v7.n10.2026

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

RESISTÊNCIA DE SENHAS EM REDES WPA2-PSK: ANÁLISE EXPERIMENTAL DE ATAQUES OFFLINE COM CPU E GPU

PASSWORD RESISTANCE IN WPA2-PSK NETWORKS: AN EXPERIMENTAL ANALYSIS OF OFFLINE ATTACKS USING CPU AND GPU

RESISTENCIA DE CONTRASEÑAS EN REDES WPA2-PSK: ANÁLISIS EXPERIMENTAL DE ATAQUES FUERA DE LÍNEA CON CPU Y GPU

Igor de Mello Santos[1], João Henrique Gião Borges[2]

e7109322
https://doi.org/10.47820/recima21.v7i10.9322

PUBLICADO: 10/2026

RESUMO

Este trabalho analisa as vulnerabilidades do protocolo WPA2 em redes sem fio residenciais, com foco na relação entre a complexidade da senha configurada e o nível de exposição da rede a ataques práticos de descoberta de credenciais. A pesquisa foi conduzida em ambiente de laboratório controlado, utilizando o sistema operacional Kali Linux e as ferramentas aircrack-ng e Hashcat para capturar o 4-way *handshake* e o PMKID de um ponto de acesso dedicado, e posteriormente aplicar ataques de dicionário e de força bruta por máscara sobre doze cenários de senha com padrões e comprimentos distintos. Os resultados mostraram que senhas previsíveis, presentes em listas de vazamentos conhecidas, foram comprometidas em poucos segundos, independentemente do uso de CPU ou GPU no processamento, enquanto senhas longas e sem relação com dados pessoais não foram identificadas durante os testes de dicionário realizados. Observou-se ainda que o custo computacional de um ataque exaustivo cresce de forma exponencial a cada dígito adicionado à senha, nas condições computacionais avaliadas, o tempo estimado para percorrer integralmente o espaço de busca de senhas numéricas com 11 dígitos ou mais aumentou substancialmente, ultrapassando a duração operacional estabelecida para os ensaios. Conclui-se que a segurança de uma rede WPA2-PSK depende, sobretudo, da escolha do usuário quanto à senha, uma vez que características estruturais do protocolo, como a possibilidade de forçar a captura do *handshake* e a exposição do PMKID, tornam qualquer senha previsível vulnerável a ataques *offline* realizados com ferramentas gratuitas e *hardware* doméstico.

PALAVRAS-CHAVE: WPA2-PSK. Segurança de Redes Wi-Fi. Ataque de Força Bruta. Entropia de Senhas. Processamento Gráfico.

ABSTRACT

This paper analyzes the vulnerabilities of the WPA2 protocol in residential wireless networks, focusing on the relationship between configured password complexity and the network's exposure to practical credential-discovery attacks. The research was conducted in a controlled laboratory environment, using the Kali Linux operating system and the aircrack-ng and Hashcat tools to capture the 4-way handshake and the PMKID of a dedicated access point, and subsequently applying dictionary and mask-based brute-force attacks across twelve password scenarios with distinct patterns and lengths.

[1] Graduando em Engenharia da Computação pelo Centro Universitário de Araraquara (UNIARA).
[2] Professor orientador do curso de Engenharia da Computação do Centro Universitário de Araraquara (UNIARA).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

The results showed that predictable passwords, present in known leaked password lists, were compromised within seconds, regardless of whether CPU or GPU was used for processing, while long passwords unrelated to personal data were not identified during the dictionary tests performed. It was also observed that the computational cost of an exhaustive attack grows exponentially with each additional digit in the password; under the evaluated computational conditions, the estimated time to fully traverse the search space for numeric passwords of 11 digits or more increased substantially, exceeding the operational duration established for the trials. It is concluded that the security of a WPA2-PSK network depends, above all, on the user's password choice, since structural characteristics of the protocol, such as the possibility of forcing handshake capture and PMKID exposure, make any predictable password vulnerable to offline attacks carried out with free tools and consumer-grade hardware.

***KEYWORDS**: WPA2-PSK. Wi-Fi Network Security. Brute Force Attack. Password Entropy. Graphics Processing.*

RESUMEN

Este trabajo analiza las vulnerabilidades del protocolo WPA2 en redes inalámbricas residenciales, centrándose en la relación entre la complejidad de la contraseña configurada y el nivel de exposición de la red a ataques prácticos de descubrimiento de credenciales. La investigación se llevó a cabo en un entorno de laboratorio controlado, utilizando el sistema operativo Kali Linux y las herramientas aircrack-ng y Hashcat para capturar el 4-way handshake y el PMKID de un punto de acceso dedicado, y posteriormente aplicar ataques de diccionario y de fuerza bruta mediante máscara sobre doce escenarios de contraseña con patrones y longitudes distintos. Los resultados mostraron que las contraseñas predecibles, presentes en listas de filtraciones conocidas, fueron comprometidas en pocos segundos, independientemente del uso de CPU o GPU en el procesamiento, mientras que las contraseñas largas y sin relación con datos personales no fueron identificadas durante las pruebas de diccionario realizadas. Se observó además que el costo computacional de un ataque exhaustivo crece de forma exponencial con cada dígito adicional en la contraseña; en las condiciones computacionales evaluadas, el tiempo estimado para recorrer por completo el espacio de búsqueda de contraseñas numéricas de 11 dígitos o más aumentó sustancialmente, superando la duración operativa establecida para los ensayos. Se concluye que la seguridad de una red WPA2-PSK depende, sobre todo, de la elección de la contraseña por parte del usuario, ya que características estructurales del protocolo, como la posibilidad de forzar la captura del handshake y la exposición del PMKID, hacen que cualquier contraseña predecible sea vulnerable a ataques offline realizados con herramientas gratuitas y hardware doméstico.

***PALABRAS CLAVE**: WPA2-PSK. Seguridad de Redes Wi-Fi. Ataque de Fuerza Bruta. Entropía de Contraseñas. Procesamiento Gráfico.*

INTRODUÇÃO

As redes locais sem fio, amplamente conhecidas pela tecnologia Wi-Fi, estão presentes em ambientes residenciais, empresariais e públicos (BOSSO; WANDERLEY; ANTUNES NETO, 2024). Nesse contexto, o protocolo WPA2 (Wi-Fi Protected Access 2) se tornou o padrão de segurança mais comum em roteadores residenciais. Apesar de seus mecanismos de proteção, o WPA2-PSK apresenta limitações de segurança relacionadas, entre outros fatores, à

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

possibilidade de verificação offline de candidatos a senha após a obtenção de determinados elementos de autenticação, o que representa um risco real aos usuários da rede. O atacante pode explorar muito mais do que só a senha da rede, podendo ter acesso aos dados e à privacidade de todos os dispositivos conectados.

O acesso não autorizado a uma rede sem fio pode gerar problemas que não se limitam só ao uso da conexão de forma ilegal. A partir dele, torna-se possível a interceptação de tráfego não protegido e a varredura de dispositivos conectados, etapas que podem preceder a exploração de serviços vulneráveis e, em cenários mais graves, o comprometimento de dados pessoais ou bancários armazenados em aplicações não devidamente protegidas, mesmo assim, muitos usuários não sabem que essas consequências podem ocorrer e por facilidade ou falta de informação, deixam suas redes com senhas fracas e fáceis de atacar (CERT.br, 2012). Esse desalinhamento entre o risco real e a percepção dos usuários é o principal motivo para investigar o problema com mais precisão.

Esta pesquisa busca analisar as vulnerabilidades do protocolo WPA2 em redes residenciais, fazendo todos os processos em ambiente controlado e usando as técnicas mais utilizadas para descoberta de senhas. O objetivo principal é entender os pontos que deixam uma rede mais ou menos vulnerável a esses tipos de ataques e indicar caminhos claros para diminuir a probabilidade de ser exposto.

A importância do trabalho não é apenas técnica, e sim mostrar de forma documentada como esses ataques funcionam na prática, a fim de que os usuários comuns e pequenas empresas repensem suas práticas de segurança, além de abrir espaço para investigações futuras na área.

A pergunta de pesquisa que se pretende responder é: Como ferramentas acessíveis podem comprometer uma rede com protocolo WPA2 e quais as características da senha impactam no seu nível de segurança? A hipótese inicial é que senhas de baixa complexidade tornarão a rede mais vulnerável a qualquer atacante com conhecimento básico, enquanto senhas longas e complexas fazem com que o processo se torne mais difícil e o custo computacional alto, resultando em ataques inviáveis. Os experimentos realizados fornecem dados importantes para a análise dos resultados.

