INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA

CAMPUS JOÃO PESSOA

CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

Samuel Lima do Nascimento

Os Riscos de Conectar-se a uma Rede Wi-Fi de Acesso Público

João Pessoa

2025

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA

CAMPUS JOÃO PESSOA

CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

Samuel Lima do Nascimento

Os Riscos de Conectar-se a uma Rede Wi-Fi de Acesso Público

Trabalho de Conclusão de Curso submetido ao Instituto Federal de Educação, Ciência e Tecnologia da Paraíba no Campus João Pessoa como requisito à obtenção do grau de Tecnólogo em Sistemas de Telecomunicações.

ORIENTADOR: Prof. Dr. Luís Romeu Nunes

João Pessoa

2025

Dados Internacionais de Catalogação na Publicação – CIP
Biblioteca Nilo Peçanha –IFPB, *Campus* João Pessoa

N244r Nascimento, Samuel Lima do.

Os riscos de conectar-se a uma rede *wi-fi* de acesso público / Samuel Lima do Nascimento. – 2025.
51 f. : il.

TCC (Graduação – Tecnologia em Sistemas de Telecomunicações) – Instituto Federal da Paraíba – IFPB / Coordenação de Tecnologia em Sistemas de Telecomunicações, 2025.
Orientador: Prof. Dr. Luís Romeu Nunes.
1. Redes *wi-fi* públicas. 2. Segurança da informação. 3. Ataques cibernéticos. 4. Proteção de dados. 5. Privacidade digital. I. Título.

CDU 004.056(043)

Bibliotecária responsável: Lucrecia Camilo de Lima – CRB15/132

Samuel Lima do Nascimento

Os Riscos de Conectar-se a uma Rede Wi-Fi de Acesso Público

Trabalho de Conclusão de Curso submetido ao Instituto Federal de Educação, Ciência e Tecnologia da Paraíba no Campus João Pessoa como requisito à obtenção do grau de Tecnólogo em Sistemas de Telecomunicações.

Aprovado Pela Banca Examinadora em: 08 de Abril de 2025.

gov.br
Documento assinado digitalmente
LUIS ROMEU NUNES
Data: 15/04/2025 20:11:30-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Luís Romeu Nunes
Orientador

gov.br
Documento assinado digitalmente
PATRIC LACOUTH DA SILVA
Data: 16/04/2025 09:40:12-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Patric Lacouth da Silva
Membro da Banca

gov.br
Documento assinado digitalmente
ERIK FARIAS DA SILVA
Data: 16/04/2025 17:52:48-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Erik Farias da Silva
Membro da Banca

João Pessoa, abril de 2025.

AGRADECIMENTOS

Primeiramente, agradeço a Deus, pois tudo que tenho e tudo que conquistei vem dele. Sem sua graça e direção, esta caminhada não teria sido possível.

Agradeço também à minha família, que sempre esteve ao meu lado, me apoiando em cada etapa. Em especial, à minha irmã Janayna e ao meu cunhado Ernesto, por todos os conselhos dados ao longo dessa trajetória, que foram fundamentais para meu crescimento pessoal e acadêmico.

Aos meus professores, expresso minha gratidão por todo o conhecimento compartilhado, pelas amizades construídas e pelas brincadeiras que tornaram essa jornada mais leve. Em especial, ao meu orientador, o professor Luís Romeu Nunes, pela disposição em me guiar neste trabalho, pela didática excepcional e pelo vasto conhecimento que tanto admiro.

Aos meus colegas de turma, que enfrentaram comigo os desafios e dificuldades do curso, pois sabemos que a caminhada foi árdua. Em especial, ao meu amigo Auristélio, que esteve comigo desde o início, compartilhando o mesmo objetivo de concluir o curso sem tropeçar no meio do caminho.

Por fim, agradeço à minha ex-namorada, que, de forma inesperada, teve um papel essencial nesta jornada ao me enviar a divulgação da inscrição para o processo seletivo do curso e me dar o apoio necessário no início dessa caminhada.

A todos que, de alguma forma, contribuíram para essa conquista, meu sincero agradecimento.

EPÍGRAFE

"Nós somos o que repetidamente fazemos. A excelência, portanto, não é um feito, mas um hábito." (Aristóteles)

RESUMO

O uso de redes Wi-Fi públicas tem se tornado cada vez mais comum devido à sua praticidade e acessibilidade. No entanto, muitos usuários desconhecem os riscos associados a essas conexões, tornando-se vulneráveis a ataques cibernéticos, como interceptação de dados, ataques Homem no Meio (*Man-in-the-Middle*, MITM) e roubo de credenciais. Este trabalho tem como objetivo analisar as principais ameaças presentes em redes sem fio de acesso público, identificando os métodos utilizados por invasores e as vulnerabilidades exploradas. Além disso, são apresentadas boas práticas e soluções para mitigar esses riscos, como o uso de Rede Virtual Privada (*Virtual Private Network*, VPN). A pesquisa destaca a importância da conscientização dos usuários sobre segurança digital, reforçando a necessidade de medidas preventivas para garantir a proteção das informações em ambientes de rede pública.

Palavras-Chave: Redes Wi-Fi públicas, Segurança da Informação, Ataques Cibernéticos, Proteção de Dados, Privacidade Digital, Vulnerabilidades em Redes.

ABSTRACT

The use of public Wi-Fi networks has become increasingly common due to their convenience and accessibility. However, many users are unaware of the risks associated with these connections, making them vulnerable to cyberattacks, such as data interception, Man-in-the-Middle (MITM) attacks, and credential theft. This work aims to analyze the main threats present in public access *wireless* networks, identifying the methods used by attackers and the vulnerabilities exploited. Additionally, best practices and solutions to mitigate these risks are presented, such as the use of a Virtual Private Network (VPN). The research highlights the importance of user awareness regarding digital security, reinforcing the need for preventive measures to ensure the protection of information in public network environments.

Keywords: Information Security, Cyberattacks, Data Protection, Digital Privacy, Network Vulnerabilities.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIAÇÕES E SIGLAS

AES *Advanced Encryption Standard* (Padrão de Criptografia Avançado)
AP Access Point (Ponto de Acesso)
ARP *Address Resolution Protocol* (Protocolo de Resolução de Endereço)
ASCII *American Standard Code for Information Interchange* (Código Padrão Americano para o Intercâmbio de Informações)
BSSID *Basic Service Set Identifier* (Identificador do Conjunto de Serviços Básico)
ESSID *Extended Service Set Identifier* (Identificador do Conjunto de Serviços Estendido)
GHz Gigahertz
IEEE *Institute of Electrical and Electronics Engineers* (Instituto de Engenheiros Eletricistas e Eletrônicos)
IV *Initialization Vector* (Vetor de Inicialização)
LAN *Local Area Network* (Rede de Área Local)
MAC *Media Access Control* (Endereço Físico)
Mbps *Megabits per second* (Megabits por segundo)
MHz Megahertz
MIMO *Multiple-Input Multiple-Output* (Múltiplas Entradas, Múltiplas Saídas)
OUI *Organizationally Unique Identifier* (Identificador Exclusivo da Organização)
PSK *Pre-Shared Key* (Chave Pré-Compartilhada)
RF *Radio Frequency* (Frequência de Rádio)
TKIP *Temporal Key Integrity Protocol* (Protocolo de Integridade da Chave Temporal)
USB *Universal Serial Bus* (Barramento Serial Universal)
WEP *Wired Equivalent Privacy* (Privacidade Equivalente ao cabeado)
WLAN *Wireless Local Area Network* (Rede Local Sem Fio)
WMAN *Wireless Metropolitan Area Network* (Rede Metropolitana Sem Fio)
WPAN *Wireless Personal Area Network* (Rede Pessoal Sem Fio)
WPA *Wi-Fi Protected Access* (Acesso Protegido Wi-Fi)
WPA2 *Wi-Fi Protected Access 2* (Acesso Protegido Wi-Fi 2)
WPA3 *Wi-Fi Protected Access 3* (Acesso Protegido Wi-Fi 3)
WWAN *Wireless Wide Area Network* (Rede de Área Ampla Sem Fio)

SUMÁRIO

1. Introdução

1.1 Contextualização

Com o aumento da demanda por conectividade, redes Wi-Fi públicas tornaram-se comuns em locais de alta circulação. Embora algumas dessas redes exijam senha para acesso, essa medida nem sempre garante segurança, pois as senhas são frequentemente divulgadas de forma pública, como em cartazes ou cardápios, no caso de restaurantes, facilitando o acesso irrestrito a qualquer pessoa no local. Assim, usuários se expõem a ataques cibernéticos, como interceptação de dados ou instalação de *malwares*, uma vez que a proteção dessas redes não é comparável à segurança encontrada em redes privadas.

1.2 Problematização

A crescente dependência de redes Wi-Fi públicas, muitas vezes usadas sem precauções adequadas, coloca em risco a segurança e a privacidade dos usuários. Mesmo quando essas redes exigem senha, a divulgação pública da mesma compromete a proteção oferecida. A falta de criptografia robusta e a vulnerabilidade a ataques, como interceptação de dados e instalação de *malwares*, evidenciam a necessidade de investigar o impacto dessas práticas inseguras. A questão central é: como garantir a segurança dos dados e a privacidade dos usuários em um ambiente onde as redes públicas são amplamente utilizadas, mas pouco seguras?

1.3 Objetivo Geral

Este trabalho visa analisar, compreender e avaliar as vulnerabilidades presentes em redes Wi-Fi de acesso público, considerando não apenas os aspectos teóricos, mas também as práticas adotadas pelos administradores de rede e usuários. Além disso, pretende-se apresentar recomendações práticas para mitigar essas vulnerabilidades, promovendo uma experiência segura de uso de redes Wi-Fi públicas.

1.4 Objetivos Específicos

Este estudo tem como objetivo principal conduzir uma pesquisa das principais vulnerabilidades previamente documentadas em redes Wi-Fi públicas, utilizando uma revisão bibliográfica como base para a investigação. Além disso, busca analisar casos práticos de ataques realizados nesses ambientes específicos, visando compreender as reais implicações dessas ameaças na segurança dos usuários. Em uma abordagem mais localizada, será realizada uma avaliação das configurações de criptografia em redes Wi-Fi públicas, abrangendo diversos pontos da cidade de Cuité de Mamanguape do estado da Paraíba, com o intuito de identificar padrões e lacunas de segurança. Por fim, o estudo se propõe a proporcionar recomendações específicas para aprimorar a

segurança em redes Wi-Fi públicas, levando em consideração tanto as práticas já estabelecidas quanto as emergentes, visando contribuir para um ambiente mais seguro e consciente no uso dessas redes.

1.5 Justificativa

A importância desta pesquisa reside na urgência de conscientizar usuários e administradores de rede sobre os riscos significativos associados ao uso de redes Wi-Fi públicas. Diante da crescente dependência da conectividade sem fio em espaços urbanos, entender as vulnerabilidades e implementar medidas de segurança torna-se imperativo para garantir a proteção das informações pessoais e a privacidade dos usuários. Além disso, ao contextualizar as descobertas em um cenário local, pretendemos oferecer insights específicos que possam contribuir para a criação de políticas mais eficazes e a adoção de práticas mais seguras.

1.6 Metodologia

A pesquisa foi conduzida em duas fases distintas. A primeira fase compreenderá uma revisão bibliográfica, abordando as vulnerabilidades conhecidas em redes Wi-Fi públicas e explorando casos práticos de ataques. A segunda fase envolverá uma pesquisa de campo em diferentes locais da cidade, onde serão analisadas as configurações de criptografia em redes Wi-Fi de acesso público. A abordagem qualitativa será empregada para coletar dados, incluindo a análise de configurações de rede e comparação com as práticas recomendadas.

2. Fundamentação Teórica

2.1 Rede Wi-Fi

A Fortinet (empresa que desenvolve e comercializa software, produtos e serviços de cibersegurança) especifica que a tecnologia Wi-Fi é uma solução de rede sem fio que viabiliza a conexão de diversos dispositivos à Internet, abrangendo desde computadores portáteis e de mesa até dispositivos móveis como smartphones e acessórios inteligentes. Além disso, essa tecnologia também possibilita a intercomunicação entre inúmeros aparelhos, estabelecendo uma rede de conexão. A ligação com a Internet é intermediada por meio de um dispositivo conhecido como roteador sem fio. Ao utilizar uma conexão Wi-Fi, você está estabelecendo uma ligação com um roteador sem fio que, por sua vez, habilita a interação da sua gama de dispositivos compatíveis com Wi-Fi com a vastidão da Internet (Fortinet, s.d).

O *Institute of Electrical and Electronics Engineers* (IEEE), formou um grupo de trabalho com o propósito de criar regras para o uso de redes sem fio. Um desses grupos é chamado de 802.11, que engloba várias especificações explicando como a comunicação deve acontecer entre um aparelho que se conecta (cliente) e um dispositivo central ou até entre dois aparelhos conectados. Com o passar do tempo, várias melhorias foram adicionadas, introduzindo novas formas de operação e tecnologia. Do ponto de vista técnico, esse conjunto de regras conhecido como IEEE 802.11, define como os aparelhos sem fio que usam Wi-Fi se comunicam, abrangendo tanto os dispositivos que criam redes, como os roteadores, quanto aqueles que permitem a conexão, como pontos de acesso sem fio. Esses pontos de acesso operam conforme diferentes regras estabelecidas pelo IEEE, conhecidas como “padrões”, que foram sendo aprovados ao longo do tempo. Cada padrão apresenta características próprias, incluindo faixas de frequência específicas, capacidades de transmissão variadas e suporte diferentes de números de canais de comunicação.

