REVISTA ACADÊMICA - ENSINO DE CIÊNCIAS E TECNOLOGIASIFSP –
CAMPUS CUBATÃO – **CATEGORIA: ARTIGO**
NÚMERO 15 – JUL/DEZ DE 2024

Análise de ataques Brute Force em Redes Wireless: Vulnerabilidades e Ferramentas

Claudionor Cosme da Silva Filho

Instituto Federal de Educação, Ciência e Tecnologia de São Paulo(IFSP), Iperó, SP, Brasil

Henderson Honorio Silva

Instituto Federal de Educação, Ciência e Tecnologia de São Paulo(IFSP), Boituva, SP, Brasil

André Luyde

Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP), Boituva, SP, Brasil

Resumo: Com a crescente conectividade e o aumento significativo de dispositivos sem fio conectados à internet, a segurança das redes wireless tornou-se uma preocupação primordial. Este trabalho examina detalhadamente uma das técnicas mais utilizadas e perigosas para explorar vulnerabilidades, os ataques de força bruta, conhecidos como "brute force". Esse método consiste em tentar adivinhar credenciais de acesso através de repetidas tentativas, comprometendo a segurança de diversos serviços. No contexto das redes sem fio, os principais alvos são pontos de acesso, roteadores e dispositivos conectados a equipamentos utilizados para a criação de redes. O estudo demonstra como os ataques de força bruta são realizados em redes sem fio, utilizando ferramentas como Airodump-ng, Aireplay-ng e Aircrack-ng, todas integradas ao sistema operacional Kali Linux. Foram analisados os tempos de quebra de senhas de diferentes complexidades, evidenciando a importância de políticas de senha robustas e configurações de segurança adequadas. Os resultados reforçam

que, apesar dos avanços nos protocolos de segurança como WPA (Wi-Fi Protected Access) e WPA2 (Wi-Fi Protected Access 2), a força bruta continua a representar uma ameaça significativa, especialmente quando senhas fracas são utilizadas. Este trabalho destaca a necessidade de senhas complexas, atualizações constantes das medidas de segurança e a educação contínua dos usuários. A pesquisa visa fornecer ferramentas e informações importantes para a proteção de redes wireless e promover o desenvolvimento de tecnologias de autenticação mais seguras.

Palavras–chave: Força Bruta. Conexão sem Fio. Teste de Penetração. Senha.

Abstract: With increasing connectivity and the significant increase in wireless devices connected to the internet, the security of wireless networks has become a primary concern. This work examines in detail one of the most used and dangerous techniques to exploit vulnerabilities: brute force attacks, known as "brute force". This method consists of trying to guess access credentials through repeated attempts, compromising the security of several services. In the context of wireless networks, the main targets are access points, routers and connected devices. The study demonstrates how brute force attacks are carried out on wireless networks, using tools such as Airodump-ng, Aireplay-ng and Aircrack-ng, all integrated into the Kali Linux operating system. Password cracking times of different complexities were analyzed, highlighting the importance of robust password policies and adequate security configurations. The results reinforce that, despite advances in security protocols such as WPA and WPA2, brute force continues to represent a significant threat, especially when weak passwords are used. This work highlights the need for complex passwords, constant updates to security measures, and ongoing user education. The research aims to provide valuable insights for protecting wireless networks and promote the development of more secure authentication technologies.

Keywords: *Brute Force.* Wireless Connection*. Pentest. Password.*

APRESENTAÇÃO DO TRABALHO

A metodologia utilizada neste artigo foi baseada em estudos e técnicas realizadas anteriormente por outros profissionais da área de segurança da informação. Inicialmente, foram identificados estudos relevantes sobre ataques brute force em redes Wireless. Diversas informações são disponibilizadas por membros dessa área, em busca de combater ameaças que surgem muitas vezes antes de criar-se mecanismos de prevenção (Ferreira & Faustino, (2009); Paim, (2014); Santos et. al, (2023)). Dessa maneira, mostra-se necessário o estudo acerca das estratégias de invasão para criar um ambiente seguro nas redes. A maioria dos ataques, como já dito anteriormente, é feito de forma mal-intencionada, e parte da vulnerabilidade é devido ao mal uso das redes por clientes/usuários que não entendem sobre os conceitos de segurança e como aplicar esses conceitos nas tecnologias, e podem cometer erros ao realizar as configurações em equipamentos da rede. Sendo assim, este trabalho apresenta ferramentas eficientes para a invasão através da força bruta e o conhecimento sobre o método em si. As ferramentas mais comuns incluem Airodump-ng, Aireplay-ng e Aircrack-ng, todas integradas ao sistema operacional Kali Linux, que é uma distribuição Linux de código aberto amplamente utilizado por profissionais de segurança e entusiastas para testes avançados de invasão e auditoria de segurança. O Kali Linux é composto por diversas ferramentas, configurações e scripts com diferentes modificações específicas do setor, fazendo com que seja possível que os usuários possam focar em atividades de engenharia reversa e detectar vulnerabilidades (KALI, 2024). Para realizar a quebra de uma senha através do ataque de força bruta são necessárias ferramentas. Foram escolhidas para este trabalho as ferramentas Airodump-ng, Aireplay-ng e Aircrack-ng. A seguir, uma breve explicação sobre elas e como funcionam.

