FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Joanderson de Pontes Andrade

Thiago Fernandes da Silva

SEGURANÇA EM REDES WI-FI: VULNERABILIDADES NOS PROTOCOLOS DE CRIPTOGRAFIA WEP E WPA/WPA2

Americana, SP

2023

FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Joanderson de Pontes Andrade

Thiago Fernandes da Silva

SEGURANÇA EM REDES WI-FI: VULNERABILIDADES NOS PROTOCOLOS DE CRIPTOGRAFIA WEP E WPA/WPA2

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Esp. Bruno Henrique de Paula Ferreira.

Área de concentração: Segurança da Informação.

Americana, SP

2023

Thiago Fernandes da Silva
Joanderson de Pontes Andrade

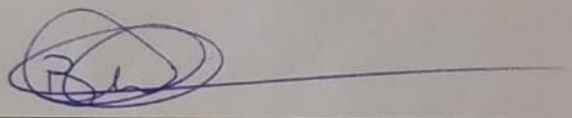
SEGURANÇA EM REDES WI-FI: VULNERABILIDADES NOS PROTOCOLOS DE CRIPTOGRAFIA WEP E WPA/WPA2

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana – Ministro Ralph Biasi.

Área de concentração: Segurança da Informação.

Americana, 17 de junho de 2023.

Banca Examinadora:



Bruno Henrique de Paula Ferreira
Especialista
FATEC Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

Rogério Nunes de Freitas
Mestre
FATEC Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

Wellington Aires da Cruz Pereira
Mestre
FATEC Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

SEGURANÇA EM REDES WI-FI: VULNERABILIDADES NOS PROTOCOLOS DE CRIPTOGRAFIA WEP E WPA/WPA2

Joanderson de Pontes Andrade, Thiago Fernandes da Silva

joanderson.andrade@fatec.sp.gov.br, thiago.silva390@fatec.sp.gov.br

Bruno Henrique de Paula Ferreira

Professor Orientador

bruno.ferreira86@fatec.sp.gov.br

Curso Superior de Tecnologia em Segurança da Informação – Faculdade de Tecnologia de Americana (FATEC Americana)

Americana – SP – Brasil

Abstract: Given the success of the IEEE 802.11 protocol in enabling physical mobility linked to the multiple computing devices, it was possible to notice the growth in the number of vulnerabilities and security incidents associated with this new technology due to various problems such as lack of software or firmware updates, discovery of insecure algorithms, equipment configuration failure, etc. Therefore, there was the need for great and continuous efforts to protect users and systems in general. Thus, this research aimed to demonstrate the exploitation of specific vulnerabilities of Wi-Fi network security protocols (WEP and WPA/WPA2) in order to highlight the risks of keeping such a network incorrectly configured or technically unattended.

Keywords: IEEE 802.11. Pentest. Cryptography. Security Protocols.

Resumo. Dado o sucesso do protocolo IEEE 802.11 em possibilitar a mobilidade física atrelada aos diversos dispositivos computacionais foi possível perceber o crescimento do número de vulnerabilidades e incidentes de segurança associadas à essa tecnologia em função de diversos problemas como falta de atualização de software ou firmware, descoberta de algoritmos inseguros, falha de configuração de equipamentos. Nesse sentido, houve a necessidade de grandes e contínuos esforços para proteger os usuários e sistemas em geral. Assim, o presente artigo objetivou demonstrar a exploração de vulnerabilidades específicas dos protocolos de segurança de redes Wi-Fi (WEP e WPA/WPA2) a fim de evidenciar os riscos em manter uma rede desse caráter incorretamente configurada ou desassistida tecnicamente.

Palavras-chave: IEEE 802.11. Pentest. Criptografia. Protocolos de Segurança.

1. INTRODUÇÃO

As redes sem fio tornaram mais prático o acesso à internet atualmente e por isso, são amplamente utilizadas em alternativa à utilização de cabeamento para conectar dispositivos à rede. Elas possuem diferentes tipos de classificações como *Wireless Personal Areal Network* (WPAN), *Wireless Metropolitan Area Network* (WMAN), *Wireless Wide Area Network* (WWAN) e *Wireless Local Area Network* (WLAN), sendo essa última o foco de estudo do projeto de pesquisa.

Conhecida como WLAN ou Rede Local de Acesso sem Fio, esse tipo de conexão proporciona mobilidade aos dispositivos que, por sua vez, se adaptam às necessidades corriqueiras dos usuários e possibilitam que eles se desloquem na área de abrangência sem perder o acesso à rede. Dentre essas tecnologias, o *Wireless Fidelity* (Wi-Fi) é a mais conhecida e utilizada na infraestrutura de rede de instalações residenciais e institucionais.

Ao mesmo tempo que facilita a navegação na internet, o Wi-Fi pode trazer consigo múltiplas brechas de segurança capazes de comprometer a segurança dos aparelhos nela conectados, em destaque seus protocolos de segurança que podem ser quebrados e possibilitar o acesso a rede Wi-Fi.

A pergunta-problema que baliza o trabalho é: quais são as possíveis vulnerabilidades relacionadas aos protocolos de criptografia presentes em redes Wi-Fi?

Esta pesquisa justifica-se como relevante porque conscientizará administradores e detentores de redes Wi-Fi demonstrando alguns possíveis métodos de exploração de suas vulnerabilidades e por consequência, auxiliará indiretamente na proteção dessas conexões sem fio.

De acordo com Severino (2013, p. 103) “são várias metodologias de pesquisa que podem adotar uma abordagem qualitativa, modo de dizer que faz referência mais a seus fundamentos epistemológicos do que propriamente a especificidades metodológicas.”

A metodologia de pesquisa possui uma abordagem qualitativa e descritiva quanto aos objetivos. Os principais métodos utilizados foram: pesquisa bibliográfica, pesquisa documental e levantamento de dados em relatórios e sites especializados.

