Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande
Coordenação do Curso Superior de Tecnologia em Telemática

Avaliação de vulnerabilidades em Redes Wi-Fi do IFPB Através da Simulação de Ataques com Microcontroladores de ESP32 e ESP8266

Adrian Bruno Soares Borges

Orientador: Dr. Alexandre Sales Vasconcelos

Campina Grande - PB
2025

Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande
Coordenação do Curso Superior de Tecnologia em Telemática

Avaliação de vulnerabilidades em Redes Wi-Fi do IFPB Através da Simulação de Ataques com Microcontroladores de ESP32 e ESP8266

Adrian Bruno Soares Borges

Monografia apresentada à Coordenação do Curso de Telemática do IFPB - Campus Campina Grande, como requisito parcial para conclusão do curso de Tecnologia em Telemática.

Orientador: Dr. Alexandre Sales Vasconcelos
Campina Grande, 2025

Catalogação na fonte:
Ficha catalográfica

B732a Borges, Adrian Bruno Soares..
Avaliação de vulnerabilidades em Redes Wi-Fi do IFPB Através da Simulação de Ataques com Microcontroladores de ESP32 e ESP8266 / Adrian Bruno Soares Borges. - Campina Grande, 2025.
55f.: il.

Trabalho de Conclusão de Curso (Graduação em Tecnologia em Telemática) - Instituto Federal da Paraíba, 2025.
Orientador: Prof. Dr. Alexandre Sales Vasconcelos.
Coorientador: Átila de Souza Medeiros.

1. Telemática - Segurança de Redes. 2.Wi-Fi. 3. ESP32. 4. ESP8266. 5. Teste de Invasão. I. Vasconcelos, Alexandre Sales (orient.). II Título.

CDU 004.056

Avaliação de vulnerabilidades em Redes Wi-Fi do IFPB Através da Simulação de Ataques com Microcontroladores de ESP32 e ESP8266

Adrian Bruno Soares Borges

Monografia aprovada como requisito parcial para a obtenção do grau de Tecnólogo em Telemática, pelo Instituto Federal da Paraíba, Campus Campina Grande, pela seguinte banca examinadora:

Dr. Alexandre Sales Vasconcelos
Orientador

Átila de Souza Medeiros
Coorientador

Dr. Moacy Pereira da Silva
Membro da banca

Dr. Marcelo Portela Sousa
Membro da banca

Campina Grande Dezembro 2025

Dedico este trabalho a todos aqueles que me incentivaram, ajudaram e tornaram possível a minha trajetória até aqui.

"O homem é algo que deve ser superado. O que fizestes para superá-lo"
Friedrich Nietzsche

Agradecimentos

Expresso minha profunda gratidão à minha família, por todo o suporte e incentivo que me forneceram ao longo deste percurso acadêmico. Aos meus amigos, agradeço pela compreensão, pelo companheirismo e por serem uma fonte constante de motivação.

Aos meus professores, em especial ao meu orientador, Professor Alexandre Sales Vasconcelos, pela orientação paciente, conhecimento compartilhado e por acreditar no potencial deste projeto. Ao meu coorientador, Átila de Souza Medeiros, por suas valiosas contribuições e apoio fundamental. A todos os docentes do curso de Telemática do IFPB, minha gratidão pelos ensinamentos que foram a base da minha formação.

Resumo

A crescente dependência de redes sem fio no ambiente acadêmico, como no Instituto Federal da Paraíba (IFPB), as torna um recurso pedagógico indispensável e, ao mesmo tempo, um alvo para atividades maliciosas. Este trabalho analisou o nível de segurança da rede Wi-Fi do IFPB, demonstrando na prática as vulnerabilidades existentes através do uso de microcontroladores. A problemática central residiu na drástica redução da barreira de entrada para a execução de ciberataques, possibilitada por dispositivos acessíveis como o ESP32 e o ESP8266.

A metodologia consistiu na simulação de ataques controlados e autorizados pela instituição, utilizando um ESP32 com firmware Marauder e um ESP8266 com código customizado para a implementação do ataque de Ponto de Acesso Falso. Foram executados testes práticos de negação de serviço (Deauthentication), captura passiva de dados (Captura de Handshake), poluição de espectro (Beacon Spam) e engenharia social (Ponto de Acesso Falso com Captive Portal). O estudo não visou apenas a identificação de falhas técnicas, mas buscou, principalmente, servir como um instrumento de conscientização, ilustrando como dispositivos baratos podem comprometer a segurança da rede e a privacidade dos usuários.

Como resultado, gerou-se um diagnóstico de segurança que evidenciou a robustez da infraestrutura contra ataques de negação de serviço, ao mesmo tempo em que expôs a eficácia da captura de credenciais via engenharia social. A conclusão fundamental do estudo é que a segurança da informação é um sistema sociotécnico onde o fator humano permanece como o elo mais fraco, mesmo em ambientes com infraestrutura técnica protegida. O trabalho valida a tese de que a barreira de entrada para ciberataques foi drasticamente reduzida, pois dispositivos de amplo acesso tecnológico (como o ESP8266) são capazes de comprometer severamente a segurança institucional através da engenharia social. Portanto, embora a instituição esteja preparada contra ataques de protocolo, a defesa mais urgente reside na conscientização dos usuários para identificar ameaças como páginas falsas e redes suspeitas.

Palavras-chave: Segurança de Redes, Wi-Fi, ESP32, ESP8266, Teste de Invasão, Conscientização.

Abstract

The growing reliance on wireless networks in the academic environment, such as at the Federal Institute of Paraíba (IFPB), makes them an indispensable pedagogical resource and, at the same time, a target for malicious activities. This work analyzed the security level of IFPB's Wi-Fi network, practically demonstrating existing vulnerabilities through the use of low-cost microcontrollers. The central issue lay in the drastic reduction of the entry barrier for executing cyberattacks, enabled by affordable devices such as the ESP32 and ESP8266.

The methodology consisted of simulating controlled attacks authorized by the institution, using an ESP32 with Marauder firmware and an ESP8266 with custom code to implement the Rogue Access Point attack. Practical tests included denial-of-service (Deauthentication), passive data capture (Handshake Capture), spectrum pollution (Beacon Spam), and social engineering (Rogue Access Point with Captive Portal). The study aimed not only to identify technical flaws but primarily sought to serve as an awareness tool, illustrating how inexpensive devices can compromise network security and user privacy.

As a result, a security assessment was generated that evidenced the infrastructure's robustness against denial-of-service attacks, while simultaneously exposing the effectiveness of credential capture via social engineering. The fundamental conclusion of the study is that information security is a sociotechnical system where the human factor remains the weakest link, even in environments with protected technical infrastructure. The work validates the thesis that the entry barrier for cyberattacks has been drastically reduced, as devices of negligible cost (such as the ESP8266) are capable of severely compromising institutional security through social engineering. Therefore, although the institution is prepared against protocol attacks, the most urgent defense lies in user awareness to identify threats such as fake pages and suspicious networks.

Keywords: Network Security, Wi-Fi, ESP32, ESP8266, Penetration Testing, Awareness.

Sumário

Lista de Abreviaturas

AP	*Ponto de acesso (Wireless Fidelity)*
BYOD	*Bring Your Own Device*
DNS	*Domain Name System (Converte nomes de domínio*
DoS	*Denial of Service*
EAPOL	*Extensible Authentication Protocol over LAN*
EDFs	*Effective Data Frames*
HTML	*HyperText Markup Language*
HTTP	*Hypertext Transfer Protocol (Protocolo de Transferência de Hipertexto)*
HTTPs	*Hypertext Transfer Protocol Secure*
IDE	*Integrated Development Environment (Ambiente de Desenvolvimento Integrado)*
IEEE	*Institute of Electrical and Electronics Engineers*
IFPB	Instituto Federal da Paraíba
IDS	*Intrusion Detection System*
IOT	*Internet of Things (Internet das Coisas)*
LCD	*Liquid Crystal Display*
MAC	*Media Access Contro*
MFP	*Management Frame Protection*
MIC	*Message Integrity Code*
MITM	*Man-in-the-Middle*
PCF	*Point Coordination Function*
PSK	*Pre-Shared Key (Chave Pré-Compartilhada)*
PTK	*Pairwise Transient Key*
RSN IE	*Robust Security Network Information Element*
SD	*Secure Digital*
SPI	*Serial Peripheral Interface (interface de comunicação serial síncrona)*
SSID	*Service Set Identifier*
TFT	*Thin-Film Transistor*
VPN	*Virtual Private Network*
Wi-Fi	*Wireless Fidelity*
WIDS	*Wireless Intrusion Detection System*
WPA2	*Wi-Fi Protected Access 2*
WPA3	*Wi-Fi Protected Access 3*

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

A sociedade atual está estruturada sobre o pilar da conectividade sem fio. No domínio da educação, as redes *Wi-Fi* firmaram-se como um componente infraestrutural essencial para as atividades de ensino e pesquisa. No Instituto Federal da Paraíba (IFPB), o acesso sem fio viabiliza a utilização de ambientes virtuais de aprendizagem, bibliotecas digitais e plataformas colaborativas, sendo um recurso indispensável para a comunidade acadêmica.

Entretanto, essa ubiquidade traz consigo desafios críticos de segurança. A elevada densidade de usuários, aliada à política *BYOD (Bring Your Own Device)*, amplia significativamente a superfície de ataque. Nesse contexto, a característica muitas vezes aberta ou compartilhada do *Wi-Fi* o torna suscetível a práticas maliciosas, que podem comprometer tanto a integridade da instituição quanto a privacidade dos dados dos usuários.

Para compreender as vulnerabilidades exploradas neste trabalho, é essencial revisitar os fundamentos do padrão *IEEE 802.11*, que rege as comunicações sem fio. Garantir a segurança destas redes permanece um desafio contínuo, visto que protocolos estabelecidos, como o *WPA2*, possuem limitações conhecidas.

Tais limitações, em determinados cenários, podem ser exploradas por atacantes com relativa facilidade. Ameaças como a negação de serviço por pacotes de *Deauthentication* e a interceptação de dados via pontos de acesso falsos *(Evil Twin)* são exemplos práticos da exploração de falhas inerentes ao projeto do protocolo [Kurose 2017].

1.1 Trabalhos Correlatos

A análise de segurança em redes *Wi-Fi* é um tema vasto, com a literatura podendo ser dividida em duas vertentes principais: a análise conceitual dos riscos institucionais e a exploração técnica de ferramentas e vulnerabilidades.

Em uma vertente mais técnica, trabalhos como o de Higor Diego [Diego 2023] demonstram a capacidade e a simplicidade de se utilizar microcontroladores como o *ESP32* para realizar varreduras em redes *Wi-Fi*.

Em contrapartida, artigos de caráter informativo, como o publicado pela AllEasy [All

Easy 2024], abordam o problema sob a ótica institucional. Eles destacam que ambientes de ensino são particularmente vulneráveis devido ao grande volume de dispositivos pessoais e à necessidade de equilibrar acesso aberto com segurança. A conclusão recorrente desses trabalhos é a necessidade de implementação de políticas de segurança robustas e, fundamentalmente, de campanhas de conscientização para os usuários, que representam a primeira linha de defesa.

Outros trabalhos focam em vulnerabilidades que este estudo também aborda:

- **Ataques de Ponto de Acesso Falso: QianLU et al. [QianLU *et al.* 2018]** detalham o funcionamento e os métodos de detecção de ataques *Evil Twin*, que interceptam o tráfego da vítima, embora muitas vezes utilizando *laptops* como plataforma de ataque.
- **Ataques de Negação de Serviço no Protocolo: Alabdulatif [Alabdulatif 2014]** e **Rango et al. [Rango Dionigi Cristian Lentini 2006]** analisaram falhas de projeto no *4-way handshake do WPA2* que permitem ataques de Negação de Serviço.
- **Poluição de Espectro: Zurutuza Roberto Uribeetxeberria [Zurutuza Roberto Uribeetxeberria 2008]** investiga a falsificação de Beacon Frames (base do ataque *Beacon Spam*) e propõe métodos para sua detecção.

Para uma melhor visualização das diferenças metodológicas e de escopo, a Tabela 1.1 apresenta um resumo comparativo dos trabalhos mencionados, detalhando as vulnerabilidades focadas e o *hardware* utilizado por cada autor em contraste com a abordagem proposta nesta pesquisa.

Tabela 1.1: *Tabela de Resumo dos Trabalhos Correlatos*

Autor(es)	**Vulnerabilidade / Ataque**	**Hardware / Metodologia**
AllEasy	Riscos institucionais (BYOD)	Análise conceitual
Higor Diego	Varredura de redes Wi-Fi	Microcontrolador ESP32
Kristiyanto	Ataque de Desautenticação (DoS)	Microcontrolador ESP8266
Alabdulatif	Negação de Serviço (DoS) no 4-way handshake	Análise de protocolo
Rango et al.	Negação de Serviço (DoS Flooding) no 4-way handshake	Análise de protocolo
Zurutuza R. U.	Falsificação de *Beacon Frames* (Beacon Spam) e detecção	Análise de protocolo e método de detecção
QianLU et al.	Ataque *Evil Twin* (Ponto de Acesso Falso) e detecção	Laptop com duas interfaces de rede sem fio

Nesse contexto, o presente trabalho se diferencia por unificar essas vertentes. Ele não apenas revisa, mas demonstra praticamente um conjunto abrangente de ataques *(Deauthen-*

tication, Captura de Handshake, Beacon Spam e Ponto de Acesso Falso) utilizando *exclusivamente* microcontroladores *(ESP32 e ESP8266)* como ferramentas de auditoria em um estudo de caso real e autorizado no IFPB Campus Campina Grande.