- Airodump-ng: É uma ferramenta integrada ao sistema operacional Kali Linux, projetada como um sniffer[1] de rede. Sua função principal é capturar e monitorar pacotes de dados transmitidos em uma rede sem fio. Uma vez que esses pacotes são capturados, o Airodump-ng os registra em um arquivo com

extensão CAP, que posteriormente é utilizado por outras ferramentas do pacote, como o Aircrack- ng [Andrade, 2016].

- Aireplay-ng: É outra ferramenta essencial do Kali Linux, é frequentemente empregada após a utilização do Airodump-ng. O propósito principal do Aireplay-ng é realizar ações de desautenticação, o que permite a captura de dados de handshake da rede. Além disso, essa ferramenta é capaz de realizar autenticações falsas, repetir pacotes interativos, injetar ARP (Address Resolution Protocol) Requests forjados e reinjetar ARP Requests (Andrade, 2016). Uma solicitação ARP é um pedido realizado por um dispositivo que deseja descobrir o endereço MAC (Media Access Control) de outro aparelho, a máquina envia um ARP Request para todos os dispositivos na rede local Broadcast buscando descobrir o destino correto (Silva, 2019).
- Aircrack-ng: É uma ferramenta crucial para a análise de criptografia em redes sem fio. Ela é especialmente conhecida por sua capacidade de realizar ataques a protocolos de segurança como WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) e WPA2 (Wi-Fi Protected Access 2). O Aircrack-ng utiliza os dados capturados previamente pelo Airodump-ng para recuperar chaves de segurança WEP de redes sem fio (Andrade, 2016).

Com o desafio de manter uma rede sem fio segura de tantas formas de invasão, foram implementados protocolos de segurança que atuam como uma barreira contra invasores. Alguns desses protocolos como o WEP, WPA WPA2 estão presentes na tecnologia desenvolvida pelo IEEE (Institute of Electrical and Electronic Engineers): O padrão IEEE 802.11 é conhecido também pela maioria como Wi-Fi (Wireless Fidelity) (Santos et. al, 2023). Cada um desses protocolos possui certo nível de segurança, porém, com o tempo, é necessário que sejam aprimorados para suprimir as necessidades relacionadas à segurança das redes sem fio.

O WEP foi introduzido em 1999 como protocolo de segurança para o padrão IEEE 802.11, apresentando dois métodos de autenticação de dispositivos: os algoritmos CRC-32 (Cyclic Redundancy Checks) e RC4 (Rivest Cipher 4). CRC-32 é um algoritmo utilizado para a análise e detecção de falhas na integridade dos dados e o RC4 é o algoritmo de criptografia simétrica (chave secreta compartilhada) para

assegurar a proteção da confidencialidade das informações de usuários que transitam na rede (Linhares & Gonçalves, 2009). O WEP é baseado em três aspectos fundamentais: integridade, que diz respeito à informação que chega sem alteração; autenticidade, onde o usuário tem sua legitimidade confirmada e a confidencialidade, que deixa as mensagens interceptadas indecifráveis. Apesar de parecer confiável, o WEP apresentou falhas graves de segurança no uso do algoritmo RC4, e unindo esse problema com outras vulnerabilidades em sua implementação, culminou no comprometimento da tecnologia. Ataques brute force se tornaram um empecilho para o protocolo, e tornou o WEP um protocolo ultrapassado [Santos et. al, 2023].

