tipos de ataques explorados pelos Rogue APs. Essa taxonomia divide os APs falsos em quatro classes: *Improperly Configured AP*, *Unauthorized AP*, *Phishing AP* e *Compromised AP*. A tabela 3 apresenta a síntese da taxonomia com as quatro classes de Rogue AP e possíveis cenários para ataques.

Uma nova forma de ativação para um Rogue AP foi descoberta, denominada SRAP (*Smartphone Rogue AP*). Essa forma consiste em instalar e configurar de forma maliciosa um Rogue AP (RAP) em um Smartphone com o Sistema Operacional (SO) Android. Seu caráter malicioso é potencializado pela facilidade de implementação e pela grande quantidade de dispositivos que utilizam esse SO.

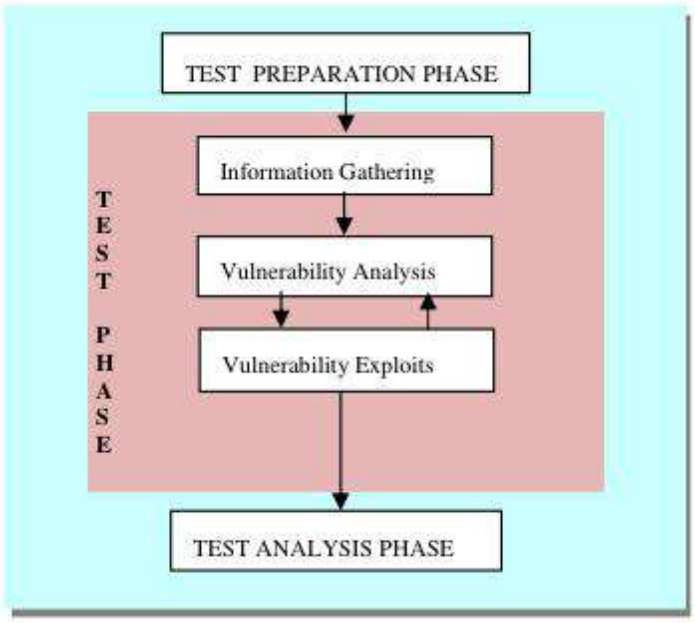
Classes de AP falsos	**Possíveis cenários para ataques**
Configuração equivocada	Insuficiente conhecimento de segurança; Configuração errada; Equipamentos defeituosos ou desatualizados
Não autorizado	Conexão a rede local (LAN) sem autorização; AP de redes vizinhas
Malicioso	Conexão maliciosa para captura de dados
Comprometido	Credenciais de acesso divulgadas

Tabela 3 – Taxonomia dos Rogue AP's

2.6 Teste de penetração (*Pentesting*)

Os testes de penetração, também conhecidos como pentesting, são um conjunto de atividades realizadas para identificar e explorar falhas e vulnerabilidades de segurança. Essas atividades ajudam a medir o nível de robustez e a segurança implementada no sistema. A metodologia do teste de penetração, ilustrada na figura 3, inclui três fases: preparação da avaliação, testes e análise de teste. A fase de teste engloba as seguintes etapas: coleta de informações, análise de vulnerabilidade e exploração de vulnerabilidade (BACUDIO et al., 2011).

Figura 3 – Fases de um teste de penetração



Fonte - (BACUDIO et al., 2011)

As técnicas de teste de penetração são um processo eficiente e amplamente utilizado em redes que já estejam em produção ou que desejam passar por uma avaliação ou auditoria, com o objetivo de identificar riscos e criar um guia para melhorar a segurança nessas redes. O executor do teste de penetração, conhecido como pentester ou *Ethical Hacker*,

pode identificar os problemas em um ambiente já em produção. Por meio desse tipo de teste, busca-se evidenciar as falhas e vulnerabilidades que poderiam ser exploradas por possíveis invasores maliciosos (Hackers) (WEIDMAN, 2014).

As estratégias do teste de penetração podem ser divididas em três categorias: Teste Caixa Preta (*Black Box*), Teste Caixa Branca (*White Box*) e Teste Caixa Cinza (*Grey Box*). Todas essas estratégias estão relacionadas à quantidade de informações prévias recebidas pelo pentester (FIGUEIREDO et al., 2020). No teste Caixa Preta, o avaliador não recebe qualquer tipo de informação sobre o ambiente a ser analisado. O objetivo é colocar o pentester em condições reais, onde ele deve agir como um atacante externo, sem nenhum conhecimento prévio da rede, e tentar encontrar uma forma de invasão.

No teste Caixa Branca, o avaliador recebe uma grande quantidade de informações sobre o ambiente a ser analisado. Nessa estratégia, o foco é simular um ataque interno, em que o atacante tem conhecimento sobre a rede, sistemas e pessoas. Essa metodologia é muito aplicada em testes específicos para uma aplicação, sistema Web, banco de dados ou rede.

No teste Caixa Cinza, o avaliador recebe certo nível de informação sobre o ambiente, informações que possivelmente são públicas ou fáceis de conseguir. Essas informações são passadas ao pesquisador com o objetivo de ganhar tempo na avaliação. O teste de intrusão não está totalmente no escuro, mas também não tem todas as informações necessárias. Durante sua avaliação, muitos pontos precisam ser descobertos. O teste Caixa Cinza pode ser tratado como um modelo intermediário entre o teste Caixa Branca e o teste Caixa Preta. Em redes Wi-Fi, a informação do nome da rede (ESSID) ou uma senha WPA/WPA2 pública podem facilitar bastante um teste de penetração. Manuais e frameworks consistentes e revisados por pares podem auxiliar na aplicação de teste de penetração efetivo e com resultados coerentes.

Algumas opções, como ISSAF (*Information System Security Assessment Framework*) e OSSTMM (*Open Source Security Testing Methodology Manual*), fornecem orientações sobre as etapas necessárias para realizar um completo teste de penetração. Para a realização de testes de penetração em redes Wi-Fi, existem muitas ferramentas de software, sistemas operacionais e hardware de grande capacidade e potência. Sistemas operacionais como Kali Linux e Backbox Linux são completas suítes de ferramentas e softwares para pentest que auxiliam muito nos procedimentos e nas etapas de um teste de penetração. Todos esses recursos possibilitam uma avaliação muito apurada e precisa dos riscos e ameaças que podem afetar essas redes, auxiliando na tomada de decisões para novos controles de segurança mais eficientes e robustos.

3 Trabalhos Relacionados

Nesta seção, abordaremos os trabalhos relacionados ao tema encontrados na literatura, especificamente sobre a exploração da vulnerabilidade do WPS. No entanto, o objetivo da monografia é investigar a infraestrutura de redes domésticas nesse problema, mas infelizmente, não há estatísticas disponíveis sobre a quantidade de aparelhos que utilizam o WPS. Portanto, os trabalhos foram divididos em duas categorias: aqueles que exploram a vulnerabilidade do WPS e aqueles que exploram vulnerabilidades em outros protocolos, como WPA e WPA2.

3.1 Trabalhos que utilizam o WPS para exploração de Vulnerabilidades

Em Lindell e Lagerholm (2019), investiga a razão que torna o WPS um método inseguro, levantando questionamentos sobre sua adequação para uso em redes corporativas. O trabalho aborda fraquezas e riscos de segurança, porém não explora outras informações importantes, como possíveis melhorias na tecnologia. Além disso, não há orientações sobre como os usuários podem se proteger contra esses ataques, o que também é crucial para a segurança da rede.

No artigo (NIKOLOV, 2018), são realizadas avaliações e ataques de vulnerabilidades. Dois tipos de ataques foram conduzidos nesta pesquisa: um envolvendo a quebra da senha WPA2 e outro atacando roteadores com WPS ativado, explorando a troca de PIN. O artigo descreve um modelo de senhas com maior nível de segurança, adequado para usuários comuns. Durante os experimentos, foram encontradas senhas que demandariam tempo infinito para serem quebradas por meio de métodos de força bruta, essas senhas eram compostas de letras aleatórias, números e símbolos especiais.