Para a realização desta pesquisa, foram aplicados, principalmente, os conhecimentos adquiridos nas disciplinas/temas: Segurança em Sistemas Operacionais e Redes de Computadores I, Metodologia de Projeto de Redes de Computadores, Gerenciamento de Redes de Computadores, Infraestrutura Física em Redes de Computadores e Protocolos de Roteamento em Redes de Computadores.

O objetivo geral da pesquisa está em realizar um teste de penetração nos protocolos de segurança de redes Wi-Fi e apontar como eles podem ser explorados e aproveitados por algum agente de ameaça com intenções maliciosas.

Quanto aos objetivos específicos, o trabalho almeja:

- Realizar pesquisa bibliográfica pontuando os conceitos fundamentais no que que tange redes Wi-Fi e teste de penetração;
- Realizar pesquisa documental em *sites*, w*hite papers* e relatórios a respeito do tema estudado em busca de levantamentos provenientes de fontes primárias de informações;
- Analisar dados e relatórios oficiais de instituições relacionadas a diversos aspectos do tema abordado pela pesquisa.

2. REVISÃO BIBLIOGRÁFICA

A ostensiva evolução da indústria de Tecnologia da Informação (TI) nas últimas décadas remete-se à célebre Lei de Moore, mencionada por Shalf (2020 apud MOORE, 1965) como um modelo técnico-econômico baseado na observação do aprimoramento contínuo dos eletrônicos ao longo dos anos. Em consequência, é notório o aumento gradual da

utilização de dispositivos móveis no mundo, que já em 2017, ultrapassou o uso de *desktops*, tornando-se principal gerador de tráfego na internet (HOWARTH, 2022).

Essa tendência de crescimento reflete-se também no eixo tecnológico *Machine-to-Machine* (M2M) e *Internet of Things* (IoT) em progressão aritmética dado que em 2019, igualou-se, em número de conexões, com aparelhos que não são desse tipo, chegando à marca de 10 bilhões e com projeção de que alcance o dobro disso até 2023 e triplique-se até 2025 (LUETH, 2020).

Nesse cenário, mediante a diversidade de demandas e padrões para implementação de suas estruturas tecnológicas, a rede sem fio dotada de atributos como adaptabilidade, flexibilidade, custo de manutenção reduzido, facilidade de instalação e utilização, é o modo de conectividade predominante nesse nicho, sendo o Wi-Fi a tecnologia mais popular e robusta (ETSI, 2017; HKCERT, 2020; LOCHHAAS, 2016).

2.1. TESDE DE PENETRAÇÃO

De acordo com Santos e Soares (2018), vulnerabilidades são falhas ou fraquezas que pode haver em um ativo, cuja sua exploração, por parte de uma ameaça, irá ocasionar em um incidente.

Segundo Dantas (2011 apud SALADIN, 2017), as vulnerabilidades podem causar danos em dispositivos, visto que são fragilidades que estes possuem. Para chegar a tal, essas vulnerabilidades podem ser exploradas por ameaças preparadas para obter informações sobre as falhas presentes em seus alvos, os dispositivos vulneráveis (SALADIN, 2017).

Conhecido como *Penetration Test* (*PenTest*, do inglês, Teste de Penetração), trata-se de simulações de tentativas de invasão, para identificação de vulnerabilidades de um dispositivo e o esforço de explorá-las (MENEZES, 2015 et al, apud MARTINS, 2018).

Nesse sentido, menciona Martins (2018, p. 32) que "*pentests* ajudam a avaliar quais vulnerabilidades podem ser exploradas e o grau de exposição da informação ou qual o nível de controle da rede um invasor poderia obter caso explore as vulnerabilidades com sucesso".

O *pentest* é composto por fases, que envolvem desde a etapa de coleta de informações para conhecimento sobre o alvo, enumeração dos serviços presentes no alvo,

análise das vulnerabilidades encontradas, a exploração de cada uma delas e o relatório com detalhes, evidenciando cada etapa. (SOBRAL e DA CRUZ, 2018).

2.2. IEEE 802.11

De acordo com o *Institute of Electrical and Electronic Engineers* (IEEE, 2007), a arquitetura do padrão 802.11 é composta por diferentes elementos que colaboram entre si para disponibilizar a WLAN e possibilitar que as estações se locomovam sem afetar as camadas superiores da rede.

Com efeito, Gast (2005, p. 13) segmenta o padrão 802.11 em quatro componentes físicos principais, sendo eles:

a. Ponto de acesso ou *Access Point* (AP): dentre outras funções, ele o define como um equipamento responsável, principalmente, pela essencial conversão de *frames* - ou quadros – para outros tipos de *frames* para que seja possível encaminhá-los a internet;

b. Sistema de distribuição: elemento lógico dessa tecnologia utilizado para encaminhamento dos *frames* ao seu destino de maneira que possua normalmente seu *backbone* estruturado no padrão *Ethernet*, podendo conectar fisicamente múltiplos possíveis AP's associados que cobririam uma área extensa;

c. Estação: dispositivo computacional, em grande maioria portátil, que possui interface de rede sem fio;

d. Meio sem fio: meio utilizado para transmitir os quadros entre estações onde estão presentes os protocolos de camada física como aqueles relacionados à radiofrequência (RF) ou infravermelho.

Nesse sentido, Tanenbaum e Wetherall (2011, p. 299) conceituam que as redes WLAN podem operar em dois modos: infraestrutura e *ad hoc*. Eles apontam que no primeiro modo cada cliente ou estação móvel qualquer conectado está associado à um AP que, por sua vez, está conectado à uma outra rede, comumente internet ou intranet. Acerca do segundo modo, os autores descrevem uma configuração em que os dispositivos se conectam diretamente à WLAN, permitindo a comunicação direta entre os clientes, sem a necessidade de AP's intermediários e sem conexão WAN.

