UNIVERSIDADE FEDERAL DE ALAGOAS
INSTITUTO DE COMPUTAÇÃO

LEANDRO MIGUEL DOS SANTOS

ANÁLISE DOS PRINCIPAIS TIPOS DE ATAQUES EM REDES SEM FIO IEEE 802.11N

Maceió
2024

LEANDRO MIGUEL DOS SANTOS

ANÁLISE DOS PRINCIPAIS TIPOS DE ATAQUES EM REDES SEM FIO IEEE 802.11N

Trabalho de Conclusão de Curso apresentado à Universidade Federal de Alagoas – UFAL, *Campus* A. C. Simões, como pré-requisito para a obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Almir Pereira Guimarães

Maceió
2024

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico
Bibliotecária: Taciana Sousa dos Santos – CRB-4 – 2062

S237a Santos, Leandro Miguel dos.
Análise dos principais tipos de ataques em redes sem fio IEEE 802.11N / Leandro Miguel dos Santos. – 2024.
59 f. : il. color.

Orientador: Almir Pereira Guimarães.
Monografia (Trabalho de Conclusão de Curso em Ciência da Computação) – Universidade Federal de Alagoas. Instituto de Computação. Maceió, 2024.

Bibliografia: f. 56-59.

1. Ataque em redes sem fio. 2. IEEE 802.11N. 3. Ataques cibernéticos. I. Título.

CDU: 004.7

LEANDRO MIGUEL DOS SANTOS

ANÁLISE DOS PRINCIPAIS TIPOS DE ATAQUES EM REDES SEM FIO IEEE 802.11N

Trabalho de Conclusão de Curso apresentado à Universidade Federal de Alagoas – UFAL, *Campus* A. C. Simões, como pré-requisito para a obtenção do grau de Bacharel em Ciência da Computação.

Data de Aprovação: 01/08/2024

Banca Examinadora

Prof. Dr. Almir Pereira Guimarães
Universidade Federal de Alagoas
Campus A. C. Simões
Orientador

Prof. Me. Petrúcio Antônio Medeiros Barros
Universidade Federal de Alagoas
Campus A. C. Simões
Examinador

Prof. Me. Giancarlo Lima Torres
Universidade Federal de Alagoas
Campus Arapiraca
Examinador

AGRADECIMENTOS

Primeiramente, agradeço a Deus, cuja orientação permitiu que meus objetivos fossem alcançados ao longo dos anos de estudo. À minha família, pelo apoio constante. Ao meu professor orientador Prof. Dr. Almir Pereira Guimarães, pelas valiosas contribuições ao longo de todo o processo. E a todos que, de alguma forma, contribuíram para a realização deste trabalho.

RESUMO

As redes sem fio representam uma evolução significativa no campo das comunicações, oferecendo conectividade sem a necessidade de cabos e permitindo que os dispositivos se comuniquem por meio de radiofrequência. A evolução contínua destas redes e sua ampla adoção as tornam essenciais em diversos contextos impulsionando a busca por segurança e eficiência na transmissão de dados, tornando-as uma parte fundamental da infraestrutura de comunicação moderna.

No entanto, a segurança em redes sem fio é uma preocupação crescente devido à sua ampla adoção e à natureza inerentemente vulnerável dessas infraestruturas. O advento destas redes trouxe consigo uma série de vantagens em termos de desempenho e alcance, no entanto introduziu novos desafios relativos à segurança.

Este estudo visa analisar os principais tipos de ataques em redes sem fio, com foco no padrão *IEEE 802.11n*, a fim de identificar fragilidades relacionadas à segurança e propor contramedidas para os ataques abordados. Durante os testes realizados, foram executados ataques de *eavesdropping*, desautenticação, captura de *handshake*, força bruta, entre outros, utilizando ferramentas como *AirCrack-ng*, *Hping3*, *Nmap*, *Hashcat* e outras para explorar vulnerabilidades em redes *wireless IEEE 802.11n*.

Os experimentos mostraram que os ataques podem causar impacto significativo em redes sem fio. O ataque de inundação de *SYN* causou indisponibilidade do serviço no ponto de acesso. O ataque de desautenticação foi eficaz em redes com protocolos *WPA* e *WPA2*. O ataque *AssRF* resultou em negação de serviço ao consumir excessivamente a memória do ponto de acesso, enquanto o ataque *AuthRF* aumentou o consumo de *CPU*, prejudicando o desempenho do ponto de acesso. O *eavesdropping* mostrou-se eficiente na captura de *handshakes* nos protocolos *WPA* e *WPA2*. Finalmente, a quebra de senha foi eficaz contra senhas fracas, destacando a importância de políticas robustas de senhas para resistir a esse tipo de ataque.

Palavras-chave: IEEE 802.11n; DoS; AssRF; AuthRF; Eavesdropping; Deauthentication.

ABSTRACT

Wireless networks represent a significant evolution in the field of communications, offering connectivity without the need for cables and allowing devices to communicate via radio frequency. The continuous evolution of these networks and their widespread adoption makes them essential in a variety of contexts, driving the search for security and efficiency in data transmission, making them a fundamental part of the modern communications infrastructure.

However, security in wireless networks is a growing concern due to their widespread adoption and the inherently vulnerable nature of these infrastructures. The advent of these networks has brought with it a number of advantages in terms of performance and range, but has also introduced new security challenges.

This study aims to analyze the main types of attacks on wireless networks, with a focus on the *IEEE 802.11n* standard, in order to identify security-related weaknesses and propose countermeasures for the attacks addressed. During the tests, attacks were carried out using eavesdropping, deauthentication, handshake capture, brute force, among others, using tools such as AirCrack-ng, Hping3, Nmap, Hashcat and others to exploit vulnerabilities in wireless *IEEE 802.11n* networks.

The experiments showed that attacks can have a significant impact on wireless networks. The *SYN* flood attack caused service unavailability at the access point. The deauthentication attack was effective on networks with *WPA* and *WPA2* protocols. The *AssRF* attack resulted in a denial of service by excessively consuming the access point's memory, while the *AuthRF* attack increased *CPU* consumption, impairing the access point's performance. The eavesdropping attack proved to be effective in capturing handshakes in the *WPA* and *WPA2* protocols. Finally, password cracking was effective against weak passwords, highlighting the importance of robust password policies to resist this type of attack.

Keywords: IEEE 802.11n; DoS; AssRF; AuthRF; Eavesdropping; Deauthentication.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACK	Reconhecimento (Sigla proveniente do inglês Acknowledgment)
AES	Padrão de Criptografia Avançada (Sigla proveniente do inglês Advanced Encryption Standard)
AP	Ponto de Acesso (Sigla proveniente do inglês Access Point)
AssRF	Association Request Flood (Sigla proveniente do inglês Inundação de solicitações de associação)
AuthRF	Authentication Request Flood (Sigla proveniente do inglês Inundação de Solicitação de Autenticação)
BSS	Conjunto de Serviço Básico (Sigla proveniente do inglês Basic Service Set)
CBC-MAC	Código de Autenticação de Mensagem por Blocos Encadeados (Sigla proveniente do inglês Código de Autenticação de Mensagem por Blocos Encadeados)
CCM	Contador com CBC-MAC (Sigla proveniente do inglês Counter with CBC-MAC)
CCMP	Protocolo de Cifragem de Blocos de Modo de Contador com Código de Autenticação de Mensagem por Blocos Encadeados (Sigla proveniente do inglês Counter Mode Cipher Block Chaining Message Authentication Code Protocol)
CID	Confidencialidade, Integridade e Disponibilidade (Sigla proveniente do inglês Confidentiality, Integrity, and Availability)
CPU	Unidade Central de Processamento (Sigla proveniente do inglês Central Processing Unit)
DS	Sistema de Distribuição (Sigla proveniente do inglês Distribution System)
DSSS	Espectro de Espalhamento por Sequência Direta (Sigla proveniente do inglês Direct-Sequence Spread Spectrum)
DoS	Negação de Serviço (Sigla proveniente do inglês Denial of Service)
ESS	Conjunto de Serviço Estendido (Sigla proveniente do inglês Extended Service Set)
GHz	Gigahertz (Sigla proveniente do inglês Gigahertz)
GPU	Unidade de Processamento Gráfico (Sigla proveniente do inglês Graphics Processing Unit)
Gbps	Gigabits por segundo (Sigla proveniente do inglês Gigabits per second)
IBSS	Conjunto de Serviço Básico Independente (Sigla proveniente do inglês Independent Basic Service Set)
ICMP	Protocolo de Mensagem de Controle da Internet (Sigla proveniente do inglês Internet Control Message Protocol)
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos (Sigla proveniente do inglês Institute of Electrical and Electronics Engineers)
IP	Protocolo de Internet (Sigla proveniente do inglês Internet Protocol)

IoT	Internet das Coisas (Sigla proveniente do inglês Internet of Things)
LAN	Rede Local (Sigla proveniente do inglês Local Area Network)
LLC	Controle de Enlace Lógico (Sigla proveniente do inglês Logic Link Control)
MAC	Controle de Acesso de Mídia (Sigla proveniente do inglês Media Access Control)
MAN	Rede de Área Metropolitana (Sigla proveniente do inglês Metropolitan Area Network)
MHz	Megahertz (Sigla proveniente do inglês Megahertz)
MIMO	Múltiplas Entradas e Múltiplas Saídas (Sigla proveniente do inglês Multiple Input Multiple Output)
MTU	Unidade Máxima de Transmissão (Sigla proveniente do inglês Maximum Transmission Unit)
MU-MIMO	Múltiplas Entradas e Múltiplas Saídas para Múltiplos Usuários (Sigla proveniente do inglês Multi-User Multiple Input Multiple Output)
Mbit	Megabit (Sigla proveniente do inglês Megabit)
Mbps	Megabits por segundo (Sigla proveniente do inglês Megabits per second)
OFDM	Multiplexação por Divisão de Frequência Ortogonal (Sigla proveniente do inglês Orthogonal Frequency-Division Multiplexing)
OSI	Interconexão de Sistemas Abertos (Sigla proveniente do inglês Open Systems Interconnection)
OWE	Criptografia Sem Fio Oportunista (Sigla proveniente do inglês Opportunistic Wireless Encryption)
PAN	Rede de Área Pessoal (Sigla proveniente do inglês Personal Area Network)
PC	Computador Pessoal (Sigla proveniente do inglês Personal Computer)
PING	Pacote de Investigação de Internet (Sigla proveniente do inglês Packet Internet Groper)
PRTG	Paessler Gráfico de Tráfego de Roteador (Sigla proveniente do inglês Paessler Router Traffic Grapher)
PSK	Chave Pré-Compartilhada (Sigla proveniente do inglês Pre-Shared Key)
SAE	Autenticação Simultânea de Iguais (Sigla proveniente do inglês Simultaneous Authentication of Equals)
SMS	Serviço de Mensagem Curta (Sigla proveniente do inglês Short Message Service)
SSID	Identificador do Conjunto de Serviços (Sigla proveniente do inglês Service Set Identifier)
SYN	Sincronizar (Sigla proveniente do inglês Synchronize)
TCP	Protocolo de Controle de Transmissão (Sigla proveniente do inglês Transmission Control Protocol)

TI	Tecnologia da Informação (Sigla proveniente do inglês Information technology)
TKIP	Protocolo de Integridade de Chave Temporal (Sigla proveniente do inglês Temporal Key Integrity Protocol)
Tcl	Linguagem de Comando de Ferramenta (Sigla proveniente do inglês Tool Command Language)
UDP	Protocolo de Datagrama de Usuário (Sigla proveniente do inglês User Datagram Protocol)
USB	Barramento Serial Universal (Sigla proveniente do inglês Universal Serial Bus)
VPN	Rede privada virtual (Sigla proveniente do inglês Virtual Private Network)
WAN	Rede de longa distância (Sigla proveniente do inglês Wide-Area Network)
WEP	Privacidade Equivalente à Cabeada (Sigla proveniente do inglês Wired Equivalent Privacy)
WLAN	Rede Local Sem Fio (Sigla proveniente do inglês Wireless Local Area Network)
WPA	Acesso Protegido Wi-Fi (Sigla proveniente do inglês Wi-Fi Protected Access)
WPA2	Acesso Protegido Wi-Fi 2 (Sigla proveniente do inglês Wi-Fi Protected Access 2)
WPA3	Acesso Protegido Wi-Fi 3 (Sigla proveniente do inglês Wi-Fi Protected Access 3)
Wi-Fi	Fidelidade Sem Fio (Sigla proveniente do inglês Wireless Fidelity)

SUMÁRIO

1 INTRODUÇÃO

1.1 Visão Geral

Redes de computadores são conjuntos de dispositivos interligados que possibilitam a troca de informações e o compartilhamento de recursos (TANENBAUM et al., 2021). Essa interconexão pode ocorrer por meio de diferentes meios, como fios de cobre, fibras ópticas e ondas de rádio (TANENBAUM et al., 2021). As redes de computadores são classificadas de acordo com sua abrangência geográfica, podendo variar de pequenas e pessoais a grandes e globais.

As Redes de Área Pessoal *(PANs)* são redes que possibilitam a comunicação entre dispositivos dentro do alcance de um indivíduo. Um exemplo típico é uma rede sem fio que conecta um computador aos seus periféricos. Outros casos incluem a conexão sem fio entre fones de ouvido e relógio a um smartphone e um reprodutor de música digital se conecta a um carro quando está dentro do alcance (TANENBAUM et al., 2021).

As Redes Locais *(LANs)* são uma infraestrutura de rede privada que opera dentro e nas imediações de um único edifício, como uma residência, um escritório ou uma fábrica. As *LANs* desempenham um papel fundamental na interconexão de computadores pessoais e dispositivos eletrônicos de consumo, facilitando o compartilhamento de recursos, como impressoras, e a troca de informações. As *LANs* utilizam muitas tecnologias diferentes de transmissão; os meios físicos comuns de transmissão são cobre, cabo coaxial e fibra óptica (TANENBAUM et al., 2021).

Uma Rede de Área Metropolitana *(MAN)* é um tipo de rede que conecta múltiplas *LANs* e usuários dentro da área de uma cidade ou região metropolitana. Possui um alcance maior que as *LANs* e menor que as redes de longa distância. Os exemplos mais conhecidos de *MANs* são as redes de *TV* a cabo (TANENBAUM et al., 2021).

Uma Rede de Longa Distância *(WAN)* é uma rede que cobre uma extensa área geográfica, podendo incluir um país inteiro, um continente ou até vários continentes. Uma *WAN* pode servir a uma organização privada, como uma *WAN* corporativa, ou pode ser um serviço comercial, como uma rede de transporte de dados oferecida por provedores de serviço de Internet ou operadoras de telecomunicações. Nesse caso, a *WAN* atua como uma rede de trânsito, transportando tráfego entre diferentes redes menores (TANENBAUM et al., 2021).

As redes sem fio *IEEE 802.11*, também conhecidas como redes *Wireless Fidelity (Wi-Fi)*, tornaram-se uma parte essencial de nossa vida cotidiana, oferecendo conectividade flexível e conveniente em diversos ambientes (ALLIANCE, 2024). No entanto, essa ubiquidade também

as tornou alvos atrativos para uma variedade de ataques cibernéticos. A segurança em redes sem fio é uma preocupação crescente devido à sua natureza suscetível a ataques e à quantidade de dados sensíveis transmitidos por essas redes.

Este trabalho de conclusão de curso propõe uma análise dos principais tipos de ataques que ameaçam a segurança das redes sem fio (KOROLKOV; KUTSAK, 2021), em especial, o padrão *IEEE 802.11n* buscando entender suas técnicas, motivações e impactos potenciais. Para esta finalidade são utilizadas as ferramentas *Hping3*, *Nmap*, *Wireshark*, *Dos tester*, *Aircrack-ng*, *Hcxtools*, *Hashcat*, *PRTG Network Monitor*, *kali linux*, *Windows 11* e *Omada software controller*.

Nesse contexto, será realizada uma revisão de literatura para identificar exemplos reais e estudos de caso que ilustrem esses tipos de ataques em ambientes *802.11n*. Além disso, serão exploradas as técnicas e as ferramentas utilizadas pelos atacantes para realizar esses ataques, bem como as estratégias de defesa e mitigação disponíveis para proteger as redes sem fio contra tais ameaças.

