PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

SEGURANÇA EM REDES WIRELESS IEEE 802.11 E SUAS VULNERABILIDADES

JOÃO ALVES DA SILVA NETO

GOIÂNIA
2021

JOÃO ALVES DA SILVA NETO

SEGURANÇA EM REDES WIRELESS IEEE 802.11 E SUAS VULNERABILIDADES

Trabalho de Conclusão de Curso apresentado por João Alves Da Silva Neto à Pontifícia Universidade Católica de Goiás como requisito parcial para obtenção do título de Bacharel em Ciência da Computação.

Orientadora:

Prof.ª Ma. Angélica da Silva Nunes.

Banca examinadora:

Prof. Me. Rafael Leal Martins

Prof. Me. Wilmar Oliveira de Queiroz

GOIÂNIA

2021

JOÃO ALVES DA SILVA NETO

SEGURANÇA EM REDES WIRELESS IEEE 802.11 E SUAS VULNERABILIDADES

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Ciência da Computação em: 10 /12/2021.

Profª. Ma Ludmilla Reis Pinheiro dos Santos.

Coordenadora de Trabalho de Conclusão de Curso

Banca Examinadora:

Orientadora: Profª. Ma Angélica da Silva Nunes

Prof. Me. Rafael Leal Martins

Prof. Me. Wilmar Oliveira de Queiroz

GOIÂNIA

2021

DEDICATÓRIA

Dedico este trabalho aos meus pais, minha família, meus amigos e acima de tudo a Deus que me deu força e coragem para vencer todos os obstáculos encontrados ao longo do curso e aos professores, pelas correções e ensinamentos que me permitiram apresentar um melhor desempenho no meu processo de formação profissional.

AGRADECIMENTOS

Agradeço a professora Angélica por todo apoio durante o desenvolvimento deste trabalho.

RESUMO

Este trabalho apresenta uma análise dos protocolos de segurança do padrão IEEE 802.11, o qual é apresentado as características de cada protocolo, bem como suas fragilidades. Para discutir os protocolos de segurança do IEEE 802.11, foi estabelecida uma base de conhecimento sobre eles mostrando a sua estrutura e suas vulnerabilidades. O protocolo de segurança IEEE 802.11 é apresentado de forma progressiva, trabalhando com outros protocolos, mecanismos e padrões existentes em cada protocolo, bem como suas vulnerabilidades que são expostas para comprovar o perigo que cada vulnerabilidade representa para os usuários, de forma a manter a importância da pesquisa de segurança para seu desenvolvimento contínuo. Sendo por fim, as vulnerabilidades relacionadas à autenticação dos protocolos WPA e WPA2 apresentadas, o que comprovou as suas falhas. Como resultado, foi verificado que mesmo com padrão IEEE 802.11 definindo protocolos de segurança ele ainda exige que os usuários, sejam eles residenciais ou comerciais compreendam sobre as formas de proteção de cada um dos protocolos.

Palavras-Chave: IEEE 802.11; Protocolos; Segurança; Vulnerabilidades.

ABSTRACT

This work presents an analysis of the security protocols of the IEEE 802.11 standard, which is presented the characteristics of each protocol, as well as your weaknesses. To discuss the security protocols of IEEE 802.11, it was established a knowledge base about them showing their structure and vulnerabilities. The IEEE 802.11 security protocol is presented progressively, working with other protocols, mechanisms and standards existing in each protocol, mechanisms and standards existing in each protocol, as well as their vulnerabilities that are exposed to prove the danger that each vulnerability represents for users, to maintain the importance of security research for its continued development. Finally, the vulnerabilities related to the authentication of the WPA and WPA2 protocols presented, which proved their flaws. As a result, it was found that even with the IEEE 802.11 standard defining security protocols it still requires that users, whether residential or commercial, understand the ways to protect of each of the protocols.