Kurose e Ross (2017, p. 533) afirmam que o bloco fundamental de uma WLAN é conhecido como conjunto básico de serviço (BSS, do inglês, B*asic Service Set*) que

compreende uma ou mais estações sem fio e uma estação base (AP) e é identificado pelos dispositivos através de um identificador definido como *Service Set Identifier* (SSID) por meio qual associa-se com clientes.

Em congruência, Gast (2005, p. 14) vai além mencionando um*a* associação de BSS's como conjunto de serviço estendido (ESS, do inglês E*xtended Service Set*) e uma rede *ad-hoc* como conjunto de serviço estendido independente (IBSS, do inglês, *Independent* B*asic Service Set*).

Considerando o modelo de referência OSI (*Open Systems Interconnection*), para Vilela (2021, p. 25) o padrão 802.11 age nas camadas inferiores do modelo, ou seja, física e enlace. Segundo ele, enquanto a camada um compreende os sinais de RF e modulação tanto para transmissão, quanto para recepção, a camada dois é responsável pelo controle de acesso ao meio compartilhado e a especificação do formato do quadro na comunicação.

Conforme Coleman e Westcott (2021) pontuam, desde a publicação do protocolo 802.11 diversas ratificações de versões anteriores e novas publicações relacionadas a melhorias e evoluções do padrão foram lançadas envolvendo as diversas variações como 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax e 802.11be, o qual ainda está em desenvolvimento.

2.3. WEP

Como Lehembre (2018a) aponta, o protocolo WEP (*Wired Equivalent Privacy*) foi apresentado no final dos anos 1990 como norma no primeiro padrão IEEE 802.11. Ele surgiu em função da preocupação relacionada aos mecanismos de segurança utilizados para o padrão IEEE 802.11, o qual apresentou ao longo do tempo uma gama de vulnerabilidades desde a sua homologação (VILELA, 2021, p. 25).

O WEP é baseado no algoritmo de criptografia RC4 (*Rivest Cipher 4*, da RSA), com uma chave secreta de 40 bits ou 104 bits sendo combinada com um *Initialization Vector* (IV, do inglês, Vetor de Inicialização) de 24 bits para criptografar uma mensagem em texto simples M e seu *checksum* - o ICV (*Integrity Check Value*, do inglês, Valor de Verificação de Integridade) (LEHEMBRE, 2018b).

2.4. WPA

De acordo com Gonçalves e Linhares (2009), o protocolo *Wi-Fi Protected Access* (WPA) surgiu como uma correção dos problemas de segurança presentes em seu antecessor WEP mediante a incorporação do protocolo de criptografia *Temporary Key Integrity Protocol* (TKIP). O WPA é um protocolo que realiza troca de chaves dinâmicas, gerando uma chave única para cada sessão de comunicação, diferentemente do protocolo WEP que utiliza uma chave estática para criptografar o tráfego de rede, além dele utilizar 48 bits para o IV (GONÇALVES e LINHARES, 2009).

Relatado também por Weidman (2014a), o WPA substitui o verificador de mensagem *Cyclic Redundancy Check*, conhecido como CRC-32 e presente no WEP, para um algoritmo denominado *Message Authentication Code* (MAC), mudança a qual proporciona maior segurança ao sistema, pois dificulta a ação de invasores que tentam calcular as alterações no ICV, campo de controle usado em quadros de redes sem fio, resultantes de mudanças em bits individuais.

2.5. WPA2

Segundo Gonçalves e Linhares (2009), conforme o tempo foi passando, o WPA começou a ter seu desempenho diminuído e necessitou de uma nova versão que gerasse mais segurança e estabilidade para as redes sem fio, o WPA2. Como sua principal mudança, houve o acréscimo do protocolo de criptografia *Advanced Encryptation Standart* (AES), menos vulnerável a possíveis falhas de segurança do que o TKIP, suportando não somente 128 bits de tamanho de chave, mas também 192 e 256 bits, proporcionando níveis mais altos de segurança em comparação ao TKIP (GONÇALVES e LINHARES, 2009).

De acordo com Weidman (2014b), no WPA2 há a implementação um protocolo de criptografia criada especificamente para segurança de redes sem fio, a qual adiciona autenticação de mensagens e integridade, evitando que dados sejam interceptados ou modificados por invasores. O autor afirma que esse protocolo é baseado no AES e é conhecido como *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol* (CCMP).

3. ESTUDO DE CASO

O cenário base desse experimento fundamenta-se nas tentativas de quebra de senha dos protocolos de segurança de redes 802.11 (WEP, WPA e WPA2) com apoio de ferramentas especializadas e equipamentos pertinentes.

3.1. MATERIAIS E MÉTODOS

Para realização dos testes, foram necessários os seguintes materiais e ferramentas:

- Roteador TP-Link TL-WR740N, comum em ambientes de redes domésticas. É um dispositivo que suporta até 150 Mbps e opera na frequência de 2,4 GHz, e que suporta os protocolos de criptografia WEP e WPA/WPA2 para configuração de segurança de rede Wi-Fi;
- Um Adaptador USB Sem Fio Wi-Fi 2.4 GHz LV-UW06;
- Sistema Operacional Kali Linux, em destaque o conjunto de ferramentas Aircrack-ng.

3.2. QUEBRA DE SENHA WEP

Segundo Weidman (2014c), o WEP é um antigo protocolo de criptografia utilizado em roteadores que apresenta diversas falhas de segurança. Ele utiliza o algoritmo de cifra de fluxo RC4 e uma chave pré-compartilhada para criptografar e descriptografar os dados transmitidos, que, no entanto, possui problemas significativos, como a falta de aleatoriedade do IV e a fragilidade do ICV que tornam possível a um invasor recuperar a chave e modificar pacotes legítimos (WEIDMAN, 2014d).