A metodologia utilizada no estudo caracteriza-se como pesquisa experimental, exploratória e quantitativa, acompanhada de análise técnica descritiva dos processos envolvidos nos ataques. Os experimentos foram realizados com o sistema operacional Kali Linux e o conjunto de ferramentas aircrack-ng. Dessa forma, o trabalho segue algumas etapas específicas, como, montar um laboratório de testes funcional, capturar *handshakes* de rede, aplicar ataques

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

de força bruta e por dicionário com o Hashcat, e estruturar os padrões de senha que têm mais vulnerabilidades. Ainda que os procedimentos de ataque por dicionário e por força bruta, bem como o uso de CPU e GPU para o processamento de candidatos, sejam amplamente discutidos na literatura de Segurança da Informação, a contribuição original deste trabalho está na organização experimental proposta, na comparação direta de desempenho entre os dois tipos de processamento e na análise quantitativa dos resultados obtidos no ambiente laboratorial especificado.

1. REFERENCIAL TEÓRICO

Esta Seção apresenta os conceitos fundamentais sobre segurança em redes sem fio, com ênfase no protocolo WPA2, suas vulnerabilidades estruturais e as principais técnicas utilizadas em ataques de descoberta de senhas, abordando também as ferramentas utilizadas nos testes práticos e os critérios que determinam o grau de resistência de uma rede a esses ataques.

1.1. Redes sem fio

1.1.1. Conceitos

Redes sem fio, também conhecidas como redes Wi-Fi, são infraestruturas de comunicação que permitem transmitir dados entre aparelhos eletrônicos sem o uso de cabos físicos, utilizando ondas de rádio como meio de propagação (FERNANDEZ, 2015). Em uma WLAN um ponto de acesso (Access Point — AP) é o que cria e gerencia a rede, enquanto os dispositivos dos usuários se conectam a ele para ter acesso à internet. Apesar de essa tecnologia ser hoje uma das formas mais comuns de conexão em casas e empresas, o fato de o sinal sem fio se propagar de forma aberta no ambiente alcançando qualquer dispositivo próximo, faz com que as comunicações fiquem expostas a riscos de segurança sem as proteções adequadas (VILELA, 2014).

1.1.2. Padrão IEEE 802.11

Segundo Moraes *et al.* (2024), o padrão IEEE 802.11 mostra todas as especificações técnicas para redes locais sem fio (WLAN), desde sua criação esse padrão vem tendo atualizações importantes com melhorias de segurança, nas frequências de operação e nas velocidades de transmissão, tornando as redes de Wi-Fi mais rápidas e eficientes. As principais versões são:

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

802.11b, Wi-Fi 1 (2,4 GHz, até 11 Mbps);
802.11a, Wi-Fi 2 (5 GHz, até 54 Mbps);
802.11g, Wi-Fi 3 (2,4 GHz, até 54 Mbps);
802.11n, Wi-Fi 4 (2,4/5 GHz, até 600 Mbps);
802.11ac, Wi-Fi 5 (5 GHz, até 6.93 Gbps);
802.11ax, Wi-Fi 6 (2,4/5 GHz, até 9.6 Gbps).

É importante observar que as denominações 'Wi-Fi 1' a 'Wi-Fi 6' correspondem a uma nomenclatura comercial adotada pela Wi-Fi Alliance a partir de 2018, aplicada retroativamente aos padrões mais antigos (802.11b, a, g, n e ac) e de forma paralela ao lançamento do 802.11ax. As designações técnicas do IEEE permanecem como a referência primária para identificação formal de cada versão do protocolo.

As redes com faixas de 2,4 GHz e 5 GHz são bem diferentes, a de 2,4 GHz é a mais usada por ter maior alcance e pode passar melhor por paredes e obstáculos, porém tem mais interferências de outros aparelhos, já a de 5 GHz foi criada para diminuir essas interferências causadas por obstáculos da faixa 2,4 GHz, oferecendo maior conectividade e menos interferência, tendo velocidades maiores, mas com menor alcance (MORAES *et al.*, 2024). No contexto desta pesquisa o adaptador de rede utilizado opera apenas em 2,4 GHz, o que limitou os testes a redes configuradas somente nessa faixa. É importante destacar que a operação em 2,4 GHz ou 5 GHz não determina, isoladamente, a resistência de uma senha a ataques offline, uma vez que essa resistência depende das características da credencial, e não da frequência de operação da rede.

1.2. Protocolo WPA2

1.2.1. Arquitetura e Modos de Operação

O WPA2 pode funcionar em dois modos de segurança, Pessoal (WPA2-PSK) e Empresarial (WPA2-EAP — Extensible Authentication Protocol), ambos utilizam o Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) que verifica a integridade e autenticidade da mensagem. No modo Pessoal uma senha PSK (Pre-Shared Key) é configurada no roteador e usada por todos os aparelhos da rede, esse é o modo mais comum em casas, por ser mais simples de configurar (KASPERSKY, 2021). No modo Empresarial a autenticação é feita por meio do protocolo 802.1X, com o suporte de um servidor Remote Authentication Dial-In User Service (RADIUS) que checa as credenciais de cada usuário, dando mais controle e segurança no acesso à rede (SANTOS, 2012). Este trabalho foca no modo Pessoal, por ser o mais usado em redes domésticas e o mais vulnerável aos tipos de ataques.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

1.2.2. PBKDF2 e Derivação de Chave

A senha que o usuário configura não é usada diretamente na criptografia, no WPA2-PSK, a senha e o Service Set Identifier (SSID) da rede são processados por uma função de derivação de chave baseada em senha, PBKDF2 com HMAC-SHA1, que faz 4096 iterações de hash sobre essa combinação da senha para criar a PMK (Pairwise Master Key), uma chave de 256 bits que é usada como base para garantir a segurança em todo o momento que está conectado à rede (MACÊDO, 2008). Esse processo faz o uso de salt e de muitas iterações para tornar a senha mais segura, foi criada para tornar ataques de força bruta computacionalmente mais custosos, porém quando o *handshake* de quatro vias é capturado, o atacante pode repetir o mesmo processo de derivação de forma *offline*, testando conjuntos de senhas sem necessidade de novas interações com a rede (MACÊDO, 2008).

1.2.3. 4-Way *Handshake*

O 4-way *handshake* é o processo onde o cliente e ponto de acesso (AP) estabelecem as chaves de sessão a partir da PMK após a autenticação, permitindo que os dois lados estejam compartilhando o mesmo segredo antes de iniciar a troca de dados (FRANÇA NETO; SOUZA; GONÇALVES, 2011). O processo ocorre em quatro mensagens trocadas entre eles, durante o processo é derivado o conjunto de chaves PTK (Pairwise Transient Key), somente para a comunicação unicast entre cliente e AP, e distribuída a GTK (Group Temporal Key), usada para tráfego broadcast e multicast (FRANÇA NETO; SOUZA; GONÇALVES, 2011). Os elementos de autenticação registrados podem permitir a verificação offline de candidatos à senha, mediante reprodução das operações criptográficas necessárias à comparação com os valores capturados, o que pode ser feito colocando a placa de rede em modo monitor durante o processo de autenticação de um cliente (FRANÇA NETO; SOUZA; GONÇALVES, 2011). Nos testes realizados neste trabalho, a captura foi feita com o uso da ferramenta airodump-ng sobre a interface wlan1 configurada em modo monitor.

1.3. Ataques a redes WPA2

1.3.1. Captura de *Handshake*

Segundo Nascimento (2025), o ataque de captura de *handshake* consiste em ativar a placa de rede em modo monitor para capturar o 4-way *handshake* trocado entre um cliente e o AP durante o processo de autenticação. Para acelerar a captura, o atacante pode enviar ataques de desautenticação (*deauth*) forjados, fazendo com que o cliente tenha que se reconectar,

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

consequentemente gerando um novo *handshake* capturável. Neste trabalho, a captura foi realizada com airodump-ng, e os quadros de desautenticação foram enviados com aireplay-ng (NASCIMENTO, 2025). Com o *handshake* capturado os ataques *offline* de descoberta de senha podem ser realizados.