Keywords: IEEE 802.11; Protocols; Safety; Vulnerabilities.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AES – Padrão de criptografia avançado - *Advanced Encryption Standard*

AC – Autoridade Certificadora

AP – Ponto de Acesso sem fio - *Acess Point*

ARP – Protocolo de Resolução de Endereço - *Address Resolution Protocol*

BIP-GMAC – Código de autenticação de mensagens de Galois do protocolo de integridade de difusão / multicast - *Broadcast/Multicast Integrity Protocol Galois Message Authentication Code*

BSS – Conjunto de serviços básicos - *Basic Service Set*

BSSID – Identificação do conjunto de serviços básicos - *Basic Service set Identification*

CBC-MAC – Código de autenticação de mensagens de encadeamento de bloco de cifra do modo de contador - *Counter Mode Cipher Block Chaining-Message Authentication Code*

CCMP – Protocolo de Código de Autenticação de Mensagens em Cadeia de Blocos de Cifra no Modo Contador - *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*

CRC – Verificação de redundância Cíclica - *Cyclic Redundancy Check*

CSMA-CA – Controle de acesso ao meio sem Fio - *Carrier Sense Multiple Access with Collision Avoidance*

CSMA-CD – Acesso múltiplo com detecção de portadora com detecção de colisão - *Carrier Sense Multiple Access with Collision Detection*

DHCP – Protocolo de Configuração Dinâmica de Endereços de Rede - *Dynamic Host Configuration Protocol*

DoS – Negação de serviço

EAP – Estrutura Analítica do Projeto - *Extensible Authentication Protocol*

EAP-pwd – Protocolo de Autenticação Extensível - *Extensible Authentication Protocol Password*

ECDH – Curva elíptica Diffie *Hellman* - *Elliptic Curve Diffie-Hellman*

ECDSA – Algoritmo de Assinatura Digital de Curva Elíptica - *Exchange and Elliptic Curve Digital Signature Algorithm*

FCS – Sequência de verificação de quadro - *Frame Check Sequence*

GCMP-256 – *Galois/Counter Mode Protocol 256-bit*

HMAC – Código de autenticação de mensagens baseado em Hash - *Hashed Message Authentication Mode*

HMAC-SHA384 – Algoritmo de hash seguro do modo de autenticação de mensagens hash - *Hashed Message Authentication Mode Secure Hash Algorithm*

HTTPS – Protocolo de Transferência de Hipertexto Seguro - *Hyper-Text Transfer Protocol Secure*

ICV – Valor de verificação de integridade - *Integrity Check Value*

IEEE – Instituto de Engenheiros Eletricistas e Eletrônicos - *Institute of Electrical and Electronic Engineers*

IETF – Força-Tarefa de Engenharia da Internet - *Internet Engineering Task Force*

IP – Protocolo de Internet - *Internet Protocol*

IoT – Internet das Coisas - *Internet of Things*

IV – Vetor de Inicialização

KCK – Chave de Confirmação de Chave - *Key Confirmation Key*

KEK – Chave de Criptografia de Chave - *Key Encryption Key*

KSA – Algoritmo de Programação de chave - *Key Scheduler Algorithm*

MAC – Controle de acesso de mídia - *Media Access Control*

MITM – Homem no meio - *Man-In-The-Middle*

MIC – Código de integridade da mensagem - *Message Integrity* Code

NAT – Tradução do Endereço da Rede - *Network Address Translation*

NIC – Placa de interface de rede - *Network Interface Card*

NMAP – Mapeador de Rede - *Network Mapper*

OSI – Sistemas Abertos de Interconexão - *Open System Interconnection*

OWE – Criptografia Oportunista Sem Fio - *Opportunistic Wireless Encryption*

PMF – Quadros de gerenciamento protegidos - *Protected Management Frames*

PMK – Chave mestra par a par - *Pairwise Master Key*

PRGA – Algoritmo de Geração Pseudoaleatória - *Pseudo Random Generation Algorithm*

PRNG – Gerador de números pseudoaleatórios - *Pseudo Random Number Generator*

PSK – Chave Pré-Compartilhada - *Pre-Shared Key*

PTK – Chave transitória emparelhada - *Pairwise Transient Key*

RADIUS – Serviço de usuário discado com autenticação remota - *Remote Authentication Dial-in User Service*

RAM – Memória de Acesso Aleatório - *Random Access Memory*

RC4 - *Rivest Cipher 4*

SAE – Autenticação simultânea de Iguais - *Simultaneous Authentication of Equals*