Como dito por Weidman (2014e), ao reutilizar os IV's e explorar as fraquezas do ICV, um invasor pode realizar uma criptoanálise e obter acesso à rede protegida pelo WEP. Para ressaltar que o WEP não é considerado seguro e recomenda-se o uso de protocolos mais robustos como o WPA e o WPA2, os quais oferecem maior proteção e criptografia, foi-se configurada uma rede Wi-Fi com parâmetros inseguros para evidência prática da existência da vulnerabilidade, visto na Figura 1 (WEIDMAN, 2014f).

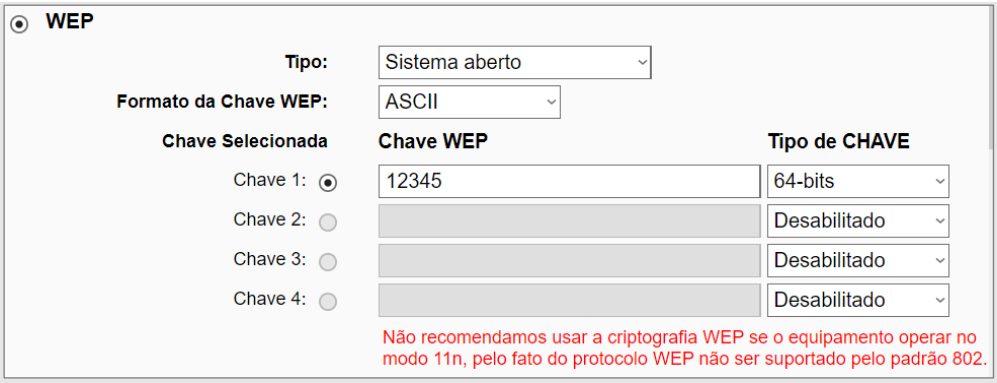


Figura 1 - Definição de senha em rede Wi-Fi com criptografia WEP

Fonte: Autores próprios (2023)

Inicialmente, foi realizada a falsificação de autenticação por meio da ferramenta Aireplay-ng, técnica mencionada por Weidman (2014g), utilizada para ludibriar o roteador e permitir que os pacotes fossem interpretados como confiáveis, comprovado na Figura 2. Para tal finalidade, foram inseridos o endereço *Media Access Control* (MAC) do ponto de acesso alvo e, posteriormente, o endereço MAC do adaptador USB sem fio Wi-Fi LV-UW06 utilizado.

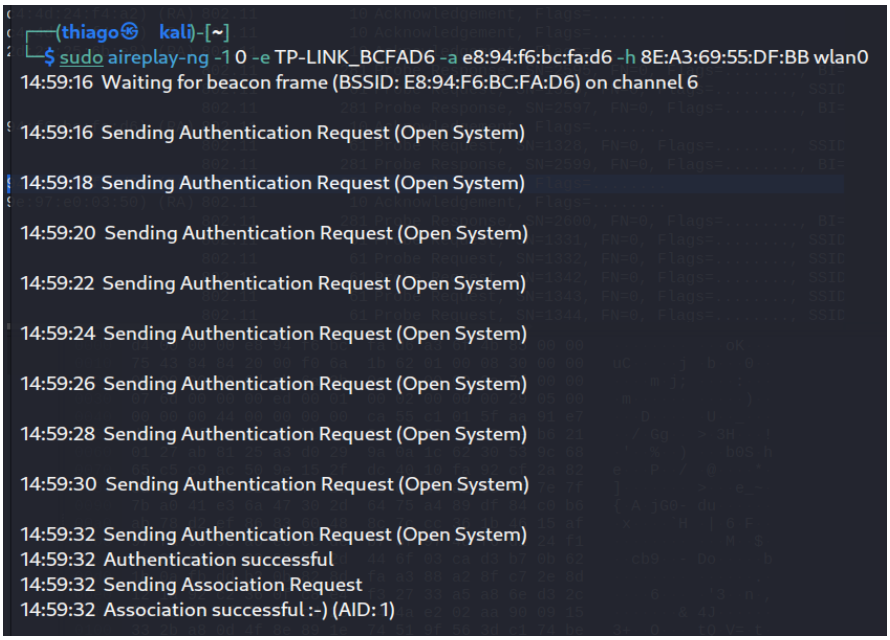


Figura 2 - Falsificação de autenticação com Aireplay-ng

Fonte: Autores próprios (2023)

Com a autenticação falsificada, ao empregar a técnica mencionada por Weidman (2014h) foi utilizada a ferramenta Airmon-ng para colocar o adaptador Wi-Fi em modo

monitor e, em seguida, foi iniciada a captura de pacotes com o software Wireshark. Com a captura de pacotes em andamento, foi dado início ao ataque para tentar quebrar a senha da rede Wi-Fi configurada, utilizando a ferramenta Aircrack-ng.

Após a obtenção da falsificação de autenticação, foi aplicada a técnica *Address Resolution Protocol* (ARP*) Request Replay*, visto na Figura 3. Segundo Weidman (2014i), esta técnica consiste em aguardar a geração de uma solicitação ARP na rede e retransmiti-la para o ponto de acesso, que retransmitirá um novo IV, assim, a quebra de criptografia vai se tornando possível a cada pacote ARP enviado. Esta técnica é amplamente utilizada por invasores para explorar vulnerabilidades em redes Wi-Fi que utilizam o protocolo WEP, sendo considerada eficiente (WEIDMAN, 2014j).