1.3.2. Ataque por Dicionário

O ataque por dicionário consiste no teste contínuo e sistemático de senhas em uma lista pré-compilada contra o hash do *handshake* capturado (NASCIMENTO, 2025). O sucesso do ataque depende da qualidade da lista utilizada e da complexidade da senha alvo, se a senha for muito complexa, o ataque pode ser concluído sem sucesso. Neste trabalho, a quebra do hash foi realizada utilizando a ferramenta aircrack-ng com o parâmetro -w, apontando para a *wordlist* rockyou.txt, o que permitiu a comparação automatizada dos valores da lista contra o MIC (Message Integrity Code) que estava no *handshake* até a descoberta da senha correta (NASCIMENTO, 2025).

1.3.3. Ataque de Força Bruta por Máscara

O ataque de força bruta por máscara gera e testa todas as combinações de senhas possíveis dentro de um padrão definido (HEIDERSCHEIDT; SILVA; URIARTE, 2022). No Hashcat, o modo -a 3 permite definir máscaras como ?d?d?d?d?d?d?d?d para senhas numéricas de oito dígitos, um padrão comum em roteadores residenciais configurados com número de CPF, data de nascimento ou número de telefone. Os testes realizados neste trabalho demonstram que esse espaço de busca de senha pode ser concluído em tempos curtos, mostrando a vulnerabilidade crítica de senhas que contêm somente números.

1.3.4. Ataque PMKID — *Clientless*

O PMKID é um identificador retirado a partir do Pairwise Master Key (PMK), que é incluído nas informações do Robust Security Network (RSN) de quadros EAPOL trocados entre cliente e ponto de acesso em redes WPA/WPA2. Em ataques de dicionário baseados em PMKID, é possível analisar esse campo para realizar a quebra de senhas sem precisar capturar todo o 4-way *handshake*, a partir de um quadro tendo o PMKID, o atacante pode calcular valores de chave pré-compartilhada (PSK), derivar a PMK e recomputar o PMKID até encontrar uma resposta, sendo conhecido como um ataque *clientless* executado de forma totalmente *offline* (OLIVEIRA, 2025). A disponibilidade desse identificador e a viabilidade da técnica dependem das características e configurações do ponto de acesso, não sendo possível pressupor que todas

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

as redes WPA2-PSK o exponham em condições equivalentes. Nesta pesquisa, essa técnica foi usada, utilizando a ferramenta hcxdumptool para captura dos quadros e extração do PMKID, seguido da conversão para o formato hc22000 com o hcxpcapngtool, permitindo o processamento dos hashes resultantes no Hashcat.

1.4. Ferramentas de auditoria

1.4.1. Kali Linux

Segundo Moreno (2016), o Kali Linux é uma distribuição do sistema operacional Linux, projetada especificamente para testes de penetração e auditorias de segurança. Sua principal característica é que o sistema operacional já vem com diversas ferramentas de segurança ofensiva, tirando a necessidade de instalação e configuração manual de cada uma. O Kali Linux serviu como ambiente base para a execução de todos os testes realizados.

1.4.2. Suíte Aircrack-ng

O aircrack-ng é um conjunto de ferramentas de código aberto com o intuito de realizar auditorias a redes sem fio, muito utilizada em pesquisas de segurança para capturar pacotes e testar a confiabilidade de algoritmos criptográficos (NASCIMENTO, 2025). Três ferramentas da suíte foram utilizadas neste trabalho:

- airmon-ng: responsável por habilitar o modo monitor na placa de rede, permitindo a captura de quadros sem estar conectado a nenhuma rede.
- airodump-ng: utilizado para fazer varredura de redes disponíveis e captura do 4-way *handshake* transmitido durante o processo de autenticação de clientes.
- aireplay-ng: usado para o envio de quadros de desautenticação, forçando o cliente a se reconectar com a rede e gerando uma nova captura de *handshake* (NASCIMENTO, 2025).

1.4.3. Adaptador TP-Link TL-WN722N

Para fazer todos os testes, foi preciso uma placa de rede com suporte a modo monitor e injeção de pacotes, funcionalidades não disponíveis na configuração utilizada da interface de rede interna do notebook. Para conseguir realizar os testes, foi utilizado o adaptador externo TP-Link TL-WN722N 150 Mbps. O adaptador opera na faixa de 2,4 GHz e para o uso do modo monitor, foi utilizada uma versão com um chipset compatível com as ferramentas da suíte aircrack-ng no Kali Linux (OLIVEIRA, 2025). Essa limitação técnica limitou os testes a redes

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

operando somente em 2,4 GHz, já que redes na frequência de 5 GHz ficam fora do alcance do adaptador.

1.4.4. Hashcat

O Hashcat é uma ferramenta de descoberta de senhas por força bruta e dicionário, conhecida como uma das melhores ferramentas para esse fim (HEIDERSCHEIDT; SILVA; URIARTE, 2022). O funcionamento da ferramenta baseia-se na geração e verificação de candidatos a senha mediante processamento de dados criptográficos obtidos nos ensaios, utilizando a GPU para acelerar o processo. O Hashcat foi utilizado para processar os *handshakes* capturados em modo dicionário -a 0 com a *wordlist* rockyou.txt. Os testes de força bruta por máscara numérica -a 3 foram aplicados em cenários de comprimento crescente e são detalhados na Seção 2.4, mostrando um custo computacional alto para senhas de maior complexidade mesmo sendo o protocolo WPA2.

1.5. Senhas e entropia

1.5.1. Conceito de entropia em senhas

Em segurança da informação, a entropia mensura o nível de complexidade e resistência de uma senha, quanto maior a entropia, mais difícil é descobrir por ataques de quebra de senha (HEIDERSCHEIDT; SILVA; URIARTE, 2022). É importante destacar que essa estimativa matemática do espaço de busca ($H = \log_2(N)$, em que N representa o número total de combinações possíveis) descreve uma condição idealizada, na qual todos os candidatos têm igual probabilidade de serem testados. Senhas criadas por usuários reais frequentemente seguem padrões, reutilizações e distribuições não uniformes, de modo que o tamanho teórico do espaço de busca não equivale necessariamente à resistência prática da senha contra estratégias de adivinhação orientadas por padrões. A entropia é calculada com base no tamanho da senha e no tamanho do alfabeto utilizado, uma senha numérica de oito dígitos possui apenas 10^8 (100 milhões) de combinações possíveis, considerando a taxa de processamento observada nos ensaios deste estudo (aproximadamente 50.848 tentativas por segundo), o tempo necessário para testar integralmente esse espaço de busca seria de aproximadamente 32,8 minutos, podendo variar conforme o hardware e a estratégia de processamento utilizados, já uma senha alfanumérica de oito caracteres com letras maiúsculas, minúsculas, números e símbolos pode apresentar um espaço de busca superior a 10^{15} combinações, nessas condições, e considerando os recursos computacionais utilizados neste estudo, o ataque exaustivo se torna

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

computacionalmente custoso, ainda que equipamentos com maior capacidade de processamento possam reduzir esse tempo.

1.5.2. Padrões de senha e vulnerabilidade

Em termos de comportamento, grande parte dos usuários utiliza senhas simples e pessoais com um padrão fácil de prever, como datas de nascimento, sequências numéricas simples, nomes próprios e palavras comuns reduzindo muito o espaço de busca mesmo quando o comprimento da senha seria o suficiente (RANDEL *et al.*, 2024). No contexto de redes Wi-Fi domésticas brasileiras, é comum o uso de senhas baseadas em CPF, número de telefone ou data de nascimento, todas com aproximadamente oito a onze dígitos numéricos. Os testes realizados confirmam essa vulnerabilidade, senhas totalmente numéricas de oito dígitos foram descobertas rapidamente, enquanto senhas alfanuméricas resistiram a muitas tentativas.

1.5.3. Boas práticas

Segundo Lima (2023), é recomendado o uso de senhas com comprimento mínimo de 12 caracteres, evitando informações pessoais na senha e buscando sempre maior complexidade, usando letras maiúsculas e minúsculas, números e caracteres especiais. Essas medidas podem aumentar o esforço computacional necessário à descoberta de credenciais, reduzindo a eficácia de estratégias baseadas em candidatos previsíveis, como ataques de dicionário ou força bruta.

2. METODOLOGIA

Esta seção descreve os procedimentos experimentais adotados para analisar as vulnerabilidades do protocolo WPA2, incluindo a configuração do ambiente de testes, a definição dos cenários de senha e a execução de cada técnica de ataque.