O WPA surgiu em 2002 como um sucessor do WEP e tinha como objetivo corrigir falhas de segurança deixadas pelo seu antecessor. Dentre essas melhorias, aquela que chamou mais a atenção foi o uso do algoritmo RC4, porém de forma mais segura, dentro do protocolo TKIP (Temporal Key Integrity Protocol) (Paim, 2014). O TKIP consegue resolver a maioria das brechas deixadas pelo WEP, e baseia-se no conceito de chaves temporais e em seu funcionamento uma chave é usada e depois de certo tempo é substituída por outra de forma dinâmica (Linhares & Gonçalves, 2002). Além desse protocolo, o WPA introduziu o MIC (Message Integrity Code), um quadro de 64 bits empregado para verificar se o material de um quadro de dados detém variações por erros de difusão ou manuseio de dados. Além disso, o MIC é responsável pela integridade dos dados transmitidos e aprimorou a gestão dos vetores de inicialização. Porém, o WPA não apenas utilizou do MIC como ferramenta de proteção, o algoritmo RC4 também foi manipulado para criptografar as mensagens, evitando a transmissão não criptografada da chave secreta.

O Wi-Fi Protected Access também oferece modos de funcionamento, como o Personal para redes domésticas e o Enterprise para ambientes corporativos, onde diferencia-se entre esses dois o modo de autenticação, já que o modelo para ambientes corporativos inclui a opção de um servidor de autenticação centralizado, na maioria das vezes um servidor RADIUS (Remote Authentication Dial-In User Service), protocolo de autenticação, autorização e contabilidade que exerce a função de permitir o gerenciamento centralizado de acesso à rede. Desse modo, o RADIUS atua como um intermediário entre os dispositivos de rede como um roteador, e os sistemas

de autenticação como um banco de dados de usuário (Linhares & Gonçalves, 2002; MADE4IT, 2024). Essas melhorias tornam o WPA uma opção mais robusta em comparação com o WEP, mitigando muitas das vulnerabilidades exploradas por ataques brute force e outras técnicas de invasão em redes sem fio. Apesar das melhorias, o WPA não é totalmente seguro, alguns de seus mecanismos de segurança são suscetíveis a ataques brute force e ataques do tipo dicionário.

Em um ataque de dicionário, o invasor utiliza uma lista pré-compilada de senhas comuns ou obtidas de vazamentos de dados anteriores. Esse método é eficaz quando senhas utilizadas são fracas ou frequentemente repetidas. O sucesso desses ataques depende da qualidade e da variedade das senhas incluídas no dicionário utilizado (Ramos, 2022). Uma brecha que pode ser utilizada através de ataques brute force é em relação à negação de serviço: o MIC possui um mecanismo de defesa contra esse tipo de ataque, entretanto quando dois MIC são avistados em menos de 60 segundos o AP (Access Point) cancela a conexão por 1 minuto e faz uma alteração na chave de integridade. Com isso, é possível com uma aplicação de pacotes malformados realizar um ataque de negação de serviço (DoS). Esse ataque cibernético é utilizado por cibercriminosos para interromper os serviços de um host que está conectado à internet para os seus usuários. Esse método consiste em sobrecarregar um servidor ou rede através de um fluxo constante de tráfego, utilizando por exemplo de solicitações falsas que atrapalham o tráfego verdadeiro, o que prejudica a disponibilidade de serviços para o usuário (Linhares & Gonçalves, 2002;).

O WPA2, sucessor do WPA, foi desenvolvido para implementar totalmente o novo padrão IEEE 802.11, trazendo avanços significativos em termos de segurança para redes sem fio. Uma das principais melhorias do WPA2 é a utilização do protocolo CCMP (Counter Cipher Mode), baseado no AES (Advanced Encryption Standard), que oferece criptografia muito mais robusta e resistente a ataques [Santos et. al, 2023]. Além disso, o WPA2 introduziu um mecanismo de pré-autenticação, que ajuda a reduzir a latência durante a transição de um ponto de acesso para outro, garantindo uma conexão mais rápida e contínua. Essas melhorias fazem do WPA2 uma escolha superior para proteção da autenticação das redes sem fio, atendendo às demandas modernas de segurança.

SIMULAÇÕES E CENÁRIOS DE TESTES

Para compreender o desempenho do processador Ryzen 5 5600G em brute force, foram simulados cenários de quebra de senhas com diferentes níveis de complexidade. A análise levou em consideração o número de cálculos por segundo que o processador é capaz de realizar, conforme descrito na Seção 1. A seguir, foram detalhados os parâmetros utilizados e os resultados obtidos.