Já em Valchanov, Edikyan e Aleksieva (2019), é apresentada uma metodologia e pesquisa realizada na cidade de Varna, a terceira maior cidade da Bulgária, utilizando o método de *WarDriving* para coleta de informações. O principal objetivo era avaliar o nível atual de segurança em Varna. Os dados coletados incluem informações de um total de 19136 redes, e os resultados obtidos foram analisados de forma sistemática, revelando que 53% das redes possuíam o WPS ativado.

3.2 Trabalhos que exploram vulnerabilidades em WPA e WPA2

Em Kohlios e Hayajneh (2018), é realizado um levantamento de todos os ataques disponíveis em uma rede Wi-Fi usando WPA2 de maneira organizada. O objetivo é fornecer

informações abrangentes que reiterem pontos-chave para uma melhor compreensão dos esquemas de criptografia. O estudo conclui que o WPA2 permite que as informações do sistema, conhecidas como frames de gerenciamento, sejam enviadas em pacotes de texto simples do cliente para o ponto de acesso. Essa vulnerabilidade possibilita que um adversário falsifique os pacotes para que pareçam vir do cliente alvo, realizando ataques como a desautenticação. O artigo também aborda o *Krack Attack*, um processo que explora o handshake de quatro vias que os protocolos de segurança sem fio usam para autenticar seus usuários ao se conectar à rede.

No artigo (KISSI; ASANTE, 2020), uma metodologia diferente é adotada, com a aplicação de testes em um laboratório de rede experimental. O estudo considerou a utilização do laboratório da rede de forma a não comprometer nenhuma rede individual ou organizacional, levando em conta a privacidade e legalidade das informações do usuário. O objetivo é realizar testes de penetração para avaliar vulnerabilidades e conduzir ataques em redes sem fio. São feitos testes de ataque ativo, em que o invasor não apenas obtém acesso a informações, mas também faz alterações nas informações da rede e até mesmo injeta pacotes fraudulentos na rede. Dessa forma, o atacante pode iniciar comandos para interromper as operações usuais da rede, como negação de serviço (DoS), sequestro de sessão, ataque de força bruta e ataque de resposta.

No trabalho de Soares e Moraes (2019), é realizada uma pesquisa para avaliar os mecanismos de segurança, efetuando experimentos de ataques ativos, como o de dicionário e força bruta, para obtenção das senhas das redes. A vulnerabilidade *Krack Attack* também é explorada com o objetivo de verificar se os dispositivos com Wi-Fi estão vulneráveis. Os resultados mostram que 31,6% das redes analisadas foram invadidas por meio de força bruta. Já na exploração do *Krack Attack*, quase 50% das redes estão propensas a sofrer ataques. O estudo destaca a importância de manter sempre os dispositivos de redes atualizados, além de utilizar senhas bem elaboradas e seguir boas práticas de segurança por parte dos usuários.

4 Desenvolvimento do Trabalho

Neste capítulo, descrevemos o desenvolvimento do presente trabalho e os equipamentos utilizados para conduzi-lo. Para realizar as tarefas, foram utilizados o software Aircrack-NG [aircrack-ng.org] no sistema Ubuntu e o aplicativo WiGLE-Wifi [wigle.net] no aparelho celular. O estudo foi conduzido através das seguintes fases: projeto de um sistema de digitalização, coleta de dados, análise de dados e comparação dos resultados.

A varredura em Valença do Piauí foi realizada começando no bairro Lavanderia e terminando no mesmo ponto, com um trajeto de retorno que totalizou aproximadamente 3 km de deslocamento. A área de análise selecionada abrange a parte central de Valença do Piauí, incluindo muitas empresas e parte dos moradores. Para monitorar e controlar o processo em tempo real, foram utilizados recursos adequados. A Figura 4 mostra a distribuição desses pontos de acesso sobrepostos ao mapa da cidade de Valença do Piauí disponibilizado pelo Google Earth [Google].

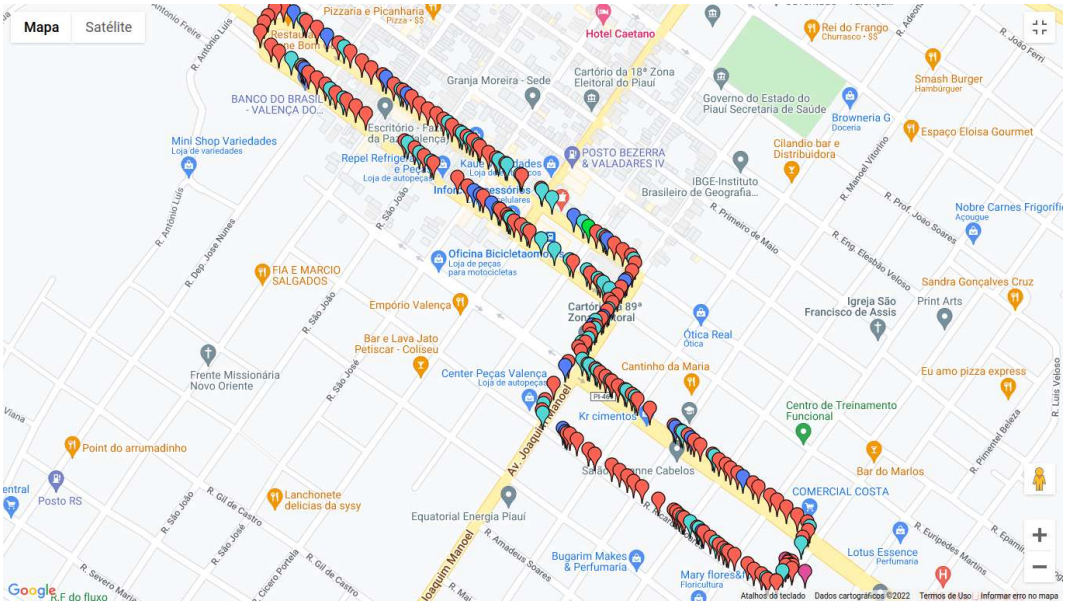


Figura 4 – Distribuição de pontos de acesso na zona comercial da cidade de Valença do Piauí

A varredura em Picos começou no bairro Centro e terminando no mesmo ponto, com um trajeto de retorno que totalizou aproximadamente 1 km de deslocamento. A área de análise selecionada abrange a parte central da cidade. O deslocamento pela área foi feito de carro, mantendo uma velocidade sustentada entre 0 e 35 km/h, com monitoramento e controle do processo em tempo real. A Figura 5 mostra a distribuição desses pontos de acesso sobrepostos ao mapa da cidade de Picos disponibilizado pelo Google Earth [Google].