2.1.1 Tipos de redes *wireless*

As redes *wireless* são redes de comunicação sem fio e podem ser categorizadas com base no quão longe seu sinal pode alcançar, os dispositivos que são usados e a forma como a informação é transmitida (Alencar, 2020).

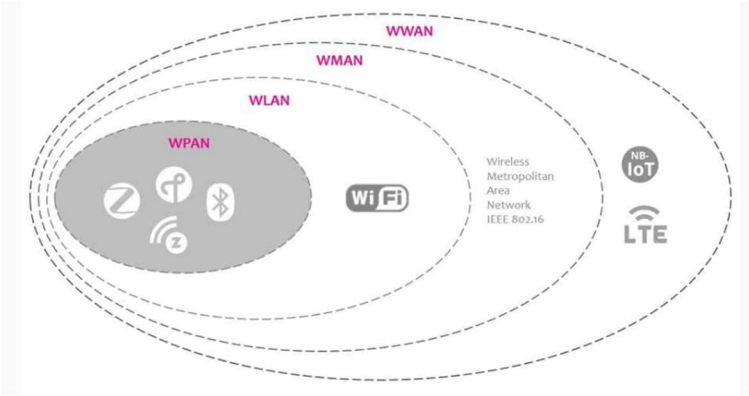
As redes *wireless* podem ser classificadas em: WPAN, WLAN, WMAN e WWAN. Descreveremos a seguir as especificidades de cada uma.

- Redes de Área Pessoal (*Wireless Personal Area Network*, WPAN): geralmente alcançam até 10 metros.
- Redes de Área Local (*Wireless Local Area Network*, WLAN): variam de 30 a 100 metros em ambientes internos e podem ultrapassar 200 metros em áreas externas.
- Redes de Área Metropolitana (*Wireless Metropolitan Area Network*, WMAN): podem cobrir uma cidade inteira, chegando a 50 km.

- Redes de Área Ampla (*Wireless Wide Area Network*, WWAN): como redes celulares (3G, 4G, 5G), têm alcance de vários quilômetros, podendo cobrir países inteiros.

Podemos ilustrar melhor as redes *wireless* na Figura 1:

Figura 1 - Tipos de redes *wireless*.



Fonte: Alencar (2020).

2.1.1.1 Redes WPAN

Uma Rede de área pessoal sem fio (*Wireless Personal Area Network*, WPAN) é um tipo de rede de curto alcance projetada para conectar dispositivos eletrônicos pessoais, como smartphones, fones de ouvido sem fio e *smartwatches*. Ela permite a comunicação direta entre dispositivos próximos, geralmente dentro de alguns metros. A WPAN desempenha um papel fundamental na criação de redes pessoais convenientes e na interconexão de dispositivos portáteis.

2.1.1.2 Redes WLAN

Uma Rede de Área Local Sem Fio (*Wireless Local Area Network*, WLAN) mais conhecida como rede Wi-Fi, é uma tecnologia de rede que oferece conectividade sem fio em uma área local, como uma casa, escritório ou espaço público. Ela permite que dispositivos como laptops, smartphones e tablets se conectem à Internet e compartilhem recursos dentro da área coberta pelo sinal sem fio.

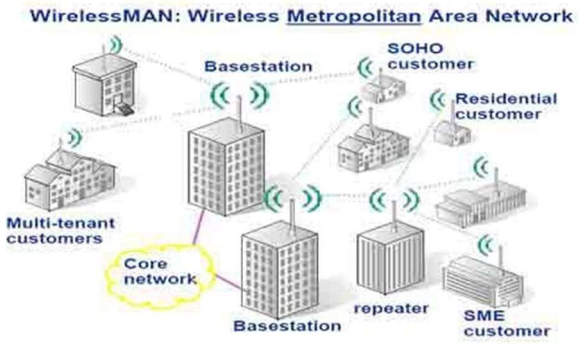
As WLANs operam com base em padrões como IEEE 802.11 (Wi-Fi) e são amplamente utilizadas em todo o mundo devido à sua conveniência e flexibilidade.

2.1.1.3 Redes WMAN

Uma Rede Metropolitana Sem Fio (*Wireless Metropolitan Area Network*, WMAN), é uma infraestrutura de rede sem fio que abrange uma área geográfica maior do que uma WLAN, como uma cidade ou área metropolitana. Ela é projetada para fornecer conectividade de rede de alta velocidade em áreas urbanas e suburbanas.

A Figura 2 demonstra um exemplo de uma rede WMAN:

Figura 2 - Rede WMAN.



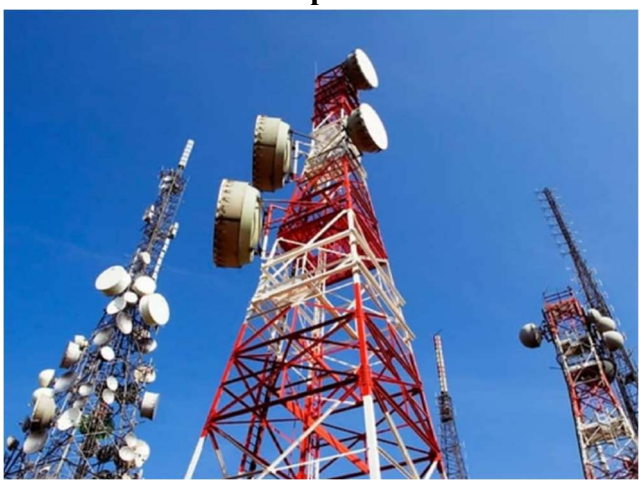
Fonte: Alencar (2020).

2.1.1.4 Redes WWAN

Uma Rede de Área Ampla Sem Fio (*Wireless Wide Area Network*, WWAN), é um tipo de rede que abrange vastas áreas geográficas, fornecendo conectividade sem fio em uma escala muito maior em comparação com as redes discutidas anteriormente. Ela é especialmente projetada para atender a áreas metropolitanas extensas, regiões rurais e até mesmo países inteiros. A WWAN opera com tecnologias de comunicação sem fio de longo alcance, como 3G, 4G e 5G, e é essencial para a cobertura móvel e acesso à Internet em larga escala.

Podemos observar na Figura 3 um sistema de antenas que são utilizadas em rede WWAN:

Figura 3 - Antenas utilizadas para formar redes WWAN.



Fonte: Alencar (2020).

2.1.2 Modos de comunicação

Na área de redes de comunicação, os modos de comunicação são aspectos cruciais que determinam como os dispositivos enviam e recebem dados entre si. Eles desempenham um papel vital na eficiência e no desempenho das redes, definindo os padrões de interação entre os dispositivos. Aqui, exploramos três modos fundamentais de comunicação: *Simplex, Half-Duplex e Full-Duplex*, descritos a seguir:

2.1.2.1 Modo Simples (*Simplex*)

O modo simplex é caracterizado pela transmissão unidirecional de dados, sem a capacidade de recebimento simultâneo. Isso significa que, em um dado momento, um dispositivo pode apenas enviar informações ou apenas receber informações, mas não ambos ao mesmo tempo. Um exemplo prático disso é a transmissão de televisão, onde os dados são enviados dos provedores para os televisores dos espectadores, sem a necessidade de um retorno direto de dados.

2.1.2.2 Modo Meio-Duplex (*Half-Duplex*)

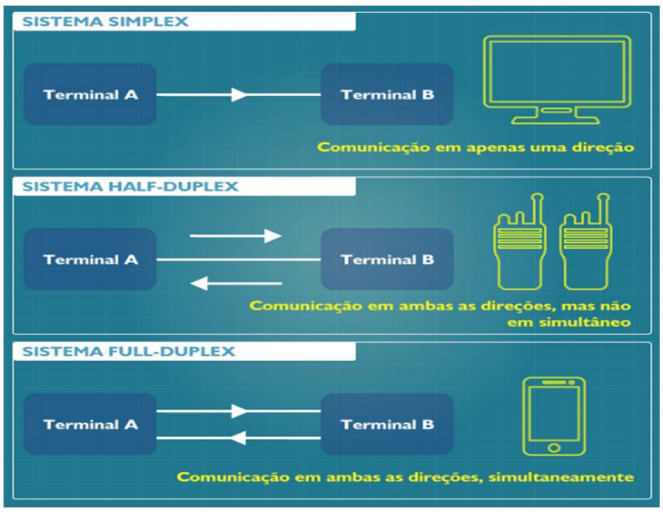
No modo meio-duplex, a comunicação bidirecional é possível, mas não simultaneamente. Dispositivos podem alternar entre enviar e receber informações. É como se fosse uma conversa em que as pessoas precisam se revezar para falar e ouvir. Este modo é comumente encontrado em sistemas de comunicação por rádio, *walkie-talkies* e até mesmo em algumas comunicações telefônicas.

2.1.2.3 Modo Duplex Completo (*Full-Duplex*)

O modo duplex completo permite a comunicação bidirecional simultânea, onde dispositivos podem enviar e receber informações ao mesmo tempo. Isso é semelhante a uma conversa em que ambas as partes podem falar e ouvir simultaneamente, tornando a comunicação mais rápida e eficaz. É amplamente utilizado em redes de computadores, telefonia moderna e outras aplicações que requerem uma transmissão simultânea e eficiente de dados em ambas as direções.

Podemos verificar melhor o funcionamento dos modos de comunicação na Figura 4.

Figura 4 - Modos de comunicação.



Fonte: Henriques (s.d).

2.1.3 Topologia de Rede Sem Fio

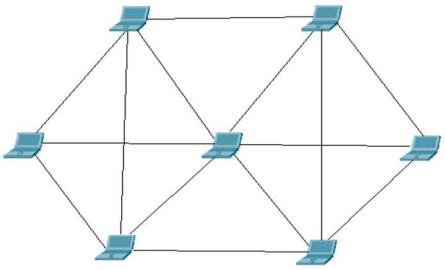
Ao projetar e implementar redes sem fio, é crucial considerar a topologia da rede, que descreve a estrutura de como os dispositivos se interconectam. Duas topologias comuns em redes sem fio são:

2.1.3.1 Topologia *Ad-Hoc*

A topologia de rede ponto a ponto (*Ad-Hoc*), é um modelo de rede dinâmico. Nesse cenário, os dispositivos se comunicam diretamente entre si, formando uma conexão temporária e descentralizada. Isso é útil em situações em que os dispositivos precisam se conectar rapidamente, como em reuniões de negócios, salas de aula ou em ambientes de uso temporário. Uma rede *Ad-Hoc* não requer um ponto de acesso central e é altamente flexível, permitindo a criação instantânea de redes onde for necessário.

A Figura 5 apresenta um exemplo de uma rede ponto a ponto:

Figura 5 - Topologia *Ad-Hoc*.



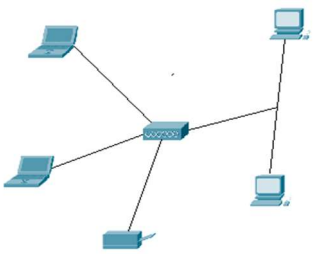
Fonte: Elaborado pelo autor (2024).

2.1.3.2 Topologia de Infraestrutura

A topologia de infraestrutura é o modelo mais comum em redes sem fio. Neste caso, os dispositivos se conectam a um ponto central chamado ponto de acesso (*Access Point*, AP). O AP atua como um intermediário que coordena e direciona o tráfego entre os dispositivos na rede e, quando necessário, para a Internet. Essa abordagem é ideal para ambientes onde a conectividade deve ser gerenciada de maneira organizada e centralizada, como em redes domésticas, empresas e locais públicos, como aeroportos ou cafés. Essas topologias oferecem flexibilidade para atender a diferentes necessidades de conectividade em ambientes diversos. A escolha entre uma topologia *Ad-Hoc* ou de infraestrutura depende dos requisitos específicos de cada cenário e das preferências de implementação (Mathias, 2000).

Na Figura 6 podemos verificar um exemplo de uma topologia de infraestrutura:

Figura 6 - Topologia Infraestrutura.



Fonte: Elaborado pelo autor (2024).

2.1.4 Roteador sem fio

Os aparelhos chamados roteadores são frequentemente vistos em casas. Eles são os dispositivos que as empresas que oferecem conexão com a Internet usam para ligar você à Internet através de cabo ou linha telefônica.

Um roteador combina as tarefas de um ponto de acesso e um roteador em um só aparelho.

Na Figura 7 podemos observar um exemplo de roteador sem fio:

Figura 7 - Roteador sem fio.

Fonte: TP-Link (s.d. b).

2.1.5 Access Point sem fio

O dispositivo conhecido como "ponto de acesso sem fio" (AP) possibilita que aparelhos sem fio se conectem a uma rede que não requer fios. Para entender o papel do ponto de acesso sem fio na rede, pense no que um amplificador faz para um sistema de som doméstico. O ponto de acesso usa a capacidade de conexão vinda de um roteador e a expande para que vários aparelhos possam usar a rede mesmo a partir de pontos mais afastados. Contudo, o ponto de acesso sem fio não se limita a aumentar apenas o alcance do Wi-Fi. Ele também oferece informações essenciais sobre os aparelhos na rede, assegura a segurança de forma ativa e serve a diversos outros propósitos práticos.