1.2 Justificativa e Relevância do Trabalho

A relevância desta pesquisa se evidencia diante de uma mudança preocupante no cenário de *cibersegurança*: a redução significativa das barreiras de entrada para a realização de ataques. Tecnologias que, anteriormente, exigiam conhecimento especializado e equipamentos de alto custo tornaram-se atualmente acessíveis por meio de dispositivos simples e de baixo valor, como os microcontroladores *ESP32* e seu predecessor, o *ESP8266*. Adquiríveis por valores que tipicamente não ultrapassam cinquenta reais a unidade, esses hardware, quando combinados com *firmware* de código aberto, como o *Marauder*, ou com códigos customizados, permitem a execução de ataques sofisticados com relativa facilidade. Tal contexto evidencia um risco concreto e frequentemente subestimado em ambientes educacionais, nos quais a percepção de segurança nem sempre acompanha a evolução das ameaças.

Dessa forma, este estudo justifica-se não apenas pela necessidade de mapear vulnerabilidades técnicas, mas também pelo seu papel como instrumento prático de conscientização. Ao demonstrar de que forma a segurança institucional pode ser comprometida, o trabalho fornece um diagnóstico tangível e fundamentado. O objetivo é converter a percepção teórica do risco em uma compreensão prática das ameaças, elemento essencial para o fortalecimento das políticas de defesa cibernética e da cultura de segurança no IFPB.

1.3 Objetivos

1.3.1 Objetivo Geral

Detectar e analisar possíveis vulnerabilidades na segurança da rede *Wi-Fi* no ambiente acadêmico do IFPB por meio da simulação de ataques utilizando microcontroladores, com o objetivo de evidenciar vulnerabilidades conhecidas do protocolo *IEEE 802.11*, incluindo a suscetibilidade a ataques de negação de serviço, interceptação de credenciais e técnicas de engenharia social. A partir desse diagnóstico prático, pretende-se propor medidas de mitigação que visem fortalecer a infraestrutura de rede e aprimorar a conscientização dos usuários.

1.3.2 Objetivos Específicos

A seguir apresentam-se os objetivos específicos que orientam a execução do trabalho.

- Revisar e fundamentar teoricamente os conceitos de segurança em redes sem fio, incluindo os tipos de ataques aplicáveis ao protocolo *IEEE 802.11*.

- Preparar o ambiente experimental, configurando e programando microcontroladores *ESP32 e ESP8266* para a simulação controlada de ataques.
- Demonstrar, de forma prática e controlada, a execução dos ataques de *Deauthentication, Captura de Handshake, Beacon Spam e Ponto de Acesso Falso com Captive Portal*.
- Analisar e documentar o impacto dos ataques na rede do campus.
- Propor recomendações de segurança e boas práticas para mitigação das vulnerabilidades identificadas, com o objetivo de fortalecer a infraestrutura e promover a conscientização dos usuários.

1.4 Metodologia

Neste capítulo, é exposto o delineamento prático da pesquisa, abrangendo a organização dos experimentos, a caracterização do ambiente de testes, os procedimentos experimentais empregados e os critérios definidos para a coleta, tratamento e análise dos dados.

1.5 Estrutura e Ambiente dos Experimentos

Os testes de segurança foram conduzidos dentro das instalações do **Instituto Federal da Paraíba (IFPB) - Campus Campina, PB**.

Para garantir a integridade da rede e minimizar qualquer impacto sobre os usuários, os experimentos foram agendados com a equipe de Tecnologia da Informação (TI) da instituição. A estrutura do experimento consistiu em um ambiente controlado, utilizando os seguintes componentes:

- **Dispositivo de Ataque:** Um microcontrolador *ESP32* com o *firmware Marauder* instalado e *ESP8266* com código customizado, atuando como as ferramentas de auditoria.
- **Dispositivo-Alvo:** Um *smartphone pessoal Samsung Galaxy M31*, de propriedade do pesquisador, para atuar como vítima controlada do ataque.
- **Dispositivo de Monitoramento:** Dispositivo celular para análise em tempo real

1.6 Autorização Institucional

A execução de qualquer teste que possa afetar a infraestrutura de rede de uma instituição exige consentimento formal. Todos os procedimentos realizados neste trabalho foram previamente comunicados e autorizados pela **Coordenação e Tecnologia da Informação**

- Campus Campina Grande, PB. A solicitação detalhava os objetivos da pesquisa e a natureza não destrutiva dos testes. A autorização formal foi concedida via e-mail, conforme apresentado na Figura documentado no Apêndice **A**

1.7 Procedimentos de Execução dos Testes

Para cada vulnerabilidade explorada, foi definido um procedimento de teste específico, conforme detalhado a seguir.

1.7.1 Ataque de Deauthentication

1. O dispositivo-alvo conectado à rede *Wi-Fi* do IFPB.
2. Utilizando o dispositivo com o *Marauder*, foi realizada uma varredura para identificar o endereço *MAC* do dispositivo-alvo e do ponto de acesso.
3. O ataque de *Deauthentication* foi iniciado, enviando pacotes forjados direcionados ao dispositivo-alvo.
4. O comportamento do dispositivo-alvo será observado para confirmar a perda de conexão com a rede.

1.7.2 Captura de Handshake

1. O dispositivo com o *Marauder* foi configurado para o modo de captura de *handshake* em um canal específico da rede *Wi-Fi*.
2. O *Marauder* foi utilizado para capturar os quatro pacotes do *4-way handshake* durante o processo de conexão.
3. O arquivo de captura contendo o *handshake* foi salvo em um cartão *SD* para análise posterior.

1.7.3 Beacon Spam

1. A lista de redes *Wi-Fi* visíveis foi verificada em um dispositivo-alvo para registrar o estado normal do ambiente.
2. O ataque de *Beacon Spam* foi iniciado no dispositivo Marauder, configurado para gerar uma grande quantidade de *SSIDs* falsos.
3. A lista de redes no dispositivo-alvo foi novamente verificada para observar a poluição do espectro com as redes "fantasmas".

1.7.4 Ponto de Acesso Falso (Evil Twin) com Captive Portal

1. O *SSID* da rede *Wi-Fi* oficial do IFPB foi identificado. O código foi programado para transmitir exatamente o mesmo nome de rede (SSID) da infraestrutura oficial ("IFPB-ALUNO"ou "IFPB-VISITA"), induzindo os dispositivos a se conectarem automaticamente ou confundindo os usuários.

2. Um microcontrolador *ESP8266* foi programado com o código-fonte desenvolvido para criar um ponto de acesso falso com o mesmo *SSID* da rede legítima. [(Github) 2025] Diferente de ferramentas prontas, optou-se por desenvolver um firmware em C/C++ (Arduino IDE). Isso permitiu a criação de páginas de phishing altamente específicas que imitavam visualmente a tela de autenticação real do IFPB, aumentando a credibilidade do ataque

3. O desenvolvimento incluiu um servidor DNS malicioso que intercepta todas as requisições de domínio e força o redirecionamento da vítima para o servidor web do atacante (Captive Portal), garantindo que a página falsa fosse exibida independentemente do site que o usuário tentasse acessar

4. Um ponto crucial do design foi configurar o módulo apenas para hospedar o portal de phishing e capturar os dados via método POST (exibindo-os no monitor serial), sem a necessidade de processar ou reencaminhar o tráfego de internet real da vítima, o que simplificou a implementação e focou na engenharia social.

5. As credenciais (`Matricula e senha`) inseridas pela vítima na página falsa foram capturadas pelo servidor web embarcado no *ESP8266* e exibidas no monitor serial do *ESP8266*. É importante notar que o módulo *ESP8266* foi configurado apenas para hospedar o portal cativo de phishing e capturar as credenciais inseridas, sem executar a intercepção ou o reencaminhamento do tráfego real da vítima para a internet..

1.8 Critérios de Avaliação e Coleta de Dados

Para medir se os objetivos de cada experimento foram alcançados, foram definidos critérios de sucesso claros e métodos de coleta de evidências.

- **Ataque de Deauthentication:** O objetivo é alcançado se o dispositivo-alvo for desconectado com sucesso da rede. A evidência será coletada através de **gravação de vídeo** da tela do dispositivo mostrando a perda de conexão.

- **Captura de Handshake:** O sucesso é medido pela obtenção de um arquivo de captura (‘.pcap‘) contendo um *handshake* válido. A evidência será a **análise do arquivo no Wireshark**, confirmando a presença dos pacotes *EAPOL (Extensible Authentication Protocol over LAN)* do handshake.

- **Beacon Spam:** O objetivo é alcançado se a lista de redes disponíveis nos dispositivos-alvo for visivelmente sobrecarregada. A evidência consistirá em **capturas de tela** do tipo "antes e depois".
- **Ponto de Acesso Falso:** O sucesso é demonstrado pela criação da rede falsa e pela captura de tentativas de conexão. A evidência será uma **captura de tela** mostrando a rede falsa na lista de redes.

Capítulo 2

Fundamentação Teórica

A execução de testes de segurança em redes sem fio pode ser realizada com uma variedade de ferramentas, que vão desde soluções de *software* robustas até *hardware* especializado. Tradicionalmente, auditores de segurança utilizam sistemas operacionais como o *Kali Linux*, que vem equipado com um vasto arsenal de *softwares* (como a *suíte Aircrack-ng e o Wireshark*), em conjunto com adaptadores de rede sem fio compatíveis com o modo monitor, como os fabricados pela *Alfa Network*. Existem também dispositivos de *hardware* dedicados, como o *WiFi Pineapple*, que oferecem uma interface simplificada para a execução de ataques complexos.

A escolha pelos microcontroladores **ESP32** e **ESP8266** não foi apenas uma decisão baseada na economia, mas sim uma escolha metodológica para provar a tese central deste trabalho: a barreira de entrada para a realização de ataques eficazes foi drasticamente reduzida. Esses dispositivos foram selecionados por três motivos principais:

- **Custo Irrisório:** Ambos os microcontroladores podem ser adquiridos por uma fração do preço de um adaptador de rede especializado, tornando-os acessíveis a um público vasto.
- **Portabilidade e Autonomia:** Por seu tamanho reduzido e baixo consumo de energia, podem ser facilmente transformados em dispositivos de auditoria portáteis, operando com pequenas baterias sem a necessidade de um *notebook*.
- **Versatilidade:** A capacidade de serem programados para tarefas específicas permite uma customização que não é facilmente alcançada com ferramentas comerciais, como demonstrado na implementação do Ponto de Acesso Falso.

2.1 Capacidades e Limitações dos Módulos ESP em Testes Wi-Fi

A viabilidade do uso dos microcontroladores *ESP32 e ESP8266* como plataformas de auditoria reside em sua capacidade de operar em modo monitor, essencial para a injeção e captura

de pacotes. Esta arquitetura torna-os ideais para demonstrar a acessibilidade da ameaça

Ataques e Vulnerabilidades Possíveis com o ESP

Os vetores de ataque demonstrados neste trabalho são possibilitados pela combinação do *hardware com o software* customizado ou de código aberto:

- Negação de Serviço (DoS): Realizado através da injeção de quadros de *Deauthentication* forjados (via Marauder ou código customizado), explorando uma falha fundamental do padrão *IEEE 802.11.*
- Captura de Handshake (Ataques Offline): A capacidade de operar em modo monitor permite a captura dos pacotes *EAPOL do 4-way handshake WPA2*, viabilizando ataques de força bruta *offline* contra a Chave Pré-Compartilhada *(PSK).*
- Engenharia Social/Phishing: A criação de um Ponto de Acesso Falso (Evil Twin) é executada de forma eficiente pelo ESP8266, que atua como *AP e servidor HTTP* embarcado, redirecionando o tráfego para um *Portal Cativo* falso e capturando credencias simuladas sem interceptar trafego real *(phishing).*
- Poluição de Espectro: O *Beacon Spam* inunda o ambiente com *SSIDs* falsos, aproveitando a falta de autenticação dos *Beacon Frames* para causar confusão e servir de "cortina de fumaça".