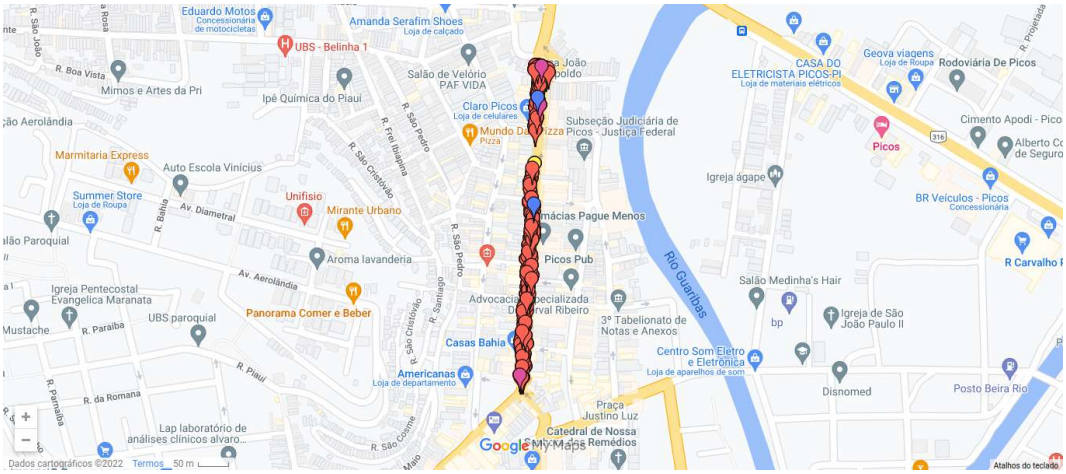


Figura 5 – Distribuição de pontos de acesso na zona comercial da cidade de Picos

4.1 Resultados

Esta seção apresenta os resultados obtidos com base nos experimentos realizados nas cidades de Picos e Valença do Piauí, visando analisar os fatores que podem influenciar o desempenho das redes wireless. Durante a varredura nessas cidades, foram capturados dados de aproximadamente 500 redes em cada localidade, totalizando 1000 redes analisadas. A pesquisa abrangeu uma distância percorrida de cerca de 3 km em Valença do Piauí e em torno de 1 km em Picos. Os dados coletados incluíram informações sobre os protocolos de segurança adotados, o status do WPS (Wi-Fi Protected Setup), os canais de comunicação e as frequências utilizadas por cada rede.

4.1.1 Valença do Piauí

Durante uma varredura na cidade de Valença do Piauí, o WiGLE Wifi capturou dados de aproximadamente 500 redes. Essa pesquisa abrangeu uma distância percorrida de cerca de 3 km dentro da área urbana mista de bairros habitacionais com bairro de áreas comerciais. Os principais dados selecionados para fins de estatística e análise incluem os protocolos de segurança adotados pelas redes, o status do WPS (Wi-Fi Protected Setup), canal de comunicação e a frequência utilizada por cada rede.

A Figura 6 apresenta os métodos de criptografia identificados durante o experimento. Os resultados mostram que apenas 2 redes utilizavam o protocolo de proteção WPA, representando uma porcentagem insignificante. Além disso, a figura revela que não foram encontradas redes sem criptografia, nenhuma rede utilizando o protocolo WEP e 11 redes com o protocolo de segurança desconhecido. A grande maioria das redes, cerca de 466, utilizava o protocolo WPA2. É interessante ressaltar que a baixa adoção do protocolo WPA e a inexistência de redes sem criptografia podem indicar uma falta de consciência ou conhecimento sobre a importância da segurança em redes wireless. Além de que a utilização do protocolo WPA2 é predominante nas redes analisadas, enquanto medidas mais robustas de segurança, como o WPA, são raramente implementadas.

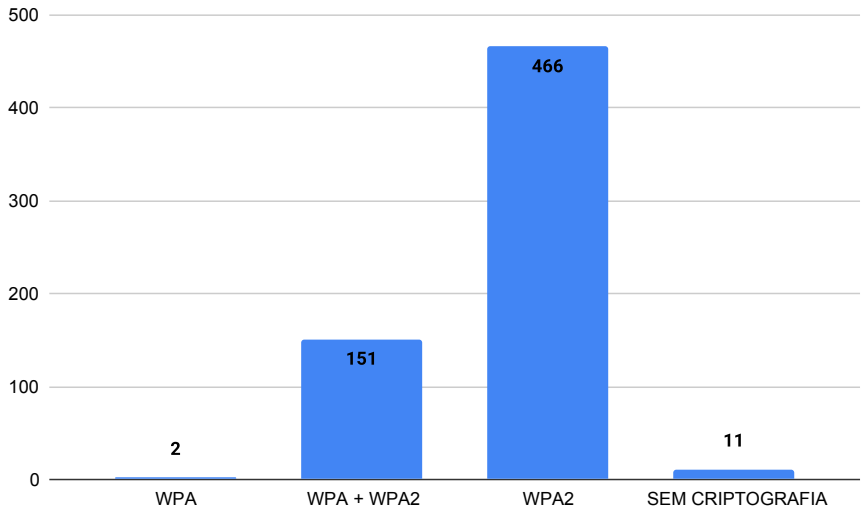


Figura 6 – Uso de criptografia Wi-Fi em Valença do Piauí.

A figura 12 apresenta a quantidade de redes em Valença do Piauí que oferecem a função WPS. Essa função é um fator importante para a segurança, como mencionado anteriormente. Observa-se que aproximadamente 69.8% das redes possuem o WPS ativado, enquanto os outros 30.2% têm essa função desativada. Apesar de o WPS ser uma funcionalidade conveniente para facilitar a configuração de dispositivos, sua ativação pode representar uma vulnerabilidade de segurança.

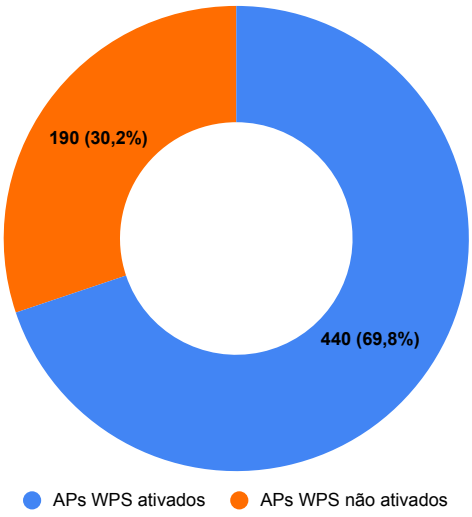


Figura 7 – Suporte WPS em Valença do Piauí.

A Figura 13 apresenta o atual cenário de utilização das frequências das redes, fornecendo uma visão sobre o nível de atualização dos equipamentos utilizados na cidade de Valença do Piauí. Das 500 redes avaliadas, 186 redes operam na frequência 5 GHz, enquanto 314 redes utilizam a frequência 2.4 GHz. Esses dados indicam uma adoção significativa da frequência 2.4 GHz, que é mais comum e amplamente suportada pelos dispositivos. No entanto, a presença de 186 redes operando na frequência 5 GHz demonstra um avanço no uso de tecnologias mais recentes. Podemos notar que há uma mistura de equipamentos mais antigos e mais modernos em uso na cidade. A atualização para frequências mais altas, como o 5 GHz, pode oferecer benefícios em termos de velocidade e capacidade de rede, além de reduzir a interferência em ambientes densos.

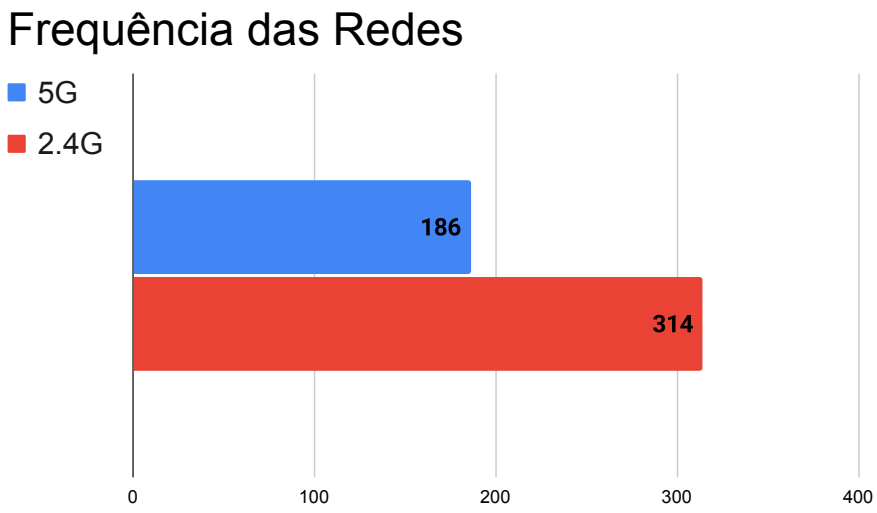


Figura 8 – Frequência das Redes em Valença do Piauí.