1.2 Motivação

Com o avanço da tecnologia e a proliferação de dispositivos conectados à Internet, as redes sem fio tornaram-se cada vez mais complexas e essenciais para a vida cotidiana. O crescente número e diversidade de dispositivos conectados, desde *smartphones* e *smartvs* até termostatos e geladeiras inteligentes, apresentam novos desafios de gerenciamento, segurança e confiabilidade para os usuários (TANENBAUM et al., 2021).

A segurança das redes sem fio *IEEE 802.11* tornou-se uma preocupação crítica, uma vez que a vulnerabilidade desses dispositivos pode representar ameaças diretas aos consumidores. O aumento de incidentes envolvendo dispositivos de Internet das Coisas *(IoT)* inseguros ou mal configurados resultou em consequências sérias, incluindo o controle remoto de dispositivos por meio de *scripts* maliciosos de terceiros (TANENBAUM et al., 2021).

Usuários indesejados, uma vez conectados à rede, podem acessar informações sensíveis, monitorar o tráfego da web ou realizar outras atividades ilegais. Tais invasões podem resultar em perdas financeiras significativas, tanto pela necessidade de reparar sistemas comprometidos quanto pela possível exposição de dados financeiros e transações confidenciais (IBM, 2024). Também podem comprometer a privacidade de funcionários, clientes e qualquer outra pessoa que utilize a rede, pois informações sensíveis podem ser capturadas, como credenciais de login, informações bancárias e comunicações privadas, expondo indivíduos a riscos de roubo de identidade e outras formas de exploração.

As violações de segurança em redes sem fio podem ter um impacto econômico significativo (IBM, 2024). Quando invasores obtêm acesso a informações confidenciais de empresas por meio de dispositivos conectados a redes desprotegidas, isso pode levar a vazamentos de dados proprietários, perda de vantagem competitiva e danos à reputação da marca (IBM, 2024). Além disso, o roubo de credenciais de login de funcionários pode permitir que invasores acessem sistemas corporativos, resultando em perdas financeiras diretas por fraudes e custos elevados de reparação. Para indivíduos, o roubo ou furto de informações pessoais e financeiras através de redes sem fio desprotegidas pode causar graves prejuízos financeiros e violação de privacidade. *Hackers* e *Crackers* podem monitorar o tráfego de dados e interceptar informações sensíveis, como *e-mails*, mensagens, fotos e histórico de navegação, violando a privacidade dos usuários. Esses riscos de privacidade podem levar a constrangimentos, chantagens e danos à reputação pessoal e profissional das vítimas.

Invasores também podem utilizar uma conexão de rede sem fio não segura para distribuir *malware* e infectar computadores. A presença de *malware* pode danificar dados, provocar a perda de informações valiosas e até mesmo interromper as operações de uma empresa, acarretando altos custos de recuperação e mitigação (IBM, 2024).

As redes sem fio evoluem organicamente à medida que os usuários adquirem novos dispositivos eletrônicos com capacidade de conexão sem fio, resultando em uma diversidade significativa de tecnologias conectadas à rede (TANENBAUM et al., 2021). A predominância de redes sem fio *IEEE 802.11*, embora conveniente, também introduz desafios específicos de desempenho e segurança (TANENBAUM et al., 2021).

Considerando o contexto atual de rápida expansão das redes sem fio e o aumento do número de dispositivos conectados, é evidente a necessidade de pesquisas aprofundadas e soluções inovadoras para garantir a segurança das redes sem fio.

1.3 Objetivo Geral

Investigar e compreender os principais tipos de ataques cibernéticos direcionados a redes sem fio *IEEE 802.11*, em especial o padrão *IEEE 802.11n*, destacando suas características, métodos de execução e impactos potenciais. O trabalho visa também identificar as vulnerabilidades mais comuns encontradas nessas redes e sugerir estratégias de prevenção e mitigação desses ataques para fortalecer sua segurança.

1.3.1 Objetivos Específicos

- Elencar conceitos fundamentais relacionados à segurança em redes sem fio;
- Examinar os tipos de ataques mais comuns enfrentados por redes sem fio;
- Realizar testes de ataques em redes sem fio *IEEE 802.11n* em ambiente de teste, exibindo seus resultados;
- Propor soluções para mitigar as vulnerabilidades identificadas e aumentar a segurança.

1.4 Estrutura do Trabalho

Além da introdução, este trabalho compreende o Capítulo 2, que oferece uma breve revisão de literatura sobre a temática abordada. O Capítulo 3 trata da fundamentação teórica, que compreende os seguintes tópicos: uma visão geral sobre assuntos abordados neste trabalho, os padrões de comunicação e protocolos de segurança em redes sem fio, juntamente com os tipos de ataques abordados. Também são exploradas as ferramentas utilizadas neste estudo. No Capítulo 4, é descrita a metodologia adotada. O Capítulo 5 apresenta um estudo de caso conduzido para a pesquisa, destacando os resultados obtidos por meio das ferramentas empregadas nos ataques. No capítulo 6 são sugeridas medidas de segurança para tornar as redes sem fio menos suscetíveis a ataques. Por fim, o Capítulo 7 engloba as conclusões e considerações finais do estudo.

2 TRABALHOS RELACIONADOS

Atualmente, a segurança em redes sem fio tem atraído a atenção de diversos pesquisadores que buscam detalhar vulnerabilidades, variados tipos de ataques e mecanismos de defesa em suas propostas. Este capítulo revisa alguns trabalhos relacionados a este campo, destacando algumas pesquisas que abordam de maneira detalhada estes aspectos da área de segurança em redes sem fio.

A pesquisa de Alanda et al. (2023) investiga ataques de desautenticação (LOUNIS et al., 2022), *fluxion* (INVOTEC, 2021), *Man-In-The-Middle* (BADHWAR, 2021), negação de serviços (KSHIRSAGAR; KUMAR, 2023) e ataque de injeção *WEP/WPA* (ATLURI; RALLABANDI, 2021) em redes sem fio, empregando métodos de teste de penetração para identificar vulnerabilidades na infraestrutura de rede e avaliar a eficácia das medidas de segurança implementadas. Os resultados destacam a necessidade crucial de uma proteção robusta para mitigar esses ataques e garantir a segurança da rede.

Por sua vez, o trabalho de Al-Shebami e Al-Shamiri (2021) descreve estratégias para aumentar a segurança das redes sem fio, compreendendo os tipos de ataques e ameaças direcionados a essas redes, identificando os métodos usados para gerenciá-las e protegê-las e, posteriormente, protegendo-as contra violações e intrusões. Além disso, ele explora medidas para evitar ou atenuar esses riscos por meio de uma série de recomendações e propostas (AL-SHEBAMI; AL-SHAMIRI, 2021).

O objetivo do trabalho de Thakur et al. (2023) é oferecer uma visão geral da criptografia, abrangendo seu desenvolvimento histórico, formas iniciais e tecnologias contemporâneas como *Wired Equivalent Privacy (WEP)*, *Wi-Fi Protected Access (WPA)* e *Wi-Fi Protected Access 2 (WPA2)* (ATLURI; RALLABANDI, 2021). Ele discute suas vulnerabilidades, aprimoramentos e aplicações na tecnologia da informação. Por fim, o documento ressalta o papel fundamental dos protocolos na área de segurança de redes sem fio para a proteção da integridade e da confiabilidade destas redes e de sistemas digitais.

O artigo de Halbouni et al. (2023) realiza uma Revisão Sistemática da Literatura para examinar três aspectos do protocolo *Wi-Fi Protected Access 3 (WPA3)* (CIAMPA, 2020): a justificativa para sua introdução, métodos de criptografia e modos operacionais e as vulnerabilidades persistentes exploradas por invasores. Este trabalho descreve os métodos de criptografia e os modos operacionais empregados no *WPA3*. Além disso, ela discute as vulnerabilidades abordadas pelo protocolo *WPA3*, bem como aquelas que ainda não foram resolvidas. O estudo conclui que o

WPA3 representa uma melhoria significativa em relação aos seus antecessores, oferecendo maior segurança e confiabilidade para redes sem fio e propõe dois métodos para reforçar a segurança das redes *WPA3*.

O objetivo do artigo de Liu (2022) é identificar e analisar medidas preventivas para proteger as redes sem fio, examinando e avaliando os comportamentos de ataques a estas redes com o objetivo de aprimorar aspectos relacionados à segurança. Os métodos de pesquisa empregados neste estudo incluem estudos de caso e relatórios. Inicialmente, uma compreensão abrangente do impacto significativo dessas ameaças foi obtida por meio do exame de casos reais de ataques a redes sem fio. Posteriormente, por meio de uma análise das táticas dos invasores, das vulnerabilidades de segurança de protocolos, das falhas de projeto e de outros fatores, foram formuladas estratégias para atenuar as ameaças à segurança da rede sem fio, a fim de enfrentar os desafios técnicos e as preocupações legais. Por fim, são propostas soluções práticas para essas ameaças.

Por fim, no trabalho de Elhigazi et al. (2020) é apresentado um algoritmo para detectar e prevenir ataques de inundação de solicitações de autenticação. A solução envolve a adição de um *buffer* de filtro para *Media Access Control (MAC)*, que verifica e mantém endereços *MAC* recebidos, e um sistema de monitoramento que detecta comportamentos suspeitos ao analisar a frequência das solicitações. Os resultados experimentais demonstram que o algoritmo proposto supera outros métodos em termos de detecção e prevenção.

3 FUNDAMENTAÇÃO TEÓRICA

3.1 Visão Geral

Este capítulo tem como objetivo proporcionar a base de conhecimento fundamental relativa a nosso trabalho através da apresentação de conceitos fundamentais relacionados a redes sem fio, incluindo os principais protocolos de comunicação, protocolos de segurança e tipos de ataques abordados neste trabalho. Também serão apresentadas as ferramentas utilizadas no estudo de caso visando explorar as vulnerabilidades inerentes a estes tipos de redes.

Para começar, é importante entender o termo *Wireless*, do inglês "sem fio", que é utilizado de forma genérica para se referir a qualquer tipo de comunicação ou conexão que não utilize cabos. O termo *Wi-Fi* é uma marca registrada da *Wi-Fi Alliance*, que define um conjunto de padrões para redes locais sem fio baseadas nos protocolos *IEEE 802.11*.

As redes sem fio são infraestruturas que permitem a comunicação entre dispositivos sem o uso de cabos. Elas utilizam ondas de rádio para transmitir dados e o Wi-Fi é um exemplo de tecnologia amplamente utilizada em redes sem fio (BARBOSA, 2022).

3.1.1 Componentes Básicos

Qualquer dispositivo sem fio presente em uma rede *Wi-Fi*, seja ele móvel ou estacionário, é categorizado como uma *estação wireless* (ASSUNÇÃO, 2013). Isso inclui dispositivos como computadores, *smartphones*, babás eletrônicas e diversos outros com capacidade de utilizar conexões sem fio (ASSUNÇÃO, 2013). Quando duas dessas estações estão conectadas, elas estabelecem um *Basic Service Set (BSS)*, que é a base para formar uma rede *Wireless LAN* (ASSUNÇÃO, 2013).

3.1.2 Modos de Operação

Modo BSS (Infraestrutura)

Um BSS é um conjunto de estações que são coordenadas por uma única entidade (ASSUNÇÃO, 2013). Essa entidade controla a transmissão e recepção de dados das estações (ASSUNÇÃO, 2013). Essa entidade também pode ser as próprias estações quando operando em modo *Ad-Hoc* ou um ponto de acesso quando em modo Infraestrutura (ASSUNÇÃO, 2013).

O padrão *IEEE 802.11* especifica dois modos de operação para redes *Wi-Fi* (ASSUNÇÃO, 2013). Ambos os modos utilizam o conceito de *BSS*, porém empregam diferentes tecnologias de rede (ASSUNÇÃO, 2013). Esses modos são conhecidos como *Ad-Hoc* e Infraestrutura

(ASSUNÇÃO, 2013). Em modo de operação infraestrutura o *BSS* deve incluir pelo menos um ponto de acesso, conforme mostrado na Figura 1.

Todos os dispositivos sem fio que desejam se conectar a um *BSS* precisam inicialmente se associar ao *Access Point (AP)* (ASSUNÇÃO, 2013). O *AP*, por sua vez, concede acesso aos dispositivos associados por meio de um Sistema de Distribuição (*DS*) (ASSUNÇÃO, 2013). O *DS* é uma parte fundamental da infraestrutura que facilita a comunicação entre os pontos de acesso (ASSUNÇÃO, 2013).

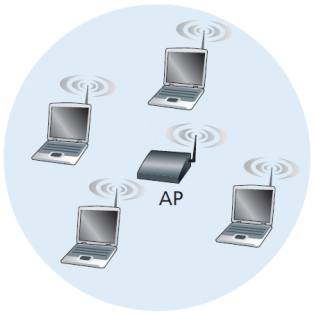

Figura 1 – Modo BSS (Infraestrutura)

Fonte: (TANENBAUM et al., 2021).

Modo IBSS (Ad-Hoc)

O *Independent Basic Service Set (IBSS)* representa a forma mais simples de rede *IEEE 802.11*, caracterizada pela comunicação direta entre estações *wireless*, seguindo um modelo ponto a ponto (ASSUNÇÃO, 2013). Esse modo de operação se configura como uma rede independente, sem interconexão com outras redes *Wi-Fi* ou cabeadas (ASSUNÇÃO, 2013). Apesar disso, essa configuração é altamente conveniente para facilitar a comunicação entre dispositivos *wireless* sem a necessidade de um ponto de acesso, conforme mostrado na Figura 2.

Figura 2 – Modo IBSS (Ad-Hoc)

Fonte: (TANENBAUM et al., 2021).

Conjunto de Serviços Estendidos (ESS)

O *Extended Service Set (ESS)* é formado pela integração de um Sistema de Distribuição entre dois ou mais *BSSs* (ASSUNÇÃO, 2013). Esse arranjo possibilita a comunicação entre dispositivos localizados em diferentes *BSSs* por meio dos pontos de acesso que os interligam, conforme mostrado na Figura 3.

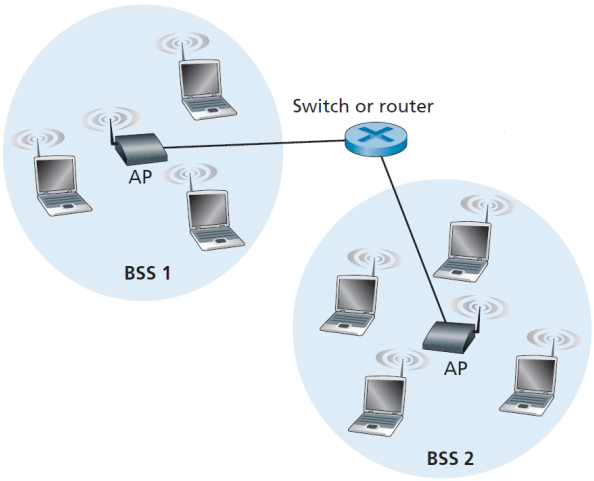

Figura 3 – Conjunto de Serviços Estendidos (ESS)

Fonte: (TANENBAUM et al., 2021).

3.2 Padrões de Comunicação em Redes sem Fio

O modelo *Open Systems Interconnection (OSI)* foi desenvolvido para padronizar internacionalmente os protocolos usados nas diversas camadas de rede. Ele é composto por sete camadas e aborda a interconexão de sistemas abertos, permitindo a comunicação entre diferentes sistemas (TANENBAUM et al., 2021). O *Wi-Fi* engloba a camada física e a camada de enlace do modelo *OSI*, incorporando protocolos de comunicação essenciais para a operação de redes sem fio. Na camada física, o *Wi-Fi* lida principalmente com aspectos relacionados às propriedades das ondas de rádio, como comprimento e amplitude (ASSUNÇÃO, 2013).

A camada de enlace, por sua vez, é dividida em duas subcamadas: a subcamada *MAC* e a subcamada de Controle de Enlace Lógico (*LLC*). A subcamada *MAC*, uma subcamada da camada de enlace, é responsável por regular a transmissão de dados e facilitar a interação com dispositivos sem fio, garantindo o acesso coordenado ao meio de transmissão (ASSUNÇÃO, 2013).

Além disso, a subcamada *MAC* oferece serviços relacionados à gestão da mobilidade dos dispositivos, como a transição entre *BSSs*, proporcionando um gerenciamento eficiente das

conexões e garantindo a continuidade do serviço enquanto os dispositivos se movem dentro da área de cobertura da rede (ASSUNÇÃO, 2013). A seguir, serão mostrados os principais padrões de comunicação utilizados em redes sem fio.