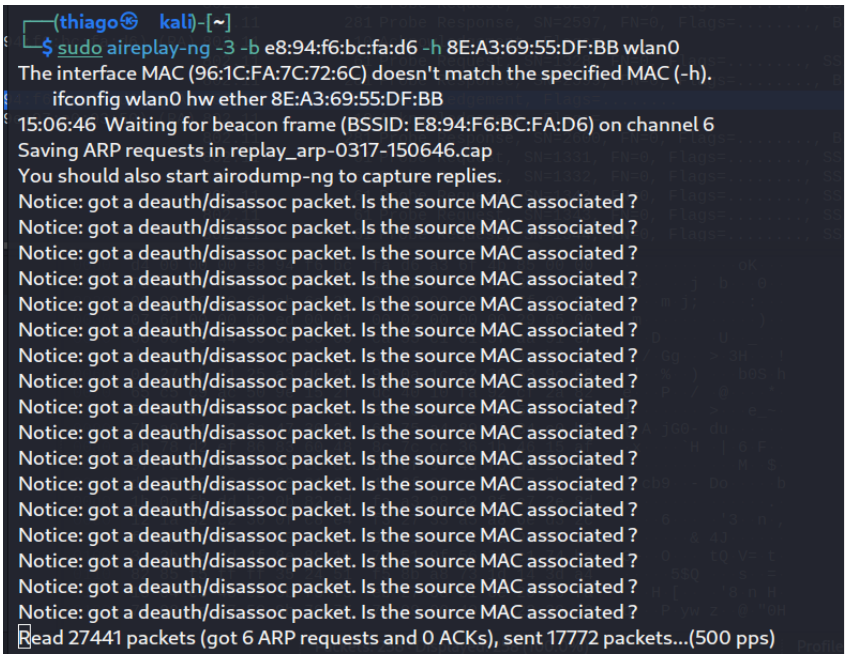


Figura 3 – Retransmissão de pacotes ARP

Fonte: Autores próprios (2023)

Com apoio de uma ferramenta de captura de tráfego específica para tecnologias 802.11, como o Airodump-n, foi possível capturar os IV's gerados na etapa anterior. De acordo com Weidman (2014k), a quantidade de IV's necessários para quebrar uma chave WEP depende do tamanho dela. É citado como exemplo que para chaves de 64 bits é necessário capturar 250.000 IV's para quebrar a senha, enquanto uma chave WEP de 148 bits exigiria a captura de 1.500.000 IV's. O campo DATA na Figura 4 mostra a quantidade de IV's capturados até o momento.

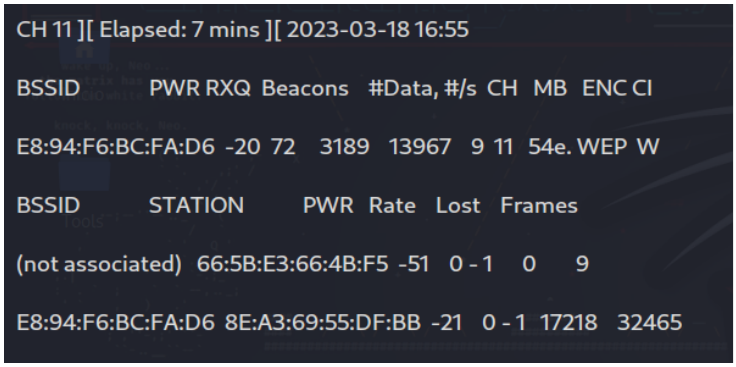


Figura 4 - Captura de IV's

Fonte: Autores próprios (2023)

Foi realizada a quebra de uma chave de 64 bits, como visto na Figura 5, para evidenciar a vulnerabilidade do protocolo WEP. Após a captura dos IV's por meio do Airodump-ng, utilizou-se a ferramenta Aircrack-ng para a análise matemática, técnica mencionada por Weidman (2014l), necessária para a quebra da criptografia. Com a aplicação dos algoritmos adequados, a ferramenta foi capaz de recuperar a senha do ponto de acesso alvo, conforme demonstrado na Figura 5, a seguir:

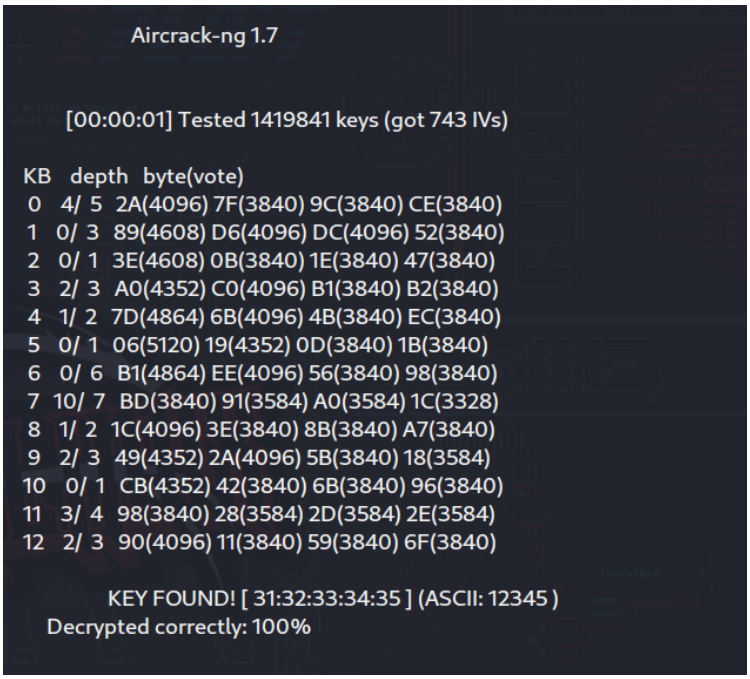


Figura 5 - Resultado da tentativa de quebra de senha

Fonte: Autores próprios (2023)

3.3. FORÇA-BRUTA EM SENHA COM CRIPTOGRAFIA WPA/WPA2

Segundo Weidman (2014m), há dois tipos de processos de conexões quando se refere a WPA e WPA 2, sendo o processo de conexão corporativa aquele que consiste em uma sequência de etapas para autenticação e estabelecimento de conexão segura em redes sem fio, que envolve um servidor *Remote Authentication Dial-In User Service* (RADIUS) e o ponto de acesso sem fio, que gera chaves de autenticação que são repassadas para o ponto de acesso sem fio e posteriormente utilizado para autenticação segura junto ao cliente por meio de um *handshake* de quatro vias.