A Figura 15 apresenta a distribuição das redes de acordo com os canais utilizados, considerando a banda larga de 2.4 GHz. Foram identificadas 98 redes no canal 1, 59 redes no canal 6 e 110 redes no canal 11. Esses dados indicam que o canal 1 é o mais utilizado pelas redes avaliadas, seguido pelo canal 11. O canal 6 apresenta uma menor quantidade de redes em comparação aos demais canais. É importante ressaltar que o uso desses canais específicos pode causar interferência mútua, especialmente nas proximidades. Recomenda-se uma análise e ajuste adequado dos canais para otimizar o desempenho e minimizar problemas de interferência em redes wireless. Dessa forma, é fundamental realizar uma configuração adequada dos canais utilizados pelas redes para evitar conflitos e garantir uma melhor experiência de conectividade para os usuários.

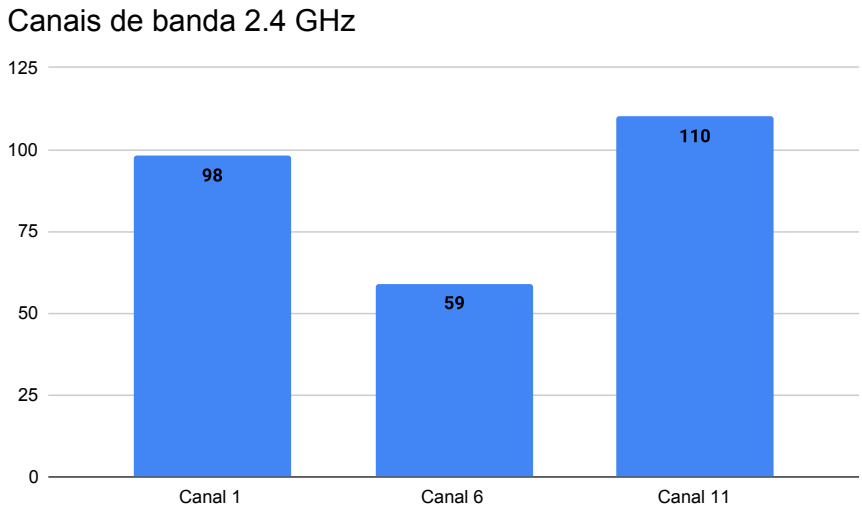


Figura 9 – Canais de banda 2.4 GHz em Valença do Piauí.

A Figura 10 apresenta a distribuição das redes de acordo com os canais utilizados, considerando a banda larga de 5 GHz. Foram identificadas 103 redes no canal 36, 17 redes no canal 48, 17 redes no canal 52, 20 redes no canal 100, 34 redes no canal 149 e 11 redes no canal 153. Esses dados indicam uma variedade de canais utilizados pelas redes de 5 GHz, o que demonstra uma maior diversidade e potencial para evitar interferências. Os canais 36 e 149 apresentam um número significativo de redes, sugerindo uma preferência pelos mesmos. É importante ressaltar que a escolha adequada do canal em redes de 5 GHz pode ajudar a minimizar a interferência e melhorar o desempenho da conectividade. Recomenda-se uma análise cuidadosa do ambiente e uma configuração adequada dos canais utilizados para garantir uma experiência de conexão mais estável e de qualidade para os usuários. Portanto, é fundamental realizar uma configuração estratégica dos canais na banda de 5 GHz para otimizar o desempenho das redes e proporcionar uma melhor experiência de internet sem fio.

Contudo os resultados obtidos por meio dos experimentos realizados para analisar os fatores que influenciam o desempenho de redes wireless na cidade de Valença do Piauí

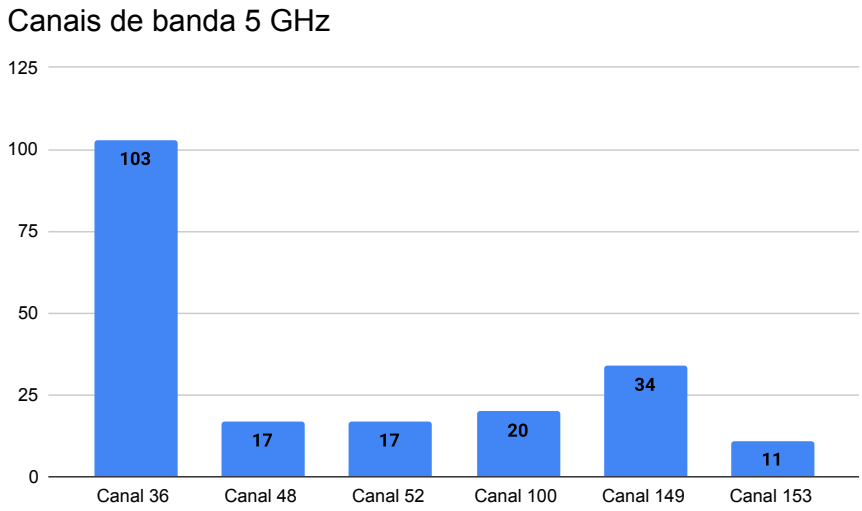


Figura 10 – Canais de banda 5 GHz em Valença do Piauí.

revelaram dados relevantes. Observou-se uma baixa adoção do protocolo de proteção WPA, com apenas 2 redes utilizando esse método de criptografia. Além disso, a ativação do recurso WPS foi constatada em aproximadamente 69.8% das redes, representando uma potencial vulnerabilidade de segurança. Quanto às frequências utilizadas, a maioria das redes (314) operava na banda de 2.4 GHz, indicando uma prevalência de equipamentos mais antigos, enquanto 186 redes adotaram a frequência de 5 GHz, demonstrando um avanço no uso de tecnologias mais recentes. Em relação aos canais utilizados, os canais 1 e 11 foram os mais frequentes na banda de 2.4 GHz, e uma variedade de canais foi identificada na banda de 5 GHz, com destaque para os canais 36 e 149. Recomenda-se uma configuração estratégica dos canais para otimizar o desempenho das redes, minimizando problemas de interferência e proporcionando uma melhor experiência de conectividade para os usuários.

4.1.2 Picos

Durante uma varredura na cidade de Picos Piauí, o WiGLE Wifi capturou dados de aproximadamente 500 redes. Essa pesquisa abrangeu uma distância percorrida de aproximadamente 1 km dentro da área urbana. Os principais dados selecionados para fins de estatística e análise incluem os protocolos de segurança adotados pelas redes, o status do WPS (Wi-Fi Protected Setup), canal de comunicação e a frequência utilizada por cada rede. A Figura 11 apresenta os métodos de criptografia identificados durante o experimento, no qual foram testadas 676 redes de internet. Os resultados mostram que apenas 2 redes utilizavam o protocolo de proteção WPA, representando um valor insignificante. Além disso, o experimento mostra que 19 redes não usam criptografia. A grande maioria das redes, cerca de 344, utilizava o protocolo WPA2. Além disso, observa-se que 311 redes

utilizavam a combinação de protocolos WPA + WPA2, indicando uma adoção de medidas de segurança mais abrangentes. Contudo, embora o protocolo WPA2 seja amplamente utilizado nas redes analisadas, é importante incentivar a implementação de medidas mais robustas de segurança, como o uso do protocolo WPA e a conscientização sobre a importância da criptografia nas redes wireless. Isso contribuirá para uma maior proteção contra possíveis ataques e garantirá a privacidade e segurança dos usuários.