SKA – Chave compartilhada para WEP

SSID – Identificador do conjunto de Serviço - *Service Set Identification*

TEK – Protocolo de integridade de chave - *Temporal Encryption Key*

TLS – Segurança da Camada de Transporte - *Transport Layer Security*

TKIP – Protocolo de integridade de chave temporal - *Temporal Key Integrity Protocol*

TMK – Chave de integridade de dados - *Temporal MIC Key*

VM – Máquina Virtual - *Virtual Machines*

WEP – *Wired Equivalent Privacy*

WIPS – Sistema de prevenção de intrusão sem fio - *Wireless Intrusion Prevention System*

Wi-Fi – Fidelidade sem fio - *Wireless Fidelity*

WLAN – Redes Locais sem fio - *Wireless Local Area Network*

WPA – *Wireless Protected Access*

WPA2 – *Wireless Protected Access 2*

WPA3 – *Wireless Protected Access 3*

SUMÁRIO

1 INTRODUÇÃO

As redes sem fio, também conhecidas como redes *wireless* surgiram como redes complementares às redes cabeadas, tendo como objetivo melhorar sua mobilidade e flexibilidade.

Graças a isso, ela vem se tornando a rede mais utilizada. “Indiscutivelmente se tornam a cada dia mais populares, sendo inegável a conveniência de sua utilização em lugares como conferências, aeroportos, cafés e hotéis” (Rufino, 2015, p. 15).

> Basta o usuário ligar seu equipamento sem fio ou notebook com placa *wireless* para que passe a ter acesso à *Internet*. Isso, porém depende da configuração dos equipamentos; no entanto, do mesmo modo que o acesso é facilitado para usuários legítimos, ele é facilitado também para possíveis hackers. (Nakamura & Geus, 2007, pp. 139-140).

Uma dessas ferramentas que vem ajudando-a a se popularizar cada vez mais é a *Internet Of Things* (IoT), ou em português, *Internet* das Coisas.

> [...] pressupõe que objetos comuns possam estar interligados à *Internet*, de modo a dotá-los da inteligência necessária para interagir e, de algum modo, auxiliar a vida das pessoas por meio da coleta de dados físicos, processamento e promoção de respostas através de atuadores eletromecânicos (Junior & Moreno, 2016, p. 270).

“Independentemente do crescimento futuro de equipamentos sem fio para *Internet*, já ficou claro que redes sem fio e os serviços móveis relacionados que elas possibilitam, vieram para ficar” (Kurose & Ross, 2014, p. 380).

Embora as redes *wireless* tenham evoluído desde seu início, a segurança não foi desenvolvida da mesma maneira, portanto, os usuários precisam tomar certos cuidados ao utilizá-la.

Segundo Gimenes (2005), quando o acesso malicioso consegue invadir, alterar ou excluir informações confidenciais, ou mesmo tornar o sistema inutilizável, a rede torna-se vulnerável. O que fez com que ao longo dos anos, políticas, tecnologias e protocolos fossem desenvolvidos para ajudar a melhorar a proteção da rede *wireless*.

O Instituto de Engenheiros Eletricistas e Eletrônicos, *Institute of Electrical and Electronics Engineers* (IEEE) padronizou as redes locais sem fio por meio do padrão IEEE

802.11 que, dentre outras coisas, define métodos para prover a confidencialidade e a integridade das informações que são transmitidas pela rede *wireless*.

O protocolo *Wired Equivalent Privacy* (WEP), *Wireless Protected Access* (WPA), *Wireless Protected Access II* (WPA2) e o *Wireless Protected Access 3* (WPA3) são os responsáveis por garantir esses mecanismos por meio da criptografia das mensagens transmitidas (Linhares & Gonçalves, 2010).

No entanto, existem técnicas que permitem capturar sinais da rede *wireless*, permitindo assim fazer uma leitura de pacotes tornando a tentativa de quebra de criptografia possível, podendo resultar em uma possível invasão bem-sucedida à uma determinada rede (Barros, 2021).