2.1. Configuração do ambiente de testes

O ambiente de testes foi estruturado de forma controlada, com equipamentos dedicados exclusivamente a essa finalidade, com o objetivo de reduzir a possibilidade de impacto em redes ou dispositivos de terceiros presentes nas proximidades. O ambiente contou com os seguintes recursos:

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

a) Sistema operacional: Kali Linux (versão 2026.2), instalado diretamente no hardware em um notebook processador AMD Ryzen 5 4600H e placa de vídeo integrada AMD Radeon Vega;

b) Adaptador de rede externo: TP-Link TL-WN722N v2/v3, baseado no chipset Realtek RTL8188EUS, utilizando o driver 8188eu (versão 5.3.9_28540.20180627), conectado via USB à interface wlan1. Esse adaptador tem suporte ao modo monitor e injeção de pacotes, recursos ausentes na placa de rede interna do notebook (wlan0, Realtek RTL8821CE);

c) Ponto de acesso: roteador doméstico modelo GPT-2741GNAC-N1 (firmware BR_g8.10_1.11(WVK.0)b46), dedicado aos testes, configurado com o protocolo WPA2-PSK na frequência de 2,4 GHz e operando com o SSID "LABORATORIO IGOR";

d) Dispositivo cliente: *smartphone* utilizado para simular conexões legítimas à rede, viabilizando a geração e a captura de *handshakes* durante os testes.

e) Ferramentas de ataque: aircrack-ng (versão 1.7) e Hashcat (versão v7.1.2), utilizadas nos procedimentos de captura e quebra criptográfica descritos nas Seções 2.3 e 2.4.

A utilização de um ponto de acesso dedicado e a filtragem dos ataques de desautenticação por BSSID e canal específicos (Seção 2.3) tiveram como objetivo reduzir a possibilidade de que esses procedimentos afetassem dispositivos externos ao ambiente de experimentos, ainda que não seja possível garantir ausência completa de interferência em redes próximas operando no mesmo canal. Para cada cenário de teste, a senha do ponto de acesso foi reconfigurada e o processo de captura e ataque foi reiniciado do zero.

Foi executado o comando airmon-ng check kill, para identificar e encerrar processos que poderiam influenciar a interface de rede no modo monitor. Com isso o processo wpa_supplicant (PID 872) foi encerrado antes da ativação do modo monitor.

Em seguida foi utilizado o comando iwconfig, para checar as interfaces de rede que estão ativas. Foram identificadas duas interfaces: wlan0 (placa interna, Tx-Power=30 dBm) e wlan1 (TP-Link externo, Tx-Power=20 dBm), as duas inicialmente em modo Managed.

2.2. Definição dos cenários de teste

A análise foi dividida em seis cenários com padrões de senhas variados, com o intuito de tornar a análise mais objetiva e clara. A seleção buscou representar padrões comuns em redes residenciais brasileiras, como sequências numéricas, palavras de vocabulário usadas no dia a dia e combinações de nomes com números (RANDEL *et al.*, 2024).

No Quadro 1 os cenários C1 a C4 representam padrões de senha com grande probabilidade de estarem em listas de senhas compiladas a partir de vazamentos reais. Por outro

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

lado, os cenários C5 e C6 foram definidos como referência para senhas de maior complexidade, diminuindo as chances de aparecerem em *wordlists*.

Além dos padrões testados no primeiro grupo (Quadro 1), foi definido um segundo grupo, focado em senhas estritamente numéricas com comprimento crescente, com o objetivo de avaliar o crescimento do espaço de busca e o custo computacional do ataque de força bruta por máscara conforme a entropia da senha aumenta (Seção 1.5.1). Ao contrário do experimento baseado em *wordlist*, estes cenários foram submetidos a um ataque de máscara exaustivo com o Hashcat, permitindo a comparação do desempenho entre CPU e GPU.

Na Tabela 1, os cenários C7 e C8 abrangem padrões numéricos curtos, mais comuns em documentos pessoais (CEP e RG). Os cenários C9 e C10 apresentam padrões de maior comprimento, como telefone e CPF. Por fim, os cenários C11 e C12 não correspondem a nenhum documento pessoal específico, servindo apenas de referência para analisar a continuidade do padrão de crescimento exponencial do espaço de busca. Em síntese, o primeiro grupo de cenários (C1 a C6) avalia principalmente a vulnerabilidade da senha ao conteúdo de uma lista específica de credenciais vazadas, enquanto o segundo grupo (C7 a C12) examina o crescimento combinatório do espaço de busca sob um conjunto restrito de caracteres numéricos.

2.3. Captura de *Handshake* e PMKID

Com o ambiente de testes configurado, a etapa seguinte consistiu em capturar o tráfego necessário para realizar os ataques *offline* de descoberta de senha, tanto pela via do 4-way *handshake* quanto pelo PMKID, conforme descrito na Seção 1.3.

Para isso, o adaptador externo TP-Link TL-WN722N foi colocado em modo monitor por meio do comando airmon-ng start wlan1, funcionalidade não disponível na placa de rede interna do *notebook* (wlan0). A ativação foi confirmada via iwconfig, que passou a mostrar a interface wlan1 operando em Mode:Monitor na frequência correspondente ao canal do ponto de acesso alvo, sem interferir na interface wlan0, mantida em modo Managed.

Em seguida, foi realizada uma varredura geral com airodump-ng wlan1 para localizar, entre as diversas redes vizinhas presentes no ambiente real de testes, o ponto de acesso de laboratório "LABORATORIO IGOR", identificado pelo BSSID (Basic Service Set Identifier) C0:3D:D9:C0:E4:30, operando no canal 11 sob protocolo WPA2 com cifra CCMP. Identificado o alvo, a captura foi filtrada especificamente para esse BSSID e canal, por meio dos parâmetros --bssid e -c 11, concentrando o monitoramento no tráfego trocado entre o AP e o dispositivo cliente conectado (STATION 10:3D:0A:CC:90:9B), como mostra a Figura 1.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Para acelerar a geração do *handshake*, foram enviados quadros de desautenticação forjados com o aireplay-ng contra o cliente conectado, forçando sua reconexão à rede e, consequentemente, uma nova troca das quatro mensagens do *handshake* (NASCIMENTO, 2025). A Figura 2 confirma a captura bem-sucedida: o cabeçalho do airodump-ng passa a exibir a informação "WPA *handshake*: C0:3D:D9:C0:E4:30", e a coluna Notes indica "EAPOL" para o cliente que teve os quadros de autenticação capturados, evidenciando que os dados necessários para o ataque *offline* já estavam disponíveis.

Além do *handshake* tradicional, a técnica de captura de PMKID descrita na Seção 1.3.4 também foi aplicada ao ambiente de laboratório, com o uso da ferramenta hcxdumptool para extração do identificador diretamente dos quadros EAPOL, dispensando a necessidade de forçar a reconexão de um cliente já associado. Os quadros capturados foram convertidos para o formato hc22000 por meio do hcxpcapngtool, permitindo o processamento posterior no Hashcat da mesma forma que os *handshakes* capturados via airodump-ng.

2.4. Quebra criptográfica (dicionário e máscara)

Com os *handshakes* capturados para cada um dos seis cenários de senha definidos no Quadro 1, foram aplicadas duas técnicas de quebra criptográfica *offline*: o ataque por dicionário e o ataque de força bruta por máscara, conforme descrito nas Seções 1.3.2 e 1.3.3.

Para o ataque por dicionário, cada *handshake* foi processado com a ferramenta aircrack-ng, utilizando o parâmetro -w apontado para a *wordlist* rockyou.txt, contendo 14.344.393 senhas compiladas a partir de vazamentos reais. O processo consiste em testar sequencialmente cada entrada da lista contra o MIC do *handshake* capturado, até encontrar uma correspondência ou esgotar a lista por completo. Em paralelo, o mesmo ataque por dicionário foi executado utilizando o Hashcat em modo -a 0, processando os handshakes na GPU integrada, permitindo a comparação de desempenho entre CPU e GPU para os cenários C1 a C6. Cabe ressaltar que essa comparação apresenta uma limitação metodológica: o processamento via CPU foi realizado com o aircrack-ng, enquanto o processamento via GPU utilizou o Hashcat. Dessa forma, os resultados obtidos não isolam exclusivamente a influência do dispositivo de processamento, podendo refletir também diferenças de implementação entre as duas ferramentas. Os resultados devem ser interpretados como uma comparação entre duas configurações de processamento e não como demonstração isolada de superioridade de hardware.