3.2.1 Padrão *IEEE 802.11*

Introduzido em 1997, foi o pioneiro entre os padrões de redes sem fio. O padrão *IEEE 802.11* opera na frequência de 2,4 *Gigahertz (Ghz)* e em velocidades de 1 ou 2 *Megabits por segundo (Mbps)* (ASSUNÇÃO, 2013). Neste padrão, as transmissões *wireless* são realizadas por meio de sinais de radiofrequência (ASSUNÇÃO, 2013).

3.2.2 Padrão *IEEE 802.11a*

Este padrão define uma velocidade máxima de 54 *Mbps* e utiliza modulação *Orthogonal Frequency-Division Multiplexing (OFDM)* em que dados são fragmentados em unidades menores e enviados simultaneamente em múltiplas faixas de frequência (ASSUNÇÃO, 2013). Além disso, oferece suporte a transmissões em velocidades de 6, 9, 12, 18, 24, 36 e 48 *Mbps*, operando na faixa de frequência de 5 *Ghz* (ASSUNÇÃO, 2013). Em relação ao alcance, é capaz de suportar dispositivos a uma distância média em torno de 60 metros em ambientes internos e até 100 metros em ambientes externos, embora isso possa variar dependendo da antena utilizada (ASSUNÇÃO, 2013). Em sua configuração inicial, é capaz de atender simultaneamente até 64 clientes conectados e disponibiliza 12 canais não sobrepostos (ASSUNÇÃO, 2013). As especificações dos padrões *IEEE 802.11a* e *IEEE 802.11b* foram divulgadas simultaneamente pelo *IEEE*, porém apenas o segundo se popularizou imediatamente (ASSUNÇÃO, 2013).

3.2.3 Padrão *IEEE 802.11b*

Esse padrão introduziu duas novas taxas de transmissão (5,5 *Mbps* e 11 *Mbps*) (ASSUNÇÃO, 2013). Semelhante ao *IEEE 802.11*, o padrão *IEEE 802.11b* opera na faixa de frequência de 2,4 *Ghz*. O *IEEE 802.11b* utiliza a técnica de modulação *Direct-Sequence Spread Spectrum (DSSS)* e oferece um alcance de até 100 metros em ambientes internos e de até 300 metros em ambientes externos, embora isso possa variar dependendo da antena utilizada (ASSUNÇÃO, 2013).

3.2.4 Padrão *IEEE 802.11g*

Esse padrão adota a modulação OFDM, assim como o padrão *IEEE 802.11a*, sendo compatível com *IEEE 802.11b* via modulação *DSSS*, operando também na frequência de 2,4 *Ghz* (ASSUNÇÃO, 2013). O *IEEE 802.11g* possui uma velocidade de 54 *Mbps* e popularizou-se imediatamente assim que ele foi introduzido em janeiro de 2003 (ASSUNÇÃO, 2013).

3.2.5 Padrão *IEEE 802.11n*

O padrão *IEEE 802.11n* se destaca por usar a tecnologia *Multiple Input Multiple Output (MIMO)* (ASSUNÇÃO, 2013). Essa tecnologia permite que o *AP* e os dispositivos se comuniquem usando várias antenas, resultando em uma velocidade de transmissão de dados aproximada de 150 *Megabit por segundo (Mbit/s)* por antena sendo compatível com os padrões *b* e *g* além de ser capaz de operar nas frequências de 2,4 *Ghz* e 5 *Ghz* (ASSUNÇÃO, 2013). Em um cenário com o padrão *IEEE 802.11n* em sua versão mais atual, é possível empregar até quatro antenas, o que possibilita ao padrão atingir uma velocidade de até 600 *Mbit/s* (ASSUNÇÃO, 2013).

3.2.6 Padrão *IEEE 802.11ac*

O padrão *IEEE 802.11ac* atinge velocidades de até 1,3 *Gigabits por segundo (Gbps)* ao utilizar a faixa de frequência de 5 *Ghz* chegando a ser três vezes mais rápido que o padrão *IEEE 802.11n* (ASSUNÇÃO, 2013). Além disso, reduz interferências ao propagar o sinal de forma mais eficiente com recursos como o beamforming (ASSUNÇÃO, 2013). O objetivo do *IEEE 802.11ac* é oferecer uma rede mais rápida e escalável que o *IEEE 802.11n*, com destaque para o uso do *Multi-User Multiple Input Multiple Output (MU-MIMO)* (IEEE, 2013) que pode transmitir um sinal de várias fontes para vários sistemas simultaneamente, e o *channel bonding* (TORGUNAKOV et al., 2022), que combina canais para aumentar a largura de banda (ASSUNÇÃO, 2013). As melhorias incluem aumento de velocidade (até 1,3 *Gbps*) e largura de banda dos canais (80 ou 160 *Megahertz (Mhz)*), com retrocompatibilidade com o *IEEE 802.11n* na frequência de 5 *Ghz* (ASSUNÇÃO, 2013).

3.2.7 Padrão *IEEE 802.11ax*

O padrão *IEEE 802.11ax* foi lançado em 2021 (RUTH, 2023). Teoricamente pode alcançar velocidade de 9,6 *Gbps*, sendo que seu foco é lidar com a crescente demanda por *Wi-Fi* em áreas de alta densidade de tráfego, como estádios, salas de concerto, transporte público e até mesmo residências com múltiplos dispositivos conectados simultaneamente (RUTH, 2023).

O *IEEE 802.11ax* incorpora várias melhorias significativas (RUTH, 2023). Ele utiliza um mecanismo multiusuário para dividir a taxa de dados entre vários dispositivos, suporta roteadores que transmitem dados para múltiplos dispositivos em um único quadro de transmissão e permite que dispositivos *Wi-Fi* agendem suas transmissões para o roteador (RUTH, 2023). Além disso, foram introduzidos mecanismos para melhorar o alcance externo das operações (RUTH, 2023).

Os aprimoramentos deste padrão visam melhorar a taxa de transferência agregada e suportar o aumento do uso do *Wi-Fi* em ambientes com grande volume de dados, nos quais é essencial o desempenho em tempo real e a eficiência energética para dispositivos móveis (RUTH, 2023).

3.3 Introdução à segurança em redes sem fio

Com o aumento da popularidade das redes sem fio, garantir a proteção dessas redes se torna uma prioridade significativa para empresas, governos e indivíduos (MUGHAL, 2022). Para a garantia de uma proteção adequada a estas redes, é necessário que a tríade referenciada como Confidencialidade, Integridade e Disponibilidade *(CID)*, que enfatiza três aspectos essenciais da segurança da informação, sejam incorporadas.

A Confidencialidade diz respeito à salvaguarda de informações sensíveis contra acesso e divulgação não autorizados (MUGHAL, 2022). Em ambientes de redes sem fio, essa confidencialidade é geralmente alcançada por meio de algoritmos de criptografia que tornam os dados ilegíveis para partes não autorizadas (MUGHAL, 2022).

A Integridade assegura que os dados permaneçam íntegros e não sejam modificados indevidamente durante sua armazenagem, transmissão e recuperação (MUGHAL, 2022). Na área da segurança sem fio, mecanismos de integridade detectam e previnem alterações não autorizadas nos dados, como a inserção de código malicioso ou a adulteração de pacotes de dados (MUGHAL, 2022).

A Disponibilidade garante que usuários autorizados possam acessar os recursos e dados da rede de forma oportuna e confiável (MUGHAL, 2022). Para manter essa disponibilidade em redes sem fio, são necessárias medidas de segurança que protejam contra ataques capazes de interromper ou degradar o desempenho da rede, como ataques de negação de serviço (*DoS*) (MUGHAL, 2022).

Em um cenário de ameaças devido às constantes mudanças, é essencial compreender e implementar estratégias que assegurem a robustez da segurança nas redes sem fio (MUGHAL, 2022). A segurança dessas redes tornou-se cada vez mais crucial à medida que a dependência

global da comunicação sem fio aumenta (MUGHAL, 2022). Embora as redes sem fio ofereçam benefícios como mobilidade e flexibilidade, elas também apresentam desafios únicos de segurança devido à sua natureza aberta e à facilidade com que os invasores podem interceptar dados transmitidos (MUGHAL, 2022). O crescimento do trabalho remoto, a proliferação de dispositivos da Internet das Coisas e a crescente demanda por conectividade constante destacam ainda mais a importância de proteger adequadamente as redes sem fio (MUGHAL, 2022).

Um dos suportes em segurança de redes sem fio é a utilização de técnicas de criptografia das informações transmitidas, que é realizada por meio de protocolos de criptografia que garantem a codificação dessas informações protegendo-as com uma chave específica antes de sua transmissão pela rede sem fio (MEYERS; WEISSMAN, 2022). Para que um dispositivo receptor consiga interpretar essas informações, é necessário possuir a chave de descriptografia correspondente. Sem acesso à chave de descriptografia, um invasor que capture quadros de dados não conseguirá interpretá-los (MEYERS; WEISSMAN, 2022). Para viabilizar a utilização de criptografia, os principais protocolos empregados em redes sem fio são listados abaixo.

3.3.1 Protocolo *WEP*

O *WEP* (BACHA, 2022) é o mais antigo dos três protocolos de segurança do padrão *IEEE 802.11*. Este protocolo utiliza uma chave de criptografia de 40 a 128 *bits* composta por uma chave combinada com um vetor de inicialização. No entanto, devido ao tamanho reduzido do vetor de inicialização, o algoritmo tende a reutilizar as chaves, facilitando a quebra da criptografia. O *WEP* é considerado inseguro e seu uso deve ser evitado. Em 2001 os fabricantes cessaram o suporte ao *WEP* (BACHA, 2022).

3.3.2 Protocolo *WPA*

O *WPA* (BACHA, 2022) foi concebido para corrigir deficiências encontradas no *WEP*. Ele introduziu uma nova abordagem de segurança, o *Temporal Key Integrity Protocol (TKIP)* (BACHA, 2022), que gera uma chave de criptografia única para cada quadro de rede sem fio, visando melhorar a segurança da conexão. O uso do *WPA* também é desaconselhado devido às vulnerabilidades apresentadas pelo *TKIP* que comprometem a segurança das redes sem fio (BACHA, 2022).

O protocolo *WPA* foi lançado como uma forma de melhorar o sistema existente *WEP* sem a necessidade de atualizações ou substituições extensivas de *hardware* (CIAMPA, 2020). O *WPA* possui dois modos operacionais: o *WPA Personal*, direcionado para uso por indivíduos ou

para pequenos escritórios com até 10 funcionários, e o *WPA Enterprise*, mais robusto, destinado a grandes empresas, escolas e entidades governamentais (CIAMPA, 2020). Os dois modos do *WPA* abordam tanto a criptografia quanto a autenticação. No *WPA Personal*, a autenticação é realizada por meio de uma chave pré-compartilhada (*PSK*), que é um valor secreto inserido manualmente no *AP* e em cada dispositivo sem fio autorizado, funcionando de forma semelhante ao segredo compartilhado do *WEP*. Ainda que o *WPA* seja uma melhoria do seu antecessor, ele não é considerado uma opção segura por possuir pontos fracos (CIAMPA, 2020).

3.3.3 Protocolo *WPA2*

O protocolo *WPA2* (CIAMPA, 2020) é fundamentado no padrão do *IEEE 802.11i*. Semelhantemente ao *WPA*, o *WPA2* apresenta dois modos de funcionamento: o *WPA2 Personal,* que é direcionado a indivíduos ou pequenos escritórios e o *WPA2 Enterprise*, que é direcionado a grandes corporações, instituições educacionais e entidades governamentais (CIAMPA, 2020). O *WPA2* aborda tanto a criptografia quanto a autenticação em redes sem fio. O protocolo de criptografia adotado pelo *WPA2* é o *Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP)* (CIAMPA, 2020), que especifica a utilização do *Counter with CBC-MAC (CCM)* (CIAMPA, 2020) que é um algoritmo de cifra geralmente aceito que assegura a confidencialidade dos dados com o *Advanced Encryption Standard (AES)* (CIAMPA, 2020). O *CCMP* requer a utilização da cifra de bloco baseada no *AES*, demandada pelo padrão WPA2 devido à sua maior segurança. (CIAMPA, 2020). O componente *Cipher Block Chaining Message Authentication Code (CBC-MAC)* (CIAMPA, 2020) do *CCMP* garante a integridade e autenticação dos dados.

A autenticação no modelo *WPA2 Enterprise* faz uso do padrão *IEEE 802.1x*, o qual oferece um nível mais elevado de segurança ao implementar autenticação baseada em portas (CIAMPA, 2020). O *IEEE 802.1x* restringe todo o tráfego em cada porta até que o cliente seja autenticado por meio de credenciais armazenadas em um servidor de autenticação (CIAMPA, 2020). O acesso ao dispositivo responsável pela autenticação é rigorosamente controlado para prevenir ataques de invasores (CIAMPA, 2020).

3.3.4 Protocolo *WPA3*

O objetivo do *WPA3* (CIAMPA, 2020) é oferecer um conjunto de recursos que simplifiquem a configuração de segurança para os usuários e aprimoram simultaneamente as proteções de segurança da rede. Quatro melhorias de segurança são implementadas no *WPA3*:

- Introduz a autenticação simultânea de iguais, (*Simultaneous Authentication of Equals (SAE)*), que reforça a segurança durante o *handshake* quando as chaves são trocadas, proporcionando uma segurança maior, mesmo quando senhas curtas ou fracas são utilizadas (CIAMPA, 2020).
- O *WPA3* suporta uma criptografia mais robusta de 192 *bits* (CIAMPA, 2020).
- O *WPA3* implementa a criptografia oportunista sem fio *(OWE)*, garantindo que cada conexão sem fio entre um cliente e um *AP* seja criptografada com uma chave única (CIAMPA, 2020). Essa medida pode mitigar os ataques de *man-in-the-middle* (CIAMPA, 2020).
- Melhorou os recursos de interação com dispositivos *IoT*, introduzindo novas maneiras de configurar a segurança para esse tipo de dispositivos.

3.4 Ataques abordados neste trabalho

3.4.1 Ataque de inundação *SYN*

O ataque de inundação *Synchronize (SYN)* é um tipo de ataque de negação de serviço (*DoS*) que utiliza uma vulnerabilidade no protocolo *Transmission Control Protocol (TCP)* para sobrecarregar um servidor com conexões falsas. Isso ocorre quando um invasor envia um grande número de segmentos *SYN* a um servidor, mas não responde aos segmentos *Acknowledgment (ACK)* que o servidor envia em resposta. Este tipo de ação, faz com que o servidor reserve recursos para essas conexões abertas, mesmo que elas nunca sejam realmente estabelecidas. Como resultado, o servidor fica impossibilitado de aceitar novas conexões, tornando-o indisponível para os usuários. (EDDY, 2011).

3.4.2 Ataque de desautenticação

No ataque de desautenticação (LOUNIS et al., 2022), um invasor se faz passar por um ponto de acesso *Wi-Fi* e envia quadros de desautenticação falsificados para os clientes *Wi-Fi* conectados. Estes clientes conectados processam os quadros de desautenticação como se tivessem sido enviados pelo ponto de acesso legítimo (LOUNIS et al., 2022). Esses quadros fazem com que os clientes *Wi-Fi* conectados invalidem sua associação e autenticação com o ponto de acesso, levando os clientes a serem desconectados da rede Wi-Fi (LOUNIS et al., 2022). Isto ocorre com

os mecanismos de segurança *WPA* e *WPA2*, pois os quadros de desautenticação são enviados em claro sem proteção contra falsificação (LOUNIS et al., 2022).

3.4.3 Ataque de inundação de requisição de associação

No ataque de inundação de requisição de associação (ELHIGAZI et al., 2020), muitas requisições de associação com endereços *MAC* falsos são enviadas pelo invasor. Ao receber as requisições, o ponto de acesso atribui largura de banda, memória e cota de processamento a cada solicitação de associação (ELHIGAZI et al., 2020). Desta forma, o invasor causa o *overflow* da tabela de associação, fazendo com que o ponto de acesso não consiga responder às requisições legítimas (ELHIGAZI et al., 2020).

3.4.4 Ataque de inundação de solicitação de autenticação

Inundação de solicitação de autenticação (ELHIGAZI et al., 2020) é o ataque em que o invasor envia um grande volume de solicitações de autenticação falsas, usando endereços *MAC* falsos. O ataque sobrecarrega o *buffer* de autenticação do ponto de acesso fazendo com que o tempo de processamento seja aumentado além de consumir mais memória do *AP* e dessa forma impedindo que o ponto de acesso responda às solicitações legítimas (ELHIGAZI et al., 2020).