Agora o processo de conexão pessoal relatado também por Weidman (2014n), não se faz necessário um servidor RADIUS e envolve apenas ponto de acesso e o cliente. Seu processo envolve apenas a utilização de chaves pré-compartilhadas e geradas através das frases-senha que são fornecidas em tentativas de conexão a uma rede Wi-Fi (WEIDMAN, 2014o).

Mencionado anteriormente e abordado por Weidman (2014p), o *handshake* de quatro vias, é uma etapa essencial na conexão de um ponto de acesso e um cliente, e durante essa fase, que um *Pairwise Master Key* (PMK) é criado na primeira etapa da conexão, usando informações como a frase-senha, conhecida como *Pre-Shared Key* (PSK), Service Set Identifier (SSID) e seu tamanho, além de outros parâmetros (WEIDMAN, 2014q).

Em seguida, de acordo com Weidman (2014r), ocorre o *handshake* de quatro vias, onde o ponto de acesso e o cliente trocam mensagens para estabelecer um canal de comunicação e trocar as chaves de criptografia. Durante esse processo, é criado um *Pairwise Transient Key* (PTK) usado para criptografar o tráfego entre o AP e o cliente, enquanto um *Group Transient Key* (GTK) é trocado para criptografar o tráfego transmitido (WEIDMAN, 2014s).

Weidman (2014t) pontua que o PTK é composto pelo PMK, *nonces*, que são números aleatórios do ponto de acesso e do cliente, e os endereços MAC. O AP e o cliente trocam *nonces* e endereços MAC para gerar o PTK, e assim, o cliente envia um *Message Integrity Code* (MIC) para garantir a integridade da mensagem, calculado com a frase-senha correta, e se o MIC estiver correto, o AP envia o GTK e o MIC para o cliente, e o cliente confirma o GTK na última etapa do *handshake* (WEIDMAN, 2014u).

De acordo com Weidman (2014v), o WPA e o WPA2 utilizam algoritmos de criptografia mais desenvolvidos em comparação ao WEP, tornando mais difícil para invasores recuperarem a chave através da captura de tráfego e realização de criptoanálise. No entanto, a fraqueza nas redes WPA/WPA2 está na qualidade da chave pré-compartilhada ou mais comumente conhecido, senha (WEIDMAN, 2014w).

Segundo Weidman (2014x), é viável realizar a quebra de uma senha por meio da captura do *handshake* de quatro vias. Para isso, utiliza-se o algoritmo de h*ashing Password-Based Key Derivation Function* 2 (PBKDF2) com a frase-senha correta e o SSID do ponto de acesso, o que possibilita a geração da chave compartilhada (PMK). Em seguida, emprega-se os nonces e endereços MAC capturados para o cálculo do PTK. Através da comparação dos MICs resultantes com os presentes no *handshake* capturado, é possível determinar a veracidade da senha utilizada. Essa técnica pode ser aplicada mediante a utilização de uma lista de palavras para tentar identificar a senha correta (WEIDMAN, 2014y).

Com o objetivo de evidenciar as vulnerabilidades existentes nos protocolos WPA e WPA2, foi realizado um teste para demonstrar como a segurança desse protocolo também pode ser comprometida por meio do uso de senhas fracas. Para essa finalidade, foi configurada uma rede Wi-Fi, visto na Figura 6, com protocolo WPA em modo de conexão pessoal e a senha "password123".

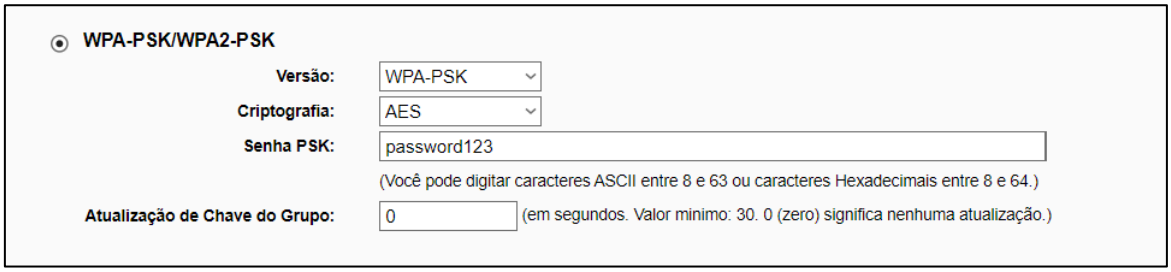


Figura 6 - Definição de senha em rede Wi-Fi com criptografia WPA/WPA2

Fonte: Autores próprios (2023)

Utilizando-se a técnica relatada por Weidman (2014z), no primeiro passo, é preciso capturar um *handshake* para prosseguir na quebra da senha da rede Wi-Fi. Para essa finalidade, foi utilizado o Airodump-ng, que segundo Weidman (2014aa), é uma ferramenta do Aircrack-ng que possibilita a monitoração do tráfego de rede e a captura do *handshake* gerado quando um dispositivo cliente se conecta à rede. Dessa forma, foi

iniciada a captura, como visto na Figura 7, informando ao Airodump-ng o endereço MAC do ponto de acesso alvo e especificando um nome de arquivo para a saída da captura (WEIDMAN, 2014ab).

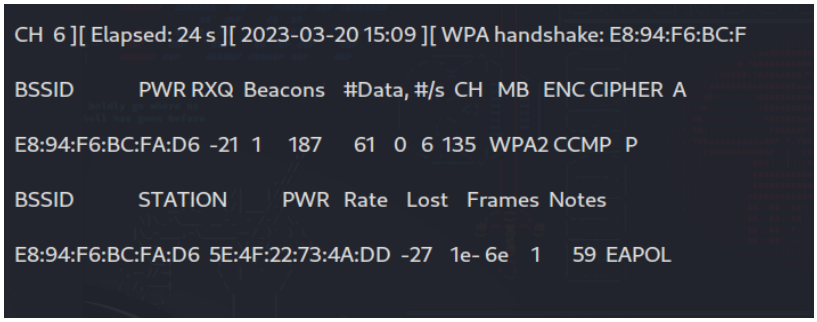


Figura 7 - Captura de *Handshake*

Fonte: Autores próprios (2023)

Conforme demonstrado, o arquivo de captura de pacotes (CAP, do inglês *Wireless LAN Packet Capture*) gerado no passo anterior foi aberto no Wireshark (ferramenta de análise de tráfego de rede), visto na Figura 8. Além disso, foi realizada a conexão manual de um dispositivo pessoal à rede Wi-Fi em questão e com om a captura do *handshake*, foi possível avançar para o próximo passo.