Os dados obtidos revelaram uma diferença significativa no tempo de quebra entre os cenários. A senha do cenário C1 (senha "12345678") foi quebrada de forma quase imperceptível, checando apenas 87 chaves do volume total da *wordlist*, como ilustra a Figura 3, evidenciando

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

que sequências numéricas simples frequentemente ficam entre as primeiras posições em *wordlists* de senhas vazadas.

Por outro lado, os cenários C5 (senha "Pedro2026") e C6 (senha "2l@dIZXg") não foram quebrados pelo ataque de dicionário, mesmo após o esgotamento completo da *wordlist* rockyou.txt, decorridos aproximadamente 14 minutos e 30 segundos de processamento, como ilustra a Figura 4, referente ao cenário C6.

O resultado confirma que senhas sem histórico de vazamentos reduzem drasticamente a eficácia do ataque por dicionário, mesmo com uma estrutura previsível como nome próprio associado a um ano recente (C5).

Diferentemente do ataque por dicionário, a força bruta por máscara gera e valida sistematicamente todas as combinações possíveis dentro de um padrão predefinido, sem depender de qualquer suposição sobre o conteúdo da senha (HEIDERSCHEIDT; SILVA; URIARTE, 2022). No Hashcat, o parâmetro? d representa um dígito numérico (0-9), de modo que uma máscara com n símbolos? d cobre um espaço de busca de exatamente 10^n combinações, refletindo o conceito de entropia numérica discutido na Seção 1.5.1.

Dessa forma, os cenários C7 a C12, definidos na Tabela 1, cujos comprimentos variam de 8 a 13 dígitos, permitiram observar de forma prática o crescimento exponencial do espaço de busca à medida que cada dígito adicional é inserido na senha. O cenário C7, configurado com 8 dígitos, teve a senha quebrada com sucesso em pouco mais de um minuto, conforme ilustra a Figura 5.

A execução do ataque por máscara utilizou o Hashcat operando em modo -a 3 (máscara), utilizando o *kernel* puro da ferramenta para paralelizar a geração e o teste de candidatos na GPU. Cada combinação passou pelo mesmo processo de derivação PBKDF2-HMAC-SHA1 detalhado na Seção 1.2.2. Por se tratar de uma função de hash internamente custosa e projetada com milhares de iterações por tentativa, o custo computacional do ataque cresceu de forma proporcional ao tamanho do espaço de busca, inviabilizando a conclusão dos testes para os cenários de maior comprimento dentro de um tempo razoável de execução. Diante dessas limitações, os testes foram interrompidos após a velocidade de processamento (H/s) se estabilizar. Essa dinâmica permitiu que o próprio Hashcat calculasse a estimativa de tempo necessário para esgotar o espaço de busca, sem a necessidade de aguardar a conclusão completa do ataque, processo já utilizado anteriormente na Seção 1.4.4. O caso mais crítico, apresentado pelo cenário C12 (13 dígitos), teve o tempo estimado de conclusão em mais de seis anos, como ilustra a Figura 6, evidenciando a inviabilidade computacional de ataques de força bruta contra senhas numéricas longas.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Cada cenário foi executado uma única vez, e os tempos registrados correspondem diretamente aos valores fornecidos pelas próprias ferramentas (aircrack-ng e Hashcat) ao término ou interrupção de cada ataque. A ausência de repetições impede a avaliação da variabilidade das medições entre execuções, constituindo uma limitação reconhecida deste estudo.

Os tempos de execução registrados, tanto para os cenários C1 a C6 (comparando CPU e GPU no mesmo ataque de dicionário) quanto para os cenários C7 a C12 (demonstrando o crescimento exponencial do custo computacional a cada dígito adicionado), são detalhados e analisados no capítulo 3.

3. RESULTADOS E DISCUSSÃO

Este capítulo apresenta a análise dos dados obtidos nos experimentos descritos no Capítulo 2. A discussão foca na comparação de desempenho do *hardware*, na eficácia dos ataques conforme o tipo de senha e nas limitações observadas durante os testes.

3.1. CPU vs iGPU

Com os *handshakes* dos cenários C1 a C6 processados tanto pelo aircrack-ng (CPU, Ryzen 5 4600H) quanto pelo Hashcat (GPU integrada Radeon Vega), foi possível comparar diretamente o desempenho dos dois dispositivos no mesmo ataque por dicionário, utilizando a mesma *wordlist* rockyou.txt em ambas as ferramentas. A Tabela 2 apresenta os tempos e as velocidades de processamento obtidos em cada dispositivo.

Os resultados mostram que a GPU processou, em média, entre 2,5 e 4,5 vezes mais chaves por segundo que a CPU (por exemplo, no cenário C4, 49.896 H/s contra 17.778 H/s), reduzindo proporcionalmente o tempo necessário para consumir a *wordlist* nos cenários C5 e C6, que não foram quebrados por nenhum dos dois dispositivos. Ainda assim, vale destacar que o resultado final, senha encontrada ou não, foi idêntico entre CPU e GPU em todos os seis cenários, uma vez que esse resultado depende exclusivamente da presença da senha na *wordlist* utilizada, não do *hardware* empregado no processamento.

Um ponto observado durante os testes foi a variação de desempenho da GPU conforme o estado térmico do dispositivo no momento da execução. No cenário C1, por exemplo, a velocidade registrada foi de apenas 24.632 H/s, quase metade da velocidade média dos demais cenários (~50.000 H/s), pois a GPU operava a uma frequência de núcleo mais baixa (400 MHz) no momento da execução, possivelmente por gerenciamento de energia do dispositivo em

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

estado ocioso antes do teste. Esse comportamento evidencia que fatores do *hardware*, como o gerenciamento de energia e a temperatura, também influenciam o tempo real de quebra na prática.

Esses resultados confirmam que, mesmo em *hardware* modesto como uma GPU integrada de *notebook*, o ganho de desempenho em relação à CPU é expressivo. Essa diferença torna os ataques *offline* por dicionário ainda mais acessíveis a atacantes com equipamentos domésticos.

3.2. Eficácia por tipo de senha

A análise de resultados dos doze cenários testados (Quadro 1, Tabelas 1 a 3), demonstra que a vulnerabilidade de uma senha depende mais da sua previsibilidade e presença em listas de vazamentos conhecidas do que apenas do seu comprimento.

Mesmo variando entre 8 e 9 caracteres, os cenários C1 a C6, baseados em padrões como sequência numérica, palavras comuns, datas, apresentaram resultados bem diferentes: os cenários C1 a C4 foram quebrados em poucos segundos tanto na CPU quanto na GPU, enquanto os cenários C5 e C6 não tiveram as senhas identificadas pelo ataque de dicionário, por não constarem na *wordlist* utilizada, mostrando que o comprimento da senha não é garantia de segurança quando o atacante consegue antecipar o padrão utilizado (RANDEL *et al.*, 2024).

Já nos cenários C7 a C12, o objetivo foi isolar a variável de comprimento de senha, mantendo o mesmo padrão (sequência numérica aleatória) e testando somente por ataque de força bruta e eliminando qualquer dependência de suposições sobre o conteúdo da senha. A Tabela 3 detalha o crescimento do tempo necessário para esgotar cada espaço de busca conforme o número de dígitos aumenta. O tempo estimado para os cenários C8 a C12 corresponde ao valor reportado pelo próprio Hashcat no campo 'Time.Estimated' de seu status de execução, calculado internamente pela ferramenta com base no espaço de busca restante e na velocidade de processamento (H/s) observada até o momento da interrupção do ataque.

A variação dos tempos valida, na prática, a progressão exponencial mostrada pela teoria de entropia (Seção 1.5.1). Como a velocidade da GPU ficou estável em praticamente 50.000 H/s em todos os testes, cada dígito adicional multiplica por aproximadamente dez o tempo necessário para a quebra. Essa diferença fica clara no cenário C7 (8 dígitos), quebrado em pouco mais de um minuto, no cenário C12 (13 dígitos), no qual a estimativa exige mais de seis anos de processamento contínuo para ser encontrado, um tempo que nas condições computacionais avaliadas neste estudo, torna o ataque impraticável, podendo ser bastante reduzido com *hardware* de maior capacidade de processamento (Seção 3.4).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Cabe destacar que o tempo registrado no cenário C7 corresponde ao momento em que aquela senha específica foi localizada dentro da sequência de candidatos testada, e não ao tempo necessário para percorrer integralmente as cem milhões de combinações do espaço de busca de oito dígitos. Já os tempos atribuídos aos cenários C8 a C12 são estimativas calculadas pelo próprio Hashcat a partir da velocidade de processamento observada, uma vez que esses ataques foram interrompidos antes da conclusão (Seção 3.4).