Observa-se na Figura 8 um exemplo de AP:

Figura 8 - Ponto de Acesso sem fio.

Fonte: Cisco (s.d. a).

2.1.6 Placa de Rede

A placa de rede, também conhecida como adaptador de rede, é um componente crucial em dispositivos eletrônicos como computadores e dispositivos móveis. Sua função essencial é possibilitar a conexão a redes de comunicação, como redes locais (LAN) ou a Internet. Agindo como uma interface entre o dispositivo e a rede, a placa de rede facilita a transmissão e recepção de dados, utilizando protocolos como Ethernet ou Wi-Fi. Essas placas podem ser integradas à placa-mãe ou conectadas externamente via USB, desempenhando um papel vital na comunicação e troca de informações em ambientes de rede.

Na Figura 9 podemos observar um exemplo de uma placa de rede:

Figura 9 - Placa de Rede.

Fonte: TP-Link (s.d. a).

2.1.7 Espectro de Frequência

De acordo com regulamentações globais, existem três segmentos de frequência ISM (*Industrial, Scientific and Medical*), uma faixa de frequência reservada para uso industrial, científico e médico, designados para comunicações sem fio que podem ser acessados sem a obrigatoriedade de obter uma licença da entidade reguladora governamental, que no caso do Brasil é a Anatel.

De acordo com Rufino (2015), os intervalos de frequência em cada uma das 3 faixas disponíveis são:

- 902 - 928 MHz;
- 2,4 - 2,486 GHz (2,4 a 2,5 GHz no Brasil);
- 5,150 - 5,825 GHz.

2.1.7.1 Frequência de 2,4 GHz

A faixa de frequência de 2,4 GHz é uma escolha comum em redes Wi-Fi devido à sua ampla disponibilidade e capacidade de penetração de obstáculos, o que a torna ideal para ambientes com várias paredes e estruturas. No entanto, essa popularidade

tem seu preço, pois a faixa de 2,4 GHz é frequentemente congestionada, resultando em interferências em ambientes onde várias redes sem fio estão em operação. A capacidade de suportar taxas de transferência de dados mais baixas é uma limitação da frequência de 2,4 GHz. Isso a torna menos adequada para aplicações que demandam largura de banda significativa, como streaming de vídeo em alta definição e jogos online com alta demanda de velocidade (Anacom, 2021).

2.1.7.2 Frequência de 5 GHz

A frequência de 5 GHz oferece várias vantagens notáveis em comparação com a frequência de 2,4 GHz. Ela proporciona mais canais disponíveis e, como resultado, reduz consideravelmente a interferência entre redes Wi-Fi vizinhas. Isso se traduz em uma conexão mais estável e confiável. Além disso, a frequência de 5 GHz suporta taxas de transferência de dados mais elevadas, tornando-se uma escolha preferida para aplicações que requerem largura de banda substancial. Contudo, é importante mencionar que a frequência de 5 GHz possui uma capacidade de penetração de sinal inferior, o que a torna mais adequada para ambientes internos ou espaços menores (Anacom, 2021).

2.1.8 Canais WLAN

Os canais utilizados em redes WLAN não se restringem apenas ao padrão IEEE 802.11 (Wi-Fi). Outras tecnologias que operam com sinais de rádio, como o *Bluetooth*, também compartilham o mesmo espectro de Radiofrequência (*Radio Frequency,* RF). Neste espectro, os canais são alocados em faixas de frequência específicas, o que desempenha um papel fundamental na prevenção de interferências e na garantia de um desempenho eficaz (Valeri, 2022).

Na tabela 1 podemos observar os canais e as frequências utilizadas em cada um deles:

Tabela 1 - Tabela de canais nas frequências de 2,4GHz e 5GHz.

Canal	Frequência (GHz)	**Canal**	Frequência (GHz)
1	2,412	**56**	5,280
2	2,417	**60**	5,300
3	2,422	**64**	5,320
4	2,427	**100**	5,500
5	2,432	**104**	5,520
6	2,437	**108**	5,540

7	2,442	**112**	5,560
8	2,447	**116**	5,580
9	2,452	**120**	5,600
10	2,457	**124**	5,620
11	2,462	**128**	5,640
12	2,467	**132**	5,660
13	2,472	**136**	5,680
14	2,484	**140**	5,700
36	5,180	**149**	5,745
40	5,200	**153**	5,765
44	5,220	**157**	5,785
48	5,240	**161**	5,805
52	5,260	**165**	5,825

Fonte: Elaborado pelo autor (2024).

2.1.9 ESSID e BSSID

O Identificador de Conjunto de Serviço Estendido (*Extended Service Set Identifier*, ESSID), é um nome único atribuído a uma rede Wi-Fi. Ele é o "nome" que você vê ao procurar redes disponíveis em seu dispositivo. O ESSID é utilizado para identificar e distinguir diferentes redes sem fio em um determinado local, permitindo que os dispositivos se conectem à rede desejada.

Exemplo de um nome de rede identificado por ESSID: IFPB VISITANTES.

O Identificador de Conjunto de Serviço Básico (*Basic Service Set Identifier*, BSSID) é um número utilizado para localizar os dispositivos em uma rede Wi-Fi, pois cada dispositivo tem um número único. O BSSID é formado por 6 grupos de dois caracteres, que podem ser separados por dois pontos ou traços.

Exemplo de formato do BSSID: 7A:EA:3A:EB:E1:67

No exemplo 7A:EA:3A:EB:E1:67, cada parte tem um significado:

- 7A:EA:3A: Identificador Organizacional Único (*Organizationally Unique Identifier*, OUI), que identifica o fabricante do dispositivo.
- EB:E1:67: Identificador específico do *hardware*, garantindo que cada BSSID seja único.

Esses identificadores desempenham papéis fundamentais nas redes Wi-Fi, garantindo que os dispositivos se conectem à rede correta e ao ponto de acesso apropriado (Antônio, 2020).

2.1.10 *Beacon Frame*

O quadro de sinalização (*Beacon Frame*) é comumente utilizado no contexto das redes Wi-Fi para se referir a um tipo especial de pacote de dados transmitido por um roteador. A principal função desses pacotes é fornecer informações cruciais aos dispositivos próximos, permitindo que eles estabeleçam conexões de rede de maneira eficaz e eficiente.

Em essência, podemos pensar no quadro de sinalização como um tipo de "farol" emitido pelo roteador para indicar a presença da rede. Esses quadros incluem dados como o nome da rede (também conhecido como SSID), detalhes sobre o método de segurança adotado e a capacidade de transmissão de dados suportada. Quando um dispositivo, como um smartphone ou um computador, está em busca de redes Wi-Fi disponíveis, ele capta esses quadros de sinalização. Com base nas informações contidas nesses quadros, o dispositivo pode tomar decisões sobre se deseja se conectar àquela rede específica ou continuar em busca de outras opções. Esse processo é especialmente valioso em áreas com múltiplas redes Wi-Fi, pois os quadros de sinalização ajudam a distinguir e identificar cada uma delas. Além disso, os quadros de sinalização desempenham um papel fundamental na avaliação da qualidade do sinal da rede. Eles contêm informações essenciais, como a força do sinal e a taxa de transmissão de dados atual. Com base nesses dados, os dispositivos podem determinar se é vantajoso se conectar à rede em questão ou se é mais apropriado buscar uma rede com um sinal mais forte. Essa funcionalidade auxilia os usuários a tomar decisões informadas sobre as redes Wi-Fi às quais desejam se conectar (Rizzon, 2024).

2.1.11 Padrões Wi-Fi

O padrão original 802.11 (também conhecido como Wi-Fi), quando se fala em velocidade de transmissão, oferece no máximo 2 Mbit/s e usa a faixa de frequência de 2,4 GHz. A família 802.11 inclui algumas melhorias principais, também chamadas de extensões ou subpadrões (Rufino, 2015).

2.1.11.1 Protocolo 802.11b (Wi-Fi 1)

Este foi um dos primeiros protocolos comerciais de Wi-Fi, lançado em 1999. Ele opera na faixa de frequência de 2,4 GHz e pode atingir velocidades de até 11 Mbit/s. Entretanto, a segurança era uma preocupação, devido à vulnerabilidade da criptografia Privacidade Equivalente à Rede Cabeada (*Wired Equivalent Privacy*, WEP) a ataques.

2.1.11.2 Protocolo 802.11a (Wi-Fi 2)

Lançado simultaneamente com o 802.11b, o protocolo 802.11a opera na faixa de frequência de 5 GHz, permitindo velocidades teóricas de até 54 Mbit/s. Apesar de oferecer maior capacidade, sua cobertura era mais limitada em comparação com o 802.11b.

2.1.11.3 Protocolo 802.11g (Wi-Fi 3)

O protocolo 802.11g, apresentado em 2003, combina a faixa de frequência de 2,4 GHz com velocidades de transmissão de até 54 Mbit/s, tornando-o popular devido à sua compatibilidade com dispositivos 802.11b.

2.1.11.4 Protocolo 802.11n (Wi-Fi 4)

Introduzido em 2009, esse protocolo trouxe uma mudança significativa ao Wi-Fi ao introduzir uma tecnologia de antenas que permitem a transmissão e recepção de vários sinais de rádio simultaneamente (*Multiple-Input Multiple-Output*, MIMO) e operações nas frequências de 2,4 GHz e 5 GHz. Isso permite velocidades de até 600 Mbit/s e uma cobertura aprimorada.

2.1.11.5 Protocolo 802.11ac (Wi-Fi 5)

Lançado em 2014, o Wi-Fi 5 trouxe melhorias substanciais em termos de velocidade e desempenho. Operando exclusivamente na faixa de 5 GHz, ele oferece velocidades de até vários gigabits por segundo, permitindo a transmissão de mídia de alta qualidade e uma experiência mais fluida em dispositivos conectados.

2.1.11.6 Protocolo 802.11ax (Wi-Fi 6)

O protocolo Wi-Fi 6, apresentado em 2019, representa uma evolução significativa na tecnologia Wi-Fi. Introduziu melhorias na eficiência espectral, permitindo que mais dispositivos se conectem simultaneamente. Além disso, oferece velocidades mais elevadas e maior eficiência energética (Cisco, 2023. b).

2.2 Algoritmos de criptografia mais comuns em redes Wi-Fi: WEP, WPA, WPA2 e WPA3

Rufino (2015) ressalta que, ao contrário das redes com cabos, onde é necessário se comunicar fisicamente ou remotamente com um componente da rede para acessar informações, nas redes sem fio, só é preciso ter um meio de receber o sinal. Isso significa que a captura das informações pode acontecer de maneira completamente passiva. O método proposto para abordar essa questão foi, no início, o WEP.

2.2.1 Algoritmo de Criptografia WEP

O WEP utiliza chaves estáticas para codificar os dados transmitidos na rede. Essas chaves são compartilhadas entre os dispositivos conectados e, uma vez definidas, permanecem constantes. O problema está na maneira como essas chaves são trocadas e armazenadas. Frequentemente, as redes WEP usa chaves predefinidas que podem ser descobertas com relativa facilidade através de métodos de análise e decodificação.

Adicionalmente, o WEP usa um vetor de inicialização (IV) curto, de 24 bits, para adicionar uma camada de complexidade à criptografia. O IV é um valor aleatório adicionado ao processo de criptografia para evitar que mensagens idênticas gerem códigos iguais. Entretanto, devido ao seu tamanho reduzido, ocorre repetições frequentes em redes com tráfego intenso, tornando a quebra da criptografia ainda mais simples. Invasores exploravam essas fragilidades por meio de ataques de dicionário e força bruta, testando diferentes combinações de chaves até encontrar a correta. Como consequência, o WEP se tornou notoriamente inseguro, levando à sua substituição por alternativas mais seguras e eficazes (REIS, s.d).

2.2.2 Algoritmo de Criptografia WPA

Segundo Rufino (2015) o Acesso Protegido por Wi-Fi (*Wi-Fi Protected Access*, WPA) é um método de segurança utilizado em redes Wi-Fi que veio como uma melhoria em relação ao WEP. Enquanto o WEP tem falhas que o torna vulnerável a ataques, o WPA busca corrigir essas vulnerabilidades. Um dos principais problemas que o WPA resolve está relacionado ao gerenciamento das chaves de criptografia. No WEP, as chaves são fixas e não mudam com frequência, o que torna mais fácil para invasores decifrarem essas chaves. Com o WPA, foi introduzido um novo sistema chamado Protocolo de Integridade de Chave Temporal (*Temporal Key Integrity Protocol*, TKIP), que torna as chaves mais fortes e as muda automaticamente em intervalos regulares. Isso torna a tarefa de adivinhar as chaves muito mais difícil para os invasores.

Além disso, o WPA também trouxe melhorias na autenticação. No WEP, a autenticação é baseada principalmente em chaves compartilhadas entre os dispositivos. No entanto, essas chaves são vulneráveis a ataques de adivinhação. No WPA, a autenticação é reforçada com uma técnica chamada de chave pré-

compartilhada (*Pre-Shared Key*, PSK), que utiliza senhas mais longas e complexas para tornar os ataques de adivinhação muito mais difíceis.