Limitações do Hardware e do Firmware Marauder

Embora eficazes, as plataformas baseadas em *ESP* não substituem ferramentas profissionais em todos os aspectos, apresentando limitações inerentes ao seu *design*:

- Poder de Processamento: O *hardware ESP* possui recursos limitados em comparação com um computador *(e.g., um laptop rodando Kali Linux).* Isso impacta a velocidade de processamento de força bruta para a quebra de senha, tarefa que deve ser realizada *offline* em um dispositivo mais potente.
- Análise *On-the-fly:* O firmware *Marauder* é otimizado para a execução de ataques e captura de dados brutos *(e.g., arquivos .pcap).* Análises complexas, inspeção profunda de pacotes *(Deep Packet Inspection) e post-processing* exigem a transferência dos dados para ferramentas mais robustas, como o *Wireshark* ou a *suíte Aircrack-ng.*

Diferencial Competitivo em Relação a Outros Equipamentos

O diferencial metodológico e prático dos módulos *ESP* em relação a outras ferramentas de auditoria como **Adaptadores Wi-Fi** de alta potência (compatíveis com modo monitor em distribuições como *Kali Linux*), **Raspberry Pi**, **WiFi Pineapple** ou o **Flipper Zero** é claramente o **custo** e a **portabilidade**.

- **Custo/Acessibilidade:** Os ESPs reduzem o custo de entrada para a fração de preço de um adaptador de rede especializado ou de um *pentesting device* profissional.
- **Portabilidade e Furtividade:** Seu tamanho diminuto e baixo consumo de energia permitem que sejam transformados em dispositivos de auditoria portáteis e discretos, operando com bateria, sem a necessidade de um *laptop*.
- **Versatilidade de Propósito Único:** Podem ser programados para tarefas altamente específicas, como a manipulação de *DNS para o Evil Twin*, otimizando recursos para um vetor de ataque isolado.

Diferenças de Ataque em Redes Wi-Fi: Apesar das funcionalidades similares de ataque *(Deauthentication, Beacon Spam)* entre essas plataformas, a distinção reside na **escala** e **complexidade** da operação:

- **Adaptadores Wi-Fi de Alta Potência (ex: Alfa Network):** Utilizados em conjunto com um *laptop (Kali Linux)*, oferecem maior poder de **injeção de pacotes** e **alcance** devido às antenas de alto ganho. Embora o *ESP32* possa atingir altas taxas de injeção (3.750 pacotes no teste de *Deauth*), o adaptador externo oferece vantagem em testes de longa distância ou em ambientes com alto ruído de radiofrequência, enquanto o *ESP* se destaca na **discreção** e **montagem autônoma**.
- **Raspberry Pi:** Possui um poder de processamento significativamente **maior** que o *ESP* e capacidade de executar sistemas operacionais completos e complexos. Isso o torna superior para **análises em tempo real**, **quebra de senha *on-the-fly*** (embora lento) e para hospedar *back-ends de phishing* mais robustos, mas perde para o *ESP* em **custo**, **tamanho** e **baixo consumo de energia**.
- **WiFi Pineapple:** É um *framework* dedicado e otimizado para ataques do tipo **Man-in-the-Middle (MITM)** e *Rogue AP*. Sua interface e automação são superiores, permitindo a criação de *Evil Twins* mais sofisticados e a interceptação e manipulação de tráfego com maior facilidade. O *ESP* é mais rudimentar e exige código customizado para o *MITM* completo, mas o *Pineapple* possui um custo de aquisição muito superior.
- **Flipper Zero:** Embora tenha capacidades de injeção de pacotes *Wi-Fi* via módulos externos (como o DevBoard ESP32 S2/S3), seu propósito original é mais amplo (*sub-GHz*, RFID, NFC). Na prática, o *Flipper* com *DevBoard* oferece uma experiência mais amigável, mas o *ESP32 (DevKit V4)* é mais direto, **mais barato** e, neste contexto, **mais fácil de customizar** para tarefas específicas de *pentesting Wi-Fi.*

Apesar de suas limitações, a capacidade do *ESP32* de realizar ataques de alto impacto, como a captura de credenciais (*Evil Twin*), o risco reside não na sofisticação do equipamento de ataque, mas na exploração do fator humano e das vulnerabilidades inerentes ao *protocolo 802.11.*

2.2 Ferramentas de Análise

A escolha das ferramentas é um fator determinante para a execução de testes de segurança. Para esta pesquisa, a metodologia se baseia na utilização de uma combinação de *hardware* com um *firmware* de código aberto. Especificamente, foi escolhido o microcontrolador *ESP32*, notável pela integração nativa de conectividade *Wi-Fi e Bluetooth*. Este *hardware* é transformado em uma ferramenta de auditoria de segurança através do firmware especializado *ESP32 Marauder*. Essa abordagem demonstra a crescente acessibilidade de recursos para testes de invasão, que antes eram restritos a especialistas com equipamentos caros.

2.2.1 O Microcontrolador ESP32

O *ESP32* é um microcontrolador da *Espressif Systems* que se destaca pela sua arquitetura *dual-core* e, principalmente, pela integração nativa de conectividade *Wi-Fi e Bluetooth* [Espressif Systems 2023]. Sua capacidade de operar em modo monitor essencial para a captura de pacotes de rede sem estar associado a um ponto de acesso o torna uma ferramenta potente para auditoria de segurança. Neste trabalho, o *ESP32* foi escolhido para ser combinado com o *firmware Marauder*. A razão para essa escolha é a eficiência: enquanto seria possível programar cada ataque individualmente, o *Marauder* oferece uma suíte de ferramentas ofensivas já compiladas e otimizadas, controladas por uma interface simples. Isso permite focar na demonstração rápida e eficaz de múltiplos vetores de ataque *(Deauthentication, Beacon Spam e Captura de Handshake)* a partir de um único dispositivo.

2.2.2 O Microcontrolador ESP8266

Predecessor do *ESP32, o ESP8266* é um microcontrolador de núcleo único, também com Wi-Fi integrado, que se popularizou por seu custo ainda mais baixo e simplicidade. Embora não possua os mesmos recursos de processamento do seu sucessor, ele é extremamente eficiente em atuar como um ponto de acesso *(Access Point).*

Embora o ESP8266 suporte monitor mode, seu uso é mais limitado e geralmente focado em funções mais simples como Deauther (como citado em trabalhos correlatos), enquanto o ESP32 é a plataforma mais robusta para a suíte Marauder. A escolha para o Evil Twin se deu por sua eficiência como AP/servidor.

Para o ataque de Ponto de Acesso Falso (*Evil Twin*) com portal cativo, o *ESP8266 foi* a escolha ideal. Sua vasta documentação e a grande quantidade de bibliotecas disponíveis na comunidade de desenvolvedores facilitam enormemente a criação de servidores web embarcados e a manipulação de requisições *DNS (Domain Name System)* para redirecionar o tráfego da vítima para uma página de phishing. Utilizar o *ESP8266* para esta tarefa específica demonstra o princípio de usar a ferramenta certa para o trabalho, otimizando recursos e aproveitando os pontos fortes de cada plataforma.

2.2.3 O Firmware Marauder

O *ESP32* Marauder é um firmware especializado que transforma o microcontrolador *ESP32* em uma ferramenta portátil para testes de invasão (*penetration testing*) em redes *Wi-Fi e Bluetooth*. Inspirado em projetos como o *ESP8266 Deauther*, o *Marauder* oferece uma suíte de funcionalidades ofensivas e defensivas, controladas por uma interface simples. Para este trabalho, as funcionalidades essenciais do *Marauder* incluem a varredura de redes, a escuta de tráfego para captura de pacotes específicos e a execução dos ataques detalhados a seguir, tudo isso a partir de um dispositivo compacto e de baixo consumo energético

Apesar de sua crescente popularidade em comunidades de segurança (*hacker spaces*, conferências e fóruns *online*), no momento da elaboração deste trabalho, não foram encontradas publicações em periódicos acadêmicos revisados por pares que utilizassem especificamente o *firmware ESP32 Marauder* como ferramenta principal de análise. Isso pode ser atribuído ao ciclo de publicação acadêmica, que tende a ser mais lento que o ritmo de desenvolvimento de ferramentas na comunidade de código aberto. No entanto, sua eficácia e funcionalidade são amplamente documentadas em repositórios de projetos e tutoriais técnicos, validando sua escolha como uma ferramenta representativa e de ponta para os fins práticos desta pesquisa. [justcallmekoko (Github) 2024].

2.3 Vetores de Ataque em Redes IEEE 802.11

Os ataques simulados nesta pesquisa exploram vulnerabilidades conhecidas no padrão *IEEE 802.11* e em sua implementação de segurança mais comum, o *WPA2 (Wi-Fi Protected Access II)*. As ameaças selecionadas são exemplos práticos de como falhas inerentes ao protocolo podem ser exploradas. A seguir, cada vetor de ataque é detalhado tecnicamente, abrangendo desde a negação de serviço até técnicas de engenharia social [Gast 2005].

2.3.1 Ataque de Deauthentication

Este ataque de negação de serviço explora uma falha no gerenciamento de sessões do protocolo 802.11. Os pacotes de gerenciamento, como os de *Deauthentication* e desassociação, não são *criptografados*, mesmo em redes seguras. Um atacante pode, portanto, forjar (ou "spoofar") um pacote de *Deauthentication*, enviando-o para um dispositivo cliente em nome do ponto de acesso (ou vice-versa). O dispositivo vítima, ao receber o pacote, acredita que a instrução é legítima e encerra sua conexão imediatamente, resultando na interrupção do serviço.

A eficácia deste ataque é bem documentada, especialmente contra redes que não implementam proteções de quadros de gerenciamento. No artigo *"Analysis of Deauthentication Attack on IEEE 802.11 Connectivity Based on IoT Technology Using External Penetration Test"* [Kristiyanto 2020], os autores investigam o impacto do ataque em dispositivos *IoT*.

No estudo de Kristiyanto, a metodologia de ataque foi semelhante à proposta neste trabalho, utilizando também o microcontrolador:

- **Ferramenta de Ataque:** Um módulo *ESP8266 NodeMCU* com programação em Lua.
- **Alvo do Teste:** Uma câmera *IP* (um dispositivo *IoT*) conectada à rede *Wi-Fi.*
- **Método:** Os pesquisadores usaram um *"script deauther"* para executar o ataque de desautenticação contra o alvo, enquanto monitoravam a rede com um *software* analisador de pacotes.
- **Paralisia da Comunicação:** O ataque causou a perda de comunicação entre a câmera *IP e o gateway*, interrompendo seu funcionamento.
- **Falha na Reconexão:** O dispositivo alvo, mesmo com seu endereço *MAC* ainda registrado no *gateway*, não conseguiu restabelecer a conexão enquanto o ataque estava ativo.
- **Evidência nos Pacotes:** A análise dos pacotes capturados mostrou a mudança no tipo de frame dos dados normais para o gerenciamento e o subtipo para *Deauthentication*, confirmando a natureza do ataque.
- **Valida a Ameaça:** O estudo de Kristiyanto [Kristiyanto 2020] serve como a prova prática do que acontece quando essa proteção não está presente, como é comum em dispositivos *IoT* ou em redes de visitantes configuradas com menos rigor.
- **Justifica as Ferramentas:** O fato de Kristiyanto [Kristiyanto 2020] também usar um *ESP8266* para realizar um ataque bem-sucedido reforça diretamente a tese central do TCC: "Microcontroladores para a execução de ciberataques".

2.3.2 Captura de Handshake e Ataques Correlatos

O processo de autenticação em redes protegidas por *WPA/WPA2* envolve uma troca de quatro pacotes entre o cliente e o ponto de acesso, conhecida como *4-way handshake* [Alabdulatif 2014]. Essa troca serve para verificar se ambos os dispositivos possuem a chave de acesso correta *(PSK - Pre-Shared Key)* e para gerar as chaves de criptografia da sessão [Rango Dionigi Cristian Lentini 2006; Alabdulatif 2014].

O ataque mais comumente associado a este processo, e um dos objetivos de teste deste TCC, é a **captura passiva do handshake**. Se um atacante, operando em modo monitor, conseguir capturar esses quatro pacotes, ele pode utilizar ferramentas *offline* para realizar ataques de força bruta ou de dicionário contra o *handshake* capturado, com o objetivo de descobrir a senha da rede *(PSK)* sem precisar interagir novamente com ela.