CONFIGURAÇÃO DO AMBIENTE DE TESTE

Processador: AMD Ryzen 5 5600G Velocidade de clock: 4.0 GHz (reduzido para 2.0 GHz devido a sobrecargas e atrasos na memória); operações por segundo: aproximadamente 100 milhões de operações teóricas por segundo, após ajustes.

SENHAS TESTADAS

As senhas foram escolhidas com base em diferentes níveis de complexidade:

- Senha simples: 8 caracteres contendo apenas letras minúsculas.
- Senha moderada: 8 caracteres contendo letras maiúsculas e minúsculas.
- Senha intermediária: 12 caracteres contendo letras maiúsculas, minúsculas e Números.
- Senha complexa: 12 caracteres contendo letras maiúsculas, minúsculas, números e Símbolos.

Tipos de senha	Combinações	Tempo estimado
Simples	0,000208 quintilhões	≈ 35 minutos
Moderada	0,053 quintilhões	≈ 6 dias
Intermediária	3,2 quintilhões	≈ 80 anos
Complexa	7,9 quintilhões	≈ 2 milhões de anos

RESULTADOS TEÓRICOS

Os cálculos teóricos consideraram o número total de combinações possíveis para cada tipo de senha e a quantidade de operações que o processador consegue realizar por segundo.

- Senha simples (8 letras minúsculas): 26 elevado a 8 combinações possíveis (aproximadamente 0,000208 quintilhões). Tempo estimado para quebra: cerca de 35 minutos.
- Senha moderada (8 caracteres com letras maiúsculas e minúsculas): 52 elevado a 8 combinações possíveis (em torno de 0,053 quintilhões). Tempo estimado para quebra: menos de 6 dias.
- Senha intermediária (12 caracteres com letras maiúsculas, minúsculas e números): 62 elevado a 12 combinações possíveis (cerca de 3,2 quintilhões). Tempo estimado para quebra: cerca de 80 anos.
- Senha complexa (12 caracteres com letras maiúsculas, minúsculas, números e símbolos): 95 elevado a 12 combinações possíveis (por volta de 7,9 quintilhões). Tempo estimado para quebra: mais de 2 milhões de anos.

DISCUSSÃO

Analisando as informações apresentadas na Tabela 1, pode-se concluir que conforme a quantidade de caracteres aumenta, e conforme o tipo de caractere é inserido nas senhas, o número de combinações possíveis também cresce. Pode ser verificado que ao inserir números, alternar letras entre maiúsculas e minúsculas, e incluir caracteres especiais em senhas, aumenta a segurança e a dificuldade dessa senha ser quebrada por alguma técnica de invasão. Dessa maneira, podemos concluir também que senhas simples podem ser quebradas de maneira mais fácil, senhas complexas aumentam exponencialmente o tempo necessário para que um ataque, como por exemplo o brute force, seja bem-sucedido. Mesmo processadores com o poder de processamento muito elevado, senhas longas e com alta variedade de tipos de caracteres são consideradas mais seguras pelo tempo necessário para serem quebradas. Esses cálculos teóricos reforçam a importância de adotar senhas

complexas e a limitação dos ataques brute force quando políticas de segurança robustas estão em vigor.

RESULTADOS E DISCUSSÃO

Os estudos realizados com as ferramentas Airodump-ng, Aireplay-ng e Aircrack-ng mostraram que é possível capturar pacotes de dados e realizar ataques brute force em redes wireless com relativa facilidade. Na pesquisa realizada, foram analisados handshakes WPA/WPA2, e as tentativas de quebra de senha resultaram em tempos variáveis, dependendo da complexidade da senha. Por exemplo, senhas simples de 8 caracteres podem ser quebradas em menos de 1 hora, enquanto senhas mais complexas (combinando letras maiúsculas, minúsculas, números e símbolos) exigiram muito mais tempo para serem decifradas. Os resultados confirmam que ataques brute force ainda são uma ameaça significativa para redes sem fio, especialmente aquelas que utilizam senhas consideradas fracas. As ferramentas analisadas em teoria são eficientes na captura de dados e na realização de ataques, destacando a necessidade de políticas de senha mais robustas e de configurações de segurança adequadas. Em casos de usuários comuns, além das informações necessárias que vêm em seus aparelhos para configuração e instalação, o conhecimento sobre a robustez de senhas também vai auxiliar para o aumento de segurança. Esses resultados ressaltam a importância de uma constante atualização das medidas de segurança e da conscientização dos usuários sobre as melhores práticas na criação e gestão de senhas.