2.2.3 Algoritmo de Criptografía WPA2

O Acesso Protegido por Wi-fi 2 (*Wi-Fi Protected Access 2*, WPA2) é uma evolução do WPA, projetado para melhorar ainda mais a segurança das redes Wi-Fi. Assim como o WPA, o WPA2 abordou várias vulnerabilidades que eram conhecidas no WEP e trouxe aprimoramentos significativos. Uma das principais melhorias do WPA2 está no tipo de criptografia que ele usa. Enquanto o WPA usa o protocolo TKIP, o WPA2 adota o Padrão de Criptografia Avançado (*Advanced Encryption Standard*, AES). O AES é considerado uma das formas mais seguras de criptografia disponíveis atualmente. Ele usa chaves mais longas e complexas, o que torna extremamente difícil para invasores decifrarem a comunicação. Outra melhoria importante do WPA2 é a introdução do protocolo de autenticação 802.1X, que é mais robusto do que a autenticação baseada em chaves compartilhadas usada no WPA. Isso ajuda a proteger ainda mais a integridade das conexões Wi-Fi (Rufino, 2015).

Em termos práticos, o WPA2 proporciona uma camada significativamente mais forte de segurança para redes Wi-Fi em comparação com o WEP e até mesmo com o WPA. Muitas redes Wi-Fi públicas e privadas adota o WPA2 como um padrão de segurança devido à sua eficácia em proteger a privacidade e os dados dos usuários. Entretanto, ao longo dos anos, também foram identificadas vulnerabilidades no WPA2, o que levou ao desenvolvimento do WPA3, uma versão ainda mais avançada e segura dos algoritmos de criptografia em redes Wi-Fi.

2.2.4 Algoritmo de Criptografía WPA3

O Acesso Protegido por Wi-fi 3 (*Wi-Fi Protected Access 3*, WPA3) é a evolução mais recente e avançada dos algoritmos de segurança para redes Wi-Fi. Assim como o WPA2, o WPA3 foi desenvolvido para abordar ainda mais desafios de segurança e proteger a privacidade dos usuários. Uma das principais melhorias do WPA3 está na maneira como ele lida com a autenticação de dispositivos. Enquanto o WPA2 depende principalmente de senhas compartilhadas (PSKs), o WPA3 introduziu um novo protocolo de autenticação chamado Autenticação Simultânea de Iguais (*Simultaneous Authentication of Equals*, SAE). Essa técnica torna muito mais difícil para os invasores adivinharem ou quebrarem senhas, mesmo que sejam simples (NetSpot, s.d).

Outra característica importante do WPA3 é a criptografia individualizada. Em redes WPA2, todos os dispositivos compartilham uma única chave de criptografia, o que significa que se um invasor obtiver essa chave, ele poderá acessar todo o tráfego da rede. No WPA3, cada dispositivo recebe uma chave de criptografia única, o que torna praticamente impossível que um invasor adivinhe a chave e comprometa a rede inteira (Ribeiro, 2018).

3. Riscos de Conexão a Redes Wi-Fi de acesso Público

3.1 Ameaça à privacidade dos usuários

O uso de redes Wi-Fi de acesso público, embora conveniente, pode apresentar riscos significativos à privacidade dos usuários. É importante entender essas ameaças para tomar medidas de segurança adequadas ao utilizar redes públicas. Alguns dos principais ataques, ferramentas e métodos utilizados que podem comprometer a privacidade do usuário incluem:

3.1.1 Kali Linux

O Kali Linux é uma distribuição do sistema operacional Linux voltada especialmente para testes de penetração, análise forense e segurança da informação. Ele é mantido e atualizado pela equipe da Offensive Security, uma das principais referências mundiais na área de segurança cibernética. O que torna o Kali Linux tão popular entre profissionais da área é o fato de que ele já vem com centenas de ferramentas pré-instaladas, prontas para uso em diversas tarefas relacionadas à segurança digital. Entre essas ferramentas estão analisadores de rede, escâneres de vulnerabilidades, ferramentas de engenharia reversa, software para ataques de força bruta e, claro, suítes específicas para redes Wi-Fi como o Aircrack-ng. Além disso, o Kali Linux é gratuito e de código aberto, o que permite que qualquer pessoa possa baixá-lo, estudá-lo e adaptá-lo às suas necessidades. A interface pode ser usada tanto em modo gráfico quanto via linha de comando, sendo muito flexível para quem já tem experiência técnica. Outro diferencial importante do Kali é o suporte a diversos ambientes, podendo ser instalado em máquinas físicas, máquinas virtuais, ou até mesmo ser executado diretamente a partir de um *pendrive*, sem a necessidade de instalação permanente no computador. Isso facilita o uso em ambientes de testes ou em auditorias temporárias (Hertzog, 2017).

3.1.2 Suíte Aircrack-ng

De acordo com Moreno (2016), o aircrack-ng representa uma suíte de ferramentas destinada à auditoria de redes sem fio. Essa abrangente coleção engloba diversas utilidades, incluindo o Airmon-ng utilizado para criar ou finalizar interfaces em modo monitor, Airodump-ng usado para capturar pacotes, Aireplay-ng contém múltiplos vetores de ataque que são combinados com outras ferramentas como o Packetforge-ng e Aircrack-ng, e entre outras ferramentas existententes no aircrack-ng. Abaixo, estão descritas algumas ferramentas disponíveis e suas principais finalidades:

3.1.2.1 Airmon-ng

A ferramenta airmon-ng é responsável por colocar a placa de rede sem fio em modo monitor. Esse modo permite que o dispositivo capture todos os pacotes que estão sendo transmitidos no ambiente, mesmo aqueles que não são destinados diretamente a ele. Em resumo, é a primeira etapa para iniciar qualquer análise ou auditoria de rede sem fio.

3.1.2.2 Airodump-ng

O airodump-ng é utilizado para monitorar o tráfego das redes Wi-Fi ao redor. Ele coleta informações como nome da rede (SSID), endereço MAC do roteador (BSSID), canal utilizado, nível de sinal e quantidade de dispositivos conectados. Além disso, é com ele que se realiza a captura de *handshakes*, necessária para a quebra da senha de redes protegidas.

3.1.2.3 Aireplay-ng

A ferramenta aireplay-ng permite a simulação de ataques em redes Wi-Fi, com o objetivo de forçar comportamentos específicos e capturar pacotes úteis para análise. Um dos usos mais comuns é a desautenticação de clientes conectados à rede, o que força uma reconexão e facilita a captura do *handshake*.

3.1.2.4 Aircrack-ng

O aircrack-ng é uma das ferramentas mais conhecidas da suíte. É com ela que se realiza a quebra da chave de segurança da rede (normalmente WPA ou WPA2-PSK). Após a captura do *handshake*, o aircrack-ng realiza um ataque de força bruta ou dicionário sobre o arquivo capturado, tentando descobrir a senha utilizada na rede.

3.1.2.5 Airbase-ng

A ferramenta airbase-ng é utilizada para criar pontos de acesso falsos (também chamados de *evil twins*). Com ela, é possível simular uma rede Wi-Fi legítima para enganar usuários e capturar informações que eles enviam ao tentar se conectar. É uma ferramenta muito utilizada em ataques de engenharia social e testes de segurança.

3.1.2.6 Airdecloak-ng

O airdecloak-ng tem uma função bastante específica: ele é capaz de remover o "ruído" de arquivos de captura que contenham redes com *cloaking* (ocultação de SSID). Em alguns casos, mesmo quando o SSID está escondido, os dados ainda são transmitidos. Essa ferramenta ajuda a limpar a captura e recuperar informações úteis.

3.1.2.7 Airolib-ng

O airolib-ng é uma ferramenta de gerenciamento de dicionários. Ele permite criar e organizar grandes listas de palavras e senhas pré-calculadas, o que torna o processo de quebra de senhas mais rápido e eficiente quando utilizado em conjunto com o aircrack-ng.

3.1.2.8 Packetforge-ng

O packetforge-ng permite a criação de pacotes personalizados, que podem ser injetados em uma rede. Isso é especialmente útil em cenários em que é necessário gerar tráfego artificial para capturar pacotes úteis ou acelerar processos de autenticação.

3.1.3 Modos de operação da placa de rede

O modo gerenciado é a abordagem convencional de operação para um STA (*Station*), que se refere a qualquer dispositivo com capacidade de se conectar a uma rede sem fio, como notebooks, smartphones e tablets. Nesse modo, a conexão é estabelecida com um ponto de acesso, e a placa de rede sem fio não tem a capacidade de monitorar e capturar dados da rede, apenas de enviar e receber informações destinadas ao STA.

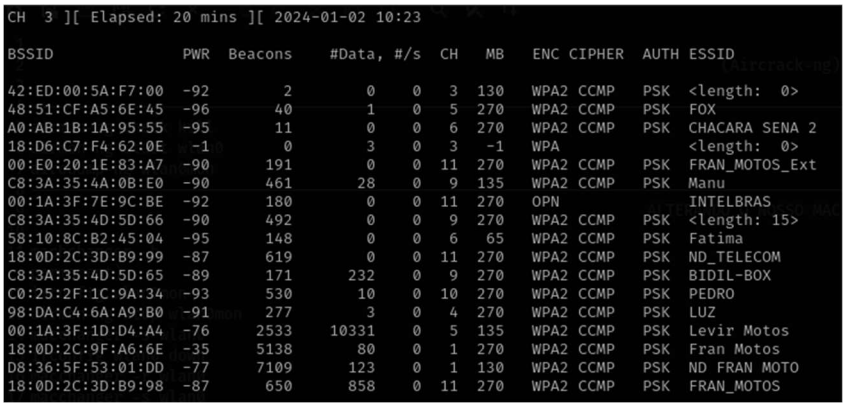
Diferentemente do modo gerenciado que uma placa de rede só processa os dados enviados diretamente ao seu endereço. O modo promíscuo altera esse comportamento, fazendo com que a placa intercepte qualquer pacote de dados que passe pela rede, independentemente do seu destino original. Isso permite analisar o tráfego de outros dispositivos, o que em condições normais não seria possível.

Por outro lado, o modo monitor é uma configuração que permite que a placa *wireless* monitore e capture todo o tráfego de dados de um Conjunto de Serviço Básico (*Basic Service Set*, BSS), que é o conjunto de dispositivos sem fio que se comunicam dentro de uma mesma rede Wi-Fi, incluindo um ponto de acesso e as estações conectadas a ele. Indo além dos dados destinados ao STA, esse modo também possibilita a captura de pacotes sem a necessidade de o invasor se associar ao ponto de acesso (Moreno 2016).

Nas Figuras 10 e 11 podemos observar um exemplo prático de uma placa de rede em modo de monitoramento:

A Figura 10 mostra a primeira parte da saída do comando airodump-ng, uma ferramenta do pacote Aircrack-ng, utilizada para capturar pacotes de redes Wi-Fi enquanto a placa de rede está no modo monitor. Esse modo permite que a placa capture pacotes sem precisar se conectar a uma rede específica:

Figura 10 – Primeira tabela do monitoramento ativo.



```
CH  3 ][ Elapsed: 20 mins ][ 2024-01-02 10:23

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

42:ED:00:5A:F7:00  -92        2        0    0   3  130   WPA2 CCMP   PSK  <length:  0>
48:51:CF:A5:6E:45  -96       40        1    0   5  270   WPA2 CCMP   PSK  FOX
A0:AB:1B:1A:95:55  -95       11        0    0   6  270   WPA2 CCMP   PSK  CHACARA SENA 2
18:D6:C7:F4:62:0E   -1        0        3    0   3   -1   WPA              <length:  0>
00:E0:20:1E:83:A7  -90      191        0    0  11  270   WPA2 CCMP   PSK  FRAN_MOTOS_Ext
C8:3A:35:4A:0B:E0  -90      461       28    0   9  135   WPA2 CCMP   PSK  Manu
00:1A:3F:7E:9C:BE  -92      180        0    0  11  270   OPN              INTELBRAS
C8:3A:35:4D:5D:66  -90      492        0    0   9  270   WPA2 CCMP   PSK  <length: 15>
58:10:8C:B2:45:04  -95      148        0    0   6   65   WPA2 CCMP   PSK  Fatima
18:0D:2C:3D:B9:99  -87      619        0    0  11  270   WPA2 CCMP   PSK  ND_TELECOM
C8:3A:35:4D:5D:65  -89      171      232    0   9  270   WPA2 CCMP   PSK  BIDIL-BOX
C0:25:2F:1C:9A:34  -93      530       10    0  10  270   WPA2 CCMP   PSK  PEDRO
98:DA:C4:6A:A9:B0  -91      277        3    0   4  270   WPA2 CCMP   PSK  LUZ
00:1A:3F:1D:D4:A4  -76     2533    10331    0   5  135   WPA2 CCMP   PSK  Levir Motos
18:0D:2C:9F:A6:6E  -35     5138       80    0   1  270   WPA2 CCMP   PSK  Fran Motos
D8:36:5F:53:01:DD  -77     7109      123    0   1  130   WPA2 CCMP   PSK  ND FRAN MOTO
18:0D:2C:3D:B9:98  -87      650      858    0  11  270   WPA2 CCMP   PSK  FRAN_MOTOS
```

Fonte: Elaborado pelo autor (2024).