Justifica-se estudar este assunto, porque as redes *wireless* existem na vida da maioria da população mundial. No entanto, a maioria não tem conhecimento das vulnerabilidades que podem sofrer ao acessar redes abertas e, portanto, podem se tornar vítimas de intrusões e permitir que os invasores exponham seus dados. Por isso, é importante mostrar as principais vulnerabilidades e informar aos usuários como se proteger ao acessar redes *wireless*.

Diante deste contexto, este projeto visa responder à seguinte questão de pesquisa: Quais são as vulnerabilidades encontradas nas redes IEEE 802.11 e como minimizar os riscos de se tornar um alvo?

1.1 Objetivo geral

Identificar vulnerabilidades e suas contramedidas em redes IEEE 802.11.

1.2 Objetivos específicos

Os objetivos específicos deste trabalho são:

- Estudar os protocolos do padrão IEEE 802.11 e seus métodos de criptografia;
- Analisar a evolução dos métodos criptográficos bem como suas fragilidades;
- Estudar ferramentas voltadas para quebra de segurança em redes IEEE 802.11;
- Realizar ataques a uma rede IEEE 802.11 simulando uma rede pública de um *Shopping Center*;
- Identificar quais as contramedidas para cada um dos ataques.

1.3 Metodologia

Esta pesquisa segundo sua natureza é um resumo do assunto, pois busca sistematizar a área de conhecimento, indicando sua evolução. Neste caso, as áreas de conhecimentos de segurança e vulnerabilidades nas redes IEEE 802.11 (Wazlawick, 2014).

Segundo Wazlawick 2014, esta pesquisa é exploratória, a qual o autor, visa examinar um conjunto de fenômenos, buscando anomalias que não sejam ainda conhecidas e que possam ser, então, a base para uma pesquisa mais elaborada.

E segundo os procedimentos técnicos esta pesquisa é bibliográfica e experimental, na qual tem levantamento de dados, análise dos mesmos e uma busca pelas causas e explicações dos dados apresentados neste trabalho.

Como um trabalho de pesquisa bibliográfica, este projeto é fundamentado em estudo de artigos, teses, livros, entrevistas e reportagens por editoras e emissoras e indexadas.

Segundo Wazlawick (2014), esta pesquisa tem efeito de investigar os dados examinados e entender suas causas e explicações. Este projeto de pesquisa se propõe a abordar o tema de segurança em redes *wireless*, por meio da identificação das vulnerabilidades de redes IEEE 802.11 além de apresentar os levantamentos de dados encontrados sobre o assunto, buscar pelas causas e explicações dos dados apresentados neste trabalho.

> [...] proteger a comunicação e os serviços em uma rede sem fio é um problema complexo. Diversas variáveis e problemas podem ocorrer e comprometer a segurança de todo o ambiente. Por causa disso foram desenvolvidas diversas soluções para fornecer a um dispositivo uma maneira de provar a sua identidade de forma confiável para outra estação da rede sem fio. Infelizmente essas soluções não funcionam tão bem como se gostaria [...] (Assunção, 2013)

Para Gil (2017), um estudo experimental depende do objeto de pesquisa, das variáveis que podem manipulá-lo, do método de controle da variável e do método de observação do efeito da variável no objeto. Por exemplo, este trabalho que visa mostrar os principais riscos que ao acessar uma rede *wireless*.

Gil (2017) define que para a realização de uma pesquisa experimental é necessário seguir os seguintes passos:

A) O problema dessa pesquisa é: Quais são as vulnerabilidades encontradas nas redes IEEE 802.11 e como minimizar os riscos de se tornar um alvo?

B) Para a definição do plano experimental, todos os protocolos de segurança foram estudados primeiro e, em seguida, foi realizada uma simulação de ataque na rede *wireless* para demonstrar as suas vulnerabilidades.

C) Quanto ao ambiente experimental foi implementado no Kali Linux.
   - Configurações da máquina:
     - Sistema Operacional: Windows 11.
     - Processador: AMD Ryzen 7 3700U com Radeon Vega Mobile Gfx, 2300 Mhz, 4 Núcleo(s), 8 Processador(es) Lógico(s).
     - Memória Acesso Aleatório (RAM) em inglês *Random Acess Memory*: 8 GB.
   - Foi utilizada a virtualização de uma máquina utilizando o VMWare versão 16.1.2 com o Kali Linux versão 2021.1.
   - Os *softwares* utilizados para fazer a simulação do ataque foram as ferramentas do aircrack-ng da versão 1.6.
     - Airodump-ng versão 1.6.
     - Aireplay-ng versão 1.6.