3.4.5 Ataque de escuta (*Eavesdropping*)

Eavesdropping (YASSINE et al., 2019) refere-se a um tipo de ataque no qual um atacante intercepta informações do sistema sem o conhecimento ou consentimento dos usuários legítimos. Esse tipo de ataque é considerado passivo, pois o invasor não interfere no funcionamento normal do sistema, limitando-se a observar as operações em curso.

3.4.6 Ataque de quebra de senha por força bruta

Um ataque de força bruta (OLALIA JR et al., 2018) é uma técnica utilizada por invasores para comprometer sistemas protegidos por senhas, envolvendo a utilização de um *software* automatizado para realizar tentativas sucessivas gerando todas as combinações possíveis em um esforço para descobrir a senha ou chave correta e, assim, obter acesso às informações desejadas.

3.5 Ferramentas utilizadas nos testes

3.5.1 *PRTG Network Monitor*

O *Paessler Router Traffic Grapher (PRTG) (PAESSLER, 2024)* é um *software* de monitoramento de rede desenvolvido pela *Paessler AG*. Ele é usado por empresas e profissionais de *TI* para monitorar o desempenho de suas redes, sistemas, aplicativos e dispositivos. O *PRTG* coleta dados em tempo real sobre o tráfego de rede, a utilização de largura de banda, a disponibilidade de servidores, o status de dispositivos de rede e uma variedade de outros parâmetros importantes para garantir que a rede funcione de maneira eficiente e sem problemas. O *software PRTG* apresenta essas informações em gráficos e relatórios intuitivos e pode enviar alertas automáticos por *e-mail*, *Short Message Service (SMS)* ou outros meios quando detecta problemas ou condições anormais na rede.

3.5.2 Kali linux

O *Kali linux* (KALI, 2024b) é uma distribuição Linux baseada no *Debian* projetada principalmente para testes de segurança e auditoria de segurança de computadores. Ele é desenvolvido e mantido pela *Offensive Security Ltd*. O *Kali* vem pré-carregado com uma ampla variedade de ferramentas de segurança cibernética, incluindo ferramentas de varredura de rede, análise de vulnerabilidades, penetração, forense digital e engenharia reversa. O *Kali* é amplamente utilizado por profissionais de segurança, *hackers* éticos, pesquisadores de segurança e entusiastas da segurança cibernética em todo o mundo.

3.5.2.1 *Aircrack-ng*

O Aircrack-ng (AIRCRACK-NG, 2024) é um conjunto de ferramentas de segurança de rede de código aberto projetada para avaliar e testar a segurança de redes sem fio. Ele é usado principalmente para testes de penetração e auditoria de segurança em redes sem fio. O *Aircrack-ng* possui várias funcionalidades, incluindo a capacidade de capturar pacotes de rede, realizar ataques de força bruta contra senhas de rede, decifrar chaves *WEP* e *WPA/WPA2*, e realizar outros tipos de análises e ataques de segurança em redes sem fio. Essa ferramenta é comumente utilizada por administradores de rede, profissionais de segurança cibernética e pesquisadores para avaliar a segurança de suas redes e identificar possíveis vulnerabilidades (AIRCRACK-NG, 2024).

3.5.3 *Windows* 11

O *Windows 11* (MICROSOFT, 2024), lançado pela Microsoft em 2021, é um sistema operacional cliente que se baseia na estrutura do Windows 10. Apresenta uma série de aprimoramentos em relação à sua versão anterior, com destaque para inovações voltadas para aprimorar a produtividade dos usuários finais. Além disso, o *Windows 11* foi concebido para atender às necessidades do ambiente de trabalho híbrido atual (MICROSOFT, 2024).

3.5.4 *Omada software controller*

O Omada software controller (TP-LINK, 2024) é uma plataforma desenvolvida para gerenciar todos os dispositivos compatíveis da *Tp-Link*, permitindo configuração centralizada em um único local. O Omada deve ser implantado em um dispositivo de *hardware* dedicado da *TP-Link* ou instalado em qualquer Computador Pessoal *(PC)* ou servidor com sistema operacional *Windows* ou *Linux*. É destinado a usuários que buscam funcionalidades avançadas além das oferecidas por roteadores convencionais. O Omada também atende às necessidades de profissionais de Tecnologia da Informação *(TI)* e empresas que demandam um gerenciamento eficiente e abrangente de sua infraestrutura de rede (TP-LINK, 2024).

3.5.5 *Hping3*

O Hping3 (KALI, 2024a) é uma ferramenta de rede que tem a capacidade de enviar pacotes *Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP) e TCP* personalizados e visualizar as respostas do alvo. Ele consegue lidar com a fragmentação, bem como com o corpo e o tamanho variável dos pacotes, e é capaz de transferir arquivos de acordo com os protocolos compatíveis (KALI, 2024a). Essa ferramenta é útil para testar regras de *firewall*, realizar varreduras de portas (falsificadas), avaliar o desempenho da rede utilizando diferentes protocolos, descobrir o *Maximum Transmission Unit (MTU)* do caminho, executar ações semelhantes ao traceroute em diferentes protocolos, identificar as impressões digitais de sistemas operacionais remotos, auditar pilhas *TCP/IP*, entre outras funções (KALI, 2024a). O *Hping3* também pode ser programado utilizando a linguagem *Tool Command Language (Tcl)*.

3.5.6 *Nmap*

O *Network Mapper (Nmap)* (NMAP, 2024) é uma poderosa ferramenta de código aberto usada para exploração de rede e auditoria de segurança. É uma ferramenta amplamente utilizado por administradores de sistemas e profissionais de segurança cibernética para descobrir

dispositivos na rede, identificar serviços em execução nesses dispositivos, mapear redes, verificar vulnerabilidades de segurança e muito mais. O *Nmap* é conhecido por sua capacidade de fornecer informações detalhadas sobre *hosts* na rede, incluindo detalhes sobre o sistema operacional, portas abertas e serviços em execução. Ele suporta uma variedade de técnicas de varredura e é compatível com várias plataformas, incluindo *Linux*, *Windows* e *macOS* (NMAP, 2024).

3.5.7 *Wireshark*

O Wireshark (WIRESHARK, 2024) é uma ferramenta de *software* de código aberto utilizada para análise de redes e solução de problemas. Ele permite aos usuários capturar e examinar o tráfego de rede em tempo real e também pode analisar arquivos a partir de dados capturados previamente. O *Wireshark* pode capturar dados de uma variedade de interfaces de rede e protocolos, fornecendo aos usuários uma visão detalhada do tráfego em sua rede. Ele é amplamente utilizado para diagnosticar problemas de rede, detectar atividades maliciosas, analisar protocolos e garantir a integridade e segurança da rede (WIRESHARK, 2024).

3.5.8 *Dos tester*

O *Dos tester* (KÜLTEKIN, 2023) é uma ferramenta *Python* (PYTHON, 2019) dedicada a testar ataques do tipo *DoS* em redes *IEEE 802.11* por meio da técnica de inundação de pacotes direcionados. Desenvolvido utilizando o *Scapy* que é uma biblioteca de manipulação de pacotes escrita em *Python* (SCAPY, 2022), esse *software* oferece uma interface de linha de comando simplificada, permitindo aos usuários injetar pacotes com facilidade e realizar testes abrangentes em suas redes (KÜLTEKIN, 2023). O *Dos-tester* demonstra eficácia ao executar uma série de ataques, incluindo a inundação de solicitações de autenticação, associação e investigação.

3.5.9 *Hcxtools*

O Hcxtools (HCXTOOLS, 2024) é um conjunto de ferramentas de linha de comando projetado para capturar, converter e manipular informações relacionadas a redes *Wi-Fi* protegidas por *WPA/WPA2*. Essas ferramentas são usadas principalmente para auditar e testar a segurança de redes sem fio, permitindo que os usuários capturem *handshakes* de autenticação *WPA/WPA2*, convertam esses *handshakes* para diferentes formatos como os aceitos pelo hashcat e realizem ataques de força bruta para recuperar senhas de rede (HCXTOOLS, 2024). O *Hcxtools* é frequentemente utilizado por profissionais de segurança cibernética, pesquisadores e entusiastas de redes para testar a robustez e identificar possíveis vulnerabilidades em redes sem fio protegidas.

É importante observar que o *hcxtools* não é compatível com sistemas operacionais *Windows*, *macOS*, *Android*, emuladores ou *wrappers* (HCXTOOLS, 2024). Ele é projetado principalmente para sistemas baseados em Linux (HCXTOOLS, 2024).

3.5.10 *Hashcat*

O *Hashcat* (HASHCAT, 2024) é uma poderosa ferramenta de quebra de senhas de código aberto, usada para recuperar senhas perdidas ou esquecidas por meio de ataques de força bruta, ataques de dicionário, ataques de máscara e outros métodos de quebra de senha. Ele suporta uma ampla variedade de algoritmos de *hash* e métodos de criptografia, tornando-o uma ferramenta versátil para testar a segurança de senhas em diversos contextos, incluindo auditorias de segurança, testes de penetração e análise forense digital. O *Hashcat* oferece suporte para processamento paralelo em *Central Processing Unit (CPUs)* e *Graphics Processing Unit (GPUs)*, permitindo uma quebra de senhas rápida e eficiente (HASHCAT, 2024).

4 METODOLOGIA

A metodologia proposta compreende quatro fases: a primeira etapa envolve a identificação das características do sistema e do escopo da pesquisa; a segunda fase estabelece os protocolos de comunicação e segurança além de abordar as ferramentas que serão empregadas no experimento a ser conduzido; a terceira etapa concentra-se na construção do ambiente de teste, que servirá como representação de uma rede sem fio; por último, a interpretação dos resultados e diagnósticos obtidos.

A fase inicial do processo aborda a caracterização do problema a ser avaliado, incluindo a delimitação do escopo, a identificação dos componentes pertinentes do sistema sob uma perspectiva de segurança.

Na segunda etapa, são estabelecidos os protocolos de comunicação e de segurança para a realização dos testes, assim como a seleção das ferramentas necessárias. O padrão de comunicação adotado foi o *IEEE 802.11n*, enquanto os protocolos de segurança incluem *WPA* e *WPA2*. As ferramentas utilizadas foram selecionadas por sua eficácia comprovada, ampla adoção na comunidade de segurança, e funcionalidades especializadas para testes de rede e segurança. As ferramentas empregadas nos testes incluem *Aircrack-ng*, *Hping3*, *Wireshark*, *Nmap*, *Hcxtools*, *Dos tester* e *Hashcat*.

A terceira etapa aborda a construção do ambiente de teste destinado a avaliar a segurança de uma rede sem fio utilizando um ponto de acesso *Tp-link EAP115* com *Service Set Identifier (SSID)* definido como AP-TESTE. Este ambiente incluirá dois *notebooks*: um com *Windows 11*, que atuará como o alvo, e outro com *Kali Linux*, que funcionará como o atacante. Ambos os *notebooks* estarão conectados ao ponto de acesso da rede sem fio. O ambiente de teste foi construído de forma que a rede ficasse isolada para evitar interferências de outros tipos de tráfego não relacionados aos ataques em análise.

A quarta etapa da metodologia contempla a avaliação dos resultados dos ataques abordados neste trabalho e sugere algumas contramedidas para mitigar os riscos de segurança.

5 ESTUDO DE CASO

5.1 Objetivos

Este estudo de caso procura analisar os principais tipos de ataques às redes sem fio *IEEE 802.11n*, utilizando um ambiente controlado (*testbed*) mostrado na Figura 4. Pretende-se compreender os riscos de segurança enfrentados por essas redes, avaliando o impacto causado pelos ataques abordados e propor contramedidas para mitigá-los. Abaixo estão descritos os equipamentos utilizados na construção da estrutura do ambiente controlado para execução dos ataques.

- *Notebook* com *Windows* 11.
- *Notebook* com *Kali GNU/Linux Rolling 2023.3*.
- Adaptador *Dual-Band wireless USB Realtek 8811CU Wireless LAN 802.11ac USB NIC*, compatível com os padrões IEEE 802.11ac, 802.11n, 802.11g, 802.11b, 802.11a.
- Ponto de acesso *Tp-link EAP115 V:4.20*, (foram utilizadas definições de fábrica para o *firewall* do dipositivo).

Com relação ao ponto de acesso, suas configurações irão variar no intuito de possibilitar diferentes cenários.

Figura 4 – Diagrama da rede sem fio utilizada nos testes

Fonte: Autor, 2024..

5.2 Modos de operação da placa wireless

5.2.1 Modo promíscuo

O modo promíscuo é um modo especial de operação de uma interface de rede em que é permitido que o dispositivo aceite quadros que não são destinados ao nó local, conforme indicado pelo endereço *MAC* do receptor (JOSHI et al., 2017). O modo promíscuo é usado principalmente para capturar todos os quadros que passam pela interface de rede, incluindo quadros destinados a outros dispositivos na rede (JOSHI et al., 2017).

5.2.2 Modo monitor

No modo monitor, o *hardware* sem fio é configurado para tornar todos os tipos de quadros IEEE 802.11 acessíveis ao usuário (JOSHI et al., 2017). Isso significa que o dispositivo em modo monitor pode capturar e acessar todos os quadros válidos, incluindo quadros de gerenciamento, controle e dados, independentemente do destino (JOSHI et al., 2017). O modo monitor permite uma visão completa do tráfego de rede sem fio e é útil para análise, monitoramento e depuração de redes (JOSHI et al., 2017).

A principal diferença entre o modo promíscuo e o modo monitor é que o modo promíscuo é mais comum em redes com fio, enquanto o modo monitor é específico para dispositivos sem fio, como em redes *Wi-Fi* (JOSHI et al., 2017). Além disso, o modo promíscuo é mais amplo, permitindo que o dispositivo receba e processe todos os pacotes que passam pela rede, enquanto o modo monitor é mais específico, permitindo que o *hardware* sem fio escute apenas os pacotes transmitidos no ar (JOSHI et al., 2017).

Para a realização de alguns dos ataques foi necessário utilizar o modo monitor da placa *wireless*. O primeiro passo é identificar o nome da interface wireless. Uma forma de fazer isso é executar o comando `sudo iwconfig`. Figura 5 mostra o resultado do comando.

O segundo passo é encerrar os processos que possam causar problemas na transição do modo infraestrutura, que é o padrão para o uso comum de uma rede sem fio *IEEE 802.11*, para o modo monitor. Para isso, foi utilizado o comando `airmon-ng check kill`.

O terceiro passo é realizar a mudança para o modo monitor. Uma das formas de executar essa mudança é utilizando o comando `airmon-ng start wlan1`. Figura 6 mostra o resultado do comando. Neste ponto a interface de rede `wlan1` está em modo monitor.

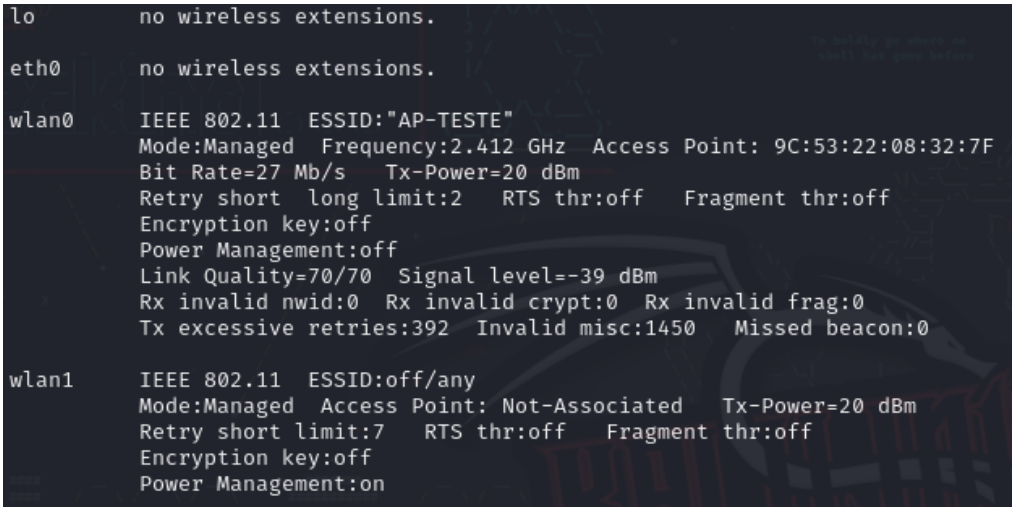

Figura 5 – Interfaces de rede disponíveis.