A primeira tabela, exibida na Figura 10, mostra os pontos de acesso (APs) detectados e suas características:

- **BSSID:** Endereço MAC *(Media Access Control*) do roteador, que se refere a um identificador único que identifica um dispositivo de rede.
- **PWR:** Força do sinal (quanto mais próximo de 0, melhor o sinal).
- **Beacons:** Pacotes de *broadcast* enviados pelo AP para anunciar sua presença. Broadcast é um tipo de transmissão em que a mesma mensagem é enviada para todos os dispositivos dentro da rede, sem a necessidade de um destinatário específico.
- **#Data, #/s:** Pacotes de dados capturados e taxa de pacotes por segundo.
- **CH:** Canal em que o AP está operando.
- **MB:** Velocidade máxima suportada.
- **ENC:** Tipo de criptografia (WPA2, WEP, etc.).
- ***CIPHER*:** Algoritmo de criptografia utilizado (CCMP, TKIP).
- **AUTH:** Método de autenticação (PSK para senha compartilhada, MGT para autenticação corporativa).
- **ESSID:** Nome da rede Wi-Fi.

A Figura 11 mostra a segunda parte resultante do comando airodump-ng:

Figura 11 – Segunda tabela do monitoramento ativo.

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
18:D6:C7:F4:62:0E	B8:AB:62:89:7D:3F	-87	0 - 1e	0	4		
C8:3A:35:4A:0B:E0	9A:77:9F:BB:A8:86	-93	0 - 1	0	39		
(not associated)	26:D9:B1:D0:3D:5D	-88	0 - 1	0	6		Maria
(not associated)	82:77:47:EC:99:71	-75	0 - 1	0	4		
(not associated)	30:4A:26:8B:6A:6E	-87	0 - 1	0	190		
C8:3A:35:4D:5D:65	04:E5:98:70:32:A8	-93	1e- 1	0	50		
C8:3A:35:4D:5D:65	64:1C:AE:F9:B8:63	-1	1e- 0	0	186		
C0:25:2F:1C:9A:34	AA:AE:74:F7:FC:57	-1	1e- 0	0	7		
C0:25:2F:1C:9A:34	0E:D8:58:DF:64:77	-90	0 - 1e	0	168		PEDRO
00:1A:3F:1D:D4:A4	1C:CC:D6:1E:0A:ED	-94	24e- 1e	0	23		
00:1A:3F:1D:D4:A4	96:A9:0E:B9:FF:08	-94	1e- 1e	0	540		Levir Motos
00:1A:3F:1D:D4:A4	06:66:27:F8:E2:C0	-77	24e- 1	0	5989		
00:1A:3F:1D:D4:A4	EE:B2:8D:38:1E:D0	-79	24e- 1e	0	4851		Levir Motos

Fonte: Elaborado pelo autor (2024).

A segunda tabela, exibida na Figura 11, mostra dispositivos conectados aos APs:

- **BSSID:** Endereço MAC do AP ao qual o dispositivo está conectado (ou "*not associated*" se não estiver conectado).
- ***STATION*:** Endereço MAC do dispositivo cliente.
- **PWR:** Força do sinal do dispositivo.
- ***Rate*:** Taxa de transmissão de dados.
- ***Lost*:** Pacotes perdidos.
- ***Frames*:** Quantidade de pacotes capturados desse dispositivo.
- ***Probes*:** Se o dispositivo estiver buscando redes, aqui aparece a lista de SSIDs que ele tentou acessar.

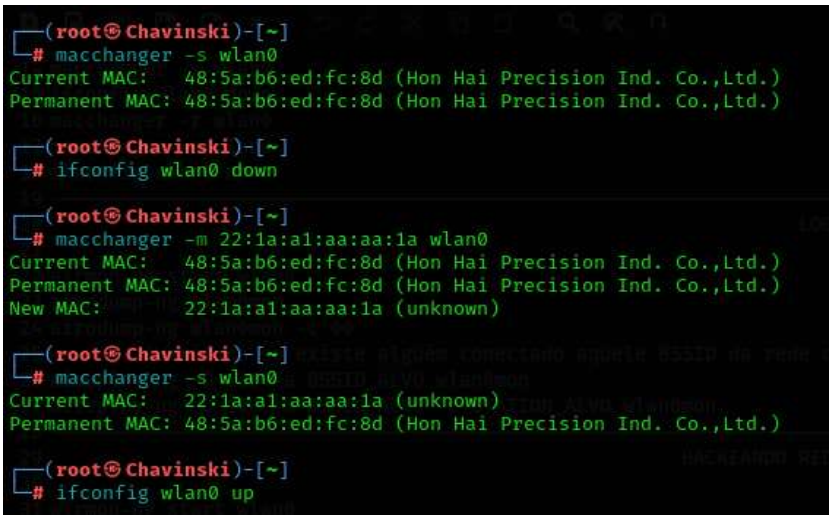
3.1.4 Clonagem de MAC

Ao clonar o endereço MAC de um dispositivo já conectado à rede, os atacantes buscam permanecer nas sombras, evitando detecção e contornando eventuais filtros de segurança baseados em MAC. Essa técnica proporciona anonimato ao atacante, permitindo que ele se infiltre na rede sem associar-se diretamente ao ponto de acesso.

Além disso, a clonagem de MAC pode ser usada como uma forma de falsificação de identidade, possibilitando ao atacante se passar por outro dispositivo autorizado na rede. Isso pode levar a acessos não autorizados a recursos e informações sensíveis.

Na Figura 12 temos um exemplo de como é realizada a troca de MAC para se passar por outro dispositivo.

Figura 12 – Alteração de MAC da placa de rede.



Fonte: Elaborado pelo autor (2024).

A Figura 12 mostra comandos sendo executados para alterar o endereço MAC da interface de rede sem fio "wlan0". Aqui está uma explicação passo a passo do que está acontecendo:

- Verificação do MAC atual:
  - O comando macchanger -s wlan0 exibe o endereço MAC atual e o permanente da interface de rede (wlan0).
  - O MAC original (permanente) é 48:5a:b6:ed:fc:8d, pertencente à fabricante Hon Hai Precision Ind. Co., Ltd.
- Desativação da interface de rede:
  - O comando ifconfig wlan0 down desativa a interface de rede sem fio (wlan0). Isso é necessário antes de modificar o endereço MAC.
- Mudança do endereço MAC:
  - O comando macchanger -m 22:1a:aa:aa:aa:1a wlan0 altera o MAC da interface para 22:1a:aa:aa:aa:1a.
  - Após a execução, a saída do comando mostra o novo MAC configurado.

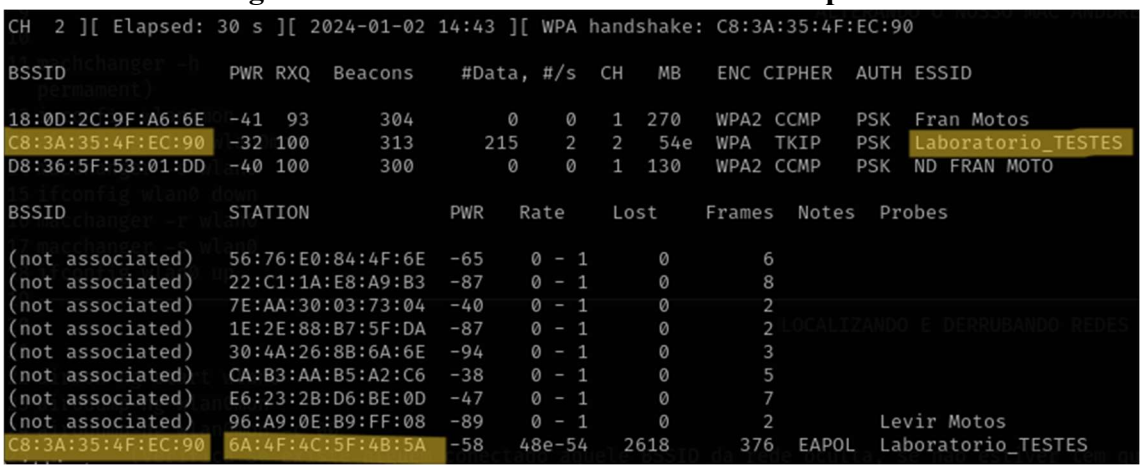
- Verificação da alteração:
  - O comando macchanger -s wlan0 é executado novamente para conferir se o MAC foi alterado com sucesso.
  - O Current MAC agora aparece como 22:1a:aa:aa:aa:1a (unknown), o que confirma a modificação.
- Reativação da interface de rede:
  - O comando ifconfig wlan0 up é executado para reativar a interface de rede sem fio e permitir a conexão normalmente com o novo endereço MAC.

3.1.5 Ataque de Desautenticação

Esse tipo de ataque envolve a manipulação de pacotes para forçar a desconexão temporária de dispositivos conectados a uma determinada rede. A consequência imediata é a interrupção temporária do serviço, causando inconvenientes para os usuários legítimos da rede.

Nas Figuras 13 e 14 podemos observar um exemplo de um ataque de desautenticação, as figuras mostram um terminal do Kali Linux onde estão sendo utilizados dois programas bastante conhecidos para testes de segurança em redes Wi-Fi, o Airodump-ng e o Aireplay-ng, que fazem parte do pacote Aircrack-ng.

Figura 13 – Monitoramento de Redes Wi-Fi próximas.

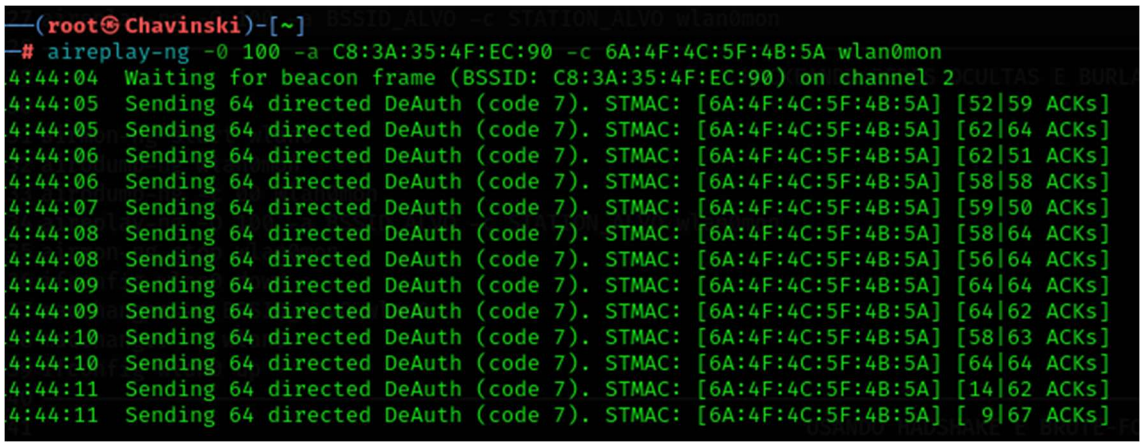


Fonte: Elaborado pelo autor (2024).

Na figura 13, o comando airodump-ng está sendo utilizado para monitorar redes Wi-Fi próximas e capturar pacotes de dados. Algumas informações exibidas:

- O BSSID: Endereço MAC do ponto de acesso (AP).
- BSSID: Endereço MAC do ponto de acesso (AP).
- PWR: Intensidade do sinal recebido.
- # Data: Pacotes capturados da rede.
- CH: Canal da rede Wi-Fi.
- ENC: Tipo de criptografia usada (WPA2, WEP, etc.).
- ESSID: Nome da rede (SSID).

Figura 14 – Ataque de Desautenticação em determinado alvo.



Fonte: Elaborado pelo autor (2024).

Na Figura 14, o comando aireplay-ng -0 5 -a CB:3A:35:AF:EC:90 wlan0mon está sendo usado para realizar um ataque de desautenticação. Algumas informações exibidas:

- "-0" indica um ataque de deauth (desautenticação).
- "100" especifica que serão enviados 100 pacotes de desautenticação.
- "-a CB:3A:35:AF:EC:90" define o BSSID do ponto de acesso alvo.
- "wlan0mon" é a interface de rede sem fio em modo monitor.

Na saída do comando, podemos ver que o ataque está enviando pacotes de DeAuth (código 7) para desconectar dispositivos conectados ao roteador alvo. O objetivo pode ser para simplesmente causar interrupção na rede ou forçar um cliente a se reconectar para capturar um aperto de mão (*handshake)*. Mais à frente veremos um exemplo de captura de *handshake* e um ataque utilizando essa captura para tentar descobrir a senha de uma rede Wi-Fi.

3.1.6 *Sniffing*

A prática de "sniffing" em redes Wi-Fi consiste na interceptação e análise do fluxo de dados que trafega em uma determinada rede sem fio. Essa técnica permite a observação das comunicações que ocorrem na rede, mesmo que não sejam diretamente destinadas ao dispositivo que realiza a captura. Nesse contexto, o objetivo é capturar informações sensíveis, como senhas e dados de login, que estão sendo transmitidos entre os dispositivos conectados à rede. Durante um ataque de "*sniffing*", um atacante pode utilizar ferramentas especializadas para capturar e analisar pacotes de dados, extraindo informações valiosas. Esse processo pode ser conduzido de maneira passiva, sem a necessidade de conexão direta à rede, ou através da criação de um ponto de acesso falso (ataque de Homem no Meio), levando os dispositivos a se conectarem a uma rede controlada pelo atacante.