No entanto, a simples captura passiva não é a única vulnerabilidade associada a esta troca de mensagens. A própria mecânica do *4-way handshake* é suscetível a **ataques ativos de Negação de Serviço *(DoS)***, que exploram falhas em seu projeto para impedir a autenticação de clientes legítimos. Outros trabalhos na área demonstraram como isso é possível:

- **Ataque de Bloqueio da Mensagem *(DoS)*:** O trabalho de Alabdulatif e Ma (2014) identificou um ataque de DoS onde um adversário impede ativamente que a Mensagem (enviada pelo cliente) chegue ao Ponto de Acesso *(AP)* [Alabdulatif 2014].
  - **Método:** O atacante bloqueia a Mensagem . O AP, que nunca recebe esta mensagem, não instala a chave de sessão *(PTK).*
  - **Resultado:** O *AP* assume que a Mensagem falhou e a reenvia repetidamente. O cliente, que já recebeu a Mensagem e atualizou seu estado, descarta essas retransmissões. Eventualmente, o *AP* atinge um tempo limite (*timeout*) e desautentica o cliente, completando o ataque de *DoS* [Alabdulatif 2014].
- **Ataque de Injeção da Mensagem (DoS Flooding):** O estudo de Rango(2006) detalha um ataque que explora a *Mensagem* (enviada pelo *AP*), que é a única mensagem no *handshake* que não possui um Código de Integridade de Mensagem *(MIC)* para verificar sua autenticidade [Rango Dionigi Cristian Lentini 2006].
  - **Método:** O atacante espera o cliente enviar a Mensagem legítima e, em seguida, injeta na rede uma *Mensagem* falsa (Msg1') com um novo número aleatório (ANonce') [Rango Dionigi Cristian Lentini 2006].
  - **Resultado:** O cliente recebe esta Msg1' falsa e calcula uma nova chave *PTK* (Chave Transiente Par a Par), é usada para criptografar o tráfego entre um cliente (como um smartphone ou laptop) e um ponto de acesso Wi-Fi.' incorreta [Rango Dionigi Cristian Lentini 2006]. Quando a *Mensagem* legítima do *AP* (baseada na *PTK* correta) chega, a verificação do *MIC* no cliente falha (pois ele usa a *PTK*' incorreta para verificar). O cliente descarta a mensagem O *AP* nunca recebe a Mensagem, atinge o *timeout* e desautentica o cliente. Se repetido, este ataque pode levar à exaustão de memória no cliente (*DoS flooding*) [Rango Dionigi Cristian Lentini 2006].

Como esses resultados ajudam este trabalho: A análise desses estudos é crucial para este TCC. Ela demonstra que a captura do *4-way handshake* não é apenas um vetor para ataques passivos de quebra de senha (como o realizado no Capítulo 4), mas também um protocolo com falhas de *design* exploráveis para ataques ativos de negação de serviço. Isso reforça a criticidade de proteger essa troca de mensagens e amplia o entendimento das vulnerabilidades inerentes ao *WPA2-PSK*, justificando a necessidade de protocolos mais robustos como o *WPA3.*

2.3.3 Beacon Spam

Os *Beacon Frames* (quadros de sinalização) são pacotes enviados periodicamente pelos pontos de acesso para anunciar sua presença e suas características, como o nome da rede (*SSID*). Eles são cruciais para a operação de uma rede *IEEE 802.11*, sendo usados para sincronizar os relógios dos nós, anunciar a existência da rede e transmitir parâmetros de configuração necessários para a conexão [Zurutuza Roberto Uribeetxeberria 2008].

No entanto, como outros quadros de gerenciamento, os *Beacon Frames* não são autenticados, o que representa uma vulnerabilidade significativa do protocolo. O ataque de *Beacon Spam*, como demonstrado neste TCC, explora essa falha ao inundar o espectro de radiofrequência com milhares de quadros de sinalização falsos, criando centenas ou milhares de redes *Wi-Fi* "fantasmas" [Zurutuza Roberto Uribeetxeberria 2008].

Essa ação causa poluição visual na lista de redes dos dispositivos, pode degradar o desempenho de alguns aparelhos e serve como uma cortina de fumaça para ocultar outras atividades maliciosas, como a criação de um Ponto de Acesso Falso. A literatura confirma que a falsificação (*spoofing*) de *Beacon Frames* é a base para diversos ataques de Negação de Serviço (DoS) e manipulação:

- **Ataques de Sincronização:** A injeção de *beacons* falsos com valores de relógio incorretos pode dessincronizar os nós. Isso pode levar à perda de pacotes em *buffer* para nós no modo de economia de energia *(PSM)* ou causar colisões e *DoS* em redes que utilizam PCF (*Point Coordination Function*).

- **Ataques ao 802.11i:** A manipulação de informações de segurança (como o *RSN IE*) em *beacons* forjados pode impedir que clientes legítimos se conectem à rede ou forçá-los a usar métodos de criptografia mais fracos (*rollback attack*) [Zurutuza Roberto Uribeetxeberria 2008].

- **Ataques de Informação Falsa:** A falsificação de parâmetros essenciais, como o número do canal em que a rede opera, pode efetivamente impedir que os dispositivos encontrem e se conectem à rede legítima [Zurutuza Roberto Uribeetxeberria 2008].

O trabalho de Martinez. (2008) propõe um método para detectar esses *beacons* falsificados, que se alinha diretamente com a natureza do ataque de *Beacon Spam* [Zurutuza Roberto Uribeetxeberria 2008].

- **Método de Detecção:** Baseia-se no monitoramento do intervalo de tempo (*Delta*) entre *Beacon Frames* consecutivos. Os *beacons* legítimos devem ser transmitidos em intervalos regulares definidos pelo *AP* (tipicamente 102.4 ms). Um ataque de *Beacon Spam*, ao injetar múltiplos *beacons* falsos entre os legítimos, necessariamente reduzirá drasticamente esse intervalo [Zurutuza Roberto Uribeetxeberria 2008].

- **Resultados:** Os experimentos mostraram que, ao medir o *Delta*, é possível identificar a presença de *beacons* falsos, pois os intervalos medidos durante o ataque tornam-se significativamente menores e mais variáveis do que o normal [Zurutuza Roberto Uribeetxeberria 2008]. Um limiar adequado permite detectar os *beacons* anômalos com poucos falsos positivos [Zurutuza Roberto Uribeetxeberria 2008].

Como esses resultados ajudam este trabalho: A análise de Martinez et al. fornece um forte suporte teórico e prático para as conclusões deste TCC sobre o *Beacon Spam*:

- **Valida a Vulnerabilidade:** Confirma que a ausência de autenticação nos *Beacon Frames* é uma fraqueza explorável [Zurutuza Roberto Uribeetxeberria 2008].
- **Demonstra o Impacto:** Ilustra como a falsificação desses quadros, um componente central do *Beacon Spam*, pode levar a diversos tipos de *DoS* e comprometer a operação da rede [Zurutuza Roberto Uribeetxeberria 2008].
- **Corrobora a Detecção Implícita:** O método de detecção baseado no intervalo de tempo valida a observação prática deste TCC de que o *Beacon Spam* causa uma "poluição"visível e anômala, detectável pela frequência anormalmente alta de *beacons* [Zurutuza Roberto Uribeetxeberria 2008].

Portanto, a literatura externa reforça a relevância de se considerar o *Beacon Spam* como uma ameaça real e a necessidade de mecanismos de detecção ou mitigação.

2.3.4 Ponto de Acesso Falso (Evil Twin)

Considerado um dos ataques de engenharia social mais eficazes contra redes *Wi-Fi, o Evil Twin* (Gêmeo Maligno) consiste na criação de um ponto de acesso malicioso com o mesmo *SSID* e, por vezes, o mesmo endereço *MAC* de uma rede legítima e confiável [QianLU *et al.* 2018]. Dispositivos que já se conectaram à rede original podem se conectar automaticamente ao *Evil Twin*, ou o usuário pode ser enganado a fazê-lo [QianLU *et al.* 2018]. Uma vez conectado, todo o tráfego da vítima passa pelo dispositivo do atacante, que pode interceptar dados não criptografados, capturar credenciais através de portais cativos falsos *(phishing)* e realizar ataques do tipo *man-in-the-middle* (MITM) [QianLU *et al.* 2018].

O trabalho de Qian LU. (2018) detalha o funcionamento e a ameaça representada por esses ataques, destacando sua facilidade de implementação e alto potencial de dano:

- **Configuração do Ataque:** Um atacante configura um dispositivo (como um laptop) com *software* específico para atuar como um *AP falso* [QianLU *et al.* 2018]. Esse dispositivo geralmente requer duas interfaces de rede sem fio: uma para se conectar à rede legítima (para ter acesso à Internet) e outra para transmitir o *SSID* falso e atrair as vítimas [QianLU *et al.* 2018].

- **Atração das Vítimas:** O atacante pode atrair vítimas passivamente, posicionando o *Evil Twin* mais próximo delas para oferecer um sinal mais forte *(RSSI* maior) do que o *AP* legítimo, fazendo com que os dispositivos se conectem automaticamente. Alternativamente, podem forçar ativamente a conexão enviando pacotes de *Deauthentication* para desconectar as vítimas do *AP* legítimo [QianLU *et al.* 2018].

- **Interceptação e Ataques Adicionais:** Uma vez que o tráfego da vítima passa pelo *Evil Twin*, o atacante pode capturar informações sensíveis (senhas, dados de cartão de crédito). Além disso, podem manipular respostas *DNS*, controlar rotas ou redirecionar o usuário para páginas de phishing (por exemplo, imitando páginas de login ou pagamento online) [QianLU *et al.* 2018].

Devido à sua natureza, o *Evil Twin* atua essencialmente como um "intermediário"ou *proxy*, encaminhando o tráfego entre a vítima e o *AP* legítimo. Essa característica de **comportamento de encaminhamento** é a base para algumas técnicas de detecção. QianLU. (2018) propuseram um método de detecção do lado do cliente baseado nesta premissa:

- **Método de Detecção:** A técnica monitora passivamente os quadros de dados 802.11 enviados pelos APs (o legítimo e o suspeito de ser Evil Twin) [QianLU *et al.* 2018]. Ela filtra esses quadros para obter estatísticas sobre o fluxo de "Quadros de Dados Efetivos"(EDFs) - quadros de dados não retransmitidos vindos da Internet [QianLU *et al.* 2018].

- **Lógica de Detecção:** O método calcula a correlação (usando o coeficiente de Pearson) entre o fluxo total de *EDFs* enviado pelo *AP* legítimo para todos os seus clientes ($S_{AP_{legit}}$) e o fluxo específico de EDFs enviado pelo *AP* suspeito para uma determinada vítima ($AP_{evil}[Vtima]$) [QianLU *et al.* 2018]. Uma alta correlação indica que o *AP* suspeito está simplesmente encaminhando o tráfego do *AP* legítimo, caracterizando-o como um Evil Twin [QianLU *et al.* 2018].

- **Resultados:** Nos experimentos de QianLU. (2018), o método alcançou uma precisão de detecção de cerca de 96% em condições de bom sinal [QianLU *et al.* 2018].

Como esses resultados ajudam este trabalho: A análise de QianLU. contribui significativamente para este TCC:

- **Confirma a Praticidade e Ameaça:** O artigo reforça a facilidade com que um ataque *Evil Twin* pode ser configurado e lançado em locais públicos, validando a relevância do cenário explorado neste trabalho [QianLU *et al.* 2018].

- **Ilustra o Mecanismo de Encaminhamento:** Descreve tecnicamente como o *Evil Twin* opera como um intermediário, o que é fundamental para entender por que ele consegue interceptar o tráfego [QianLU *et al.* 2018].

- **Apresenta uma Abordagem de Detecção:** Embora este TCC se concentre na demonstração do ataque e na conscientização, o trabalho de QianLU. mostra que existem abordagens técnicas (mesmo do lado do cliente) para detectar ativamente esses ataques, baseadas na análise estatística do tráfego. Isso pode ser um ponto interessante para sugestões de trabalhos futuros.

Portanto, a pesquisa sobre *Evil Twins* confirma a gravidade da ameaça e a importância da conscientização, ao mesmo tempo que aponta para possíveis soluções técnicas de detecção que complementam a defesa baseada no fator humano.

2.3.5 Conscientização como Ferramenta de Defesa

Embora existam medidas técnicas robustas para mitigar muitos dos ataques descritos como a adoção de protocolos mais seguros *(WPA3)*, a implementação de proteção para quadros de gerenciamento *(MFP/802.11w)*, e o uso de sistemas de detecção de intrusos *(WIDS/WIPS)* a segurança da informação é um sistema sociotécnico onde o fator humano é frequentemente o elo mais fraco. Conforme demonstrado neste trabalho através da simulação dos ataques de *Deauthentication* (Negação de Serviço), Captura de *Handshake*, *Beacon Spam* (Poluição de Espectro) e *Ponto de Acesso Falso* (*Evil Twin*), a conscientização do usuário final é uma camada de defesa indispensável, aplicável em diferentes graus a cada um desses vetores.

- **Contra Ataques de Negação de Serviço (*Deauthentication*):** Embora a principal defesa contra este ataque seja técnica (como o *MFP*, que parece estar implementado no IFPB, conforme os resultados do Capítulo 4), a conscientização do usuário ainda tem um papel. Usuários cientes de que desconexões forçadas e inexplicáveis podem ser um sintoma de ataque podem relatar esses incidentes à equipe de TI mais rapidamente, auxiliando na identificação de possíveis ameaças ou falhas.

- **Contra Captura de *Handshake*:** A captura em si é passiva, mas a sua utilidade para o atacante depende da força da senha *(PSK)*. Usuários conscientes da importância de senhas complexas (mesmo em redes como a IFPB-VISITA) exercem pressão indireta para que senhas mais fortes sejam utilizadas pela administração. Além disso, a conscientização sobre os riscos de redes com chaves compartilhadas pode levar os usuários a adotarem práticas mais seguras, como o uso de *VPNs* para proteger seu tráfego, mesmo que a senha da rede seja comprometida.