Fonte: Autor, 2024.

Figura 6 – Interface de rede alterada para o modo monitor.

Fonte: Autor, 2024.

5.2.3 Modo infraestrutura

O modo infraestrutura é o modo padrão de operação da interface de rede em dispositivos clientes, como *notebooks*, *smartphones* e *tablets*, permitindo que esses dispositivos se conectem a um ponto de acesso. Para alterar a placa de rede do modo monitor para o modo infraestrutura foi utilizado o comando `airmon-ng stop wlan1`. Figura 7 mostra o resultado do comando.

Figura 7 – Interface de rede alterada para o modo infraestrutura.

Fonte: Autor, 2024.

5.3 Ataque de inundação *SYN*

5.3.1 Ataque de inundação de *SYN* direcionado a porta 80 de um dispositivo na rede

O objetivo deste ataque é sobrecarregar o dispositivo alvo com um grande volume de solicitações *SYN* falsas, visando esgotar seus recursos e impedir que ele responda a solicitações

legítimas. Neste cenário o notebook kali com *Internet Protocol (IP)* `192.168.1.111` é o atacante e o dispositivo windows com *IP* `192.168.1.145` é o alvo.

O primeiro passo é a identificação de portas abertas no alvo. Para fazer essa identificação foi utilizado a varredura de portas[1] do *nmap* por meio do comando `nmap -sS 192.168.1.145`.

A flag `-sS` indica o uso da varredura *TCP SYN*. Esta é a opção de varredura padrão e mais popular. É veloz, vasculhando milhares de portas por segundo, invisível para *firewalls* intrusivos, é camuflada e de baixo impacto uma vez que não completa conexões *TCP*. Funciona em qualquer pilha *TCP* padronizada, sem depender de particularidades de plataformas específicas. É capaz de distinguir com precisão portas abertas, fechadas e filtradas. A sequência `192.168.1.145` é o endereço *IP* do destino para o qual a varredura está sendo realizada. Figura 8 mostra o resultado da execução da varredura de portas.

```
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
```

Figura 8 – Resultado da varredura de porta.

Fonte: Autor, 2024.

O segundo passo é a execução do ataque utilizando o comando `hping3 -c 20000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.145`. A flag `-c` define como 20000 o número de pacotes a serem enviados, `-d` define o tamanho do dado, `-S` especifica a flag `SYN` para pacotes *TCP*, `-w` define o tamanho da janela *TCP*, `-p` especifica a porta de destino, `-flood` faz com que os pacotes sejam enviados o mais rápido possível, `-rand-source` randomiza os endereços *IP* de origem e `192.168.1.145` é o endereço *IP* do alvo.

Figura 9 mostra a utilização da *CPU* do dispositivo. Podemos verificar que o consumo estava em *0%* antes do ataque e teve um leve aumento durante o ataque, chegando a um consumo máximo de *3%*. O ataque afetou de forma mínima a *CPU* do dispositivo alvo.

[1] A varredura de portas é uma técnica utilizada para identificar quais portas em uma rede estão acessíveis e podem estar prontas para receber ou enviar dados (AVAST, 2024).

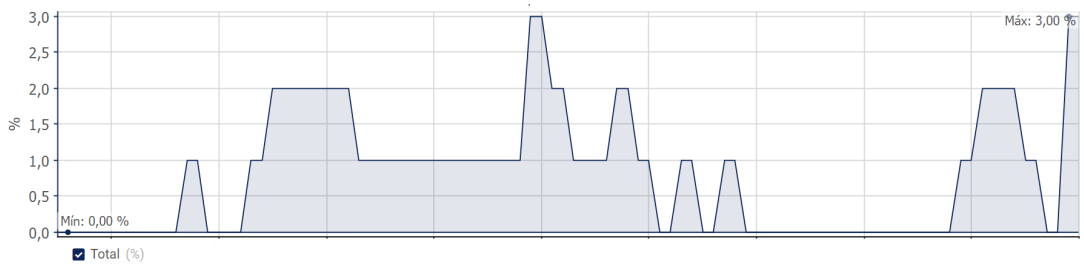

Figura 9 – Utilização da *CPU* do dispositivo conectado ao *AP*.

Fonte: Autor, 2024.

Na Figura 10, é apresentado o gráfico de tráfego. Antes do ataque, observa-se que o tráfego estava em *0 Mbit/s*. Durante o ataque, há um aumento notável no tráfego, atingindo um pico máximo de *11,5 Mbit/s*.

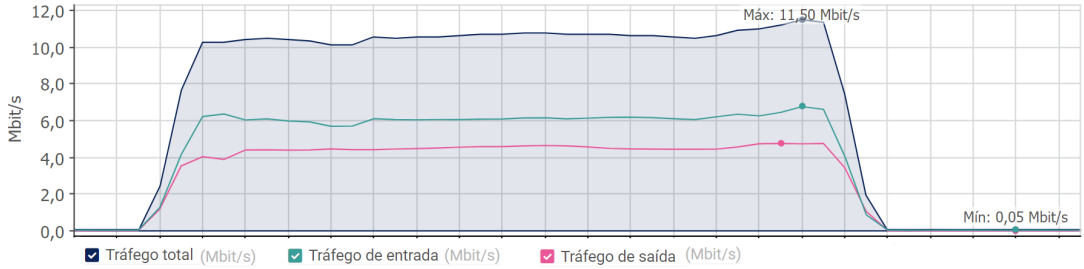

Figura 10 – Tráfego *Wi-Fi* do dipositivo conectado ao *AP*.

Fonte: Autor, 2024.

5.3.2 Ataque de inundação de *SYN* direcionado a porta 80 do ponto de acesso

O objetivo deste ataque é sobrecarregar o ponto de acesso com um grande volume de solicitações SYN falsas, visando esgotar seus recursos e impedir que ele responda a solicitações legítimas. Neste caso, o *notebook kali* com *IP* `192.168.1.111` é o atacante e o ponto de acesso *Tp-link EAP115* com *IP* `192.168.1.120` é o alvo.

O primeiro passo é identificar portas abertas no alvo que, neste caso, será o *AP*. Para esta tarefa foi utilizada a ferramenta *nmap*. Figura 11 mostra o resultado da varredura de porta onde é possível verificar que a parta *80* está aberta.

```
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
44443/tcp open  coldfusion-auth
```

Figura 11 – Identificação de portas abertas no *AP*.

Fonte: Autor, 2024.

O segundo passao é a realização do ataque utilizando as informações obtidas na varredura de porta feita no *AP*. Neste passo foi utilizado o comando `hping3 -c 20000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.120`.

Figura 12 mostra a utilização do canal antes do ataque. A figura indica que o canal tem baixa utilização. A taxa de recepção (*RX*) e de transmissão (*TX*) de quadros é baixa e não há indicador de interferência. A utilização total do canal é de *17%* e está classificado como bom.

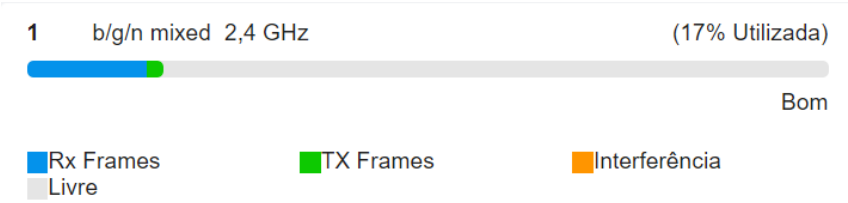

Figura 12 – Utilização do canal de rádio do *AP* antes do ataque.

Fonte: Autor, 2024.

A Figura 13 mostra a utilização do canal durante o ataque. Aqui é possível verificar que o ataque causou impacto significativo na utilização do canal. É notável o aumento da taxa de recepção de quadros (*RX*) e surgimento de interferência. A utilização do canal chegou a *90%*, que é bem próxima de sua capacidade máxima.

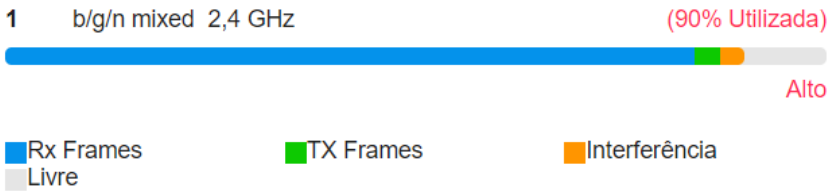

Figura 13 – Gráfico de utilização do canal de rádio do *AP* durante o ataque.

Fonte: Autor, 2024.

Figura 14 mostra o uso da *CPU* e da memória antes e durante um ataque. A análise da figura revela um impacto significativo na utilização da *CPU* do ponto de acesso, enquanto houve uma leve alteração no consumo de memória. Antes do ataque, a *CPU* operava a *1%* de sua capacidade, enquanto a memória estava em *68%*. Durante o ataque, a *CPU* foi sobrecarregada, atingindo *100%* de sua capacidade, enquanto a memória subiu para *75%*. Ainda durante o ataque, ocorreram oscilações subsequentes, com a *CPU* atingindo *51%* de utilização e a memória permanecendo em *76%* e posteriormente a *CPU* retornando a *99%* e a memória mantendo-se em *75%* de utilização. Essa sobrecarga resultou em múltiplos reinícios do ponto de acesso, causando indisponibilidade do serviço.

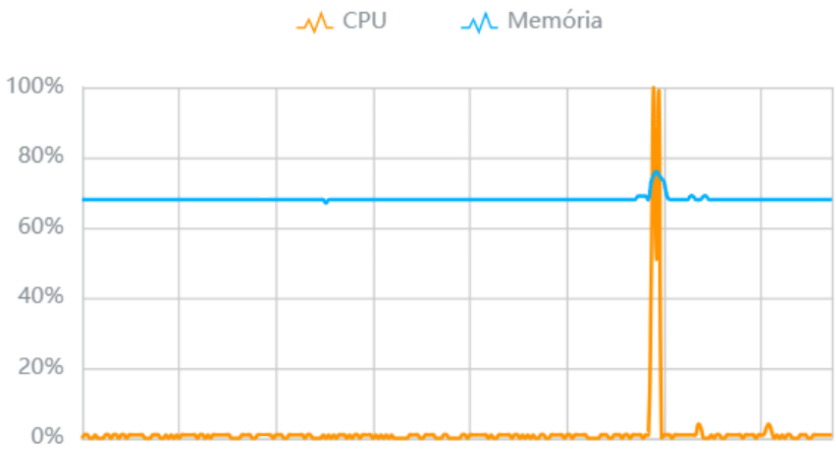

Figura 14 – Gráfico de *CPU* e memória do *AP*.

Fonte: Autor, 2024.

A Tabela 1 mostra os valores de *CPU* e memória antes e durante o ataque.

	CPU (%)	**Memória (%)**
Antes do ataque	1	68
Durante o ataque	100	75
Durante o ataque	51	76
Durante o ataque	99	75

Tabela 1 – Uso de *CPU* e Memória do *AP*

Fonte: Autor, 2024.

Figura 15 revela uma variação significativa no tempo de resposta relacionado ao aplicativo *ping* durante o ataque de inundação de *SYN*, com um aumento substancial em comparação ao período prévio. Antes do ataque, o tempo de resposta do aplicativo *ping* mantinha-se em torno de *1 milissegundo*, enquanto durante o ataque atingiu picos de até *457 milissegundos*. Além disso, é notável uma elevada taxa de perda de pacotes durante o ataque, chegando a atingir *80%* de perda.

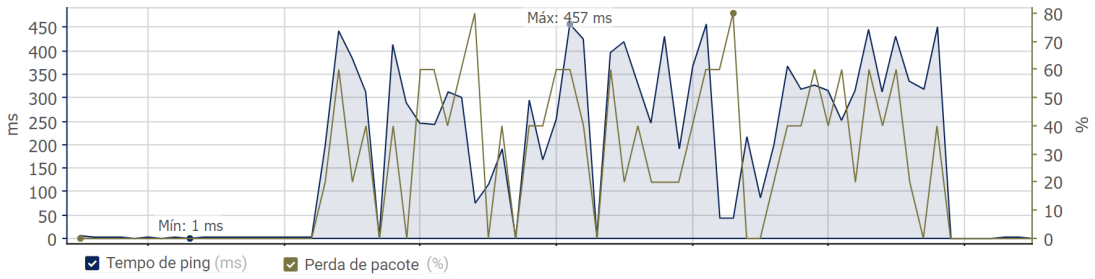

Figura 15 – Gráfico de tempo de ping e perda de pacote do *AP*.

Fonte: Autor, 2024.

Figura 16 mostra o tempo de atividade e inoperância do ponto de acesso. Destaca-se em vermelho no gráfico os períodos em que o *AP* ficou inoperante, o que ocorreu em vários momentos durante o ataque de inundação de *SYN*.

Figura 16 – Tempo de atividade e inoperância do *AP*.

Fonte: Autor, 2024.

5.4 Ataque de desautenticação

Este ataque visa interromper a conexão entre um dispositivo e o ponto de acesso da rede *Wi-Fi* tornando a rede indisponível. Neste cenário, o *notebook kali* é o atacante e o *notebook Windows* com *MAC 14:85:7F:5D:29:65* é o alvo.

O primeiro passo é colocar a placa *wireless* do *notebook kali* no modo monitor como foi demonstrado na Seção 5.2.2. O segundo passo é monitorar o tráfego. Para executar este passo foi utilizada a ferramenta *airodump-ng* como o comando `airodump-ng wlan1 --channel 1`.

Na Figura 17 é possível identificar o *AP* alvo com *MAC 9C:53:22:08:32:7F* e *SSID AP-TESTE* que está operando no canal 1. Nesta figura também é possível identificar o endereço *MAC 14:85:7F:5D:29:65* do dispositivo conectado ao *AP*.

```
CH  1 ][ Elapsed: 1 min ][ 2024-05-23 01:43

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

14:CC:20:DD:E3:B8   -1   0        0        2    0   1   -1   WPA              <length:  0>
9C:53:22:08:32:7F  -54 100      814       37    0   1  130   WPA2 CCMP   PSK  AP-TESTE

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

9C:53:22:08:32:7F  14:85:7F:5D:29:65  -61    0 - 6e     0       65
```

Figura 17 – Monitoramento da rede sem fio.

Fonte: Autor, 2024.

Com as informações obtidas durante o monitoramento, exibidas na Figura 17, é possível

executar o ataque de desautenticação utilizando o comando `aireplay-ng --deauth 0 -c 14:85:7F:5D:29:65 -a 9C:53:22:08:32:7F wlan1`.

O aireplay-ng é a ferramenta do aircrack-ng que injeta pacotes em uma rede sem fio. A flag `-deauth` com valor `0` indica que o comando deve ser executado até que seja interrompido pelo usuário. A flag `-c` define o endereço *MAC* do dispositivo que será desautenticado. A flag `-a` define o endereço *MAC* do *AP* e `wlan1` é o nome da interface de rede no modo monitor.

Na Figura 18 podemos ver o que a ferramenta exibe durante a execução do ataque.

```
Waiting for beacon frame (BSSID: 9C:53:22:08:32:7F) on channel 1
Sending 64 directed DeAuth (code 7). STMAC: [14:85:7F:5D:29:65] [11|27 ACKs]
Sending 64 directed DeAuth (code 7). STMAC: [14:85:7F:5D:29:65] [24|41 ACKs]
Sending 64 directed DeAuth (code 7). STMAC: [14:85:7F:5D:29:65] [ 0|21 ACKs]
Sending 64 directed DeAuth (code 7). STMAC: [14:85:7F:5D:29:65] [ 0|21 ACKs]
Sending 64 directed DeAuth (code 7). STMAC: [14:85:7F:5D:29:65] [ 0|54 ACKs]
Sending 64 directed DeAuth (code 7). STMAC: [14:85:7F:5D:29:65] [ 0|54 ACKs]
Sending 64 directed DeAuth (code 7). STMAC: [14:85:7F:5D:29:65] [ 0|59 ACKs]
Sending 64 directed DeAuth (code 7). STMAC: [14:85:7F:5D:29:65] [61|89 ACKs]
```

Figura 18 – Ataque em execução.

Fonte: Autor, 2024.

Neste ponto, enquanto o ataque estiver em execução, o dispositivo alvo será desconectado e ficara impossibilitado de se reconectar ao *AP*.