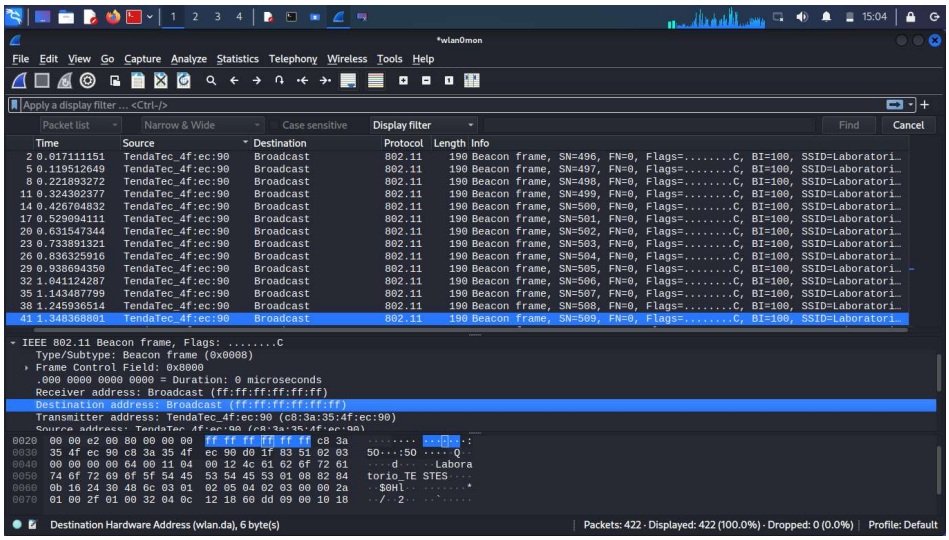
Esse ataque tende a ser mais bem-sucedidos em redes Wi-Fi abertas (sem senha) ou que não utilizam criptografia, pois a ausência de proteção facilita o acesso e a leitura

das informações transmitidas, tornando a rede um alvo mais vulnerável. Nessas circunstâncias, a rede se torna mais suscetível à interceptação e visualização não autorizada do tráfego de dados. Em redes desprovidas de criptografia ou com criptografia Open, dados como senhas e informações de login são transmitidos sem qualquer forma de codificação, facilitando a leitura e captura por um possível atacante. Essa vulnerabilidade pode resultar na exposição de informações confidenciais.

Como medida preventiva, é altamente recomendável adotar protocolos de criptografia mais robustos, tais como WPA2 ou WPA3. Esses protocolos proporcionam camadas adicionais de segurança, dificultando significativamente a execução de "*sniffing*" e assegurando a integridade e confidencialidade das comunicações na rede Wi-Fi.

A Figura 15 ilustra uma captura real de pacotes realizada por meio da ferramenta *Wireshark*, que permite a interceptação e análise do tráfego em redes sem fio.

Figura 15 – *Sniffing* com *Wireshark* em uma rede Wi-Fi.



Fonte: Elaborado pelo autor (2024).

No exemplo, é possível observar *frames*, que são pequenas unidades de dados transmitidas na rede, e *Beacon Frames*, que são sinais enviados periodicamente pelo roteador para anunciar a existência da rede Wi-Fi. Ferramentas como essa podem ser utilizadas para auditoria e monitoramento legítimos, mas também podem ser exploradas por atacantes para interceptar dados em redes vulneráveis, como destacado anteriormente.

3.1.7 Ataque de Homem no Meio (*Man-in-the-Middle*)

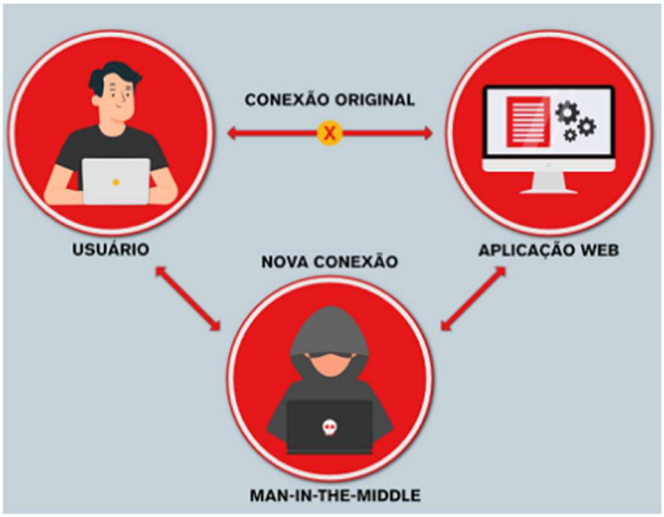
Um dos ataques mais comuns em redes Wi-Fi públicas é o chamado Homem no Meio (*Man-in-the-Middle*, MitM). Um invasor intercepta a comunicação entre o usuário e uma aplicação web. Em vez de o usuário se conectar diretamente ao serviço desejado, o atacante se posiciona entre os dois, criando uma nova conexão e capturando informações sensíveis, como credenciais de login e dados bancários. Esse

tipo de ataque é especialmente perigoso em redes Wi-Fi públicas desprotegidas, pois facilita a interceptação do tráfego sem que a vítima perceba.

Um exemplo prático desse cenário pode ser observado quando o usuário tenta acessar o site do seu banco: o invasor intervém no seu acesso, estabelecendo uma conexão entre você e o banco, obtendo acesso a informações confidenciais, como a senha da sua conta, informações de cartões, tokens e outros métodos de autenticação, conquistando, assim, acesso à sua conta (Gogoni, 2020).

A figura 16 ilustra o funcionamento do ataque *Man-in-the-Middle*:

Figura 16 – Ataque Homem no Meio.



Fonte: Claranet (s.d)

3.1.8 *Honeypot e Evil Twin*

Diversas técnicas são empregadas por invasores, como a criação de redes pote de mel (*honeypot*), que são pontos de acesso falsos usados para atrair conexões e monitorar atividades. Embora *honeypots* sejam normalmente usados por pesquisadores de segurança para detectar ataques, criminosos também podem implantá-los em locais legítimos, como hotéis e restaurantes, para capturar dados de usuários desavisados.

Além disso, há a utilização do ataque gêmeo malvado (*evil twin*), que é um tipo de técnica de falsificação (*spoofing)*, ou seja, uma falsificação de identidade no ambiente Wi-Fi. Nesse ataque, o hacker cria um ponto de acesso idêntico à rede legítima, copiando seu nome (SSID) e método de autenticação. Para tornar o golpe mais eficaz, a rede original pode ser desativada, forçando dispositivos configurados para conexão automática a se conectarem ao ponto de acesso falso.

Em ambos os cenários, o invasor pode monitorar as atividades dos usuários, capturar credenciais, acessar dados sensíveis e até disseminar *malwares* (Gogoni, 2020).

3.1.9 Fragilidade na autenticação WEP

A identificação de vulnerabilidades na autenticação WEP é um tema crucial quando se trata da segurança em redes Wi-Fi. A histórica adoção da criptografia WEP revela falhas substanciais que comprometem a efetividade dos mecanismos de proteção. O principal problema com o WEP é que os Vetores de Inicialização (*Initialization Vector*, IVs) são relativamente curtos, o que significa que eles podem ser facilmente repetidos em uma rede ocupada, facilitando ataques de criptoanálise como foi mencionado no item 2.5.1. Isso torna o WEP vulnerável a ataques de captura de pacotes e recuperação da chave de criptografia.

Os IVs são valores de inicialização que são combinados com uma chave pré-compartilhada para criptografar os dados transmitidos através da rede sem fio. Eles são usados juntamente com a chave WEP para gerar o fluxo de bits (*binary digit*) pseudoaleatório que é então combinado com os dados para produzir o texto cifrado.

Segue na Tabela 2 um passo a passo de como é realizado o ataque por criptoanálise:

Tabela 2 - Procedimento de Ataque à Criptografia WEP.

Passo	Comando	Descrição da Ação
1	`airmon-ng start wlan0`	Ativa o modo de monitoramento da placa de rede sem fio (`wlan0`).
2	`airodump-ng wlan0mon`	Inicia o monitoramento do tráfego de rede na interface em modo monitor (`wlan0mon`).
3	(Análise da saída de `airodump-ng`)	Identifica a rede alvo e obtém o BSSID (endereço MAC do roteador alvo).
4	`airodump-ng -c 2 --bssid A0:AB:1B:1A:95:55 -w ChaveWEP wlan0mon`	Inicia a captura de pacotes direcionada ao canal (`-c 2`) e BSSID (`--bssid A0:AB:1B:1A:95:55`) da rede alvo, salvando-os no arquivo `ChaveWEP.cap` .
5	`aireplay-ng -3 -b A0:AB:1B:1A:95:55 -h F6:6C:2B:D5:70:FF wlan0mon`	Injeta pacotes ARP (`-3`) na rede alvo (`-b A0:AB:1B:1A:95:55`) falsificando o MAC do cliente (`-h F6:6C:2B:D5:70:FF`) para acelerar a captura de IVs.
6	`aircrack-ng -a 1 -e NOME_DA_REDE ChaveWEP.cap`	Executa a criptoanálise (`-a 1` para WEP) no arquivo de captura (`ChaveWEP.cap`) para descobrir a chave da rede (`-e NOME_DA_REDE`).

Fonte: Elaborado pelo autor (2025).

3.1.10 Ataque de força bruta WPA/WPA2

Esse tipo de ataque explora a vulnerabilidade nos protocolos de segurança WPA e WPA2, especificamente durante o processo de *handshake*, que é a troca de mensagens entre um dispositivo cliente e um ponto de acesso para estabelecer uma

conexão segura. Um atacante captura o *handshake* e, em seguida, utiliza técnicas de força bruta para tentar adivinhar a senha por meio de sucessivas tentativas.

Ferramentas como Aircrack-ng são frequentemente empregadas para realizar esse tipo de ataque, que é um dos métodos mais conhecidos para comprometer a segurança de redes Wi-Fi protegidas por senhas fracas.

Na Tabela 3, é possível acompanhar o passo a passo da realização de um ataque de força bruta: Para essa demonstração, foi criada uma rede Wi-Fi com o nome 'laboratorio_teste' e senha 'laboratorio123'.

Tabela 3 - Etapas e Comandos do Ataque de Força Bruta WPA/WPA2.

Passo	Comando	Descrição do Processo
1	`airmon-ng start wlan0`	Ativação da interface de rede sem fio (`wlan0`) para o modo de monitoramento, permitindo a captura de tráfego não direcionado.
2	`airodump-ng -c 2 --bssid C8:3A:35:4F:EC:90 -w Captura_laboratorio wlan0mon`	Inicialização do monitoramento no canal específico (`-c 2`) da rede alvo (BSSID `C8:3A:35:4F:EC:90`), salvando os pacotes capturados no arquivo `Captura_laboratorio.cap` .
3	(Análise da saída de `airodump-ng`)	Identificação de um cliente (Station) conectado à rede alvo (BSSID `C8:3A:35:4F:EC:90`). Exemplo de cliente: `6A:AF:4C:5F:4B:5A` .
4	`aireplay-ng -0 100 -a C8:3A:35:4F:EC:90 -c 6A:4F:4C:5F:4B:5A wlan0mon`	Execução do ataque de desautenticação (`-0 100`) direcionado ao cliente (`-c 6A:4F:4C:5F:4B:5A`) conectado à rede alvo (`-a C8:3A:35:4F:EC:90`) para forçar a reconexão e capturar o handshake WPA.
5	(Verificação da saída de `airodump-ng`)	Confirmação da captura do handshake WPA, indicado pela mensagem "WPA handshake: C8:3A:35:4F:EC:90".
6	(Verificação dos arquivos gerados)	Verificação da criação do arquivo `.cap` (`Captura_laboratorio-01.cap`), contendo os pacotes capturados, incluindo o handshake.
7	`aircrack-ng -b C8:3A:35:4F:EC:90 -w /home/chavinski/Documentos/wordlist.txt Captura_laboratorio-01.cap`	Execução do ataque de força bruta (`aircrack-ng`) utilizando um dicionário de senhas (`-w /home/chavinski/Documentos/wordlist.txt`) contra o handshake capturado (`Captura_laboratorio-01.cap`) da rede alvo (`-b C8:3A:35:4F:EC:90`).
8	(Análise da saída de `aircrack-ng`)	Exibição da senha da rede Wi-Fi ("KEY FOUND! [laboratorio123]") após a correspondência ser encontrada no dicionário.

Fonte: Elaborado pelo autor (2025).

A eficácia do ataque por força bruta, mostrado na Tabela 3, depende principalmente da qualidade e da variedade da *wordlist* utilizada. Essa *wordlist* nada mais é do que um arquivo de texto contendo uma grande quantidade de possíveis combinações de senhas. Na prática, é possível encontrar listas com milhares de senhas

prontas para serem utilizadas nesses testes, o que aumenta consideravelmente as chances de sucesso.

É importante destacar que essas senhas não são testadas diretamente no roteador da rede alvo. Em vez disso, ferramentas como o aircrack-ng utilizam o *handshake* previamente capturado para fazer a comparação com cada senha da *wordlist*. Essa forma de atuação é vantajosa porque evita que o roteador identifique e bloqueie várias tentativas de acesso, o que poderia ocorrer em um ataque direto.

4. Estudo de Caso na cidade de Cuité de Mamanguape

Para compreender a segurança das redes Wi-Fi na cidade de Cuité de Mamanguape, foi realizado um estudo de caso focado exclusivamente em redes públicas, desconsiderando redes de uso pessoal ou privado. A análise teve como objetivo identificar os padrões de segurança adotados nos principais pontos de acesso da cidade, priorizando áreas centrais e locais com maior fluxo de pessoas. Além disso, foram observados os canais de transmissão utilizados, os quais, embora não sejam o foco principal, podem influenciar na qualidade e segurança da comunicação sem fio.