- **Contra *Beacon Spam*:** Este ataque visa diretamente confundir o usuário. A conscientização é a principal defesa aqui. Usuários instruídos sobre a aparência normal da lista de redes e alertados sobre a possibilidade de *SSIDs* falsos duplicados são menos propensos a se conectar acidentalmente a um *Evil Twin* escondido no meio da "poluição visual". Saber identificar a rede legítima e desconfiar de múltiplas redes idênticas é crucial.

- **Contra *Ponto de Acesso Falso* (*Evil Twin*):** Este ataque, como demonstrado pelos resultados práticos deste TCC (Capítulo 4), depende quase inteiramente de enganar o usuário. A conscientização é a defesa primária e mais eficaz. Educar os usuários sobre os riscos, ensiná-los a identificar redes suspeitas (ex: uma rede normalmente segura que subitamente pede login via portal web, a verificar sempre a presença do cadeado de segurança *(HTTPS)* e o endereço correto antes de inserir credenciais , e a desconfiar de portais cativos que pedem informações sensíveis são ações cruciais.

Como a abordagem de conscientização ajuda este trabalho: Discutir a conscientização em relação a todos os ataques simulados, e não apenas ao *Evil Twin*, fortalece este TCC de várias maneiras:

- **Reforça a Tese Central:** Enfatiza a mensagem principal do trabalho sobre a importância da conscientização como complemento indispensável às defesas técnicas.
- **Oferece uma Visão Holística:** Mostra que a segurança não depende apenas da infraestrutura, mas de uma cultura de segurança que envolve toda a comunidade acadêmica.
- **Aumenta a Relevância Prática:** Transforma a análise técnica das vulnerabilidades em recomendações práticas e acionáveis para os usuários finais, aumentando o impacto e a utilidade do diagnóstico de segurança realizado.
- **Cria Coerência:** Conecta a fundamentação teórica sobre os ataques (Capítulo 2) com os resultados práticos (Capítulo 4) e as recomendações finais (Capítulo 5), criando um fluxo lógico mais coeso.

Portanto, abordar a conscientização de forma abrangente solidifica o argumento de que, mesmo diante de ameaças técnicas variadas, o usuário educado e vigilante é uma peça fundamental na estratégia de segurança *cibernética* do IFPB.

Capítulo 3

Desenvolvimento e Implementação dos Módulos de Teste

Este capítulo apresenta de forma detalhada o processo de construção e configuração dos módulos de *hardware e software* utilizados na etapa experimental deste estudo. Para cada ferramenta de auditoria empregada, são descritos os componentes selecionados, o esquema de montagem e a lógica de implementação, de modo a fornecer suporte técnico consistente para a análise e interpretação dos resultados obtidos.

3.1 Implementação do Módulo de Auditoria ESP32 Marauder

Para a execução dos ataques de Negação de Serviço *(Deauthentication), Captura de Handshake e Poluição de Espectro (Beacon Spam)*, foi desenvolvido um dispositivo portátil baseado no microcontrolador *ESP32* e no *firmware Marauder*. A concepção do módulo visou a autonomia e a portabilidade, eliminando a necessidade de um computador externo durante os testes de campo.

3.1.1 Componentes do Hardware

A seleção dos componentes foi pautada pela compatibilidade com o *firmware* e pela funcionalidade integrada.

- **Microcontrolador:** Foi utilizado um módulo **ESP32 WROOM-32 DevKit V4**. Este componente foi escolhido por sua arquitetura *dual-core*, capacidade de operar em modo monitor e suporte nativo às bibliotecas exigidas pelo *Marauder*. A pinagem do módulo é apresentada na Figura 3.1.
- **Interface de Usuário:** Para a interação com o *firmware*, foi integrado um **Display LCD TFT SPI de 2.8 polegadas**, com *driver* **ILI9341** e resolução de 240x320 pixels

(Figura 3.2). Este *display* permite a visualização da interface gráfica do *Marauder* e o controle das funções de ataque em tempo real.

- **Armazenamento de Dados:** O próprio módulo do *display TFT* integra um **leitor de cartão Micro SD**, essencial para salvar os arquivos de captura de *handshake* (*.pcap*) e outros logs gerados durante os testes.

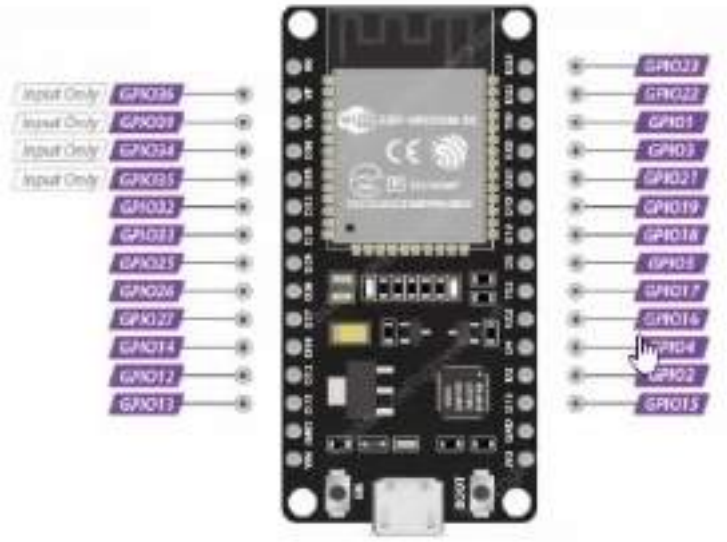

Figura 3.1: *Diagrama de pinagem do ESP32 DevKit V4.*
[Clube do Maker 2024]

Figura 3.2: *Display TFT SPI de 2.8 polegadas com driver ILI9341.*
[randomnerdtutorials 2024]

3.1.2 O Firmware ESP32 Marauder

Marauder é um firmware especializado para *penetration testing* em redes *Wi-Fi e Bluetooth*. A versão do *firmware* **ESP32 Marauder v1.8.6** utilizada neste projeto representa um ponto de maturidade, consolidando funcionalidades importantes.

- **Lógica de Operação:** O *firmware* otimiza o uso do *hardware do ESP32*, oferecendo uma suíte completa de ferramentas que podem ser controladas via interface gráfica (*no display TFT*) ou por linha de comando (*via porta serial*).
- **Ataque de Deauthentication:** O módulo utiliza a funcionalidade *Deauth do Marauder* para forjar pacotes de *Deauthentication*. O ataque é executado enviando o pacote diretamente ao endereço *MAC* do dispositivo-alvo (*Dispositivo-Alvo*). em nome do Ponto de Acesso legítimo, explorando o fato de que *gerência frames* 802.11 não são criptografados.
- **Captura de Handshake:** A ferramenta configura o rádio do *ESP32* para o Modo Monitor em um canal específico da rede-alvo. Quando o dispositivo-alvo tenta se reconectar (*seja por um ataque de Deauth ou naturalmente*), o Marauder capta a troca dos quatro pacotes *EAPOL do 4-way handshake WPA2*, salvando-os no cartão *SD* para análise *offline* e eventual quebra de senha (*força bruta ou dicionário*).
- **Beacon Spam:** O módulo gera e transmite milhares de *Beacon Frames* falsos em rápida sucessão. Essa técnica inunda o espectro de rádio, criando uma poluição visual na lista de redes disponíveis nos dispositivos e servindo como cortina de fumaça para outras ações.

3.1.3 Esquema de Montagem e Conexões

O protótipo foi montado utilizando uma mini breadboard (matriz de contatos) de 400 pontos, uma escolha que priorizou a modularidade e a facilidade de manutenção durante a fase de testes. Diferente de uma placa de circuito impresso soldada, a breadboard permitiu ajustes rápidos no cabeamento e a substituição ágil de componentes, caso necessário. A conexão física entre os terminais do *ESP32* e o módulo de display foi realizada através de jumpers do tipo macho-fêmea e macho-macho, garantindo a integridade elétrica do circuito.

A comunicação de dados entre o microcontrolador *ESP32*, o display *TFT* e o leitor de cartão *SD* ocorre via protocolo SPI *(Serial Peripheral Interface)*. Este barramento síncrono é fundamental para o projeto, pois permite altas taxas de transferência de dados, essenciais para a atualização fluida da interface gráfica e para a gravação rápida dos pacotes de rede capturados *(sniffing)* no cartão *SD* sem perda de frames.

No esquema adotado, ambos os periféricos *(Display e SD)* compartilham os mesmos barramentos de Clock *(SCK)*, *Master Output Slave Input (MOSI) e Master Input Slave Output (MISO)*, diferenciando-se apenas pelos pinos de seleção de escravo *(Chip Select - CS)*, que permitem ao *ESP32* endereçar comandos especificamente para o *display* ou para o cartão de memória conforme a necessidade do *firmware*.

É importante ressaltar que todo o sistema opera com lógica de tensão de 3.3V, fornecida pelo regulador interno do próprio kit de desenvolvimento *ESP32*, que por sua vez é alimentado via porta USB (5V). O mapeamento rigoroso dos pinos seguiu a documentação

oficial do projeto *Marauder* para garantir a compatibilidade do driver de vídeo, conforme detalhado na Tabela 3.1, ilustrado na montagem final (Figura 3.3).

Tabela 3.1: *Mapeamento de Pinos do Display/Módulo SD para o ESP32.*

Função	**Pino 2.8"TFT / SD**	**Pino ESP32 (GPIO)**
Alimentação	VCC	3V3
Aterramento	GND	GND
Comunicação SPI (Display e SD)		
SDA (*MOSI*)	MOSI	GPIO23
SCL (*SCK*)	SCK	GPIO18
MISO (*Data Out*)	MISO	GPIO19
Pinagem de Controle		
Chip Select (Display)	CS	GPIO17
Data/Command	D/C	GPIO16
Reset	RESET	GPIO05
Chip Select (SD)	SD_CS	GPIO12

Figura 3.3: *Protótipo do módulo ESP32 Marauder montado em breadboard. O autor (2025)*

Figura 3.4: *Esquemático eletrônico*

3.2 Implementação do Módulo ESP8266 Evil Twin

Para a execução do ataque de Ponto de Acesso Falso com *Portal Cativo*, optou-se pelo desenvolvimento de uma solução customizada, utilizando o microcontrolador *ESP8266*. Esta escolha permitiu a criação de uma página de *phishing* específica para o contexto do IFPB, aumentando a eficácia da demonstração.

3.2.1 Componentes de Hardware e Software

- **Microcontrolador:** Foi utilizado um módulo *NodeMCU ESP8266*. Sua arquitetura de núcleo único e a vasta biblioteca de servidores *web* o tornam ideal para atuar de forma eficiente como um Ponto de Acesso e Servidor *HTTP (Hypertext Transfer Protocol)* embarcado (Figura 3.5).
- **Software de Desenvolvimento:** O código-fonte foi desenvolvido em C/C++ utilizando a **IDE do Arduino**, com foco nas bibliotecas que gerenciam redes *Wi-Fi*, servidor *DNS e web*.

3.2.2 Bibliotecas de Software

O firmware desenvolvido, disponível no repositório do autor [(Github) 2025], executa uma sequência de passos para enganar a vítima e capturar suas credenciais.

1. **Criação do Ponto de Acesso Falso:** O ESP8266 é inicializado em modo *Access Point*, criando uma rede *Wi-Fi* com o mesmo *SSID* da rede oficial do IFPB.

2. **Servidor DNS Malicioso:** Um servidor *DNS* é configurado no dispositivo. Sua função é responder a qualquer requisição de nome de domínio (e.g., `google.com`, `ifpb.edu.br`) com o endereço de *IP* do próprio *ESP8266.*

3. **Redirecionamento (Portal Cativo):** Quando a vítima se conecta à rede falsa e tenta acessar qualquer site, o servidor *DNS* força o redirecionamento para o servidor *web* embarcado no *ESP8266.*

4. **Página de Phishing:** O servidor *web* entrega ao navegador da vítima uma página *HTML* falsa, que simula a tela de autenticação da rede do *IFPB*, solicitando `matrícula e senha`.

5. **Captura de Credenciais:** As informações inseridas pela vítima no formulário são enviadas via método POST para o *ESP8266*, que as exibe no monitor serial, completando o ataque.

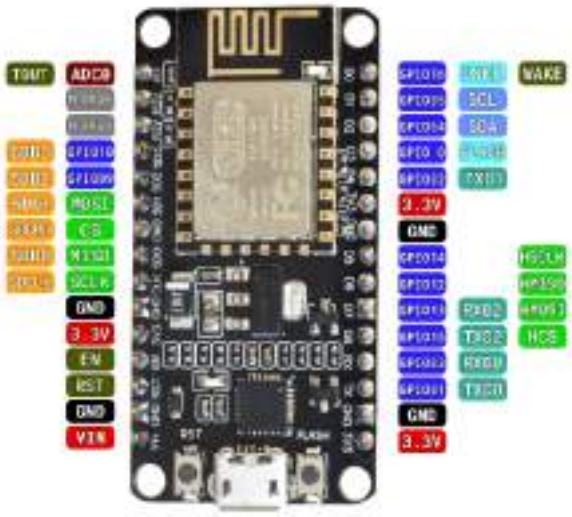

Figura 3.5: *Módulo NodeMCU ESP8266 utilizado para o ataque Evil Twin.*
[clubedomaker 2024]

A implementação destes dois módulos distintos demonstra a flexibilidade e o poder da ferramenta, mostrando como diferentes plataformas podem ser otimizadas para a execução de vetores de ataque específicos.