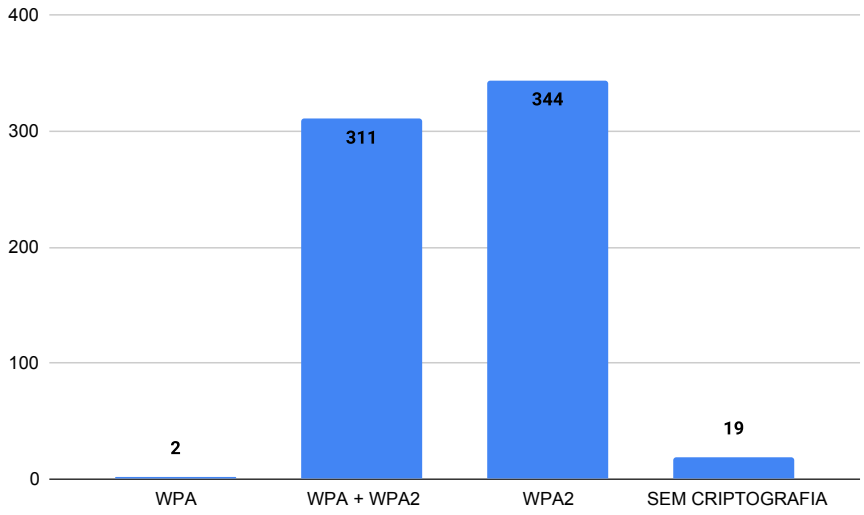


Figura 11 – Uso de criptografia Wi-Fi em Picos Piauí.

A figura 12 mostra o número de redes em Valença do Piauí que disponibilizam a opção WPS. Essa característica é um elemento crucial para a segurança, como mencionado anteriormente. Verifica-se que cerca de 54.1% das redes têm o WPS habilitado, enquanto os restantes 45.9% não possuem essa funcionalidade ativada. Embora o WPS seja uma função conveniente para simplificar a configuração de dispositivos, sua ativação pode representar uma brecha de segurança.

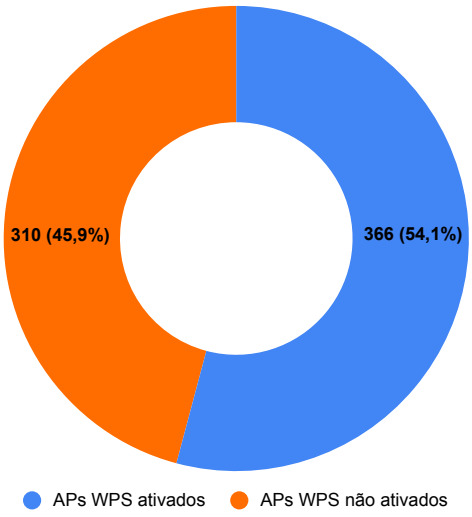


Figura 12 – Suporte WPS em Picos Piauí.

A Figura 13 apresenta o atual cenário de utilização das frequências das redes, fornecendo uma visão sobre o nível de atualização dos equipamentos utilizados na cidade de Valença do Piauí. Das 500 redes avaliadas, 226 redes operam na frequência 5 GHz, enquanto 274 redes utilizam a frequência 2.4 GHz. Esses dados indicam uma adoção significativa da frequência 2.4 GHz, que é mais comum e amplamente suportada pelos dispositivos. No entanto, a presença de 226 redes operando na frequência 5 GHz demonstra um avanço no uso de tecnologias mais recentes. Podemos notar que há uma mistura de equipamentos mais antigos e mais modernos em uso na cidade. A atualização para frequências mais altas, como o 5 GHz, pode oferecer benefícios em termos de velocidade e capacidade de rede, além de reduzir a interferência em ambientes densos.

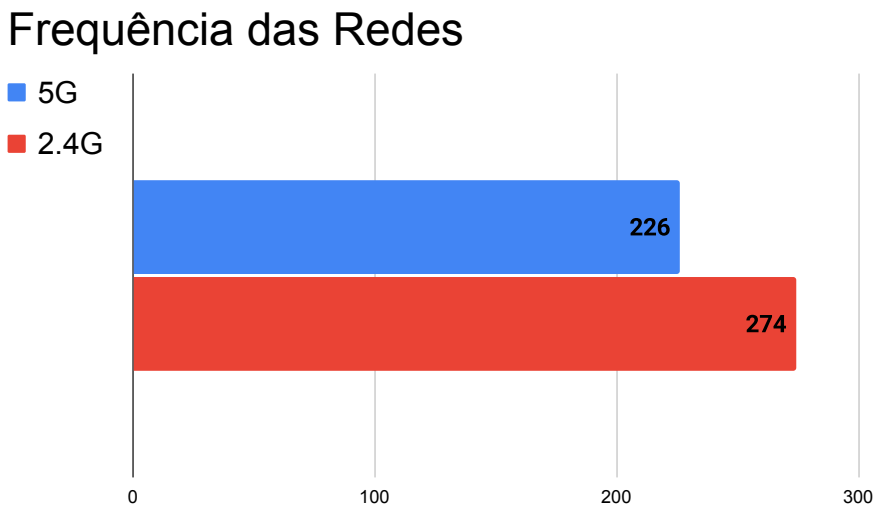


Figura 13 – Frequência das Redes em Picos Piauí.

A Figura 15 apresenta a distribuição das redes de acordo com os canais utilizados, considerando a banda larga de 2.4 GHz, no experimento foram encontrados 160 redes que foi possível identificar os canais de banda. Foram identificadas 64 redes no canal 1, 33 redes no canal 6 e 63 redes no canal 11. Esses dados indicam que o canal 1 é o mais utilizado pelas redes avaliadas, seguido pelo canal 11. O canal 6 apresenta uma menor quantidade de redes em comparação aos demais canais. É importante ressaltar que o uso desses canais específicos pode causar interferência mútua, especialmente nas proximidades. Recomenda-se uma análise e ajuste adequado dos canais para otimizar o desempenho e minimizar problemas de interferência em redes wireless. Dessa forma, é fundamental realizar uma configuração adequada dos canais utilizados pelas redes para evitar conflitos e garantir uma melhor experiência de conectividade para os usuários.

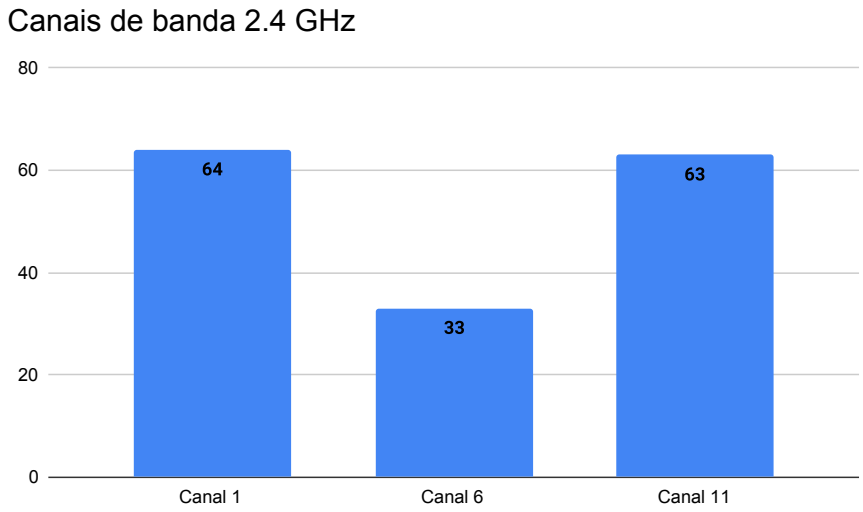


Figura 14 – Canais de banda 2.4 GHz em Picos Piauí.