As redes *Wi-Fi* de hoje, que utilizam os padrões *IEEE 802.11*, geralmente criptografam os quadros de dados durante a transmissão (REEN et al., 2023). No entanto, os quadros de gerenciamento, como (des)autenticação, (des)associação, *beacons* e *probes*, são enviados sem criptografia para garantir compatibilidade entre todos os clientes (REEN et al., 2023). Essa vulnerabilidade permite que atacantes desconectem repetidamente dispositivos clientes de uma rede, falsificando pacotes *Wi-Fi* e transmitindo mensagens de desautenticação (REEN et al., 2023).

5.5 Ataque de inundação de requisição de associação

O ataque *Association request flood (AssRF)* visa sobrecarregar um ponto de acesso *Wi-Fi* com um grande número de solicitações de associação falsas. Isso pode inundar o *AP* e impedi-lo de atender a solicitações de dispositivos reais, causando instabilidade ou indisponibilidade da rede *Wi-Fi*. Neste caso o *notebook kali* é o atacante e o ponto de acesso *Tp-link EAP115* é o alvo.

Inicialmente deve-se alterar a placa *wireless* do *notebook* para o modo monitor como visto na Seção 5.2.2. Para que o ataque seja executado é necessário o endereço *MAC* da interface

de rede utilizada para realizar o ataque, o *MAC* do dispositivo alvo e o seu *SSID*. Para obter as informações relativas ao *AP* alvo foi utilizado o comando `airodump-ng wlan1 --channel 1` já descrito na Seção 5.4. O resultado do monitoramento do *canal 1* pode ser visto na Figura 17.

Para realização deste ataque foi utilizada a ferramenta *DoS-Tester*, utilizando o seguinte comando: `python3 dos_tester.py -src E0:1C:FC:DC:F3:1C -dst 9C:53:22:08:32:7F -i wlan1 -p assocReq -c 99999999 -ssid "AP-TESTE"`.

A flag `-src` indica o endereço *MAC* de origem, `-dst` indica o endereço *MAC* de destino, `-i` indica a interface de rede, `-p` indica o tipo de pacote, `-c` indica o número de pacotes a serem enviados e `-ssid` indica o *SSID* do *AP*.

Para monitorar o ponto de acesso foi utilizado o *Omada Controller*. Figura 19 mostra a largura de banda do ponto de acesso antes da ocorrência do ataque. Pode-se identificar que a largura de banda está classificada como boa, utilizando apenas *13%* de sua capacidade, não havendo interferência e a taxa de recepção (*RX*) e de transmissão (*TX*) de quadros é baixa.

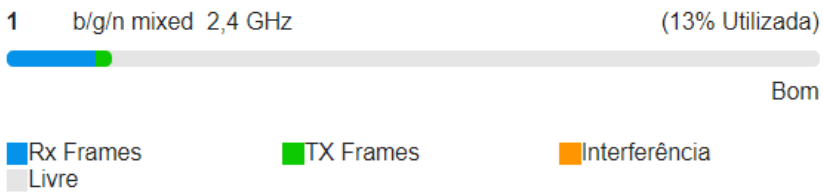

Figura 19 – Gráfico de utilização do canal de rádio do *AP* antes do ataque.

Fonte: Autor, 2024.

Figura 20 mostra o impacto causado pelo ataque. Podemos visualizar o alto consumo do canal utilizando *92%* de sua capacidade. Houve um aumento considerável na taxa de recepção (*RX*) e de transmissão (*TX*) de quadros, além do surgimento de interferência no canal.

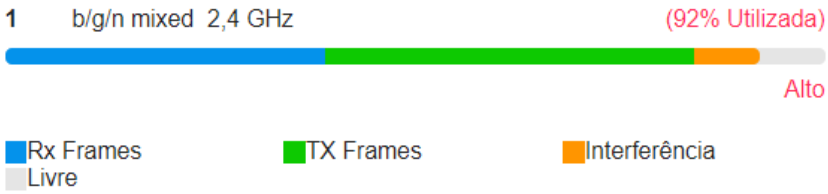

Figura 20 – Gráfico de utilização do canal de rádio do *AP* durante o ataque.

Fonte: Autor, 2024.

Figura 21 mostra a utilização de *CPU* e memória do ponto de acesso. No gráfico podemos visualizar o momento anterior ao ataque onde o consumo de memória está em *68%* e a utilização do processador está em *1%*. No período em que o *AP* foi submetido ao ataque, a utilização do

processador não teve alteração significativa, passando de *1%* para *2%*. Já o consumo de memória aumentou significativamente, indo de *68%* para *93%*. Neste ponto, ocorreu a negação de serviço, indicada pela descontinuidade no gráfico de *CPU* e memória.

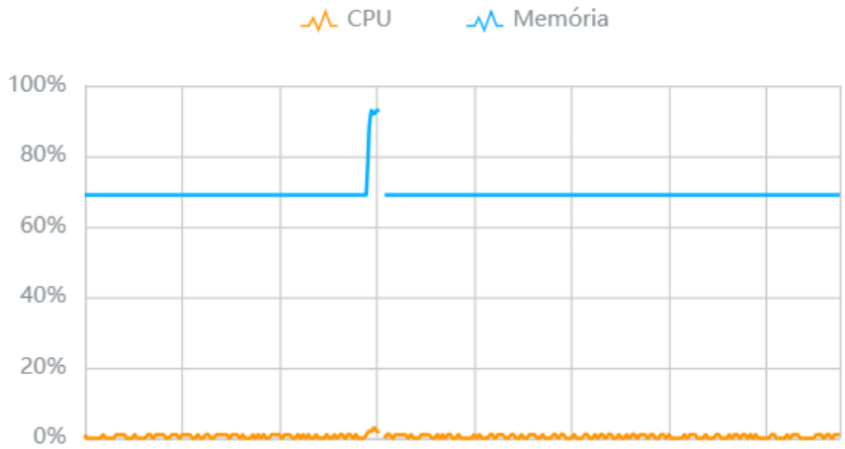

Figura 21 – Gráfico de uso de *CPU* e memória do *AP*.

Fonte: Autor, 2024.

A Tabela 2 traz os valores de *CPU* e memória indicados pelo *Omada Controller* antes e durante o ataque.

	CPU (%)	**Memória (%)**
Antes do ataque	1	68
Durante o ataque	2	93

Tabela 2 – Uso de *CPU* e memória do *AP*

Fonte: Omada Controller, 2024.

5.6 Ataque de inundação de solicitação de autenticação

O objetivo do ataque *Authentication Request Flood (AuthRF)* é sobrecarregar o ponto de acesso com um grande volume de solicitações de autenticação falsas, visando esgotar os recursos do ponto de acesso e torná-lo inoperável para os usuários. Neste caso, o *notebook Kali* será o atacante e o ponto de acesso *Tp-link EAP115* será o alvo.

O primeiro passo para a execução do ataque é alterar a placa *wireless* do *notebook* para o modo monitor como demonstrado na Seção 5.2.2.

O segundo passo é obter o endereço *MAC* do *AP* alvo. Para executar este passo foi utilizado o comando `airodump-ng wlan1 --channel 1` já descrito na Seção 5.4.

Com o endereço *MAC* do *AP* é possível realizar o ataque utilizando o comando `python3 dos_tester.py -src E0:1C:FC:DC:F3:1C -dst 9C:53:22:08:32:7F -i wlan1 -p authReq -c 99999999`.

Figura 22 mostra que a utilização do canal antes do início do ataque está em *14%*. Observa-se uma baixa utilização de quadros recebidos (*RX*) e transmitidos (*TX*). Apesar de uma pequena interferência, a utilização do canal é classificada como boa.

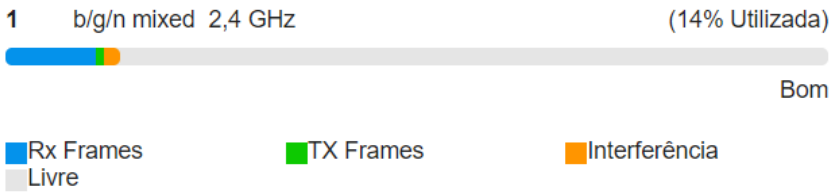

Figura 22 – Gráfico de utilização do canal de rádio do *AP* antes do ataque.

Fonte: Autor, 2024.

Figura 23 mostra a utilização do canal durante o ataque. Neste gráfico, é possível identificar um aumento na taxa de quadros recebidos (*RX*) e transmitidos (*TX*), além do aumento na interferência. A utilização total saiu de *14%* para *91%* mostrando que o canal está operando próximo de sua capacidade máxima.

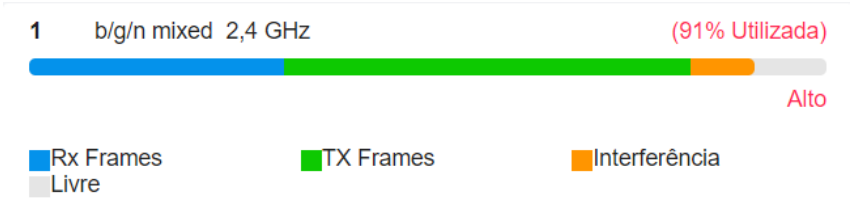

Figura 23 – Gráfico de utilização do canal de rádio do *AP* durante do ataque.

Fonte: Autor, 2024.

Figura 24 mostra que durante o ataque, o recurso mais sobrecarregado no ponto de acesso foi a *CPU*. Antes do ataque, a utilização da *CPU* oscilava entre *0%* e *1%*. Durante o ataque, essa utilização aumentou para *88%*, oscilou entre *85%* e *87%*. Embora não tenha havido uma mudança significativa no consumo de memória do *AP*, o ataque teve um impacto substancial, levando a *CPU* do *AP* a operar próximo de sua capacidade máxima, mas não chegou a provocar negação de serviço.

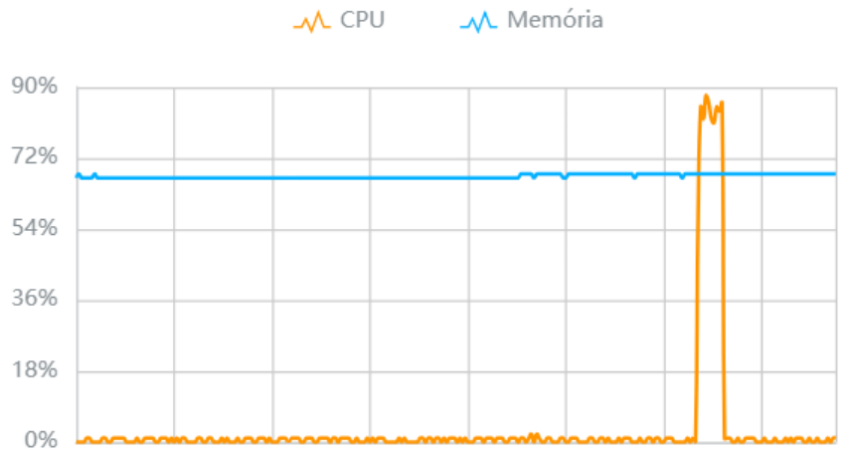

Figura 24 – Gráfico de utilização de *CPU* e memória do *AP*.

Fonte: Autor, 2024.

Na Tabela 3 estão os dados precisos de *CPU* e memória indicados pelo *Omada Controller* antes e durante o ataque.

	CPU (%)	**Memória (%)**
Antes do ataque	1	68
Durante o ataque	88	68

Tabela 3 – Uso de *CPU* e Memória do *AP*

Fonte: Omada Controller, 2024.

5.7 Ataque de escuta (*Eavesdropping*)

Este ataque tem o objetivo de interceptar a comunicação do usuário, comprometendo a confidencialidade de seus dados. Neste cenário, o *notebook Kali* será o atacante e o *notebook Windows 11* será o alvo.

Para executar este ataque é obrigatório que a placa de rede do dispositivo invasor suporte o modo monitor. O primeiro passo é alterar o modo de operação da placa de rede para o modo monitor, como mostrado na Seção 5.2.2.

O segundo passo é a captura do *handshake* transmitido entre alvo e o ponto de acesso. Para realizar a captura foi utilizada a ferramenta *hcxdumptool* como o comando: `hcxdumptool -i wlan1 -c 1a -w wpa-psk-aes-senha1.pcapng`.

A opção `-i` especifica a interface de rede no modo monitor, enquanto a opção `-c` indica o canal em que o ponto de acesso está operando, neste caso, o *canal 1*. A banda em que o *AP* está operando, que é *2,4 GHz*, é representada pela letra `a`. Por fim, a opção `-w` indica o nome do arquivo no qual o *handshake* será salvo.

Figura 25 mostra o resultado do ataque de escuta. Aqui, são exibidas informações como a frequência e o canal onde o ataque está sendo executado, o endereço *MAC* do dispositivo operando no referido canal e o *SSID* do ponto de acesso. Na última linha, há a indicação de que o *handshake* foi capturado.

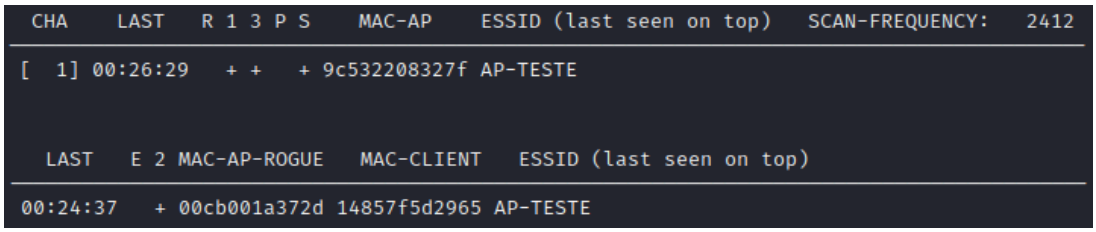

Figura 25 – *Handshake* capturado.

Fonte: Autor, 2024.

Figura 26 exibe o arquivo de saída resultante do ataque de escuta. Na imagem, podemos identificar as quatro vias do *handshake* do protocolo *WPA2*. Os *handshakes* capturados no ataque de escuta serão utilizados no ataque de quebra de senha. Foram capturados *handshakes* dos protocolos *WPA* e *WPA2*.

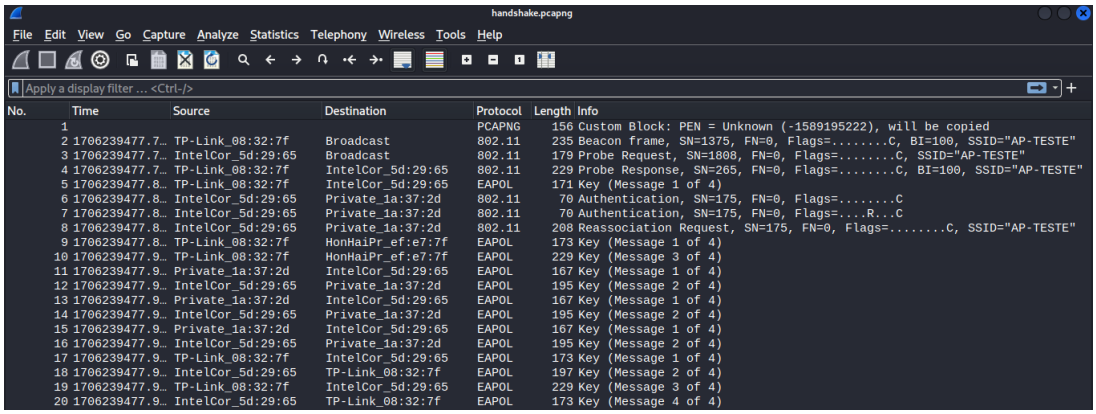

Figura 26 – Arquivo pcapng aberto com wireshark.

Fonte: Autor, 2024.

5.8 Quebra de senha

Para o ataque de quebra de senha foram utilizadas quatro (04) senhas utilizando os padrões *WPA* e *WPA2*. Estas senhas foram classificadas como muito fraca, fraca, forte e muito forte. Para classificar as senhas desta forma foi utilizado o teste de força da senha do Centro Acadêmico de Computação e Comunicações da Universidade de Illinois (UIC.EDU, 2024). Neste teste as senhas são classificadas de acordo com uma série de características. A cada característica atendida a senha recebe um acréscimo na nota e a cada característica não atendida recebe uma

redução na nota (UIC.EDU, 2024). Os atributos avaliados são os seguintes: número de caracteres, letras maiúsculas, letras minúsculas, números, símbolos, números ou símbolos intermediários e conter todos os atributos citados anteriormente (UIC.EDU, 2024).