A comparação entre os dois grupos de testes revela que a quebra de uma rede WPA2 depende da combinação de dois fatores: a previsibilidade da senha (que determina a vulnerabilidade ao ataque de força bruta) e a entropia/comprimento (que define a resistência à força bruta). Credenciais que combinam comprimento e aleatoriedade, como no cenário C6 ("2l@dIZXg"), demonstram ser mais resistentes a ambos os métodos de ataque dentro do período analisado, reforçando as boas práticas de segurança apresentadas na Seção 1.5.3.

3.3. Limitações do WPA2

Os experimentos realizados demonstram que a principal fragilidade do protocolo WPA2 não está em falhas criptográficas do CCMP ou do PBKDF2 em si, mas na forma como o processo de autenticação depende de uma única chave pré-compartilhada (PSK), configurada manualmente pelo usuário e compartilhada por todos os dispositivos da rede (KASPERSKY, 2021). Após a captura do 4-way *handshake*, o atacante tem todas as informações necessárias para repetir o processo de derivação da PMK de forma totalmente *offline*, sem interagir novamente com o ponto de acesso (MACÊDO, 2008). Essa característica reduz a eficácia de controles preventivos como bloqueio de IP ou limite de tentativas, já que esses mecanismos atuam apenas sobre ataques online, mecanismos detectivos, como sistemas de monitoramento de rede, ainda podem contribuir para identificar indícios de atividade suspeita nas etapas que precedem o ataque *offline*, como o envio de quadros de desautenticação.

Essa dependência da PSK é agravada por duas características estruturais observadas na prática. A primeira é a possibilidade de forçar a captura do *handshake* por meio de quadros de desautenticação, que no padrão IEEE 802.11 não são autenticados nem criptografados, permitindo que qualquer dispositivo próximo derrube a conexão de um cliente legítimo e capture a nova troca de *handshake* gerada na reconexão (NASCIMENTO, 2025). A segunda é a existência do ataque por PMKID, que dispensa até mesmo a presença de um cliente conectado, bastando que o ponto de acesso responda a uma tentativa de associação para expor o identificador necessário ao ataque *offline* (OLIVEIRA, 2025). Em ambos os casos, o atacante

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

não depende de vulnerabilidades de implementação, mas de características relacionadas ao funcionamento do protocolo.

Os resultados do capítulo 3 reforçam essa conclusão: os cenários C1 a C4 mostraram que, após a captura do *handshake*, o tempo de exposição de uma senha previsível se mede em segundos, independentemente do *hardware* utilizado (Tabela 2). Já os cenários C7 a C12 demonstraram que a única defesa realmente eficaz contra a quebra *offline* é o aumento do espaço de busca através de senhas mais longas e aleatórias, e não mecanismos de proteção do próprio protocolo (Tabela 3). Ou seja, a resistência do WPA2-PSK aos procedimentos de verificação offline de credenciais depende significativamente da imprevisibilidade da senha configurada, sem prejuízo da importância de outros mecanismos de proteção da rede.

Essas limitações estruturais, amplamente conhecidas pela comunidade de segurança, motivaram o desenvolvimento de protocolos mais recentes. A análise de novos protocolos foge ao escopo deste trabalho, mas representa um caminho natural para pesquisas futuras sobre segurança em redes Wi-Fi.

3.4. Limitações metodológicas do estudo

A confirmação da hipótese inicial sobre a relação entre complexidade de senha e vulnerabilidade em redes WPA2 exige contextualizar algumas limitações metodológicas antes de realizar as conclusões deste trabalho.

A limitação inicial está relacionada ao *hardware* utilizado na captura de tráfego. O adaptador TP-Link TL-WN722N opera exclusivamente na faixa de 2,4 GHz (Seção 1.4.3), o que restringiu todos os testes a redes configuradas nessa frequência. Roteadores atuais configurados com a funcionalidade de *band steering*, que prioriza a conexão de clientes compatíveis à faixa de 5 GHz, inviabilizariam esse experimento com o equipamento utilizado nesta pesquisa.

Do mesmo modo, o *hardware* utilizado na quebra das senhas (CPU Ryzen 5 4600H e GPU integrada Radeon Vega) representa um poder computacional de entrada. Um atacante com uma GPU dedicada alcançaria tempos de quebra menores que os apresentados nas Tabelas 2 e 3, o que reforça que os valores absolutos de tempo registrados nesta pesquisa devem ser interpretados como limite inferior de risco, não como medida definitiva.

A segunda limitação refere-se à *wordlist* utilizada. Os resultados de sucesso ou falha do ataque por dicionário, principalmente nos cenários C5 e C6, são específicos ao conteúdo da rockyou.txt. O uso de uma *wordlist* mais recente, com maior volume, ou focada em padrões de usuários brasileiros, poderia alterar esses resultados.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Além disso, os tempos estimados para os cenários C8 a C12 (Tabela 3) foram calculados a partir da velocidade de processamento observada nos primeiros segundos de execução, sem que os ataques tenham sido concluídos, o que não captura eventuais variações de desempenho da GPU ao longo de execuções mais longas, como aquecimento ou ajuste térmico de clock (*throttling*).

Por fim, cada um dos doze cenários de senha foi testado uma única vez, em um único ponto de acesso e em um único ambiente de laboratório. Essa abordagem é adequada aos objetivos exploratórios da pesquisa, mas não permite afirmações estatísticas sobre variância entre execuções, nem generalização para diferentes fabricantes e firmwares de roteadores, que podem responder de forma distinta a ataques de desautenticação e à geração do *handshake*.

Figura 1. airodump-ng filtrado no BSSID alvo

```
CH 11 ][ Elapsed: 24 s ][ 2026-04-21 13:25

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

C0:3D:D9:C0:E4:30  -30  93      275        0    0  11  130   WPA2 CCMP   PSK  LABORATORIO

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

C0:3D:D9:C0:E4:30  10:3D:0A:CC:90:9B  -41    0 - 6      0        1
```

Fonte: O autor (2026).

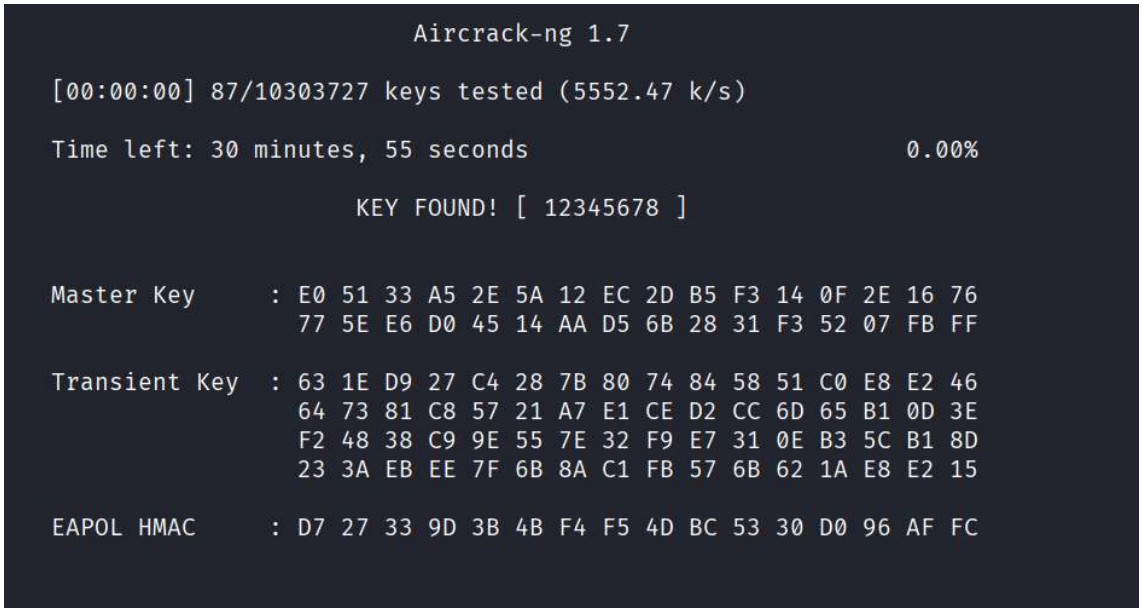
Figura 2. *Handshake* capturado

```
CH 11 ][ Elapsed: 8 mins ][ 2026-04-21 13:34 ][ WPA handshake: C0:3D:D9:C0:E4:30

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

C0:3D:D9:C0:E4:30  -33   0     4711      697    0  11  130   WPA2 CCMP   PSK  LABORATORIO

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

C0:3D:D9:C0:E4:30  D4:5B:51:AB:96:9B  -81   24e- 6      1      756  EAPOL
C0:3D:D9:C0:E4:30  10:3D:0A:CC:90:9B  -40    0 - 6      0     2583
```

Fonte: O autor (2026).