Capítulo 4

Resultados e Análise dos Experimentos

Este capítulo apresenta e analisa os resultados práticos obtidos a partir da execução controlada e autorizada dos quatro vetores de ataque em redes *Wi-Fi* do IFPB Campus Campina Grande, conforme a metodologia estabelecida. Os experimentos foram realizados utilizando o módulo *ESP32* com *firmware Marauder* e o módulo *ESP8266* com código customizado, demonstram tanto a robustez da infraestrutura de rede contra certas ameaças quanto a sua vulnerabilidade a ataques de engenharia social, validando a tese central deste trabalho.

4.1 Ataque de Negação de Serviço (Deauthentication)

O primeiro teste visou executar um ataque de Negação de Serviço *(DoS)* por *Deauthentication*. O objetivo era desconectar forçadamente um dos dispositivos-alvo controlados (smartphone Samsung Galaxy M31 ou notebook Samsung galaxy book 2), que atuava como vítima, da rede *Wi-Fi* do campus

4.2 Procedimento e Resultado

Para a execução, o dispositivo-alvo foi conectado a rede do campus IFPB. O dispositivo de ataque, um microcontrolador *ESP32 com firmware Marauder* , foi então utilizado para realizar uma varredura, identificando os endereços MAC do dispositivo-alvo e do ponto de acesso *(AP)* ao qual ele estava conectado.

1. **Varredura de Rede (Deauthentication Scan):** Inicialmente, o módulo *ESP32 Marauder* realizou uma varredura para identificar as redes *(APs)* e os clientes conectados *(Stations)* no ambiente. A Figura 4.1 ilustra esta etapa, mostrando o resultado da varredura na interface gráfica do Marauder.

2. **Seleção de Alvo:** Em seguida, o pesquisador navegou até o menu de seleção de alvos. Na tela de *Access Points* e posteriormente na tela de *Select Stations*, o **endereço**

MAC do Ponto de Acesso legítimo (**IFPB**) e o **endereço MAC** do dispositivo-alvo controlado *(o smartphone do pesquisador)* foi identificado, conforme detalhado na Figura 4.2.

3. **Execução do Ataque:** Com os MACs alvo e AP definidos, o ataque **"Deauth Targeted"** foi iniciado a partir do menu *WiFi Attacks*. O Marauder começou a enviar pacotes de *Deauthentication* forjados, direcionados ao dispositivo-alvo em nome do *AP*. A Figura 4.3 exibe a tela de execução do ataque, reportando uma intensa rajada de **3.750 pacotes por segundo**.

O dispositivo-alvo foi monitorado continuamente para observar o critério de sucesso definido: a perda de conexão. O resultado observado foi que o ataque se mostrou ineficaz. Apesar da intensa rajada de pacotes de *Deauthentication*, o dispositivo-alvo não sofreu qualquer interrupção de conectividade, e a rede do campus permaneceu estável e funcional.

Execução do Ataque

A análise abaixo compara o desempenho observado com a média esperada para este tipo de vetor de ataque, abordando a eficácia e as anomalias volumétricas.

Eficiência Comparativa

Diferente de ataques de força bruta que exigem milhões de tentativas, o ataque de *Deauth* explora uma vulnerabilidade no gerenciamento de quadros do protocolo *802.11*. Em cenários ideais sem proteção de quadros de gerenciamento, a eficiência é extremamente alta:

- **Comparativo de Equipamentos:** Quando comparado a outros vetores de Negação de Serviço *(DoS)*, o ataque de *Deauth* é singularmente eficiente. Equipamentos de *hardware* limitado, como microcontroladores *ESP8266* (ex: *Deauth Watch*) ou ferramentas como o *Flipper Zero*, conseguem o mesmo resultado de desconexão que um computador robusto rodando *Kali Linux* com uma placa *Alfa* de alta potência. A diferença reside no alcance e na taxa de injeção, mas não na quantidade de pacotes necessária para o êxito lógico do ataque: o protocolo aceita o comando de desconexão independentemente da potência do *hardware* emissor, desde que o sinal chegue ao alvo.

Análise do Volume de Pacotes Observado

Este fenômeno não reflete a necessidade padrão do ataque, mas sim uma resposta do atacante a condições adversas na rede. As principais causas para esse volume excessivo são:

1. **Proteção da Rede (Management Frame Protection - MFP):** A causa para a ineficácia dos primeiros pacotes e a consequente inundação (*flood*) contínua é a presença do padrão **IEEE 802.11w** (PMF - *Protected Management Frames*).

- Quando o PMF está ativo, comum em *WPA3* e opcional em *WPA2*), os quadros de gerenciamento como o de *Deauthentication* são criptografados ou assinados.
- O cliente alvo recebe os pacotes injetados pelo atacante, mas os descarta silenciosamente por falharem na verificação de integridade.
- Como o cliente não se desconecta, a ferramenta de ataque (configurada em *loop*) continua enviando milhares de pacotes na tentativa de obter êxito, gerando o volume absurdo observado sem, contudo, efetivar a desconexão.

2. **Perda de Sinal e Interferência:** Em segunda instância, se o atacante estiver distante ou houver alta interferência no canal, os pacotes podem ser corrompidos fisicamente antes de chegarem ao alvo. Isso força a ferramenta a retransmitir continuamente os quadros.

Conclusão do Resultado: A necessidade de uma quantidade massiva de pacotes indica falha na exploração da vulnerabilidade padrão. Em uma rede vulnerável típica, a desconexão é imediata com tráfego mínimo. O alto volume registrado confirma que o mecanismo de defesa da rede o *802.11w* impediram a aceitação do comando de desautenticação, transformando um ataque lógico preciso em uma tentativa ineficiente de inundação por força bruta.

4.2.1 Limitação do Protocolo IEEE 802.11w

O padrão *IEEE 802.11w*, também conhecido como *Management Frame Protection (MFP)* ou *Protected Management Frames (PMF)*, foi desenvolvido para abordar uma vulnerabilidade crítica nos padrões *Wi-Fi* anteriores, como o *WPA2*. A principal limitação que ele foi criado para superar a falta de autenticação ou criptografia nos quadros de gerenciamento *802.11*, como os pacotes de *Deauthentication* e *Desassociation*.

A Solução do MFP e sua Limitação:

- **Assinar Criptograficamente** os quadros de gerenciamento unicast *(direcionados a um único cliente)*.
- **Criptografar** e usar Mecanismos de Integridade de Mensagem *(MIC)* para quadros *multicast e broadcast*.

O Efeito do MFP na Prática (e sua Limitação no Contexto de Ataque):

Quando o *MFP* está ativo, um atacante, como o que usou o *firmware Marauder* no *ESP32*, tenta executar um ataque de Negação de Serviço *(Deauthentication)*:

- O dispositivo cliente e o Ponto de Acesso *(AP)* recebem o pacote de *Deauthentication* forjado.

- Como o pacote não possui a assinatura criptográfica válida ou falha na verificação de integridade, ele é silenciosamente descartado.
- Dessa forma, o ataque de *Deauthentication* direto é neutralizado, e o cliente não perde a conexão.

Limitação do MFP/802.11w

Embora o *802.11w* seja altamente eficaz contra a injeção de quadros de gerenciamento, ele não é a solução para todas as falhas de segurança do *Wi-Fi*. A principal limitação do *MFP* é que ele não impede ataques que não dependem da injeção de pacotes de gerenciamento:

- **Não Protege Contra Engenharia Social/Evil Twin:** O MFP não pode evitar que um atacante crie um Ponto de Acesso Falso *(Evil Twin)* com o mesmo nome de rede *(SSID)* para enganar o usuário. Esse ataque de engenharia social é realizado em uma camada superior e contorna a proteção do protocolo *802.11w*, como evidenciado pelo sucesso do ataque no IFPB.
- **Compatibilidade e Configuração** O *MFP* é opcional em redes *WPA2-Personal/Enterprise*, o que significa que se o *AP* ou o cliente não o suportarem ou não o ativarem corretamente, a vulnerabilidade permanece.

Em resumo, o *802.11w (MFP)* é uma contramedida técnica robusta que neutralizou a ameaça de Negação de Serviço no IFPB , mas sua limitação reside no fato de que ele não é uma defesa contra a exploração do fator humano

4.2.2 Análise do Resultado: Uma Infraestrutura Resiliente

A ineficácia da tentativa de negação de serviço evidencia a robustez das configurações de segurança adotadas na infraestrutura de rede do IFPB. Este resultado atesta a competência da equipe de Tecnologia da Informação do campus na implementação de mecanismos de segurança modernos.

A Coordenação de TI, em resposta a um formulário enviado sobre os mecanismos de defesa, **Confirmou** que a mitigação do ataque é atribuída a dois fatores principais:

- **Implementação do Padrão 802.11w (Management Frame Protection - MFP):** As redes corporativas do IFPB *WPA2/WPA3-Enterprise* não apenas suportam, mas exigem a proteção MFP. Este padrão de segurança criptografa os frames de gerenciamento, incluindo os de *Deauthentication.* Consequentemente, os pacotes forjados e não assinados, enviados pelo *Marauder*, foram criptograficamente inválidos e prontamente descartados pelo ponto de acesso e pelo cliente, tornando o ataque inócuo. *Deauthentication.* Consequentemente, os pacotes forjados e não assinados, enviados pelo *Marauder*, são prontamente descartados pelo ponto de acesso e pelo cliente, tornando o ataque inócuo.

- **Arquitetura de Rede com Roaming Rápido:** Arquitetura de Rede com *Roaming* Rápido: Foi confirmado que a infraestrutura de rede utiliza protocolos de *roaming* rápido (e.g., 802.11k/r/v). Esta arquitetura garante que, mesmo na remota hipótese de um cliente ser momentaneamente desconectado de um AP, ele se reassociaria quase que instantaneamente a outro AP vizinho com sinal mais forte, tornando a interrupção imperceptível para o usuário.

Este resultado prático, agora comprovado factualmente pela equipe de TI, demonstra a eficácia das contramedidas teóricas e serve como um excelente exemplo de como uma configuração de rede bem-executada pode neutralizar um dos ataques mais comuns em ambientes *Wi-Fi*.

Figura 4.1: *Deauthentication Scan. O autor (2025)*

Figura 4.2: *Deauthentication Mac. O autor (2025)*

Figura 4.3: *Deauthentication. O autor (2025)*

4.3 Captura de Handshake em Rede PSK

O segundo teste visou demonstrar a vulnerabilidade da autenticação *WPA2-PSK (Pre-Shared Key)*, utilizada em redes de acesso mais simples, como a `IFPB-VISITA`. O objetivo era capturar passivamente o *4-way handshake*, o processo de autenticação que ocorre quando um dispositivo se conecta a uma rede protegida por senha.

4.3.1 Procedimento e Resultado

1. **Seleção da Ferramenta:** No dispositivo *ESP32 com firmware Marauder*, foi acessado o menu "WiFi Sniffers".

2. **Ativação do Sniffer:** Dentro deste menu, a função específica **"EAPOL/PMKID Scan"** foi selecionada, conforme demonstrado na Figura 4.4. Esta função instrui o dispositivo a monitorar passivamente o espectro *Wi-Fi* em busca de pacotes *EAPOL (Extensible Authentication Protocol over LAN)*, que compõem o *4-way handshake*.

3. **Execução da Captura:** O dispositivo foi direcionado a monitorar o canal da rede-alvo (`IFPB-VISITA`). A Figura 4.4 mostra a tela do *Marauder* durante a execução, monitorando ativamente o tráfego em busca de pacotes *EAPOL*.

4. **Geração do Handshake:** Para induzir a captura, um dos dispositivos-alvo controlados pelo pesquisador *(smartphone ou notebook)* foi conectado à rede `IFPB-VISITA`. A conexão do dispositivo-alvo gerou o tráfego de autenticação necessário, que foi imediatamente detectado e capturado pelo *Marauder*.

Utilizando o *Marauder*, o ataque foi direcionado à rede `IFPB-VISITA`. O dispositivo obteve **sucesso** na captura do *4-way handshake*, salvando os pacotes de autenticação em um arquivo *.pcap* no cartão *SD* para análise *offline*.(Figura 4.5)

A captura bem-sucedida confirma a vulnerabilidade teórica das redes que dependem de uma chave pré-compartilhada. Embora o ataque não revele a senha diretamente, ele fornece a um atacante os dados necessários para conduzir um ataque de força bruta ou de dicionário offline. A segurança de redes desse tipo, portanto, não reside no protocolo em si, mas é inteiramente dependente da complexidade e da entropia da senha escolhida.