D) A coleta de dados foi feita de forma bibliográfica buscando artigos, livros e documentos mais recentes para responder a seguinte questão: Quais são as vulnerabilidades ao acessar uma rede sem fio e como minimizar esse risco?
   - Quais são as vulnerabilidades ao acessar uma rede sem fio:
     Foi feito o teste das principais vulnerabilidades dos protocolos do IEEE 802.11 para saber se realmente a rede é vulnerável.
   - Como minimizar os riscos:
     Em concordância com a pesquisa bibliográfica na parte prática foram apontados os pontos de defesa dos ataques.
   - Foram capturados os dados trafegados na rede utilizando o *a*irodump-ng. Com ele foi possível ter acesso aos dados da vítima como o endereço Mac do *Access Point*, saber qual o tipo de cifra que a vítima utiliza, qual o protocolo de segurança e outros dados.

E) A análise dos dados foi realizada através de elementos que foram obtidos do qual se procede a análise dos fatos. De posse dessas análises os resultados foram discutidos visando inferir conhecimentos relativos às condições das principais vulnerabilidades e

as mais frequentes a rede sem fio, para incluí-las como indicadores de alerta para a população.

Foram analisados todos os resultados obtidos a partir dos ataques de captura e de invasão com o interesse de evitar a vulnerabilidade de cada protocolo do IEEE 802.11;

F) O trabalho foi registrado em forma de uma monografia de TCC.

1.4 Estrutura da monografia

O Capítulo 2 apresenta as redes sem fio e descreve os conceitos e recursos principais do padrão IEEE 802.11.

No terceiro capítulo os protocolos de criptografia WEP, WPA, WPA2 e WPA3 são definidos detalhadamente, e é feita comparação entre os protocolos, levando em consideração a confiabilidade, a integridade, a autenticidade e a vulnerabilidade.

No quarto capítulo, é apresentado o ambiente de testes e as ferramentas que foram utilizadas para a simulação do ataque a uma rede aberta.

O quinto capítulo apresenta as vulnerabilidades de autenticação dos protocolos WPA e WPA2 por meio de três ataques diferentes. O primeiro tipo de ataque é um ataque de desautenticação, seguido por ataque *rogue* AP e finalizando com MITM, em que cada um são apresentadas suas conclusões e métodos de segurança específicos para evitá-los.

O último capítulo descreve as conclusões obtidas durante o desenvolvimento deste trabalho e recomendações para trabalhos futuros sobre questões importantes e complementares para redes IEEE 802.11.

2 PADRÃO IEEE 802.11

2.1 Características

Existem muitos padrões de Rede Local sem Fio (WLAN), mas considerando 2021, o mais popular e comumente utilizado é o IEEE 802.11, que consiste em um conjunto de padrões e especificações de rede sem fio para manter sua padronização (Assunção, 2013).

Com isso em mente, foi proposto um modelo de referência do modelo *open system interconnection* (OSI) em português sistemas abertos de interconexão para redes *wireless*, que visa cobrir a camada física e a camada de enlace de dados. Portanto, além de ser o padrão mais utilizado, o IEEE 802.11 também define uma combinação de protocolos de comunicação para redes sem fio (Rufino, 2015).

Segundo Rufino (2015) o padrão IEEE 802.11 usa um método chamado CSMA / CA (*Carrier Sense Multiple Access com Collision Avoidance*), que é semelhante à Ethernet LAN. CSMA / CD (*Carrier Sense Multiple Access com Collision Detection*), é um método de transmissão com maior grau de ordenação e parâmetros mais restritivos que seu antecessor (CSMA / CD), o que ajuda a reduzir a ocorrência de conflitos na rede.

Quando o nível do sinal intermediário aumenta, as máquinas interconectadas pela rede reconhecem a colisão. Antes da transmissão efetiva do pacote de dados, a estação informará a transmissão e o tempo necessário para realizar a tarefa. Desta forma, as estações não tentarão transmitir porque sabem que o canal está sendo usado por outra máquina, mas o tempo que a máquina espera por elas para enviar os pacotes de dados não é incerto ou aleatório, elas vão detectar quando o meio está livre (RUFINO, 2015).