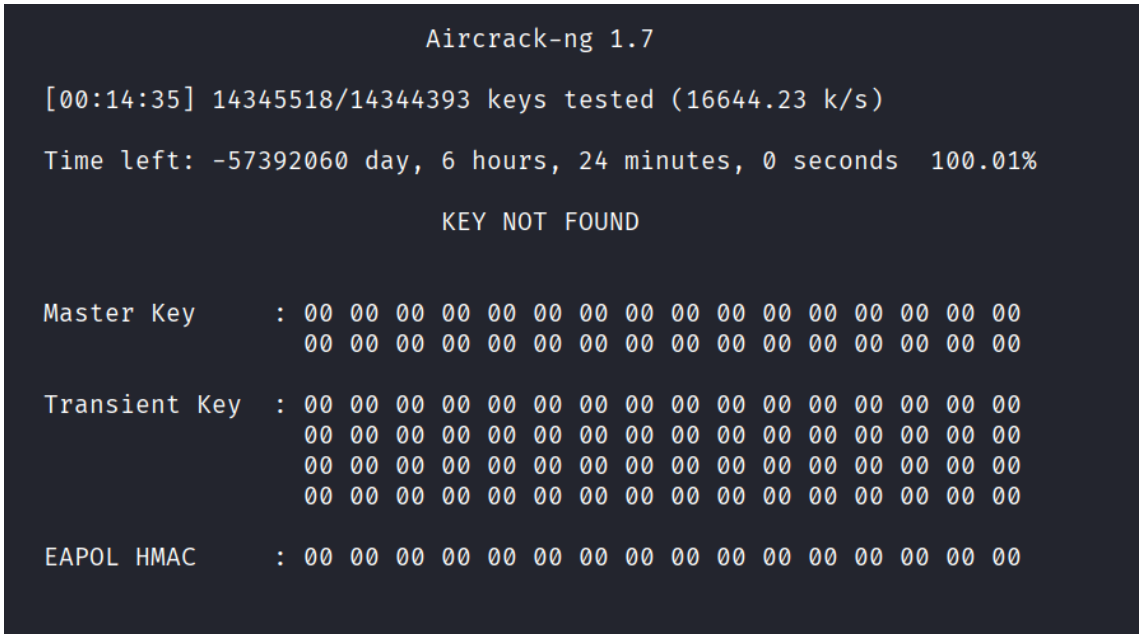
Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Figura 3. Quebra por dicionário, cenário C1



Fonte: O autor (2026).

Figura 4. Tentativa de quebra por dicionário sem sucesso, cenário C6



Fonte: O autor (2026).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Figura 5. Quebra por força bruta (máscara), cenário C7

```
2aca5c2207bde771093e08bc387d8090:c03dd9c0e430:82cebc01a9e6:LABORATORIO IGOR:70150900

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: cenario7-1.hc22000
Time.Started.....: Thu Sep  3 21:38:29 2026, (1 min, 41 secs)
Time.Estimated...: Thu Sep  3 21:40:10 2026, (0 secs)
Kernel.Feature...: Pure Kernel (password length 8-63 bytes)
Guess.Mask.......: ?d?d?d?d?d?d?d?d [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#01........:    50848 H/s (95.41ms) @ Accel:26 Loops:512 Thr:256 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 5151744/100000000 (5.15%)
Rejected.........: 0/5151744 (0.00%)
Restore.Point....: 479232/10000000 (4.79%)
Restore.Sub.#01..: Salt:0 Amplifier:8-9 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01...: 78946723 → 73616623
Hardware.Mon.#01.: Temp: 56c Fan:  0% Util: 99% Core:1500MHz Mem:1600MHz Bus:16

Started: Thu Sep  3 21:38:25 2026
Stopped: Thu Sep  3 21:40:12 2026
```

Fonte: O autor (2026).

Figura 6. Estimativa de tempo para força bruta, cenário C12

```
Session..........: hashcat
Status...........: Running
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: cenario12.hc22000
Time.Started.....: Fri Sep  4 15:29:17 2026, (5 secs)
Time.Estimated...: Mon Nov 29 06:12:10 2032, (6 years, 86 days)
Kernel.Feature...: Pure Kernel (password length 8-63 bytes)
Guess.Mask.......: ?d?d?d?d?d?d?d?d?d?d?d?d [13]
Guess.Queue......: 1/1 (100.00%)
Speed.#01........:    50817 H/s (95.41ms) @ Accel:26 Loops:512 Thr:256 Vec:1
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 239616/10000000000000 (0.00%)
Rejected.........: 0/239616 (0.00%)
Restore.Point....: 0/1000000000000 (0.00%)
Restore.Sub.#01..: Salt:0 Amplifier:6-7 Iteration:1024-1536
Candidate.Engine.: Device Generator
Candidates.#01...: 5234567899999 → 5549423456999
Hardware.Mon.#01.: Temp: 54c Fan:  0% Util: 99% Core:1500MHz Mem:1600MHz Bus:16
```

Fonte: O autor (2026).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Quadro 1. Cenários de senha definidos para os testes

Cenário	Tipo de senha	Senha
C1	Sequência numérica	12345678
C2	Palavra comum (vocabulário)	internet
C3	Palavra + número (padrão comum)	senha123
C4	Nome próprio + número	Pedro123
C5	Nome próprio + ano recente	Pedro2026
C6	Alfanumérica aleatória complexa	2l@dIZXg

Fonte: O autor (2026).

Tabela 1. Cenários de senha definidos para os testes

Cenário	Tipo de senha	Senha	Dígitos	Espaço de busca
C7	CEP	70150900	8	10^8
C8	Celular sem DDD	955103826	9	10^9
C9	Telefone fixo com DDD	1190305768	10	10^{10}
C10	CPF	32145698799	11	10^{11}
C11	Aleatório	654629878571	12	10^{12}
C12	Aleatório	7215623251018	13	10^{13}

Fonte: O autor (2026).

Tabela 2. Comparação de desempenho CPU (aircrack-ng) vs GPU (Hashcat), cenários C1 a C6

Cenário	Senha	Tempo CPU	Velocidade CPU	Tempo GPU	Velocidade GPU	Resultado
C1	12345678	~instantân	5.552 k/s	3s	24.632 H/s	Encontrad

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

		eo				a
C2	internet	~instantâneo	14.976 k/s	~1s	50.558 H/s	Encontrada
C3	senha123	18s	19.295 k/s	3s	50.039 H/s	Encontrada
C4	Pedro123	1min58s	17.778 k/s	23s	49.896 H/s	Encontrada
C5	Pedro2026	14min30s (esgotada)	16.750 k/s	3min12s (esgotada)	49.877 H/s	Não encontrada
C6	2l@dIZXg	14min35s (esgotada)	16.644 k/s	3min13s (esgotada)	49.834 H/s	Não encontrada

Fonte: O autor (2026).

Tabela 3. Escalonamento de entropia numérica (GPU, ataque de máscara), cenários C7 a C12

Cenário	Dígitos	Espaço de busca	Velocidade (GPU)	Tempo até encontrar / estimado
C7	8	10^8	50.848 H/s	1min41s — Encontrada
C8	9	10^9	50.749 H/s	5h28min (estimado)
C9	10	10^{10}	50.752 H/s	2d6h (estimado)
C10	11	10^{11}	49.713 H/s	23d6h (estimado)
C11	12	10^{12}	50.768 H/s	227d23h (estimado)
C12	13	10^{13}	50.817 H/s	6 anos e 86 dias (estimado)

Fonte: O autor (2026).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

4. CONSIDERAÇÕES FINAIS

Este estudo analisou na prática as vulnerabilidades do protocolo WPA2 em redes domésticas, com foco em responder à questão central apresentada na introdução: como ferramentas acessíveis podem comprometer uma rede com esse protocolo, e quais parâmetros de criação de senha definem seu nível de segurança.