Figura 4.4: *Marauder PMKID Handshake. O autor (2025)*

Figura 4.5: *Arquivo pcap. O autor (2025)*

4.4 Poluição de Espectro (Beacon Spam)

Este teste objetivou demonstrar a facilidade de se criar desinformação e confusão no ambiente de radiofrequência.

4.4.1 Procedimento e Resultado

O *ESP32 Marauder* foi configurado para inundar o espectro com *Beacon Frames* falsos, clonando o *SSID* da rede `IFPB-ALUNO`. O resultado, documentado na Figura 4.6, foi imediato e eficaz.

- **Antes do Ataque:** A lista de redes no dispositivo-alvo era clara e organizada.
- **Durante o Ataque:** A lista foi instantaneamente sobrecarregada com dezenas de ocorrências do mesmo *SSID*, tornando difícil para um usuário identificar a rede legítima.

4.4.2 Análise do Resultado

O sucesso deste ataque demonstra uma vulnerabilidade fundamental do padrão 802.11: a falta de autenticação dos *Beacon Frames*. Mais do que um simples incômodo, este ataque tem implicações de segurança sérias. Ele pode ser usado como uma "cortina de fumaça"para ocultar um Ponto de Acesso Falso *(Evil Twin)* entre as dezenas de redes clonadas, aumentando drasticamente a probabilidade de um usuário se conectar à rede maliciosa por engano.

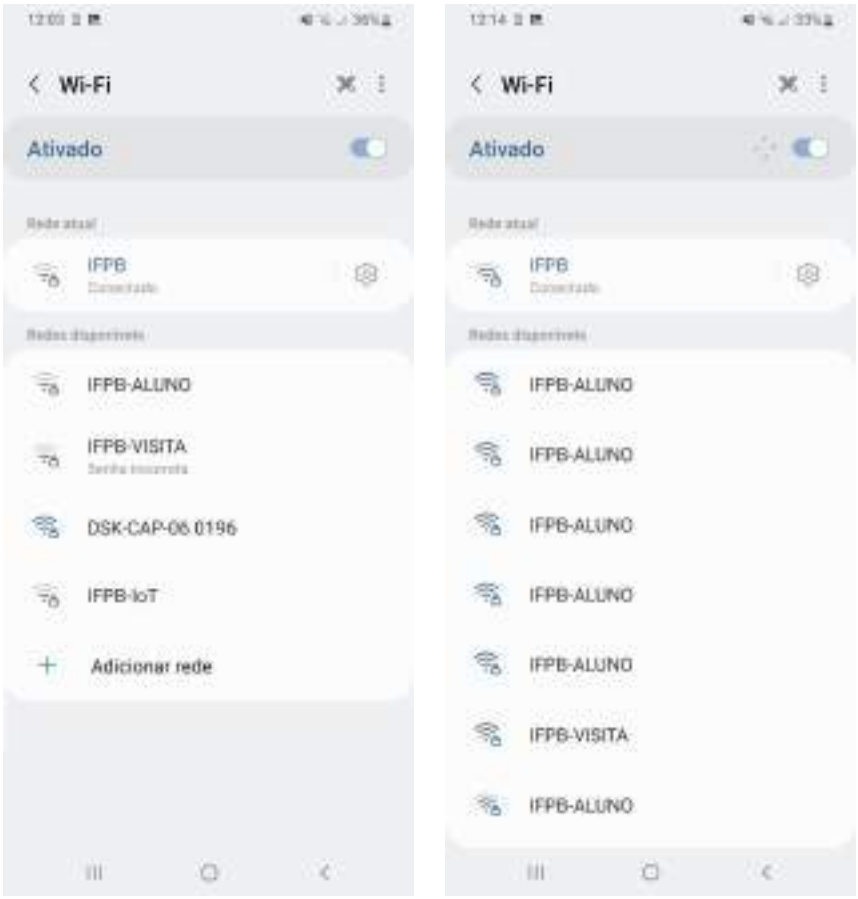

Figura 4.6: *Lista de ponto de acesso sem fio. O autor (2025)*

4.5 Ponto de Acesso Falso (Evil Twin) com Portal Cativo

Este foi o teste mais crítico, focando no vetor de ataque de engenharia social para a captura de credenciais.

4.5.1 Procedimento e Resultado

Utilizando o módulo *ESP8266* com o firmware customizado, foram criados dois Pontos de Acesso Falsos, clonando os *SSIDs* `IFPB-ALUNO` e `IFPB-VISITA`. Ambos os *APs* implementavam um portal cativo com uma página de *phishing* que simulava a tela de autenticação da instituição (Figura 4.7). O teste foi conduzido por aproximadamente 47 minutos em uma área de circulação do campus.

Conforme evidenciado na Figura 4.8, a página de administração do servidor *ESP8266* registrou a **captura de credenciais de acesso reais** (matrículas e senhas) de múltiplos usuários que, enganados pela aparência legítima do portal, inseriram seus dados.

4.5.2 Análise do Resultado

O sucesso deste ataque, comprova que, mesmo diante de uma infraestrutura de rede robusta e protegida (como evidenciado pelo fracasso do ataque de *Deauthentication*), o **fator humano permanece como o elo mais vulnerável**.

Este ataque de engenharia social contorna eficazmente todas as proteções técnicas *(WPA3-Enterprise, MFP, etc.)*, pois não ataca o protocolo, mas sim a percepção e a confiança do usuário. O resultado reforça de maneira inequívoca a tese central desta monografia: ferramentas de custo irrisório, como o *ESP8266*, podem ser utilizadas para executar ataques de alto impacto, comprometendo de forma decisiva a segurança da informação e a privacidade dos dados de toda a comunidade acadêmica.

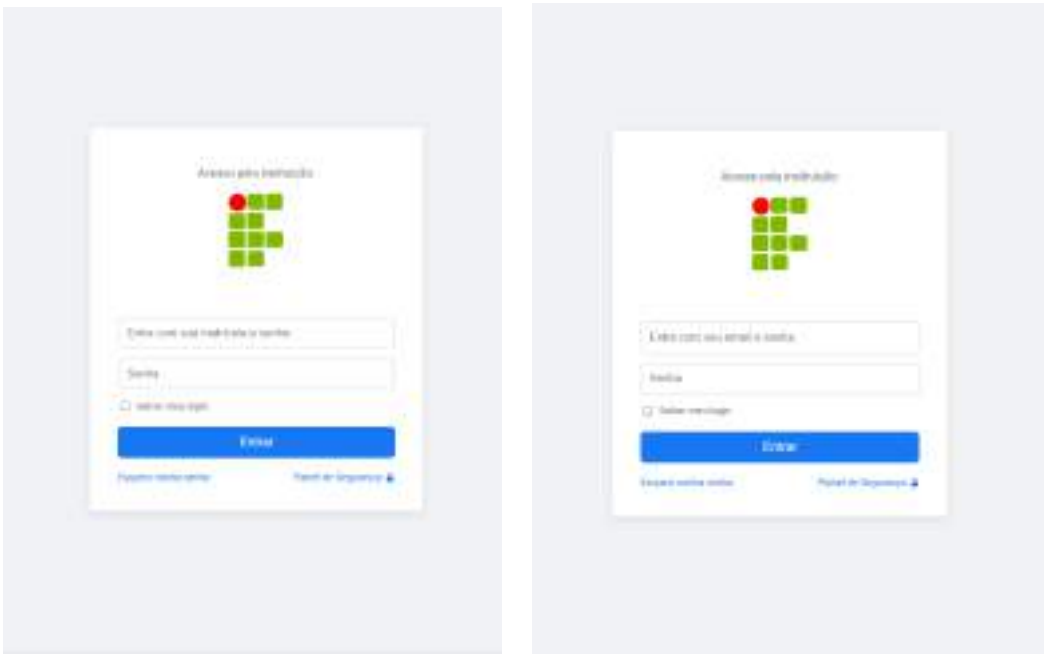

Figura 4.7: *Portal Cativo. O autor (2025)*

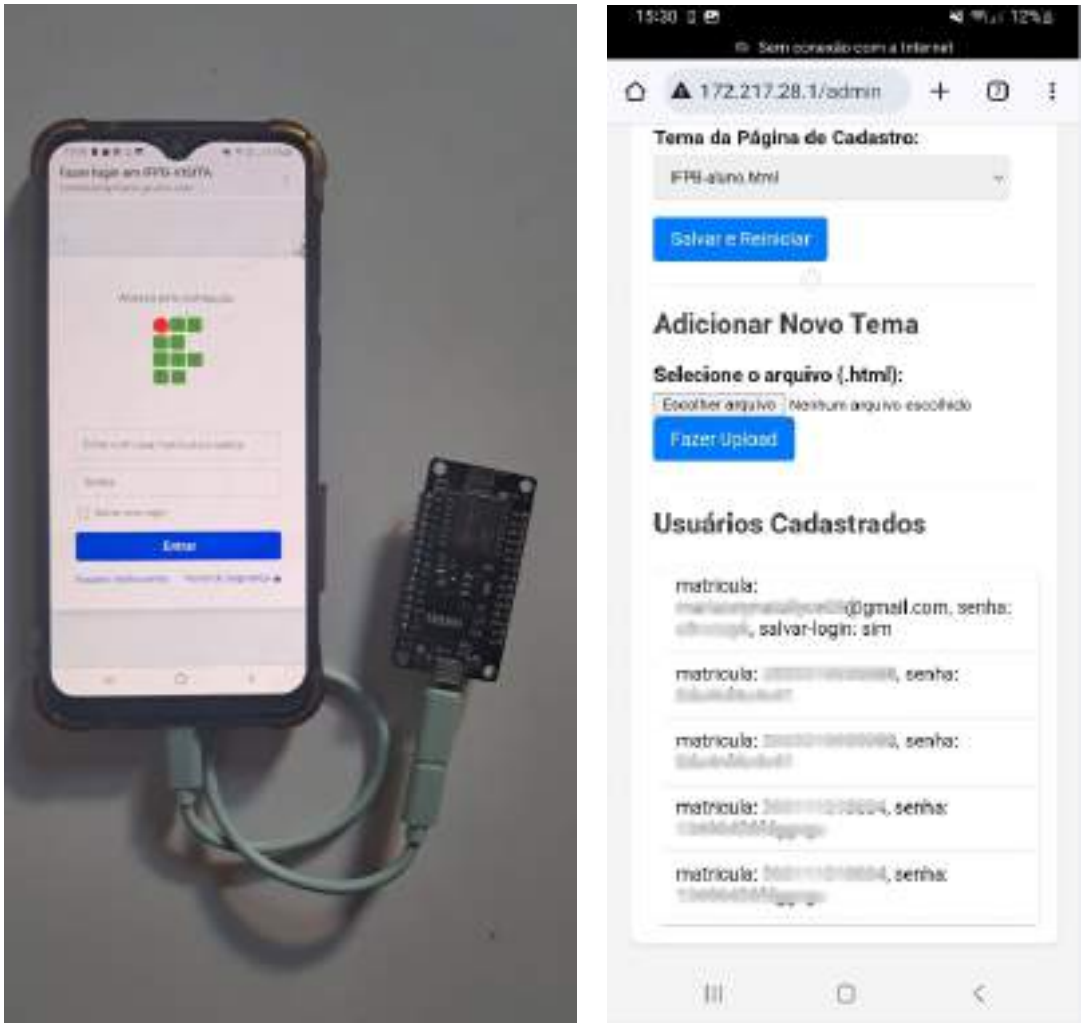

Figura 4.8: *Portal Cativo. O autor (2025)*

4.6 Resultados e Discussão

A análise conjunta dos experimentos revela uma dicotomia na segurança da rede *Wi-Fi* do IFPB. Por um lado, a infraestrutura lógica demonstrou alta resiliência contra ataques diretos ao protocolo *(Negação de Serviço)*, graças à adoção de padrões modernos como o *802.11w*. Por outro lado, a camada humana mostrou-se suscetível, permitindo que ataques de Engenharia Social *(Evil Twin)* contornassem defesas tecnológicas avançadas como o *WPA3-Enterprise*. Isso valida a premissa de que a democratização do *hardware* ofensivo *(ESP32/ESP8266)* exige uma mudança de paradigma na defesa, focando tanto na configuração técnica quanto na educação do usuário.

É importante, contudo, reconhecer as limitações deste estudo. Os microcontroladores utilizados, apesar de eficazes para a captura e injeção de pacotes, possuem limitações de processamento que impedem a realização de ataques de força bruta *(cracking)* em tempo real no próprio dispositivo, exigindo processamento *offline* posterior.

Capítulo 5

Considerações Finais e Sugestões para Trabalhos Futuros

Este trabalho teve como objetivo detectar e analisar vulnerabilidades na segurança da rede *Wi-Fi* do IFPB, utilizando os microcontroladores como ferramentas de auditoria. Os experimentos controlados realizados permitiram não apenas validar essa proposta, como também evidenciar um ponto crítico na segurança da informação: a coexistência entre uma infraestrutura técnica robusta e vulnerabilidades decorrentes do comportamento humano.