Para executar a quebra de senha foi utilizada a ferramenta *hashcat* com máscaras que são formatos predefinidos que indicam a estrutura das senhas que serão geradas durante ataques de força bruta. O primeiro passo é a conversão do arquivo *pcapng*, obtido através da ferramenta *hcxdumptool*, para o formato *.hc22000*, aceito pelo *hashcat*. Foi utilizado o seguinte comando `hcxpcapngtool -o handshake_convertido.hc2200 -E essidlist handshake.pcapng`.

A flag `-o` indica o nome do arquivo que será resultante da conversão para o formato `hc22000`. A flag `-E` gera uma lista contendo `SSIDs` caso tenham sido capturados `handshakes` de outros dispositivos, por fim `handshake.pcapng` que é o nome do arquivo que será convertido.

O segundo passo envolve a quebra de senha, utilizando a ferramenta *hashcat* com o comando `hashcat -m 22000 handshake_convertido.hc22000 -a 3 ?d?d?d?d ?d?d?d?d`. A quebra de senha ocorrerá através do método de força bruta, utilizando apenas a *CPU*.

A flag `-m` indica o tipo de hash que será utilizado. Em seguida, vem o nome do arquivo convertido para o formato aceito pelo `hashcat`. A flag `-a 3` indica que será utilizado o ataque de força bruta e por último a máscara `?d?d?d?d?d?d?d?d` que especifica uma sequência de *8* dígitos.

Figura 27 mostra que a senha numérica de *8* dígitos *12345678* foi decifrada em menos de *1* segundo. A senha utilizada neste caso foi classificada como muito fraca e o padrão de segurança utilizado foi o *WPA*.

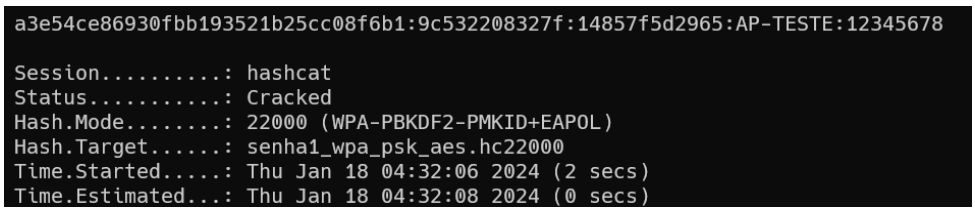

Figura 27 – Hashcat, senha muito fraca WPA.

Fonte: Autor, 2024.

Figura 28 mostra a senha *12345678*, utilizando o padrão *WPA2*, sendo decifrada em menos de *1* segundo.

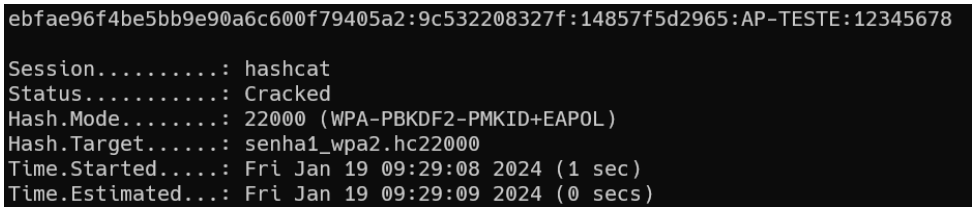

Figura 28 – Hashcat, senha muito fraca WPA2.

Fonte: Autor, 2024.

Para realizar o ataque na segunda senha foi utilizado o seguinte comando: `hashcat -m 22000 handshake_convertido.hc22000 -a 3 ?l?s?l?l?l?l?l?l`. Neste caso, a máscara especifica uma senha composta por uma letra minúscula e um símbolo especial seguido de seis letras minúsculas.

Figura 29 mostra que a estimativa de tempo para a quebra da senha *p@ssword* é de 13 dias e 15 horas. A senha utilizada neste caso foi classificada como fraca e o padrão de segurança utilizado foi o *WPA*.

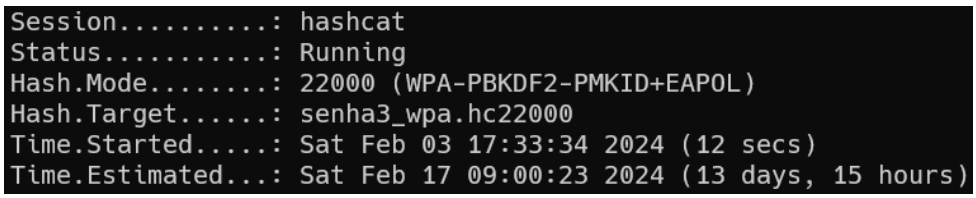

Figura 29 – Hashcat, senha fraca WPA.

Fonte: Autor, 2024.

Figura 30 mostra que a utilização do padrão *WPA2* acarreta um tempo de 16 dias e 23 horas para decifrar a senha *p@ssword*.

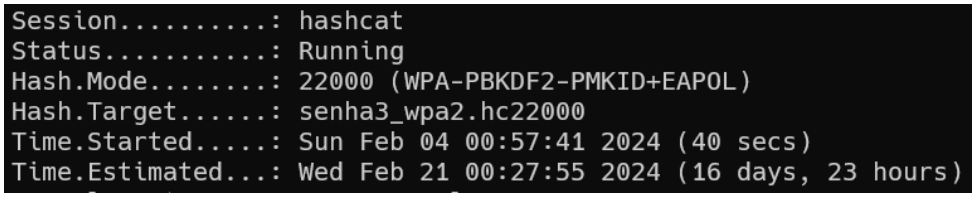

Figura 30 – Hashcat, senha fraca WPA2.

Fonte: Autor, 2024.

Para realizar o ataque na terceira senha foi utilizado o seguinte comando: `hashcat -m 22000 handshake_convertido.hc22000 -a 3 ?d?l?d?l?d?l?d?l?d?l`. A máscara especifica uma sequência alternada de dígitos e letras minúsculas em que `?d` representa um dígito (0-9) e `?l` representa uma letra minúscula (a-z).

Figura 31 mostra que o tempo estimado para quebrar a senha é de 60 dias e 18 horas. Neste caso, a senha utilizada foi *1q2w3e4r5t* sendo avaliada como forte. O padrão de segurança utilizado aqui foi o *WPA*.

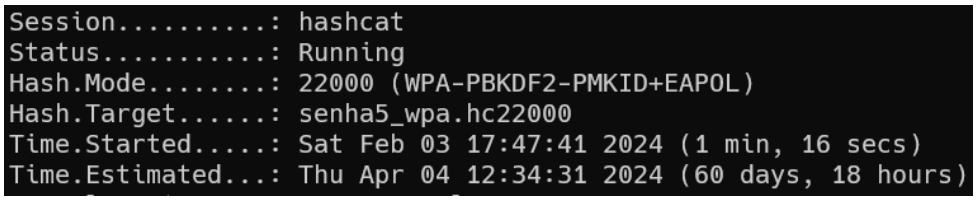

Figura 31 – Hashcat, senha forte WPA.

Fonte: Autor, 2024.

Figura 32 mostra que utilizando o padrão de segurança *WPA2*, o tempo estimado para conseguir quebrar a senha *1q2w3e4r5t* é de 76 dias e 3 horas.

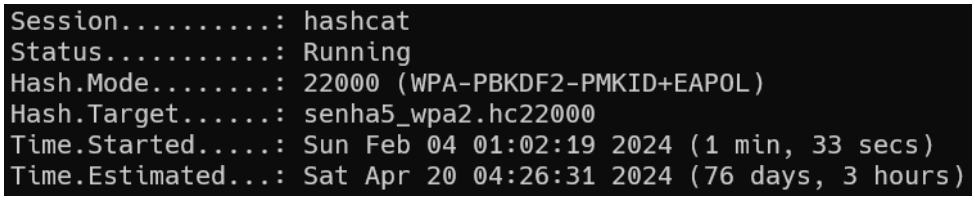

Figura 32 – Hashcat, senha forte WPA2.

Fonte: Autor, 2024.

Na realização do ataque na quarta senha foi utilizado o seguinte comando: `hashcat -m 22000 handshake_convertido.hc22000 -a 3 ?u?l?l?l?s?u?s?u?l?l?l?l`. Neste caso, a máscara especifica uma senha de doze dígitos composta por letras maiúsculas (*?u*), letras minúsculas (*?l*) e caracteres especiais (*?s*).

Figura 33 mostra que a estimativa de quebra da senha *Ofar-E*Qnmcm* é superior a 10 anos. Aqui a senha utilizada está classificada como muito forte e o padrão de segurança utilizado foi o *WPA*.

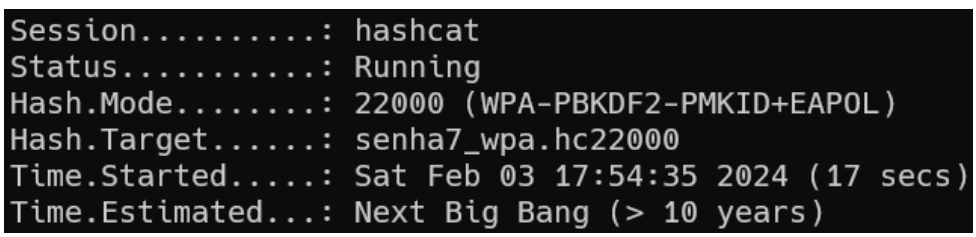

Figura 33 – Hashcat, senha muito forte WPA.

Fonte: Autor, 2024.

Figura 34 mostra que utilizando o padrão de segurança *WPA2*, o tempo estimado para decifrar a senha *Ofar-E*Qnmcm* maior que 10 anos.

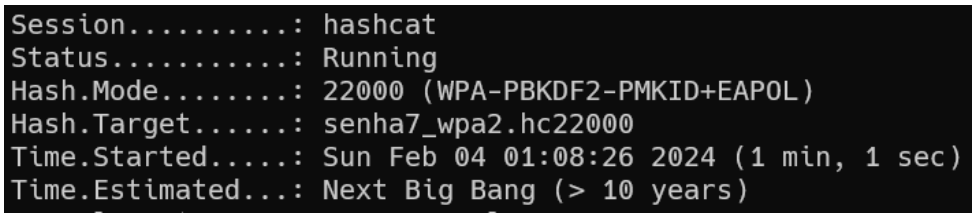

Figura 34 – Hashcat, senha muito forte WPA2.

Fonte: Autor, 2024.

Figura 35 apresenta o gráfico do tempo estimado para quebrar senhas. É evidente que a senha classificada como muito fraca é facilmente decifrada por meio de ataques de força bruta, independentemente do uso do padrão *WPA* ou *WPA2*. A senha classificada como fraca, tem uma estimativa de quebra de *13* dias no padrão *WPA* e *16* dias no padrão *WPA2*, o que é factível por meio de ataques de força bruta. Para a senha classificada como forte, a estimativa de quebra é de *60* dias no padrão *WPA* e de *76* dias no padrão *WPA2*, evidenciando um aumento no tempo necessário para decifrar a senha ao mudar do *WPA* para o *WPA2*. Já a senha classificada como muito forte possui uma estimativa de tempo para ser quebrada de mais de *10* anos, tornando inviável sua quebra por força bruta. Nesse caso, por conta da estimativa imprecisa do *hashcat*, não foi observada uma diferença na utilização dos padrões *WPA* e *WPA2*.

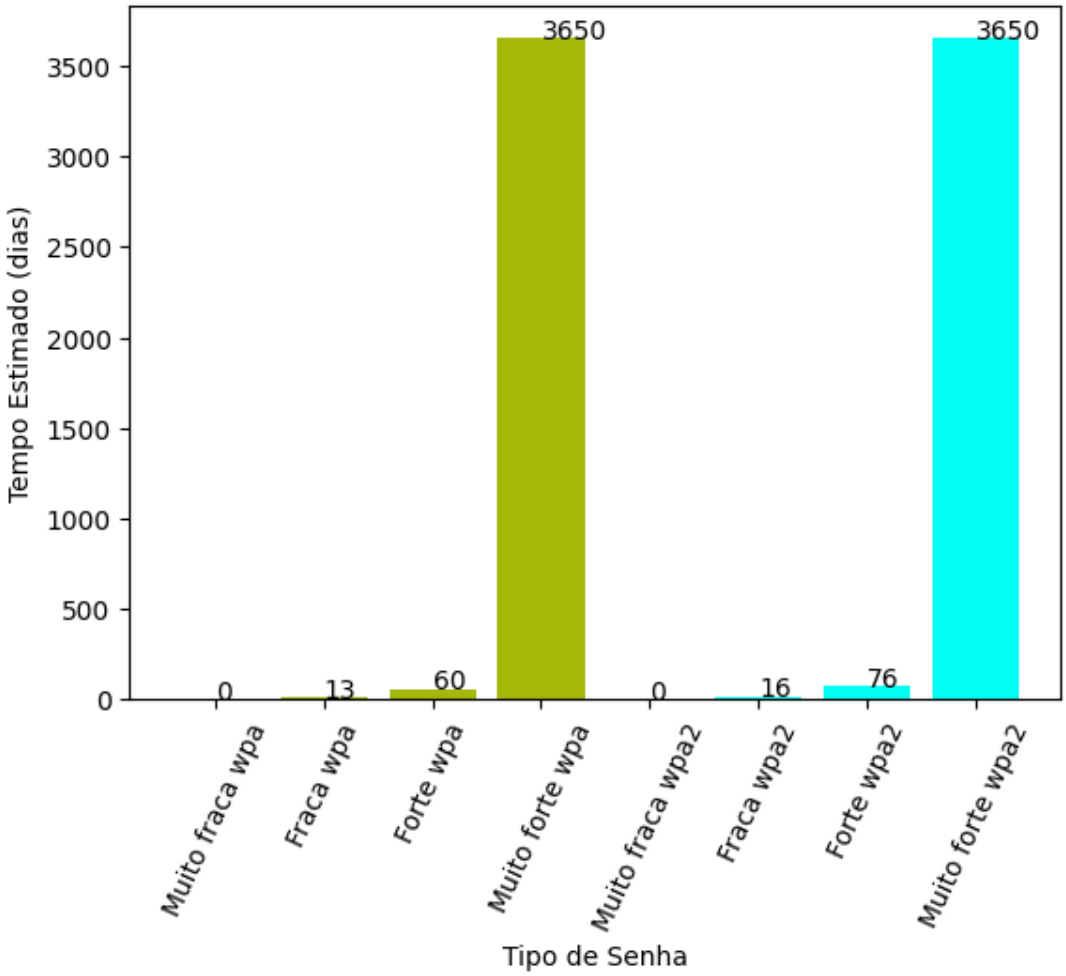

Figura 35 – Tempo estimado para quebra de senha.

Fonte: Autor, 2024.

Quando uma senha leva mais de *3650* dias (*10* anos) para ser quebrada, o *Hashcat* não fornece uma estimativa específica, mas simplesmente indica que o tempo de quebra excede esse limite. Na Figura 35, nos casos onde ocorre essa limitação, o tempo de quebra dessa senha foi arredondado para *3650* dias como uma maneira de representar essa informação no gráfico.

6 MEDIDAS DE SEGURANÇA

Neste capítulo, serão apresentadas algumas medidas destinadas a reforçar a segurança das redes *Wi-Fi* visando dificultar o sucesso de possíveis ataques por parte de potenciais invasores.

No âmbito da tecnologia *Wi-Fi*, segurança compreende dois aspectos essenciais. Em primeiro lugar, trata-se do controle sobre quem pode acessar e configurar sua rede e dispositivos (ALLIANCE, 2024). Em segundo lugar, refere-se à proteção dos dados transmitidos pela sua rede *Wi-Fi*, assegurando que não sejam visualizados por partes não autorizadas (ALLIANCE, 2024).

É recomendada a atualização regular de *firmware* e dispositivos. Manter o *firmware* de dispositivos, roteadores e *hardware Wi-Fi* atualizados é crucial para corrigir vulnerabilidades conhecidas e garantir a segurança da rede (TIMONERA; BASAN, 2024). Alterar os nomes de rede *Wi-Fi* (*SSIDs*) e senhas padrão por senhas complexas dificulta significativamente o acesso não autorizado (TIMONERA; BASAN, 2024). Utilizar protocolos de criptografia robustos, como *WPA2* ou *WPA3*, garante uma comunicação segura e protegida contra ataques de força bruta e interceptação de dados (KARASEK, 2018). Sempre que possível, recomenda-se a utilização dos protocolos de criptografia mais recentes (KARASEK, 2018).