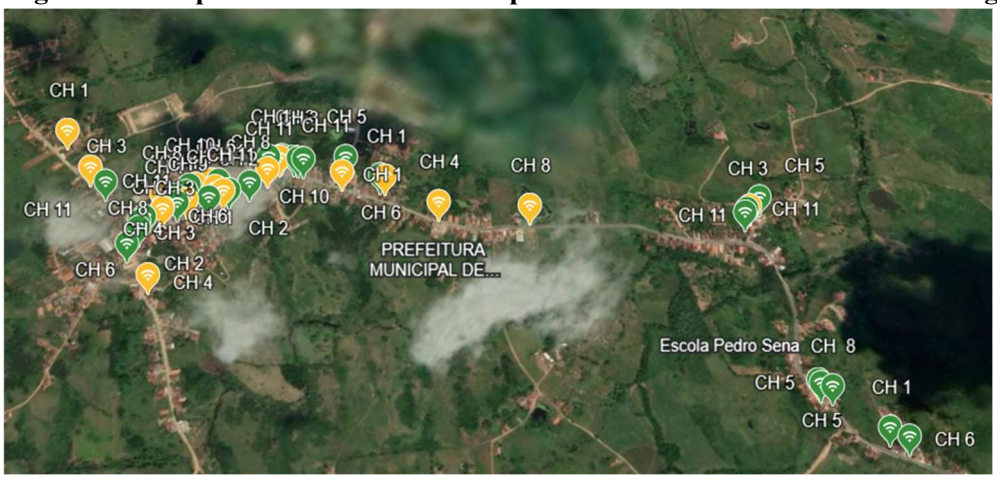
O levantamento foi conduzido no dia 24 de fevereiro de 2025, com início às 20h e término às 23h30. A coleta de dados foi feita utilizando um notebook com o sistema operacional Kali Linux, configurado em modo de monitoramento ativo. O equipamento permaneceu dentro de um carro durante todo o processo, sendo conduzido lentamente pelos pontos estratégicos da cidade. A identificação das redes e a coleta de informações sobre criptografia e canais foram realizadas com o auxílio da ferramenta Airodump-ng, e os dados exibidos na tela foram registrados por meio de fotografias, garantindo a integridade das informações capturadas.

Para assegurar a precisão dos resultados, foram feitas duas passagens por cada local de análise, em horários distintos dentro do intervalo de coleta. Também foi realizado o georreferenciamento das redes públicas detectadas com o auxílio do Google Earth, facilitando a organização espacial dos dados. Importante destacar que, para evitar inconsistências e a inclusão de redes falsas, foram analisados os nomes das redes Wi-Fi em associação com o nome ou características do local onde estavam situadas, garantindo maior confiabilidade às informações coletadas.

4.1 Análise das Criptografias e Canais das Redes Wi-Fi Públicas

A Figura 17 apresenta o mapeamento de redes Wi-Fi públicas identificadas na cidade, destacando os diferentes tipos de criptografia utilizados e os canais de transmissão de cada uma.

Figura 17 – Mapeamento de redes Wi-Fi públicas na cidade de Cuité de Mamanguape.



Fonte: Elaborado pelo autor (2025).

Cada ponto de acesso foi identificado e classificado com base no tipo de criptografia empregada, sendo que:

- Ícones amarelos representam redes que utilizam WPA.
- Ícones verdes indicam redes protegidas com WPA2.

Além disso, foi adicionada uma legenda com os canais de transmissão utilizados por cada rede, permitindo uma análise da distribuição do espectro de frequência. Como mostrado na Figura 17, observa-se uma predominância de redes com criptografia WPA2, indicando um nível de segurança mais elevado em comparação ao WPA.

A análise desses dados permite identificar possíveis vulnerabilidades e interferências entre redes, contribuindo para futuras recomendações de melhoria na segurança e desempenho das conexões públicas.

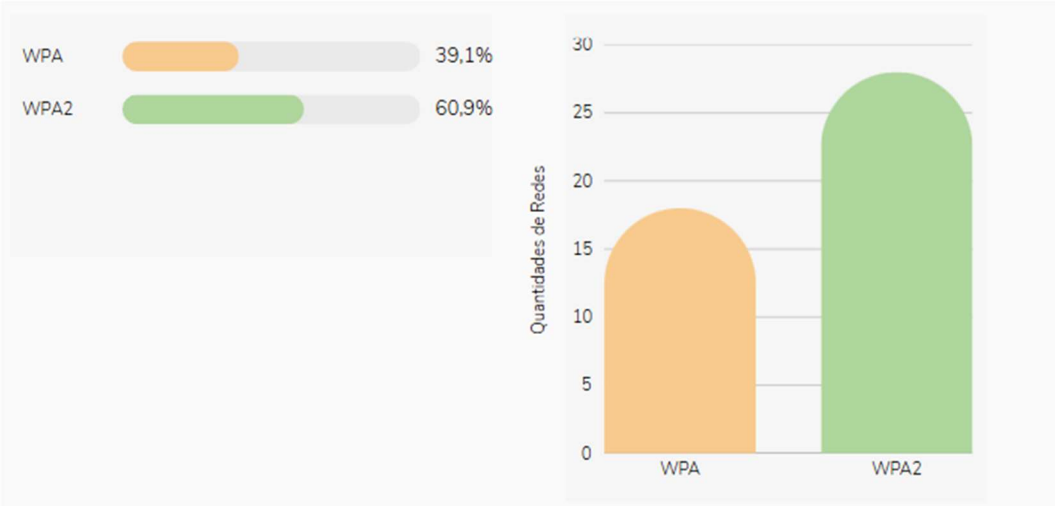
4.1.1 Distribuição das Criptografias Utilizadas

Durante o estudo de caso, foram analisadas 46 redes Wi-Fi públicas na cidade. Os resultados demonstraram que a maioria das redes utiliza o protocolo WPA2, totalizando 28 redes (60,87%), enquanto 18 redes (39,13%) ainda operam com WPA. Esses dados indicam uma predominância do WPA2, que é considerado um protocolo mais seguro em relação ao WPA, embora ainda existam redes que utilizam uma tecnologia menos robusta em termos de proteção.

A presença significativa de redes com WPA pode representar um risco de segurança para os usuários, visto que esse protocolo possui vulnerabilidades conhecidas e métodos de ataque que podem comprometer sua integridade. Esse levantamento reforça a importância da adoção de práticas mais seguras para a proteção das redes públicas e dos dados dos usuários.

É apresentado na Figura 18 a distribuição das redes Wi-Fi analisadas no estudo, destacando a proporção entre redes configuradas com WPA e WPA2.

Figura 18 – Distribuição das redes Wi-Fi por tipo de criptografia.

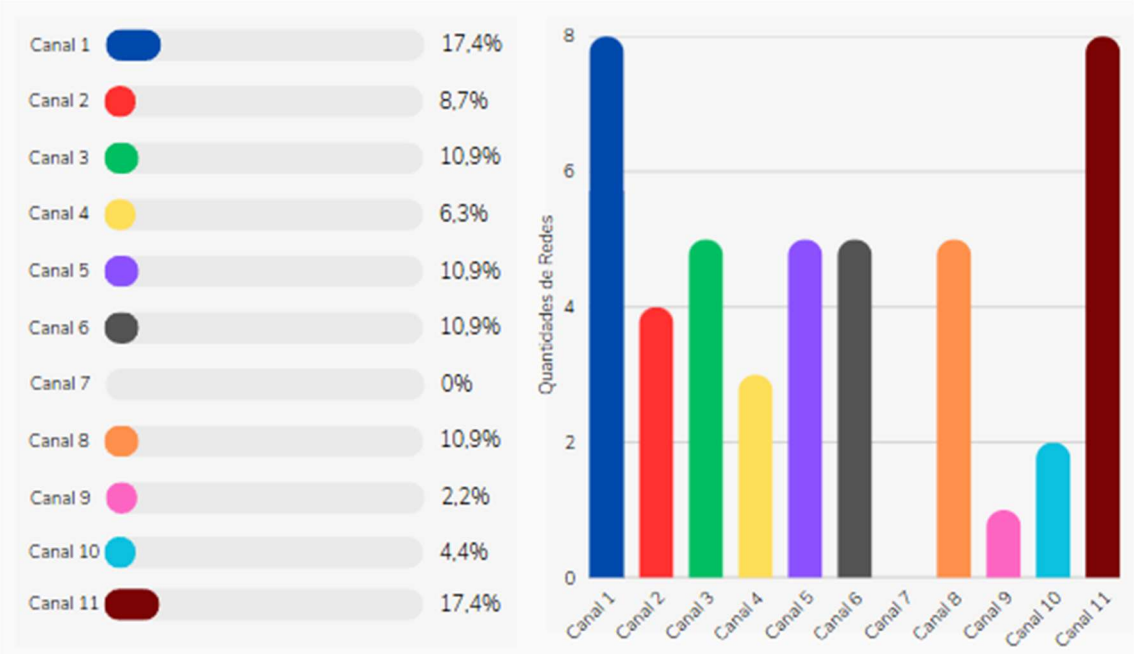


Fonte: Elaborado pelo autor (2025).

4.1.2 Distribuição dos Canais Utilizados

Na análise das redes identificamos a distribuição dos canais utilizados para transmissão do sinal. A figura 19 mostra a distribuição dos canais utilizados pelas redes analisadas:

Figura 19 – Distribuição dos canais Wi-Fi.



Fonte: Elaborado pelo autor (2025).

Como podemos verificar na figura 19 os canais mais utilizados foram os canais 1 e 11, ambos com 8 redes configuradas, seguidos pelos canais 3, 5, 6 e 8, cada um em 5 redes. Os canais 2 e 4 apresentaram uma utilização menor, com 4 e 3 redes, respectivamente. Já os canais 9 e 10 foram os menos utilizados, em 1 e 2 redes configuradas.

A escolha dos canais influencia diretamente na qualidade da conexão, uma vez que redes operando no mesmo canal podem sofrer interferências, especialmente em locais com alta densidade de redes Wi-Fi. Idealmente, a distribuição dos canais deveria ser melhor equilibrada para minimizar sobreposições e melhorar a eficiência do espectro de frequências disponível.

5. Orientações para proteção e privacidade do usuário

5.1 Boas práticas de segurança para usuários de redes Wi-Fi públicas

Segundo a Kaspersky, empresa especializada em segurança digital, muitos locais como cafeterias, shoppings e aeroportos oferecem redes Wi-Fi públicas para seus clientes. Embora seja conveniente para acessar e-mails, redes sociais e outros serviços online, essas conexões podem representar riscos. Criminosos costumam monitorar esse tipo de rede para capturar dados sigilosos, como credenciais bancárias e senhas (Kaspersky, s.d).

Para minimizar esses riscos, especialistas em segurança recomendam algumas medidas:

- **Ficar atento ao risco:** Redes Wi-Fi abertas não são seguras por padrão, exigindo precaução ao acessá-las.

- **Todos os dispositivos estão vulneráveis:** Laptops, smartphones e tablets podem ser alvos de ataques.

- **Desconfiar de redes suspeitas:** Criminosos podem criar pontos de acesso falsos com nomes parecidos com os de redes legítimas para capturar informações dos usuários.

- **Confirmar a autenticidade da rede:** Antes de se conectar, verifique com os funcionários do estabelecimento qual é a rede oficial.

- **Usar uma VPN:** A VPN cria um canal seguro, protegendo os dados contra interceptação.

- **Evitar acessar informações sensíveis:** Sempre que possível, evite realizar transações financeiras ou acessar contas importantes em redes públicas.

- **Priorizar a rede do celular:** Para acessos mais sigilosos, a conexão via rede móvel é uma opção mais segura.

- **Manter os dispositivos protegidos:** Ter um bom antivírus atualizado pode prevenir ataques.

5.2 Recomendações para os administradores de Wi-Fi de acesso público.

Com o aumento do uso de redes sem fio abertas, garantir a segurança se tornou essencial para os estabelecimentos que oferecem esse serviço. Algumas medidas podem ajudar a proteger tanto os provedores quanto os usuários:

- **Usar criptografia forte:** Configurar a rede com protocolos de segurança atualizados, como WPA3, reduz os riscos de invasão.

- **Implementar autenticação segura:** Exigir senhas robustas e, se possível, autenticação em duas etapas.

- **Manter os sistemas atualizados:** Atualizações frequentes corrigem falhas e melhoram a segurança.

- **Monitorar a rede:** Sistemas de detecção ajudam a identificar atividades suspeitas rapidamente.

- **Minimizar a retenção de dados:** Armazenar apenas as informações estritamente necessárias reduz os impactos de eventuais ataques.

- **Educar os usuários:** Disponibilizar informações sobre boas práticas de segurança pode evitar muitos problemas.

- **Estabelecer regras claras de uso:** Uma política de responsabilidade ajuda a orientar os usuários e a evitar abusos na rede.

- **Contar com especialistas:** Consultar profissionais de segurança cibernética periodicamente pode fortalecer a infraestrutura.