Os resultados obtidos são compatíveis com a hipótese de que a previsibilidade e o comprimento das senhas influenciam a resistência aos procedimentos de descoberta de credenciais avaliadas. Senhas de baixa complexidade, principalmente aquelas já expostas em listas de vazamentos conhecidas, foram comprometidas em poucos segundos, tanto na CPU quanto na GPU, enquanto a senha mais longa e imprevisível, do cenário C6, não teve sua credencial identificada nem pelo ataque por dicionário nem pelo ataque de força bruta dentro do tempo de teste. Além disso, os cenários C7 a C12 mostraram que o custo computacional de um ataque exaustivo cresce exponencialmente a cada dígito adicionado à senha, nas condições computacionais avaliadas neste estudo que empregaram uma GPU integrada, não um hardware dedicado, a quebra de senhas numéricas com onze dígitos ou mais se tornou impraticável, podendo esse tempo ser significativamente reduzido com equipamentos de maior capacidade de processamento.

Seguindo além das questões de complexidade de senha, os experimentos mostraram limitações estruturais do mecanismo de autenticação do WPA2-PSK, sem que isso represente o comprometimento do algoritmo de criptografia em si. A falta de autenticação nos quadros de desautenticação, permitindo forçar a reconexão dos dispositivos para capturar o *handshake*, juntamente com a exposição do PMKID sem a necessidade de um cliente conectado, ampliam significativamente a superfície de ataque. Na prática, essas falhas mostram que qualquer atacante com ferramentas gratuitas e equipamentos domésticos pode invadir uma rede sem precisar de técnicas avançadas.

Na prática, os resultados reforçam que a principal defesa eficaz ao alcance do usuário comum é a utilização de senhas longas, aleatórias e sem relação com dados pessoais. Soluções como bloqueio de tentativas atuam apenas sobre ataques online e não impedem o processamento offline de candidatos já capturados, que representa a ameaça mais realista de comprometimento identificada neste estudo, ainda assim, mecanismos detectivos, como o monitoramento de rede, podem contribuir para identificar indícios das etapas que precedem esse tipo de ataque.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

É preciso considerar que essas conclusões devem ser interpretadas considerando as limitações metodológicas do estudo, no qual os experimentos foram realizados com um único modelo de ponto de acesso, operando exclusivamente em 2,4 GHz, com um conjunto limitado de credenciais, ferramentas e capacidade computacional (hardware de entrada). Essa delimitação impede a generalização direta dos tempos obtidos para todas as redes residenciais.

Como caminhos para pesquisas futuras, sugere-se a repetição dos experimentos com diferentes fabricantes e firmwares de roteador, o uso de *wordlists* mais recentes e adaptadas a padrões brasileiros, e a extensão da análise a *hardware* de quebra mais potente, capaz de avaliar com maior precisão o tempo real de exposição de senhas de alta entropia. Sugere-se também a investigação de protocolos mais recentes, cuja avaliação ficou fora do escopo deste trabalho, mas que representam uma evolução direta das limitações estruturais aqui identificadas no WPA2.

REFERÊNCIAS

BOSSO, Caio Pelizzer; WANDERLEY, Giovanni Luiz da Silva; ANTUNES NETO, Joaquim M. F. Análise das tecnologias Li-Fi e Wi-Fi: comparativos de desempenho, segurança e aplicações em ambientes urbanos. Prospectus, Itapira, v. 6, n. 2, p. 473-518, jul./dez. 2024. Disponível em: https://prospectus.fatecitapira.edu.br/index.php/pst/article/download/265/212/528. Acesso em: 5 maio 2026.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). Cartilha de Segurança para Internet: versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 3 abril 2026.

FERNANDEZ, Marcial Porto. Rede de computadores. 2. ed. Fortaleza: EdUECE, 2015.

FRANÇA NETO, Ivan Luiz de; SOUZA, Eduardo Ferreira de; GONÇALVES, Paulo André da Silva. Segurança no processo de autenticação de redes IEEE 802.11. In: CONGRESSO DE INICIAÇÃO CIENTÍFICA EM COMPUTAÇÃO (CONIC), 19.; CONGRESSO DE INICIAÇÃO TECNOLÓGICA EM INFORMÁTICA (CONITI), 3.; JORNADA DE INICIAÇÃO CIENTÍFICA (JOIC), 7., 2011, Recife. Anais [...]. Recife: Centro de Informática, Universidade Federal de Pernambuco, 2011.

HEIDERSCHEIDT, Henrique; SILVA, Eduardo Brandt Silveira da; URIARTE, Luiz Ricardo. A influência da entropia das senhas na defesa contra ataques de força bruta. Revista de Extensão e Iniciação Científica da UNISOCIESC, Blumenau, v. 10, n. 1, 2022. Disponível em: https://dalfovo.com/ojs/index.php/reis/article/view/399. Acesso em: 6 maio 2026.

KASPERSKY. WEP, WPA, WPA2 e WPA3: diferenças e explicação. [S. l.]: Kaspersky Lab, 2021. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/wep-vs-wpa. Acesso em: 29 março 2026.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

LIMA, Guilherme Vidal de Negreiros. Uma visão sobre segurança em soluções IOT para ambientes residenciais. 2023. Trabalho de Conclusão de Curso (Graduação em Tecnologia em Telemática) – Instituto Federal da Paraíba, Campina Grande, 2023.

MACÊDO, Carlos José. Evolução da segurança em redes sem fio. 2008. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Centro de Informática, Universidade Federal de Pernambuco, Recife, 2008. Disponível em: https://www.cin.ufpe.br/~tg/2008-1/maccj.pdf. Acesso em: 29 março 2026.

MORAES, F.; SILVA, T.; CEOLIN, S. R.; AZEVEDO, R. P. de. Análise e otimização da rede Wi-Fi num ambiente corporativo. RETEC – Revista de Tecnologias, Ourinhos, v. 17, n. 2, p. 53-71, jul./dez. 2024.

MORENO, Daniel. Introdução ao Pentest. 2. ed. São Paulo: Novatec, 2016.

NASCIMENTO, Samuel Lima do. Os riscos de conectar-se a uma rede Wi-Fi de acesso público. 2025. Trabalho de Conclusão de Curso (Graduação em Tecnologia em Sistemas de Telecomunicações) – Instituto Federal da Paraíba, Campina Grande, 2025.

OLIVEIRA, Hudson Yuri de. Análise de segurança de redes sem fio utilizando pentest. 2025. Trabalho de Conclusão de Curso (Bacharelado em Engenharia de Computação) – UNIFEV – Centro Universitário de Votuporanga, Votuporanga, 2025.

RANDEL, João Roberto; SERRÃO, Jorge Siqueira; ROMÃO, Hugo Lima; LOBO, Felipe Leite; HENKLAIN, Marcelo Henrique Oliveira; FEITOSA, Eduardo Luzeiro. Caracterização de senhas utilizadas pela comunidade universitária como ponto de partida para o desenvolvimento de capacitação em cibersegurança. In: WORKSHOP SOBRE EDUCAÇÃO EM COMPUTAÇÃO (WEI), 32., 2024, Brasília. Anais [...]. Porto Alegre: SBC, 2024. p. 680-681. Disponível em: https://doi.org/10.5753/wei.2024.2617. Acesso em: 8 maio 2026.

SANTOS, Rafael Ramon. Implementação de uma rede sem fio Mesh com autenticação centralizada utilizando um servidor RADIUS. 2012. Trabalho de Conclusão de Curso (Graduação em Tecnologia em Sistemas para Internet) – Universidade Tecnológica Federal do Paraná, Curitiba, 2012.

VILELA, Douglas Willer Ferrari Luz. Segurança em redes sem fio: estudo sobre o desenvolvimento de conjuntos de dados para comparação de IDS. 2014. Dissertação (Mestrado em Engenharia Elétrica) – UNESP, Ilha Solteira, 2014.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.