A tentativa de ataque de Negação de Serviço *(Deauthentication)* não obteve êxito, indicando que a infraestrutura de rede do campus adota mecanismos avançados de proteção, como o *padrão 802.11w (Management Frame Protection – MFP)*. Esse resultado demonstra a maturidade do ambiente técnico e o trabalho eficaz da equipe de Tecnologia da Informação do IFPB na implementação de contramedidas contra ataques voltados ao protocolo.

Entretanto, a execução bem-sucedida do ataque de Ponto de Acesso Falso *(Evil Twin)*, associado a um portal cativo, revelou a principal vulnerabilidade identificada neste estudo: o fator humano. A obtenção de credenciais reais de usuários, por meio de um dispositivo de custo reduzido como o *ESP8266,* mostrou que ataques baseados em engenharia social são capazes de contornar defesas tecnológicas sofisticadas. Assim, a ameaça não está limitada à complexidade de ferramentas ou ao poder computacional do atacante, mas à exploração da confiança e do comportamento do usuário.

Conclui-se que, embora a instituição esteja bem-preparada contra ameaças que visam o protocolo, a maior brecha de segurança reside na conscientização de sua comunidade. A facilidade com que um ataque de alto impacto foi realizado reforça a relevância deste trabalho como um diagnóstico prático e um chamado à ação para fortalecer a cultura de segurança no ambiente acadêmico.

5.1 Conscientização: Ataques e Prevenções

A defesa mais eficaz contra ataques de engenharia social, como o *Evil Twin*, é um usuário educado e vigilante. As medidas de segurança podem ser divididas em duas frentes: ações para a **infraestrutura da instituição** e ações de **conscientização para os usuários**. [Rahime Belen-Saglam, Vincent Miller, 2023]

5.1.1 Prevenção Contra Ataque de Negação de Serviço (Deauthentication)

- **Medida de Infraestrutura (Já Implementada no IFPB):** O ataque de *Deauthentication*, executado pelo *firmware Marauder no ESP32*, revelou-se consistentemente ineficaz contra os clients e o ponto de acesso da rede alvo. Este insucesso prático serviu como um indicador primário de que a rede possuía um mecanismo de mitigação ativo contra a injeção de quadros de gerenciamento. Posteriormente, a Coordenação de TI da instituição validou esta observação, confirmando formalmente que a infraestrutura está configurada com a implementação obrigatória do padrão *IEEE 802.11w (Management Frame Protection - MFP).* Este mecanismo criptografa os quadros de gerenciamento, o que impediu que os pacotes forjados desconectassem os usuários. A recomendação é, portanto, manter essa configuração robusta como obrigatória em todas as redes corporativas."

- **Ação do Usuário:** Neste caso específico, a proteção é de responsabilidade da infraestrutura. O usuário não tem como se prevenir ativamente, mas pode relatar à equipe de TI quedas de conexão frequentes e inexplicáveis para que investiguem a causa.

5.1.2 Prevenção Contra Captura de Handshake

- **Medida de Infraestrutura:**

  Uso de Senhas Fortes: A captura do *handshake* em si não revela a senha, apenas fornece os dados para um ataque de força bruta offline. Portanto, a segurança da rede `IFPB-VISITA` (e outras redes *PSK*) depende diretamente da complexidade da senha. A instituição deve garantir que a senha seja longa, complexa e trocada periodicamente.

- **Ação do Usuário:** A recomendação é evitar o tráfego de dados sensíveis nessas redes e, idealmente, utilizar sempre uma VPN (Virtual Private Network), que adiciona uma camada robusta de criptografia, protegendo os dados mesmo que a senha da rede seja comprometida. O usuário deve estar ciente de que a segurança da comunicação depende da força daquela senha única.

5.1.3 Prevenção Contra Poluição de Espectro (Beacon Spam)

- **Medida de Infraestrutura: Sistemas de Detecção de Intrusos (WIDS/WIPS):** Implementar sistemas que monitoram o espectro de radiofrequência para detectar anomalias, como o surgimento súbito de centenas de *SSIDs* idênticos. Esses sistemas podem alertar os administradores sobre a ocorrência do ataque.

- **Ação do Usuário (Conscientização): Identificar a Rede Correta:** Os usuários devem ser instruídos a ignorar a "poluição visual"e a ter cuidado redobrado para selecionar a rede legítima. Em caso de dúvida, devem desconectar o *Wi-Fi*, esperar alguns minutos e tentar novamente. O principal risco deste ataque é servir como "cortina de fumaça"para ocultar um Ponto de Acesso Falso.

5.1.4 Prevenção Contra Ponto de Acesso Falso (Evil Twin) com Portal Cativo

Este é o ataque mais perigoso identificado, pois explora o fator humano.

- **Medidas de Infraestrutura:**

  Implementação do WPA3-Enterprise: O *WPA3* oferece proteção aprimorada contra esse tipo de ataque. Ele pode exigir validação do certificado do ponto de acesso, tornando mais difícil para um "gêmeo maligno"se passar pela rede oficial sem gerar um alerta de segurança no dispositivo do usuário. **Certificados Digitais no Portal Cativo:** O portal cativo oficial da instituição deve, obrigatoriamente, usar *HTTPS* com um certificado digital válido. Isso permite que o navegador do usuário exiba o "cadeado de segurança". A ausência desse cadeado ou um alerta do navegador sobre um certificado inválido são sinais claros de uma página falsa. **Monitoramento de APs Falsos:** Utilizar soluções de WIPS para identificar e, se possível, localizar geograficamente pontos de acesso não autorizados que estejam clonando os *SSIDs* da instituição. [Shrivastava Mohd Saalim Jamal 2020]

- **Ações do Usuário (Conscientização):**

  Sempre Verifique o Endereço e o Cadeado: Antes de inserir matrícula e senha, o usuário deve verificar a barra de endereços do navegador. A página é segura? O endereço é o oficial do IFPB?. **Desconfie de Comportamentos Estranhos:** Se o dispositivo se conectar a uma rede que normalmente é segura (como a `IFPB-ALUNO`) e, de repente, solicitar um login através de uma página *web*, isso é um forte indício de um ataque de *Evil Twin*. Redes Enterprise (que usam matrícula e senha diretamente nos ajustes de Wi-Fi) não devem redirecionar para portais cativos. **Desativar a Conexão Automática:** Os usuários podem desativar a função de "conectar-se automaticamente"às redes públicas. Isso força

o usuário a escolher manualmente a rede a cada vez, aumentando a chance de perceber algo suspeito.

5.2 Sugestões para Trabalhos Futuros

A presente pesquisa abre caminhos para futuras investigações que podem aprofundar o entendimento e a defesa contra ameaças em redes sem fio. Sugere-se:

1. **Análise do Protocolo WPA3:** Investigar a resiliência do protocolo *WPA3*, sucessor do *WPA2*, contra os ataques demonstrados, especialmente em relação à proteção dos quadros de gerenciamento e à autenticação em redes abertas.

2. **Desenvolvimento de um Sistema de Detecção de Intrusos (IDS):** Utilizar microcontroladores como *ESP32* para criar um sistema distribuído e capaz de detectar anomalias na rede, como a presença de Pontos de Acesso Falsos ou ataques de *Deauthentication*, alertando os administradores em tempo real.

3. **Exploração de Vetores de Ataque via Bluetooth:** O *firmware ESP32 Marauder* possui funcionalidades para auditoria em *Bluetooth*. Um trabalho futuro poderia explorar essas capacidades para analisar vulnerabilidades em dispositivos *IoT (Internet of Things)*, fones de ouvido e outros periféricos presentes no ambiente acadêmico.

4. **Estudo de Usabilidade em Segurança:** Realizar um estudo focado na interação humano-computador para avaliar o nível de percepção de risco dos usuários do IFPB. Os resultados poderiam ser utilizados para criar materiais de conscientização mais eficazes e direcionados, com base nas dificuldades e nos equívocos mais comuns observados na comunidade.

Apêndice A

Autorização Institucional

Abaixo segue a comunicação por e-mail que formaliza a autorização para a realização dos testes práticos descritos neste trabalho.

Figura A.1: *Comunicação por e-mail com a autorização para os testes.*

Referências Bibliográficas

[Alabdulatif 2014] ALABDULATIF, X. M. A. *Analysing the EAP-TLS Handshake and the 4-Way Handshake of the 802.11i Standard*. 2014. IEEE Electronic Library (IEL) Journals. Disponível em: <https://infonomics-society.org/wp-content/uploads/ijisr/published-papers/volume-4-2014/Analysing-the-EAP-TLS-Handshake-and-the-4-Way-Handshake-of-the-802-11i-Standard.pdf>. 2, 13, 14

[All Easy 2024] All Easy. *Segurança wireless em instituições de ensino*. 2024. Artigo online. Disponível em: <https://alleasy.com.br/seguranca-wireless-em-instituicoes-de-ensino/>. 1

[Clube do Maker 2024] Clube do Maker. *ESP32 Pinout: Detalhes e Conexões*. 2024. Artigo online. Disponível em: <https://clubedomaker.com/esp32-pinout>. 21

[clubedomaker 2024] clubedomaker. *ESP32 Pinout: Detalhes e Conexões*. 2024. Artigo online. Disponível em: <https://clubedomaker.com/esp32-pinout>, urldate = 2025-09-30. 25

[Diego 2023] DIEGO, H. *Explorando redes com ESP32 Wifi*. 2023. Artigo online. Disponível em: <https://dev.to/higordiego/explorando-redes-com-esp32-wifi-4b09>. 1

[Espressif Systems 2023] Espressif Systems. *ESP32 Series Datasheet*. [S.l.], 2023. Disponível em: <https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf>. 11

[Gast 2005] GAST, M. S. *Redes Sem Fio 802.11: O Guia Definitivo*. 2. ed. Sebastopol, CA: O'Reilly Media, 2005. 12

[(Github) 2025] (GITHUB), A. *CaptivePortal-Esp8266: A simple Captive Portal for ESP8266*. 2025. Repositório de Software. Disponível em: <https://github.com/ADRY4N/CaptivePortal-Esp8266>. 6, 24

[justcallmekoko (Github) 2024] justcallmekoko (Github). *ESP32 Marauder*. 2024. Repositório de Software. Disponível em: <https://github.com/justcallmekoko/ESP32Marauder>. 12

[Kristiyanto 2020] KRISTIYANTO, E. E. Y. *Analysis of Deauthentication Attack on IEEE 802.11 Connectivity Based on IoT Technology Using External Penetration Test*. 2020. Artigo online. Disponível em: <https://journal.binus.ac.id/index.php/commit/article/view/6337/3826>. 12, 13

[Kurose 2017] KUROSE, J. F. *Redes de Computadores e a Internet: Uma Abordagem Top-Down*. 6. ed. São Paulo: Pearson Education do Brasil, 2017. 1

[QianLU *et al.* 2018] QIANLU *et al. Client-Side Evil Twin Attacks Detection Using Statistical Characteristics of 802.11 Data Frames*. 2018. Miscellaneous. Disponível em: <https://

www.jstage.jst.go.jp/article/transinf/E101.D/10/E101.D_2018EDP7030/_article>. 2, 16, 17

[Rahime Belen-Saglam, Vincent Miller, 2023] Rahime Belen-Saglam, Vincent Miller,. *A Systematic Literature Review on Cyber Security Education for Children*. 2023. IEEE Electronic Library (IEL) Journals. Disponível em: <https://ieeexplore-ieee-org.ez291.periodicos.capes.gov.br/stamp/stamp.jsp?tp=&arnumber=10022010>, urldate = 2023. 38

[randomnerdtutorials 2024] randomnerdtutorials. *ESP32: Tela sensível ao toque TFT LCD – 2,8 polegadas ILI9341 240×320 (Arduino IDE)*. 2024. Artigo online. Disponível em: <https://randomnerdtutorials.com/esp32-tft-touchscreen-display-2-8-ili9341-arduino/>. 21

[Rango Dionigi Cristian Lentini 2006] RANGO DIONIGI CRISTIAN LENTINI, S. M. F. D. *Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i*. 2006. Miscellaneous. Disponível em: <https://doi.org/10.1155/WCN/2006/47453>. 2, 13, 14

[Shrivastava Mohd Saalim Jamal 2020] SHRIVASTAVA MOHD SAALIM JAMAL, K. K. P. *EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WiFi*. 2020. IEEE Electronic Library (IEL) Journals. Disponível em: <https://ieeexplore-ieee-org.ez291.periodicos.capes.gov.br/stamp/stamp.jsp?tp=&arnumber=8989802>. 39

[Zurutuza Roberto Uribeetxeberria 2008] ZURUTUZA ROBERTO URIBEETXEBERRIA, M. F. U. *Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i*. 2008. Miscellaneous. Disponível em: <https://www.researchgate.net/publication/4339361_Beacon_Frame_Spoofing_Attack_Detection_in_IEEE_80211_Networks>. 2, 15, 16