5.3 Educação e conscientização dos usuários

Informar os usuários sobre boas práticas de segurança é essencial para reduzir riscos. Uma maneira eficiente de conscientização é a colocação de cartazes informativos nos locais que oferecem Wi-Fi público. Algumas sugestões incluem:

- **Títulos chamativos:** "Proteja seus dados! Dicas para usar o Wi-Fi com segurança."

- **Dicas rápidas e objetivas:** "Use uma VPN", "Evite transações bancárias", "Prefira redes seguras".

- **Passo a passo:** Orientações sobre como configurar uma VPN ou identificar redes falsas.

- **Alerta sobre *phishing*:** Explicar como reconhecer e evitar links fraudulentos.

- **Destaque para sites seguros:** Ressaltar a importância de acessar apenas páginas com "https://".

- **QR Codes:** Direcionar para guias completos e ferramentas de segurança.

- **Canal de suporte:** Disponibilizar contatos para dúvidas ou relatos de atividades suspeitas.

- **Design atrativo:** Uso de cores chamativas e imagens claras para melhor engajamento.

- **Mensagem positiva:** Encorajar práticas seguras de forma didática e acessível.

Posicionar os cartazes estrategicamente em áreas de grande circulação, como recepções e salas de espera, pode aumentar sua efetividade e garantir que mais pessoas se conscientizem sobre a segurança digital.

6. Conclusão

Este trabalho teve como objetivo analisar os riscos associados ao uso de redes Wi-Fi públicas, destacando suas vulnerabilidades e os possíveis ataques que podem comprometer a segurança dos usuários. A pesquisa incluiu a identificação das redes disponíveis na cidade de Cuité de Mamanguape, avaliando seus padrões de criptografia e a distribuição dos canais utilizados.

Os resultados obtidos mostraram que, das 46 redes analisadas, 39,13% utilizam WPA e 60,87% utilizam WPA2. Nenhuma das redes pesquisadas utilizava WEP, um protocolo já considerado obsoleto e altamente vulnerável, e também não foi identificado o uso de WPA3, o padrão mais recente e mais seguro disponível atualmente. Embora o protocolo WPA2 seja mais seguro que o WPA, ambos ainda estão sujeitos a ataques de força bruta e outras técnicas de invasão.

A distribuição dos canais revelou uma tendência de concentração em canais específicos, o que pode gerar interferências e comprometer a qualidade da conexão, levando em consideração que pode existir a presença de redes Wi-Fi de uso privado próximas utilizando o mesmo canal. Além disso, a ausência de redes utilizando WPA3 reforça a necessidade de atualização dos padrões de segurança adotados.

A pesquisa reforça a importância de medidas preventivas para aumentar a segurança ao utilizar redes Wi-Fi públicas. Usuários devem evitar acessar informações sensíveis sem o uso de VPNs ou conexões seguras, enquanto administradores de redes devem adotar criptografias mais robustas, políticas de segurança mais rígidas e adotar o uso de placas no estabelecimento que ajude a informar os clientes das melhores técnicas de segurança.

Por fim, este estudo contribui para a conscientização sobre os riscos das redes públicas sem fio e serve como base para futuras investigações sobre métodos mais eficazes de proteção contra ataques cibernéticos nesse contexto.

7. Sugestões para trabalhos Futuros

São apresentados a seguir algumas sugestões para melhor avançar nos estudos relativos aos riscos associados ao uso de redes Wi-Fi públicas, destacando suas vulnerabilidades e os possíveis ataques que podem comprometer a segurança dos usuários.

7.1 Análise de Vulnerabilidades em Dispositivos IoT Conectados a Redes Wi-Fi:

Seria de grande relevância para futuras pesquisas aprofundar a análise das vulnerabilidades de segurança presentes nos dispositivos da Internet das Coisas (IoT) quando integrados a redes Wi-Fi. Considerando a crescente proliferação desses dispositivos em diversos ambientes e suas, por vezes, limitadas capacidades de segurança, torna-se imperativo investigar as potenciais brechas que podem ser exploradas por agentes maliciosos. Estudos futuros poderiam enfocar a identificação de vulnerabilidades comuns em diferentes categorias de dispositivos IoT, a avaliação dos riscos associados à exploração dessas falhas em redes Wi-Fi e a proposição de estratégias de mitigação e fortalecimento da segurança específicas para esses dispositivos. Adicionalmente, a pesquisa poderia explorar a interação entre essas vulnerabilidades e as fragilidades inerentes aos protocolos Wi-Fi, oferecendo uma compreensão mais abrangente dos desafios de segurança no ecossistema IoT.

7.2 Desenvolvimento e Análise de Scripts para Monitoramento e Detecção de Ataques *Honeypot* e *Evil Twin* em Redes Wi-Fi:

Outra direção promissora para trabalhos futuros reside no desenvolvimento e na análise de scripts e ferramentas automatizadas para o monitoramento e a detecção de ataques avançados em redes Wi-Fi, como *honeypots* e *evil twin*. A implementação de um *honeypot* Wi-Fi como uma armadilha para atrair atacantes possibilitaria a análise detalhada de suas táticas e ferramentas. Paralelamente, a ameaça representada por ataques de *evil twin*, com a criação de pontos de acesso falsos para interceptar comunicações, demanda soluções de detecção eficazes. Pesquisas futuras poderiam concentrar-se na criação de scripts eficientes para identificar atividades suspeitas relacionadas a esses tipos de ataques, analisar o comportamento do tráfego em redes *honeypot* para identificar padrões de ataque e desenvolver mecanismos de alerta e resposta automatizados. A integração de técnicas de inteligência artificial e aprendizado de máquina também poderia ser explorada para aprimorar a precisão e a capacidade de detecção dessas ferramentas.

7.3 Estudo do Impacto de Interferências e Congestionamento no Desempenho e Segurança de Redes Wi-Fi:

A influência de interferências de outros dispositivos sem fio e o congestionamento do espectro de radiofrequência representam fatores que podem afetar não apenas o desempenho, mas também a segurança das redes Wi-Fi.

Investigações futuras poderiam analisar como essas condições podem ser exploradas por atacantes, seja para dificultar a detecção de atividades maliciosas ou para degradar a qualidade do sinal e facilitar ataques de negação de serviço. Além disso, a exploração de técnicas para mitigar os efeitos da interferência e do congestionamento, visando aprimorar a resiliência e a segurança das redes Wi-Fi em ambientes com alta densidade de dispositivos, seria uma contribuição valiosa.

7.4 Análise Comparativa de Ferramentas de Auditoria e Teste de Penetração em Redes Wi-Fi:

Uma análise comparativa detalhada das diversas ferramentas de auditoria e teste de penetração disponíveis para redes Wi-Fi poderia fornecer insights significativos para a área de segurança. Esta pesquisa poderia avaliar a funcionalidade, a precisão, a usabilidade e a eficácia de diferentes ferramentas na identificação e exploração de vulnerabilidades em variadas configurações de rede e protocolos de segurança. Os resultados poderiam constituir um guia prático para profissionais de segurança e pesquisadores, auxiliando na seleção das ferramentas mais adequadas para diferentes cenários de avaliação de segurança.

REFERÊNCIAS

ALENCAR, Felipe: O que é uma rede *wireless* e como ela funciona?. Disponível em: <https://www.hardware.com.br/artigos/o-que-e-uma-rede-wireless-e-como-funciona/>. Acesso em 13 de março de 2025.

ANACOM: Internet - Wi-Fi 2,4 GHz vs Wi-Fi 5GHz - Quais as diferenças e qual usar?. Disponível em: <https://www.anacom-consumidor.pt/-/internet-wi-fi-2-4-ghz-vs-wi-fi-5ghz-quais-as-diferencas-e-qual-usar->. Acesso em 11 de março de 2025.

ANTÔNIO, Adriano: O que é ESSID & BSSID? E saiba também como eles são identificados e como funcionam!. Disponível em: <https://www.pmgacademy.com/blog/o-que-e-essid-bssid/>. Acesso em 10 de março de 2025.

CISCO: Access Point sem fio. [s.d.]a. Disponível em: <https://www.cisco.com/site/br/pt/products/networking/wireless/access-points/index.html>. Acesso em 13 de março de 2025.

CISCO: O que é 802.11ax?. [s.d.]b. Disponível em: <https://www.cisco.com/c/pt_br/products/wireless/what-is-802-11ax.html>. Acesso em 08 de março de 2025.

CLARANET: Ataque *man-in-the-middle* (MitM). Disponível em: <https://www.claranet.com/br/blog/man-in-the-middle-o-que-e>. Acesso em 07 de março de 2025.

FORTINET: O que é rede sem fio: Como o Wi-Fi funciona Tipos de redes sem fio. Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/wireless-network>. Acesso em 10 de abril de 2025.

GOGONI, Ronaldo: Por que você não deve usar Wi-Fi público, segundo o FBI. Disponível em: <https://tecnoblog.net/responde/por-que-voce-nao-deve-usar-wi-fi-publico-segundo-o-fbi>. Acesso em 09 de março de 2025.

HENRIQUES, Hugo: Introdução às redes industriais. Disponível em: <https://materialpublic.imd.ufrn.br/curso/disciplina/1/53/1/5>. Acesso em 11 de março de 2025.

HERTZOG, Raphaël: Kali Linux Revealed: Mastering the Penetration Testing Distribution. Wilmington: Offensive Security, 2017.

KASPERSKY: Segurança do Wi-Fi público. [s.d.]. Disponível em: <https://www.kaspersky.com.br/resource-center/preemptive-safety/public-wifi>. Acesso em 07 de março de 2025.

MATHIAS, André: IEEE 802.11 - Redes sem Fio. Disponível em: <https://www.gta.ufrj.br/grad/00_2/ieee/index.html>. Acesso em 09 de março de 2025.

MORENO, Daniel: *Pentest* em Redes Sem Fio. São Paulo: Novatec, 2016.

NETSPOT: WPA3: A vanguarda da segurança do WiFi. Disponível em: <https://www.netspotapp.com/pt/blog/wifi-security/what-is-wpa3.html>. Acesso em 11 de março de 2025.

REIS, Lucas: IEEE 802.11 e o *Wired Equivalent Privacy* (WEP). Disponível em: <https://www.gta.ufrj.br/grad/08_1/ieee802-11/>. Acesso em 06 de março de 2025.

RIBEIRO, Gabriel: Tudo sobre o protocolo WPA3 que deixa a internet Wi-Fi mais segura. Disponível em: <https://www.techtudo.com.br/noticias/2018/04/tudo-sobre-o-protocolo-wpa3-que-deixa-a-internet-wi-fi-mais-segura.ghtml>. Acesso em 08 de março de 2025.

RIZZON: O que é: Beacon Frame. Disponível em: <https://napoleon.com.br/glossario/o-que-e-beacon-frame/>. Acesso em 13 de março de 2025.

RUFINO, Nelson: Segurança em redes sem fio. São Paulo: Novatec, 2015.

TP-LINK: Adaptador de Rede Gigabit PCI Express. [s.d.]a. Disponível em: <https://www.tp-link.com/br/home-networking/adapter/tg-3468/>. Acesso em 13 de março de 2025.

TP-LINK: Roteador Wi-Fi 6 Gigabit Dual Band AX1500. [s.d.]b. Disponível em: <https://www.tp-link.com/br/home-networking/wifi-router/archer-ax12/>. Acesso em 13 de março de 2025.

VALERI, Vitor: O que são os canais das faixas de frequências de 2,4GHz e de 5GHz? Qual o melhor?. Disponível em: <https://www.oficinadanet.com.br/internet/31827-o-que-sao-os-canais-das-faixas-de-frequencia-de-2-4ghz-e-de-5ghz-qual-o-melhor>. Acesso em 10 de março de 2025.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
Campus João Pessoa - Código INEP: 25096850
Av. Primeiro de Maio, 720, Jaguaribe, CEP 58015-435, João Pessoa (PB)
CNPJ: 10.783.898/0002-56 - Telefone: (83) 3612.1200

Documento Digitalizado Restrito

TCC Versão Final

Assunto:	TCC Versão Final
Assinado por:	Samuel Nascimento
Tipo do Documento:	Anexo
Situação:	Finalizado
Nível de Acesso:	Restrito
Hipótese Legal:	Informação Pessoal (Art. 31 da Lei no 12.527/2011)
Tipo do Conferência:	Cópia Simples

Documento assinado eletronicamente por:

- **Samuel Lima do Nascimento**, **DISCENTE (20212430008) DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES - JOÃO PESSOA**, em 16/04/2025 19:35:24.

Este documento foi armazenado no SUAP em 16/04/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1464670
Código de Autenticação: ef3014462e

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
Campus João Pessoa - Código INEP: 25096850
Av. Primeiro de Maio, 720, Jaguaribe, CEP 58015-435, João Pessoa (PB)
CNPJ: 10.783.898/0002-56 - Telefone: (83) 3612.1200

Documento Digitalizado Ostensivo (Público)

TCC Versão Corrigida

Assunto:	TCC Versão Corrigida
Assinado por:	Adaildo Gomes
Tipo do Documento:	Anexo
Situação:	Finalizado
Nível de Acesso:	Ostensivo (Público)
Tipo do Conferência:	Documento Original

Documento assinado eletronicamente por:

- **Adaildo Gomes D Assuncao Junior**, **COORDENADOR(A) DE CURSO - FUC1 - CCSTST-JP** , em 24/04/2025 10:43:31.

Este documento foi armazenado no SUAP em 24/04/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1469413
Código de Autenticação: 0ef1419b8f