No contexto da segurança da informação, o *NIST* [1] fornece diretrizes para a implementação de autenticação digital em sistemas de informação por meio do documento "*NIST Special Publication 800-63*"(NIST, 2024). Adotar as políticas de senha recomendadas pelo NIST é uma das melhores formas de se proteger de um ataque de quebra de senha, as diretrizes incluem:

Comprimento da senha: Senhas devem ter no mínimo *12* caracteres (NIST, 2024). Não há limite máximo de comprimento de senha (NIST, 2024).

Composição da senha: Senhas devem ser compostas por caracteres *ASCII*, incluindo espaços (NIST, 2024). Caracteres especiais não são mais obrigatórios (NIST, 2024).

Autenticação multifator (*MFA*): O uso de *MFA* é recomendado como medida de segurança adicional, mesmo para senhas fortes (NIST, 2024).

Lista de bloqueio de senhas: O uso de listas de bloqueio é recomendado para impedir o uso de senhas comuns e comprometidas (NIST, 2024).

Expiração de senha: A expiração periódica de senha não é mais recomendada (NIST, 2024).

[1] O Instituto Nacional de Padrões e Tecnologia (do inglês National *Institute of Standards and Technology - NIST*) é uma agência federal dos Estados Unidos que se dedica ao desenvolvimento e à promoção de padrões em diversas áreas como tecnologia da informação, engenharia e etc (NIST, 2024).

Memorização de senha: O *NIST* reconhece a importância de senhas memorizáveis e sugere o uso de frases-chave ou técnicas de memória para auxiliar na criação de senhas fortes (NIST, 2024).

Utilizar ferramentas de monitoramento de rede permite detectar atividades suspeitas, como tráfego não autorizado ou tentativas de acesso indevido (KARASEK, 2018). Utilizar *Virtual Private Network (VPN)* ao se conectar a redes *Wi-Fi* públicas adiciona uma camada extra de segurança à comunicação (TIMONERA; BASAN, 2024). Posicionar o ponto de acesso longe de paredes e em locais que minimizem a propagação do sinal para fora do estabelecimento (KARASEK, 2018). Isso ajuda a prevenir o acesso indevido à rede e à captura de informações por parte de terceiros (KARASEK, 2018). Ativar os mecanismos de segurança disponíveis no *AP* como *firewall* fornece proteção adicional contra *hackers* (TIMONERA; BASAN, 2024). Além dessas soluções, os usuários podem implementar outras contramedidas para proteger suas redes *Wi-Fi* contra ataques de desautenticação: ocultar o *SSID Wi-Fi*, dificultando a identificação e o direcionamento da rede por parte de atacantes (REEN et al., 2023). Desabilitar a administração remota do roteador via *Wi-Fi* para evitar acessos não autorizados (REEN et al., 2023).

Filtragem de endereços *MAC* pode ser utilizada para gerenciar o acesso em redes sem fio utilizando uma tabela de controle no ponto de acesso (LAWRENCE; VANI, 2011). Quando utilizada, o *AP* verifica se o endereço *MAC* do cliente que está tentando se conectar corresponde a um endereço autorizado previamente registrado na tabela do *AP* (LAWRENCE; VANI, 2011). Se houver correspondência, a solicitação de acesso é concedida; caso contrário, é rejeitada. Apesar de eficaz em redes domesticas, essa abordagem não é adequada para ambientes empresariais maiores, devido à dificuldade de adicionar os endereços *MAC* em todos os *APs* devido à mobilidade do sistema nesse contexto (LAWRENCE; VANI, 2011).

Outra forma de proteção é utilizar a técnica de Filtragem de Padrão de Tráfego (*FPT*). Esta técnica envolve o ponto de acesso interrompendo o processamento de quadros de solicitação de autenticação/associação ao receber um volume específico de quadros por segundo (LAWRENCE; VANI, 2011). A aplicação da filtragem de padrão de tráfego ocorre após a verificação do estado de autenticação do remetente do quadro de solicitação de associação recebido (LAWRENCE; VANI, 2011). Se o remetente estiver autenticado, a solicitação é processada; caso contrário, a FPT é ativada (LAWRENCE; VANI, 2011). Se o número de quadros de solicitação de autenticação ou associação recebidos por segundo exceder o número especificado, eles serão descartados; caso contrário, serão processados (LAWRENCE; VANI, 2011).

7 CONCLUSÃO

Este estudo analisou os principais tipos de ataques e contramedidas em redes sem fio *IEEE 802.11n*, abordando conceitos básicos de segurança. Os resultados demonstraram que o ataque de inundação de *SYN* causou uma significativa indisponibilidade do serviço do ponto de acesso, enquanto o ataque de desautenticação foi eficaz em desconectar dispositivos conectados ao *AP*. O ataque *AssRF* comprometeu consideravelmente os recursos do *AP*, resultando em negação de serviço, e o ataque *AuthRF* impactou a performance do *AP* devido ao alto consumo da *CPU*. A técnica de eavesdropping mostrou-se eficiente na captura de *handshakes*, e a quebra de senha foi eficaz em senhas fracas, evidenciando a necessidade de políticas de senhas robustas.

Com base nos resultados dos testes, conclui-se que os ataques abordados neste trabalho representam um sério problema de segurança para redes sem fio *IEEE 802.11n*. Esses ataques podem consumir os recursos dos dispositivos causando uma negação de serviços, interceptação de dados e quebra de senhas fracas, resultando em graves violações de segurança.

Apesar dos resultados, o estudo enfrentou limitações significativas, incluindo a impossibilidade de realizar os testes em redes corporativas e a falta de equipamentos com padrões de segurança mais recentes, como o *WPA3*. Recomenda-se que futuras pesquisas explorem esses padrões mais atuais e seguros em ambientes corporativos, além de realizar testes com ferramentas de *hardware* mais avançadas para um panorama mais completo.

REFERÊNCIAS

AIRCRACK-NG. **Aircrack-ng**. 2024. Disponível em: https://www.aircrack-ng.org/. Acesso em: 22 de fevereiro de 2024.

AL-SHEBAMI, T. A. A.; AL-SHAMIRI, A. Y. R. Wireless LAN security. In: **2021 IEEE 6th International Conference on Signal and Image Processing (ICSIP)**. [S.l.]: IEEE, 2021.

ALANDA, A.; HIDAYAT, R.; SATRIA, D.; MOODUTO, H. A.; PRAVAMA, D. Security analysis of wireless network using penetration test ing method. In: **2023 International Conference on Information Technology and Computing (ICITCOM)**. [S.l.]: IEEE, 2023.

ALLIANCE, W.-F. **Wi-fi alliance**. 2024. Disponível em: <https://www.wi-fi.org/>. Acesso em: 30 de janeiro de 2024.

ASSUNÇÃO, M. F. A. **Wireless Hacking - Ataque E Segurança De Redes Sem Fio Wi-Fi**. Minas gerais: Visual Books, 2013. 15–179 p. ISBN 9788575022825.

ATLURI, S.; RALLABANDI, R. Deciphering WEP, WPA, and WPA2 pre-shared keys using fluxion. In: **Smart Computing Techniques and Applications**. Singapore: Springer Singapore, 2021. p. 377–385.

AVAST. **What is port scanning and how does it work?** 2024. Disponível em: <https://www.avast.com/business/resources/what-is-port-scanning>. Acesso em: 7 de maio de 2024.

BACHA, D. **CCNP and CCIE enterprise core ENCOR 350-401 exam cram**. Upper Saddle River, NJ, USA: Pearson IT Certification, 2022.

BADHWAR, R. Man-in-the-middle attack prevention. In: **The CISO's Next Frontier**. Cham: Springer International Publishing, 2021. p. 223–229.

BARBOSA, A. **Você sabe qual é a diferença entre Wireless e Wi-Fi?** 2022. Disponível em: <https://brwifi.net/voce-sabe-qual-e-a-diferenca-entres-as-redes-wireless-e-wi-fi/>. Acesso em: 15 de maio de 2024.

CIAMPA, M. **CompTIA security+ guide to network security fundamentals**. 7. ed. Florence, AL, USA: Course Technology, 2020.

EDDY, W. M. Syn flood attack. In: ____. **Encyclopedia of Cryptography and Security**. Boston, MA: Springer US, 2011. p. 1273–1274. ISBN 978-1-4419-5906-5. Disponível em: <https://doi.org/10.1007/978-1-4419-5906-5_276>.

ELHIGAZI, A.; RAZAK, S.; HAMDAN, M.; ABDALLA, B.; ABAKER, I.; ELSAFI, A. Authentication flooding dos attack detection and prevention in 802.11. In: . [S.l.: s.n.], 2020. p. 325–329.

HALBOUNI, A.; ONG, L.-Y.; LEOW, M.-C. Wireless security protocols WPA3: A systematic literature review. **IEEE Access**, Institute of Electrical and Electronics Engineers (IEEE), v. 11, p. 112438–112450, 2023.

HASHCAT. **Hashcat - advanced password recovery**. 2024. Disponível em: <https://hashcat.net/hashcat>. Acesso em: 24 de fevereiro de 2024.

HCXTOOLS. **hcxtools: A small set of tools to convert packets from capture files to hash files for use with Hashcat or John the Ripper**. 2024. Disponível em: https://github.com/ZerBea/hcxtools. Acesso em: 22 de fevereiro de 2024.

IBM. **What Is a Data Breach?** 2024. <https://www.ibm.com/topics/data-breach>. Acesso em: 20 de junho de 2024.

IEEE. **IEEE Standard for Information Technology: Telecommunications and Information Exchange Between Systems : Local and Metropolitan Area Network– Specific Requirements. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Enhancements for very high throughput for operation in bands below 6 GHz**. [S.l.: s.n.], 2013.

INVOTEC. **Fluxion Hacking: 4 Things You Need To Know To Protect Yourself**. 2021. Disponível em: <https://www.invotec.com.au/what-should-i-know-about-fluxion-hacking-and-protection/>. Acesso em: 15 de junho de 2024.

JOSHI, D.; DWIVEDI, V. V.; PATTANI, K. De-authentication attack on wireless network 802.11i using kali linux. **International Research Journal of Engineering and Technology (IRJET)**, v. 4, p. 1666–1669, 2017.

KALI. **Hping3**. 2024. Disponível em: <https://www.kali.org/tools/hping3/>. Acesso em: 22 de fevereiro de 2024.

KALI. **Kali Linux**. 2024. Disponível em: <https://www.kali.org/>. Acesso em: 22 de fevereiro de 2024.

KARASEK, J. **Security 101: Protecting Wi-Fi Networks Against Hacking and Eavesdropping - Wiadomości bezpieczeństwa - Trend Micro PL**. 2018. Accessed: 2024-06-23. Disponível em: <https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/security-101-protecting-wi-fi-networks-against-hacking-and-eavesdropping>.

KOROLKOV, R. Y.; KUTSAK, S. V. Analysis of attacks in IEEE 802.11 networks at different levels of OSI model. **Nauk. Visnyk Natsionalnoho Hirnychoho Universytetu**, n. 2, p. 163–169, 2021.

KSHIRSAGAR, D.; KUMAR, S. An ontology approach for proactive detection of HTTP flood DoS attack. **Int. J. Syst. Assur. Eng. Manag.**, v. 14, n. S3, p. 840–847, 2023.

KÜLTEKIN, Ö. **dos-tester-802.11: It's a Python tool that tests some DoS attacks on 802.11 networks with flooding desired packets. Developed with Scapy**. 2023. Disponível em: <https://github.com/oz9un/dos-tester-802.11>. Acesso em: 22 de fevereiro de 2024.

LAWRENCE, D. L. A.; VANI, B. A comparative study of the available solutions to minimize denial of service attacks in wireless lan. **International Journal of Computer Technology and Applications**, v. 2, 11 2011.

LIU, Y. Security in wireless networks: Analysis of WI-fi security and attack cases study. In: **2022 International Conference on Artificial Intelligence in Everything (AIE)**. [S.l.]: IEEE, 2022.

LOUNIS, K.; DING, S.; ZULKERNINE, M. Cut it: Deauthentication attacks on protected management frames in wpa2 and wpa3. In: ____. [S.l.: s.n.], 2022. p. 235–252. ISBN 978-3-031-08146-0.

MEYERS, M.; WEISSMAN, J. S. **Mike Meyers' CompTIA Network+ certification passport, seventh edition (exam N10-008)**. [S.l.]: McGraw Hill Professional, 2022.

MICROSOFT. **visão geral Windows 11 para administradores - What's new in Windows**. 2024. Disponível em: <https://learn.microsoft.com/pt-br/windows/whats-new/windows-11-overview>. Acesso em: 22 de fevereiro de 2024.

MUGHAL, A. A. Well-architected wireless network security. **Journal of Humanities and Applied Science Research**, v. 5, n. 1, p. 32–42, dez. 2022. Disponível em: <https://journals.sagescience.org/index.php/JHASR/article/view/52>.

NIST. **NIST Special Publication 800-63-3**. 2024. Acesso em: 30 de janeiro de 2024. Disponível em: <https://pages.nist.gov/800-63-3/sp800-63-3.html>.

NMAP. **Nmap: The network mapper - Free Security Scanner**. 2024. Disponível em: <https://nmap.org/>. Acesso em: 22 de fevereiro de 2024.

OLALIA JR, R. L.; SISON, A. M.; MEDINA, R. P. Security assessment of brute-force attack to subset sum-based verifiable secret sharing scheme. In: **Proceedings of the 4th International Conference on Industrial and Business Engineering**. New York, NY, USA: ACM, 2018. Disponível em: <https://doi.org/10.1145/3288155.3288190>.

PAESSLER. **PRTG Network Monitor – All-in-one network monitoring tool**. 2024. Disponível em: <https://www.paessler.com/prtg/prtg-network-monitor>. Acesso em: 22 de fevereiro de 2024.

PYTHON. **Python**. [S.l.]: Python.org, 2019. Disponível em: <https://www.python.org/>. Acesso em: 10 de junho de 2024.

REEN, R. S.; DHARMANI, G.; GOTHWAL, R.; ABDALLAH, E. G. Evaluation of wireless deauthentication attacks and countermeasures on autonomous vehicles. In: **2023 10th International Conference on Dependable Systems and Their Applications (DSA)**. [S.l.]: IEEE, 2023.

RUTH, C. **The evolution of WI-Fi technology and standards**. [S.l.]: IEEE SA, 2023. Disponível em: <https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/>. Acesso em: 22 de fevereiro de 2024.

SCAPY. **Scapy**. 2022. Disponível em: <https://scapy.net/>. Acesso em: 10 de junho de 2024.

TANENBAUM, A.; FEAMSTER, N.; WETHERALL, D. **Computer Networks, Global Edition**. 6. ed. Londres, England: Pearson Education, 2021.

THAKUR, H. N.; HAYAJNEH, A. A.; THAKUR, K.; KAMRUZZAMAN, A.; ALI, M. L. A comprehensive review of wireless security protocols and encryption applications. In: **2023 IEEE World AI IoT Congress (AIIoT)**. [S.l.]: IEEE, 2023.

TIMONERA, K.; BASAN, M. **The Best Security for Wireless Networks**. 2024. Accessed: 2024-05-23. Disponível em: <https://www.esecurityplanet.com/trends/the-best-security-for-wireless-networks/>.

TORGUNAKOV, V.; LOGINOV, V.; KHOROV, E. A study of channel bonding in IEEE 802.11bd networks. **IEEE Access**, v. 10, p. 25514–25533, 2022.

TP-LINK. **Software Controlador Omada**. 2024. Disponível em: <https://www.tp-link.com/br/business-networking/omada-sdn-controller/omada-software-controller/>. Acesso em: 22 de fevereiro de 2024.

UIC.EDU. **Password Meter - A visual assessment of password strengths and weaknesses**. 2024. Disponível em: https://www.uic.edu/apps/strong-password. Acesso em: 30 de janeiro de 2024.

WIRESHARK. **Wireshark · about**. 2024. Disponível em: https://www.wireshark.org/about.html. Acesso em: 22 de fevereiro de 2024.

YASSINE, M.; SHOJAFAR, M.; HAQIQ, A.; DARWISH, A. **Cybersecurity and Privacy in Cyber Physical Systems**. [S.l.: s.n.], 2019. ISBN 9781138346673.