É uma forma eficaz de gerenciar e classificar o tráfego de pacotes de dados em uma rede de computadores. Tem um impacto relacionado na redução de conflitos. No entanto, é importante notar que a intenção de apenas transmitir pacotes de dados aumentará o tráfego, afetando o desempenho de a Web. O dispositivo na (WLAN) deve detectar o meio para verificar a potência (o estímulo de RF está acima de um certo limite) e esperar que o meio esteja livre antes de transmitir (RUFINO, 2015).

2.2 Elementos de uma rede sem fio

2.2.1 *Access Point* – (AP)

O *Access Point* (AP) atua como uma ponte de passagem de dados entre a rede fixa (com fio) e o cliente. Em comparação direta com a rede com fio, é como se o AP desempenhasse o papel de *switch* e a onda de rádio fizesse o papel do cabo (Nakamura & Geus, 2007).

É possível ser utilizado como um servidor *Dynamic Host Configuration Protocol* (DHCP), que ele interpreta com a *Network Address Translation* (NAT) para fazer a tradução do endereço para satisfazer vários usuários com apenas um endereço *Internet Protocol* (IP).

2.2.2 *Service Set Identification* – (SSID)

Segundo (Kurose & Ross, 2014) o *Service Set Identification* (SSID), consiste em um conjunto de caracteres alfanuméricos usados para identificar redes sem fio. A maioria dos dispositivos sem fio habilita a transmissão SSID por padrão para habilitar a localização do AP durante a implantação.

Kurose, 2014 aconselha que depois de implementar este método, a transmissão do SSID do AP deve ser desabilitada, preservando assim direitos de acesso "desconhecidos" e permitindo que apenas usuários que conheçam um SSID válido entrem. Se o sistema de criptografia não estiver habilitado, o SSID pode ser usado como senha para usuários não autorizados, pois o AP só pode ser autenticado se o usuário conhecer os caracteres exatos que identificam os direitos de acesso à rede e utilizar as informações disponíveis.

2.2.3 Controle de Acesso ao Meio – (MAC)

Segundo Rufino (2015), para que uma rede funcione de forma eficiente e eficaz, seja *Ethernet* ou Wi-Fi, cada dispositivo da rede deve ter a sua identidade para que mecanismos que controlam a rede consigam organizar a mesma. A identificação é definida pelo IEEE como um número único para cada dispositivo fabricado no mundo para evitar qualquer tipo de conflito ou conflito entre eles.

O Wi-Fi inclui a camada física e a camada de enlace de dados do modelo OSI, na qual na camada física, lida com questões relacionadas às ondas de rádio (comprimento, amplitude etc.).

Na camada de enlace, tem-se a subcamada de *Media Access Control*, (MAC) em português controle de aceso de mídia é responsável por controlar a transmissão de dados e fornecer interação com dispositivos cabeados (se houver). A camada MAC também fornece serviços relacionados ao gerenciamento da mobilidade dos dispositivos.

Para mover pacotes de dados no canal compartilhado, a camada MAC usa o método *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA), muito semelhante ao *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD) do *Ethernet*.

A diferença é que o CSMA/CD retransmite quando ocorre um conflito, enquanto o CSMA/CA evita completamente o conflito. Em termos de endereçamento, o formato do endereço MAC do *Wireless Fidelity*, (*Wi-Fi)* em português fidelidade sem fio é o mesmo do *Ethernet*, ambos com 12 caracteres hexadecimais.