A Figura 10 apresenta a distribuição das redes de acordo com os canais utilizados, considerando a banda larga de 5 GHz. Foram identificadas 71 redes no canal 36, 12 redes no canal 48, 36 redes no canal 52, 43 redes no canal 100, 43 redes no canal 149 e 14 redes no canal 153. Esses dados indicam uma variedade de canais utilizados pelas redes de 5 GHz, o que demonstra uma maior diversidade e potencial para evitar interferências. Os canais 36, 100 e 149 apresentam um número significativo de redes, sugerindo uma preferência pelos mesmos. É importante ressaltar que a escolha adequada do canal em redes de 5 GHz pode ajudar a minimizar a interferência e melhorar o desempenho da conectividade. Recomenda-se uma análise cuidadosa do ambiente e uma configuração adequada dos canais utilizados para garantir uma experiência de conexão mais estável e de qualidade para os usuários. Portanto, é fundamental realizar uma configuração estratégica dos canais na banda de 5 GHz para otimizar o desempenho das redes e proporcionar uma melhor experiência de internet sem fio.

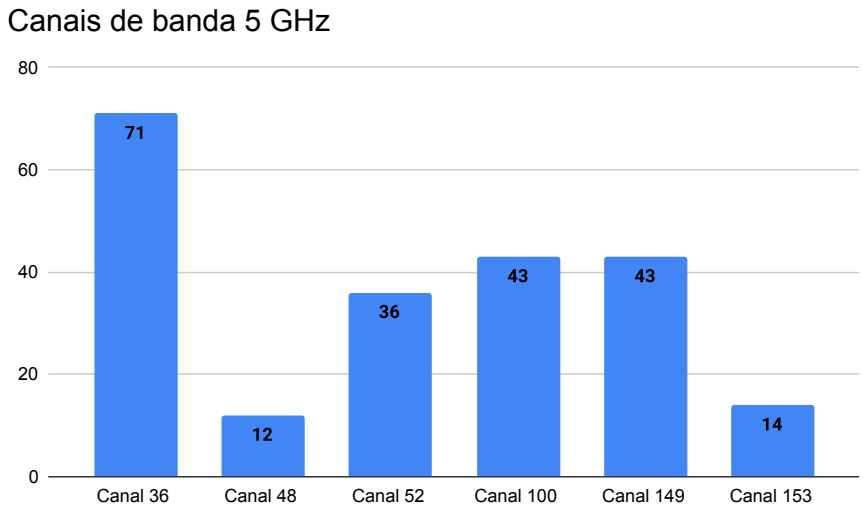


Figura 15 – Canais de banda 5 GHz em Picos Piauí.

Contudo os resultados obtidos por meio dos experimentos realizados para analisar os fatores que influenciam o desempenho de redes wireless na cidade de Picos Piauí revelaram dados relevantes. Observou-se uma baixa adoção do protocolo de proteção WPA, com apenas 2 redes utilizando esse método de criptografia. Além disso, a ativação do recurso WPS foi constatada em aproximadamente 54.1% das redes, representando uma potencial vulnerabilidade de segurança. Quanto às frequências utilizadas, a maioria das redes operava na banda de 2.4 GHz, indicando uma prevalência de equipamentos mais antigos, enquanto 186 redes adotaram a frequência de 5 GHz, demonstrando um avanço no uso de tecnologias mais recentes. Em relação aos canais utilizados, os canais 1 e 11 foram os mais frequentes na banda de 2.4 GHz, e uma variedade de canais foi identificada na banda de 5 GHz, com destaque para os canais 36, 100 e 149. Recomenda-se uma configuração estratégica dos canais para otimizar o desempenho das redes, minimizando problemas de interferência e proporcionando uma melhor experiência de conectividade para os usuários.

4.1.3 Fabricantes de Equipamentos de Redes e Segurança

Nesta seção, discutiremos a importância de identificar os fabricantes de equipamentos de redes em relação à segurança cibernética. Abordaremos como essa informação pode afetar a avaliação dos riscos, a implementação de medidas de segurança e a integração com as políticas de segurança da organização. Além disso, descreveremos em detalhes como realizamos a análise dos endereços MAC capturados e a relevância da base de dados fornecida pelo Wireshark através da ferramenta OUI Lookup.

4.1.3.1 A Importância de Identificar Fabricantes

A diversidade de fabricantes de equipamentos de redes implica em diferentes abordagens em relação à segurança. Alguns fabricantes são conhecidos por investirem significativamente em pesquisa e desenvolvimento de medidas de segurança, enquanto outros podem não dar a devida atenção a esse aspecto. Identificar o fabricante de cada dispositivo na rede nos permite entender melhor as práticas de segurança associadas a esses dispositivos e suas implicações para a segurança geral da rede.

4.1.3.2 Segurança Baseada no Fabricante

Cada fabricante possui sua própria política de segurança, o que pode afetar a confiabilidade e robustez dos dispositivos produzidos. Fabricantes com histórico de vulnerabilidades recorrentes podem representar um risco maior para a segurança da rede. Por outro lado, fabricantes com boas práticas de segurança podem fornecer atualizações e patches regulares para mitigar vulnerabilidades conhecidas. Conhecer o fabricante de um dispositivo permite avaliar seu nível de segurança e adotar medidas adequadas para proteger a rede.

4.1.3.3 Atualizações e Patches

A identificação dos fabricantes dos equipamentos de rede é essencial para garantir a aplicação atempada de atualizações e patches de segurança. Fabricantes comprometidos com a segurança costumam fornecer atualizações regulares para corrigir vulnerabilidades conhecidas. Ao conhecer o fabricante de um dispositivo, podemos acompanhar proativamente as atualizações disponibilizadas, minimizando a janela de exposição a possíveis ameaças e ataques.

4.1.3.4 Avaliação de Riscos

A análise dos fabricantes dos dispositivos presentes na rede permite a realização de uma avaliação mais precisa dos riscos de segurança. Com base em relatórios de segurança e histórico de vulnerabilidades associados a cada fabricante, podemos identificar possíveis pontos fracos na infraestrutura de rede. Essa análise nos auxilia a priorizar medidas de segurança para dispositivos mais suscetíveis a ameaças e ataques, fortalecendo a proteção geral da rede.

4.1.3.5 Integração com Políticas de Segurança

A informação sobre os fabricantes dos equipamentos de rede pode influenciar diretamente as políticas de segurança da organização. Dependendo do perfil de segurança de cada fabricante, podem ser necessárias adaptações nas políticas de permissões, controle de acesso e outras diretrizes de segurança. Além disso, em casos extremos, a identificação

de fabricantes com histórico crítico de vulnerabilidades pode levar à decisão de substituir dispositivos ou evitar futuras aquisições da mesma marca.

4.1.3.6 Análise com OUI Lookup do Wireshark

Para realizar a análise dos fabricantes associados aos endereços MAC capturados durante nossa pesquisa, utilizamos a ferramenta OUI Lookup disponibilizada pelo Wireshark. Essa ferramenta permite consultar uma extensa base de dados de fabricantes, associando os três primeiros octetos do endereço MAC (também conhecidos como OUI - Organizationally Unique Identifier) às empresas ou entidades responsáveis pela fabricação dos dispositivos. Com essa análise, pudemos identificar os fabricantes presentes em nossa rede de estudo e compreender melhor o perfil de segurança dos dispositivos utilizados.

Ao considerar os resultados obtidos com a análise dos endereços MAC e a associação aos fabricantes, reforçamos a importância dessa abordagem para a compreensão e aprimoramento da segurança de redes. A integração de informações sobre os fabricantes aos processos de gestão de segurança pode potencializar a eficácia das medidas adotadas para proteger a rede contra ameaças e vulnerabilidades, garantindo a confiabilidade e a robustez da infraestrutura de rede.