CONCLUSÃO

Este estudo explorou a técnica de ataques brute force em redes sem fio, destacando a vulnerabilidade de diversos protocolos de segurança e a eficácia das ferramentas utilizadas em testes de invasão. Os resultados indicaram que, apesar dos avanços nos protocolos de segurança, o brute force ainda representa uma ameaça significativa, especialmente quando senhas fracas são utilizadas. Recomenda-se que os usuários e administradores de redes wireless adotem senhas complexas e

regularmente atualizadas, além de implementar métodos de autenticação mais robustos, como o uso de WPA2 com AES. Adicionalmente, a educação contínua sobre práticas de segurança e a atualização constante dos protocolos de segurança são cruciais para mitigar riscos. Para futuros estudos a respeito desse assunto, é recomendável a investigação de novas tecnologias de autenticação e a melhoria dos algoritmos de criptografia para tornar as redes wireless ainda mais seguras contra-ataques brute force e outras formas de invasão. Portanto, é possível concluir que embora existam diversas ferramentas e métodos à disposição para proteger redes sem fio, a evolução constante das ameaças cibernéticas exige um compromisso contínuo com a segurança e a inovação da tecnologia.

REFERÊNCIAS

ANDRADE, D.; DE, M. J. Análise de riscos e vulnerabilidades em redes sem fio. Bauru São Paulo: Centro Universitário Sagrado Coração UNISAGRADO, 2016.

FERREIRA, N. M.; FAUSTINO, P. S. Segurança em redes locais sem fio: um estudo de caso em Marabá. Marabá Pará: Repositório Institucional Unifesspa, 2007.

DIORIO, R. F.; SERAFIM, E.; ALVES, K. R.; MEIRA, M. C. Ataques de força bruta: um estudo prático. Capivari São Paulo: Departamento de Informática, IFSP, 2019.

LINHARES, A. G.; GONÇALVES, P. de S. Uma análise dos mecanismos de segurança de redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w. Recife: Universidade Federal de Pernambuco, Centro de Informática, 2009.

PAIM, R. R. WEP, WPA e EAP. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2014. Disponível em: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/downloads/trabalho.pdf. Acesso em: 13 de dezembro de 2024.

AMD. AMD Ryzen™ 5 5600G Processor. Disponível em: https://www.amd.com/en/support/downloads/drivers.html/processors/ryzen/ryzen-5000-series/amd-ryzen-5-5600g.html. Acesso em: 20 agosto de 2024.

RAMOS, M. B. et al. Redes neurais recorrentes para geração de senhas em ataques de força bruta baseado em dicionário. Uberlândia Minas Gerais: Universidade Federal de Uberlândia, 2022.

DOS SANTOS, G. N.; BAUER, V. H. L.; DA SILVA, C. A. Análise e teste de vulnerabilidade de redes Wireless em instituições de ensino que utilizam o protocolo WPS. Campo Grande Mato Grosso do Sul: Universidade Federal de Mato Grosso do Sul (UFMS), 2023.

SILVA, C. A. S. Análise de vulnerabilidades em redes Wireless: proposta de soluções para ataques do tipo MITM. São Luís Maranhão: Universidade Estadual do Maranhão, 2019.

PAESSLER AG. Network Sniffer - O que é, como funciona e para que serve. 2024. Disponível em: :https://www.paessler.com/br/network_sniffer#:~:text=1.,e%20solucionar%20problemas%20de%20desempenho. Acesso em : 19 de dezembro de 2024.

MADE4IT. Por que ter um servidor RADIUS próprio?. 2024. Disponível em: https://made4it.com.br/por-que-ter-um-servidor-radius-proprio/#:~:text=O%20que%20%C3%A9%20um%20Servidor,bancos%20de%20dados%20de%20usu%C3%A1rio). Acesso em: 19 de dezembro de 2024.

ZSCALER**.** What is a Denial of Service Attack?. 2024. Disponível em: https://www.zscaler.com/br/resources/security-terms-glossary/what-is-a-denial-of-service-attack. Acesso em: 19 dezembro de 2024.

KALI. What is Kali Linux?. 2024. Disponível em: https://www.kali.org/docs/introduction/what-is-kali-linux/. Acesso em: 19 dezembro de 2024.