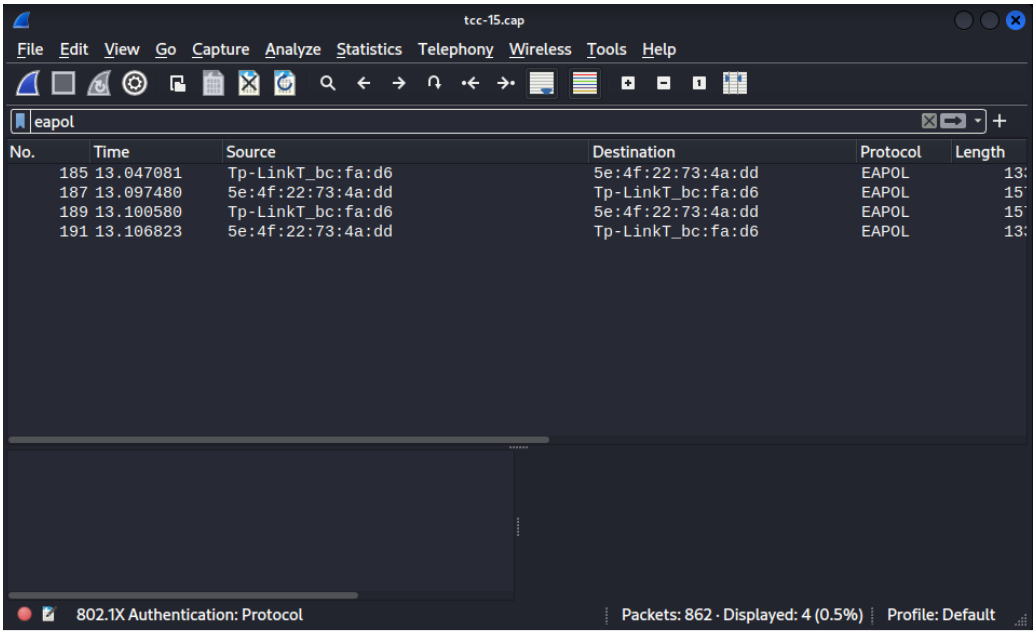


Figura 8 - Captura de *Handshake* no Wireshark

Fonte: Autores próprios (2023)

Com o *handshake*, pode-se partir para a quebra da senha por meio de um ataque de força-bruta, de acordo com Weidman (2014ac). Para esse fim, é necessária uma lista de palavras comuns de senhas, conhecida como *wordlist.*

Por meio da lista de palavras, segundo Weidman (2014ad), é possível comparar os valores das *hashes* das senhas com os presentes no *handshake* capturado, e caso os valores correspondam, a senha será descoberta, desde que a palavra-chave conste na *wordlist*. O exemplo a seguir evidencia como o arquivo da lista de palavras e o arquivo CAP capturado. Os demais passos de captura são executados pela ferramenta Aircrack-ng, que no caso apresentado, identificou que a senha utilizada na rede Wi-Fi é "password123", conforme evidenciado na Figura 9, em sequência:

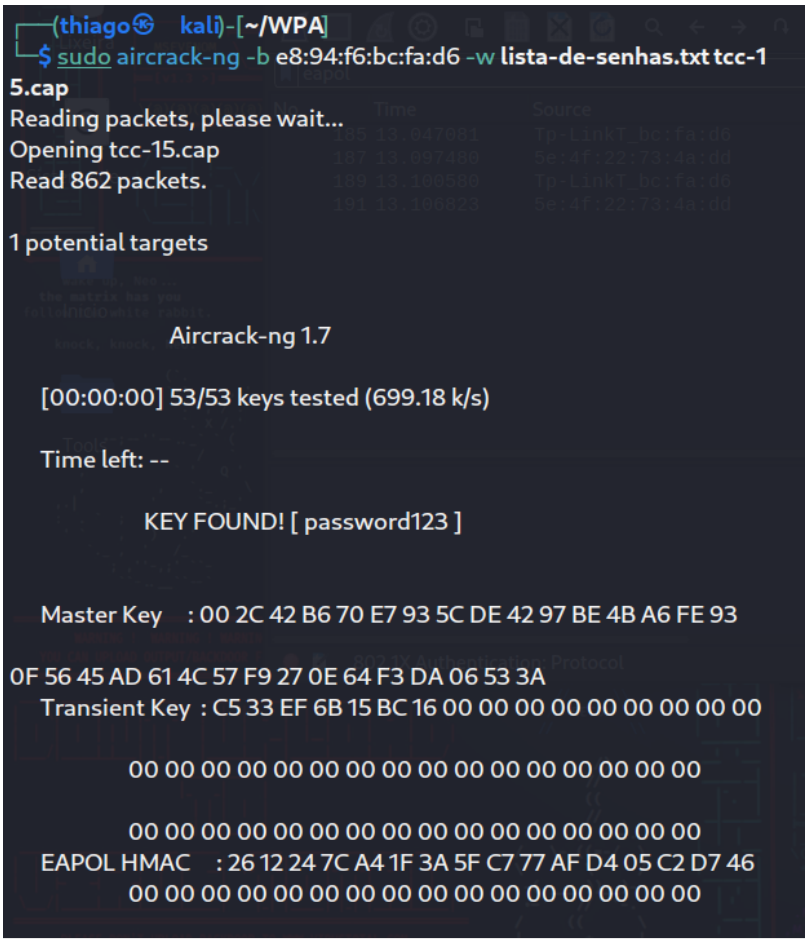


Figura 9 - Quebrando senha WPA/WPA2

Fonte: Autores próprio (2023)

4. CONSIDERAÇÕES FINAIS

Nesse estudo, com base na utilização de ferramentas e técnicas de teste de penetração voltado à quebra de criptografia atrelada aos protocolos de segurança inerentes ao padrão IEEE 802.11 comprovou-se a existência de vulnerabilidades nos protocolos de criptografia WEP e WPA/WPA2 cujas consequências resultam no comprometimento da segurança de acessos a essas redes.