Os dados utilizados nesta pesquisa foram obtidos por meio de uma varredura realizada com a ferramenta Aircrack-NG. Durante essa varredura, os endereços MAC dos dispositivos presentes na rede foram capturados. Para identificar os fabricantes de cada dispositivo, foi desenvolvido um algoritmo em Python capaz de extrair os 6 primeiros dígitos do endereço MAC, que correspondem à identificação da marca do fabricante.

O algoritmo de identificação dos fabricantes foi essencial para a posterior análise dos dados coletados. Com os 6 primeiros dígitos do endereço MAC em mãos, foi possível determinar a marca do fabricante associada a cada dispositivo presente na rede.

Para realizar a associação entre os dígitos do endereço MAC e as marcas dos fabricantes, utilizamos o banco de dados do Wireshark. Esse banco de dados contém informações abrangentes sobre os prefixos de endereços MAC e suas respectivas marcas de fabricantes. A consulta aos dados do Wireshark foi feita por meio da ferramenta OUI Lookup, acessível pelo link https://www.wireshark.org/tools/oui-lookup.html.

Tabela 4 – Principais Fabricantes de Dispositivos de Redes de Picos

Fabricante	Quantidade de Dispositivos
ZTE	172
Intelbras	32
Huawei	85
TP-Link	98

Na Tabela 4, podemos observar os quatro principais fabricantes identificados na varredura de Picos - PI, juntamente com a quantidade de dispositivos associados a cada marca.

A presença predominante de equipamentos fabricados pela ZTE destaca-se nessa análise.

Tabela 5 – Principais Fabricantes de Dispositivos de Redes de Valença do Piauí

Fabricante	Quantidade de Dispositivos
Huawei	336
Tenda	53
Intelbras	46
ZTE	42

Já na Tabela 5, podemos observar os quatro principais fabricantes identificados na varredura de Valença do Piauí e a quantidade de dispositivos. Aqui a presença predominante de equipamentos fabricados é pela Huawei muito devido a um dos dois principais Provedores utilizar apenas equipamentos dessa marca.

É de suma importância saber quais fabricantes estão sendo usadas no equipamentos de redes,Os roteadores desempenham um papel fundamental na conectividade moderna, permitindo que dispositivos se comuniquem e acessem a internet de forma eficiente. No entanto, o universo dos roteadores é vasto e diversificado, com uma ampla gama de marcas e modelos disponíveis. Compreender as nuances das marcas de roteadores e suas configurações é crucial para garantir uma rede segura e bem administrada. Cada marca possui sua própria abordagem técnica e protocolos de segurança que impactam diretamente na experiência do usuário e na proteção dos dados.

Uma das diferenças mais significativas entre as marcas de roteadores é o processo de configuração inicial e o gerenciamento subsequente. Algumas marcas adotam senhas padrão para o primeiro acesso à interface de administração do roteador. Essas senhas são frequentemente amplamente conhecidas e documentadas, o que pode representar um risco significativo de segurança. Caso os usuários não alterem essas senhas padrão, suas redes ficam vulneráveis a ataques cibernéticos, uma vez que invasores experientes podem explorar essa lacuna para acessar e controlar os dispositivos conectados.

Por outro lado, algumas marcas têm uma abordagem mais segura e obrigam os usuários a alterar as senhas de acesso padrão durante a configuração inicial. Esse procedimento aumenta consideravelmente a proteção da rede, uma vez que impede o uso de senhas amplamente conhecidas. Essa prática encoraja a criação de senhas fortes e únicas, dificultando a invasão por parte de atores maliciosos.

Além disso, as configurações de segurança, as opções de *firewall*, as atualizações de *firmware* e os recursos de monitoramento variam entre as marcas de roteadores. Algumas marcas investem mais recursos em protocolos de segurança avançados, como *VPNs* integradas, detecção de intrusões e segmentação de rede, enquanto outras podem não oferecer tantos recursos de proteção. Portanto, a escolha da marca do roteador pode ter um impacto direto na segurança e na capacidade de defesa contra ameaças cibernéticas.

Em resumo, o conhecimento das marcas de roteadores e suas configurações é vital para manter uma rede segura e eficiente. Compreender as diferenças técnicas e as abor-

dagens de segurança de cada marca pode ajudar os usuários a tomar decisões informadas ao escolher um roteador e configurá-lo adequadamente. A consciência sobre senhas padrão e a prática de alterá-las durante a configuração inicial são passos essenciais para evitar vulnerabilidades e ataques indesejados. Portanto, investir tempo na pesquisa das opções disponíveis e no aprendizado das práticas recomendadas é uma ação que contribui diretamente para a proteção de sua rede e de seus dados.

5 Conclusão

O presente trabalho apresenta uma pesquisa de segurança em redes sem fio realizada nas cidades de Valença do Piauí e Picos. A técnica utilizada como base foi o *WarDriving*. A resposta à questão principal do estudo pode ser formulada da seguinte forma: os resultados mostram um aumento significativo na segurança das redes Wi-Fi nas cidades, mas ainda há necessidade de mais melhorias. As principais recomendações podem ser direcionadas para os seguintes pontos:

1. Aumentar a conscientização sobre os problemas de segurança e o impacto que podem ter nos usuários.

2. Utilizar apenas o método WPA2. Se houver necessidade de oferecer suporte a dispositivos mais antigos, criar uma rede separada e limitada que suporte o modo WPA/WPA2 misto.

3. Desativar o WPS para todos os dispositivos.

4. Procurar sempre utilizar métodos de criptografia em conjunto com o WPA2, sempre que possível.

5. Atualizar o firmware usado pelo roteador sem fio para a versão mais recente disponível.

6. Outra opção é o uso de um firmware alternativo, como o OpenWRT/DD-WRT, no qual os problemas de segurança são geralmente corrigidos mais rapidamente.

Como diretrizes para trabalhos futuros, podem ser realizados ataques ativos de força bruta e um estudo comparativo do nível de segurança em amplas regiões de Valença do Piauí e arredores.

Referências

ALLIANCE, W.-F. Wi-fi protected access: Strong, standards-based, interoperable security for today's wi-fi networks. *White paper, University of Cape Town*, p. 492–495, 2003. Citado na página 26.

BACUDIO, A. G. et al. An overview of penetration testing. *International Journal of Network Security & Its Applications*, Academy & Industry Research Collaboration Center (AIRCC), v. 3, n. 6, p. 19, 2011. Citado na página 36.

CAÇADOR, D. M. *Segurança e mobilidade em redes IEEE 802.11: modelo de suporte à decisão na escolha de arquitecturas e tecnologias de redes sem fios*. Tese (Doutorado), 2014. Citado 3 vezes nas páginas 20, 21 e 25.

CANCELA, L. B. et al. A importância da segurança da informação em redes wi-fi. Citado na página 17.

COMPTON, S.; HORNAT, C. 802.11 denial of service attacks and mitigation. *SANS Institute InfoSec Reading Room*, p. 14–18, 2007. Citado 2 vezes nas páginas 34 e 35.

ENGST, A.; FLEISHMAN, G. *Kit do iniciante em redes sem fio: o guia prático sobre redes Wi-Fi para Windows e Macintosh*. [S.l.]: São Paulo. Ed.: Pearson Makron Books, 2005. Citado na página 17.

FENG, P. Wireless lan security issues and solutions. In: IEEE. *2012 IEEE symposium on robotics and applications (ISRA)*. [S.l.], 2012. p. 921–924. Citado na página 23.

FIGUEIREDO, D. A. et al. Vulnerabilidades em redes wi-fi de instituições de ensino superior: um estudo de múltiplos casos. *Research, Society and Development*, v. 9, n. 2, p. e178921979–e178921979, 2020. Citado na página 37.