Em análise, foram identificados problemas significativos de segurança no protocolo WEP, que é mais antigo e defasado. Esses problemas foram corrigidos no protocolo WPA, o qual é recomendado como substituição ao WEP. No entanto, também foram encontrados problemas de segurança para esse sucessor.

Apesar das vulnerabilidades, medidas adotadas pelos administradores dessas redes podem dificultar o trabalho de pessoas maliciosas e tornar a rede mais segura. Um exemplo é a utilização de senhas fortes, que devem ser longas, complexas, únicas e dinâmicas. É importante evitar senhas comuns e previsíveis, como sequências numéricas ou palavras do dicionário. Recomenda-se o uso de combinações de letras maiúsculas e minúsculas, números e caracteres especiais para fortalecer a segurança das senhas.

Há também a necessidade de monitoração da rede através de ferramentas especializadas e registro de eventos, observando tentativas de acesso não autorizado ou atividades de força bruta. Além disso, a restrição de acesso físico aos dispositivos de rede ou ambientes críticos pode ajudar a evitar a manipulação e mitigar riscos relacionados a segurança da informação.

Espera-se que este projeto conscientize usuários e administradores de redes da existência de problemas que possam comprometer a segurança de suas redes sem fio evidenciando alguns métodos passíveis de serem utilizados por pessoas mal-intencionadas. Para trabalhos futuros, planeja-se testes no atual padrão de protocolo de segurança para redes Wi-Fi: WPA3.

REFERÊNCIAS

CISCO. **Cisco Annual Internet Report (2018–2023)**. [S. L.], 2020.

COLEMAN, David D.; WESTCOTT, David A. CWNA **Certified Wireless Network Administrator Study Guide: Exam CWNA-108**. 6. ed. Indianapolis, In: John Wiley & Sons, 2021. 1088 p.

ETSI. **IPv6-based Internet of Things Deployment of IPv6-based Internet of Things**. Valbonne, França, 2017.

GAST, Matthew S. 802.11 **Wireless Networks: The Definitive Guide**. 2. ed. Sebastopol, CA: O'Reilly, 2005.

HKCERT. **Device (Wi-Fi) Security Study: March 2020**. [S. L.], 2020.

HOWARTH, Josh. **Internet Traffic from Mobile Devices (2022)**. Exploding Topics, disponível em: <https://explodingtopics.com/blog/mobile-internet-traffic>. Acesso em: 20 nov. 2022.

IEEE STD 802.11-2007. **Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications**. Institute of Electrical and Electronic Engineers (IEEE), Revision of IEEE Std 802.11-1999, New York: IEEE Press, 2007.

KUROSE, James F.; ROSS, Keith W. **Computer Networking: A Top-Down Approach**. 7th ed. Boston: Pearson, 2017.

LEHEMBRE, Guillaume. **Wi-Fi security – WEP, WPA and WPA2**. 2005. Disponível em: https://repository.root-me.org/Réseau/EN%20-%20Hacking%20wifi.pdf. Acesso em: 03 abr. 2023.

LINHARES, André Guedes; GONÇALVES, PA da S. **Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11 w**. Universidade Federal de Pernambuco (UFPE)-Centro de Informática (CIn), 2009.

LOCHHAAS, Mark. **Wireless Connectivity for the Internet of Things**. [S. L.]: Advantech, 2016.

LUETH, Knud Lasse. **State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time**. IoT Analytics, disponível em: <https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time>. Acesso em: 20 nov. 2022.

MARTINS, Jonathan dos Santos. **EXPLORAÇÃO DE VULNERABILIDADES EM REDES IOT**, 2018.

SALANDIN, Alexander Torette. **Exploração de vulnerabilidades em pequenas empresas**. 2017.

SANTOS, E. E.; SOARES, T. M. M. K. **Riscos, ameaças e vulnerabilidades: o impacto da segurança da informação nas organizações**. 2018.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico**. São Paulo, SP: Cortez, 2013.

SHALF, John. The future of computing beyond Moore's Law. **Phil. Trans. R. Soc. A**, Berkeley, CA, v. 378, n. 2166, p. 1-15, mar. 2020.

SOBRAL, Maria Gabriele De Freitas Xavier; DA CRUZ, RAINNY SANTOS. **ANÁLISE DE VULNERABILIDADE DE REDES LOCAIS, UM ESTUDO DE CASO: IFPR-CAMPUS PARANAGUÁ**, 2018.

TANENBAUM, A. S.; WETHERALL, D. J. **Computer Networks**. 5. ed. Boston: Pearson, 2011.

VILELA, Douglas Willer Ferrari Luz. **DESENVOLVIMENTO DE IDS BASEADO NO MODELO DE RNA ARTMAP FUZZY COMO FERRAMENTA DE SEGURANÇA EM REDES WI-FI**. 2021. 67 f. Tese (Doutorado) - Curso de Engenharia Elétrica, Faculdade de Engenharia, Universidade Estadual Paulista "Júlio de Mesquita Filho", Ilha Solteira, 2021.

WEIDMAN, G. **Testes de Invasão: Uma Introdução Prática ao Hacking**. 1ª ed. São Paulo: Novatec, 2014.