FLEISHMAN, G.; MOSKOWITZ, R. Weakness in passphrase choice in wpa interface. *Wi-Fi Networking News. Acessado 21 de dezembro de 2006 em URL: http://wifinetnews. com/archives/002452. html*, 2003. Citado na página 26.

FLUHRER, S.; MANTIN, I.; SHAMIR, A. Weaknesses in the key scheduling algorithm of rc4. In: SPRINGER. *International Workshop on Selected Areas in Cryptography*. [S.l.], 2001. p. 1–24. Citado na página 25.

GAST, M. *802.11 wireless networks: the definitive guide*. [S.l.]: "O'Reilly Media, Inc.", 2005. Citado na página 20.

KISSI, M. K.; ASANTE, M. Penetration testing of ieee 802.11 encryption protocols using kali linux hacking tools. *International Journal of Computer Applications*, v. 975, p. 8887, 2020. Citado na página 39.

KOHLIOS, C. P.; HAYAJNEH, T. A comprehensive attack flow model and security analysis for wi-fi and wpa3. *Electronics*, Multidisciplinary Digital Publishing Institute, v. 7, n. 11, p. 284, 2018. Citado na página 38.

KUMAR, U.; GAMBHIR, S. A literature review of security threats to wireless networks. *International Journal of Future Generation Communication and Networking*, v. 7, n. 4, p. 25–34, 2014. Citado na página 27.

KUROSE, J. F.; ROSS, K. W.; ZUCCHI, W. L. *Redes de Computadores ea Internet: uma abordagem top-down*. [S.l.]: Pearson Addison Wesley, 2007. Citado na página 25.

LINDELL, J.; LAGERHOLM, F. *WPS-WiFi Protected Setup: En studie om Wi-Fi Protected Setup som autentiseringsmetod*. 2019. Citado na página 38.

LINHARES, A. G.; GONÇALVES, P. A. d. S. Uma análise dos mecanismos de segurança de redes ieee 802.11: Wep, wpa, wpa2 e ieee 802.11 w. *Universidade Federal de Pernambuco (UFPE)-Centro de Informática (CIn)*, 2009. Citado na página 24.

LÓPEZ-PÉREZ, D. et al. Ieee 802.11 be extremely high throughput: The next generation of wi-fi technology beyond 802.11 ax. *IEEE Communications Magazine*, IEEE, v. 57, n. 9, p. 113–119, 2019. Citado na página 17.

LOUNIS, K.; ZULKERNINE, M. Wpa3 connection deprivation attacks. In: SPRINGER. *International Conference on Risks and Security of Internet and Systems*. [S.l.], 2019. p. 164–176. Citado na página 28.

MA, L. et al. Rap: Protecting commodity wi-fi networks from rogue access points. In: *The fourth international conference on heterogeneous networking for quality, reliability, security and robustness & workshops*. [S.l.: s.n.], 2007. p. 1–7. Citado na página 35.

MOHTADI, H.; RAHIMI, A. New attacks on wi-fi protected setup. *Advances in Computer Science: an International Journal*, v. 4, n. 5, p. 127–132, 2015. Citado na página 15.

NIKOLOV, L. G. Wireless network vulnerabilities estimation. *Security & Future*, Scientific Technical Union of Mechanical Engineering"Industry 4.0", v. 2, n. 2, p. 80–82, 2018. Citado na página 38.

RUFINO, N. M. d. O. *Segurança em redes sem fio: aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth*. [S.l.]: Novatec Editora, 2019. Citado na página 17.

SARI, A.; KARAY, M. et al. Comparative analysis of wireless security protocols: Wep vs wpa. *International Journal of Communications, Network and System Sciences*, Scientific Research Publishing, v. 8, n. 12, p. 483, 2015. Citado na página 23.

SCARFONE, K. et al. Guide to securing legacy ieee 802.11 wireless networks. *NIST Special Publication*, Citeseer, v. 800, p. 48, 2008. Citado na página 19.

SCARFONE, K. et al. Technical guide to information security testing and assessment. *NIST Special Publication*, v. 800, n. 115, p. 2–25, 2008. Citado na página 22.

SHARMA, N.; BARWAL, P. N.; NOIDA, C. Study of dos attacks on ieee 802.11 wlan and its prevention/detection techniques. *International Journal of Engineering Science and Innovative Technology (IJESIT)*, v. 3, n. 3, p. 245, 2014. Citado 2 vezes nas páginas 33 e 34.

SILVA, C. d. S. *Vulnerabilidade do WPS (Wi-fi Protected Setup) nas redes sem fio*. 2014. Citado na página 29.

SILVA, P. A. B. F. da. Ieee 802.11 ax networks: Study and assessment of new techniques for the mac layer. 2017. Citado na página 21.

SOARES, L.; MORAES, I. Uma avaliação de vulnerabilidades em protocolos de autenticação para redes sem fio ieee 802.11. In: SBC. *Anais da III Escola Regional de Informática do Rio de Janeiro*. [S.l.], 2019. p. 37–40. Citado na página 39.

STANGARLIN, D. P.; FILHO, W. P. *Análise de desempenho de redes sem fio com diferentes protocolos de criptografia*. 2017. Citado na página 27.

TANENBAUM, A. S. Redes de computadores. ed. *Campus-Tradução da Terceira Edição, Rio de Janeiro*, 2003. Citado na página 17.

TANENBAUM, J.; WETHERALL, D. *Redes de computadores. Tradução: Daniel Vieira*. [S.l.]: Pearson Prentice Hall: São Paulo, 2011. Citado na página 14.

TEWS, E.; BECK, M. Practical attacks against wep and wpa. In: *Proceedings of the second ACM conference on Wireless network security*. [S.l.: s.n.], 2009. p. 79–86. Citado na página 23.

VALCHANOV, H.; EDIKYAN, J.; ALEKSIEVA, V. A study of wi-fi security in city environment. In: IOP PUBLISHING. *IOP Conference Series: Materials Science and Engineering*. [S.l.], 2019. v. 618, n. 1, p. 012031. Citado na página 38.

VANHOEF, M.; PIESSENS, F. Key reinstallation attacks: Forcing nonce reuse in wpa2. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. [S.l.: s.n.], 2017. p. 1313–1328. Citado na página 27.

VIEHBÖCK, S. Brute forcing wi-fi protected setup. *Wi-Fi Protected Setup*, v. 9, 2011. Citado 2 vezes nas páginas 15 e 28.

WALIULLAH, M.; GAN, D. Wireless lan security threats & vulnerabilities. *International Journal of Advanced Computer Science and Applications*, Citeseer, v. 5, n. 1, 2014. Citado na página 33.

WEIDMAN, G. *Testes de Invasão: Uma introdução prática ao hacking*. [S.l.]: Novatec Editora, 2014. Citado na página 37.

TERMO DE AUTORIZAÇÃO PARA PUBLICAÇÃO DIGITAL NA BIBLIOTECA "JOSÉ ALBANO DE MACEDO"

Identificação do Tipo de Documento

( ) Tese

( ) Dissertação

(X) Monografia

( ) Artigo

Eu, **Carlos Daniel da Silveira Santos**, autorizo com base na Lei Federal nº 9.610 de 19 de Fevereiro de 1998 e na Lei nº 10.973 de 02 de dezembro de 2004, a biblioteca da Universidade Federal do Piauí a divulgar, gratuitamente, sem ressarcimento de direitos autorais, o texto integral da publicação **"Avaliação do Uso das Redes Wi-fi na cidade de Valença do Piauí e Picos"** de minha autoria, em formato PDF, para fins de leitura e/ou impressão, pela internet a título de divulgação da produção científica gerada pela Universidade.

Picos-PI 14 de Agosto de 2023.

Carlos Daniel da Silveira Santos

Assinatura