2.2.4 *Beacon Frame*

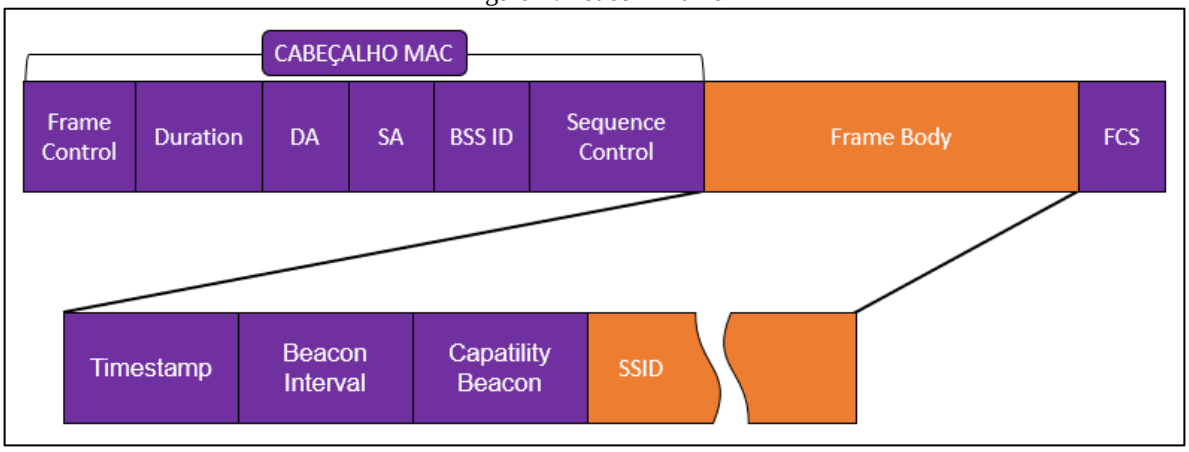
Os clientes que procuram uma rede precisam saber se existe um *hub* para que possam estabelecer a conexão correta com um determinado *hub*, que enviará um sinal para transmitir informações sobre sua existência.

Esse tipo de informação é denominado *beacon frame*, que se refere a um sinal de envio gratuito que pode orientar os clientes a entender a existência de um concentrador. Esses sinais podem ser suprimidos, sendo necessária apenas uma configuração simples no *hub*, com o objetivo de o ambiente no qual o *hub* esteja localizado não tenha livremente acesso às suas características, dificultando a utilização de uma determinada rede em um determinado ambiente.

O uso do *Beacon frame* é uma das ferramentas de administração que é utilizada em WLANS baseadas no IEEE 802.11, que contém todos os dados sobre a rede, simplificando assim o gerenciamento de redes sem fio e faz com que o AP e os dispositivos sem fio, o utilize para enviar quadros de gerenciamento da rede periodicamente. Assim, ele consegue anunciar a presença de uma rede sem fio e permite sincronizar a transmissão dos dados.

Os quadros de *beacon frame* consistem em um cabeçalho MAC o corpo e uma sequência de verificação de *frames* conforme apresentado na Figura 1.

Figura 1: *Beacon Frame*



Fonte: Figura adaptada do: (Vasconcellos, 2013) com o conteúdo desenvolvido pelo autor deste trabalho.

O cabeçalho MAC é composto dos campos:

- *Frame Control:* é composto por vários subcampos projetados para especificar diferentes características do quadro a ser enviado;
- *Duration*: é o encarregado por carregar a ID de associação da estação que transmite o quadro e o valor de duração definido para cada tipo de *frame*;
- DA: é o endereço para um quadro ou pacote de dados é enviado pela rede;
- SA: é o endereço de origem do quadro está sendo enviado;
- BSS ID: é o endereço único de 48 *bits* que identifica de maneira única um AP e um conjunto de estações sem fio (STA);
- *Sequence Control*: é utilizado para manter o fluxo do quadro, tem comprimento de 16 *bits* e é composto por um subcampo *Sequence Number* (12 *bits*) e um *Fragment Number* (4 *bits*). No caso de retransmissão, ambos permanecem inalterados.

No corpo do quadro, ficam todas as informações do *beacon frame*, tendo alguns campos como opcionais e outros obrigatórios, sendo os obrigatórios o:

- *Timestamp*: tempo em referência ao quadro de *beacon*, que é utilizado pelos dispositivos conectados, para sincronizar com a WLAN;
- *Beacon Interval*: intervalo de tempo entre duas transmissões de *beacon* consecutivas no quadro;
- *Capability Beacon:* informações sobre a capacidade da rede e do dispositivo;

- SSID: é o nome da rede ele é o principal componente dos *beacon*s, sendo a parte central de seu processo.

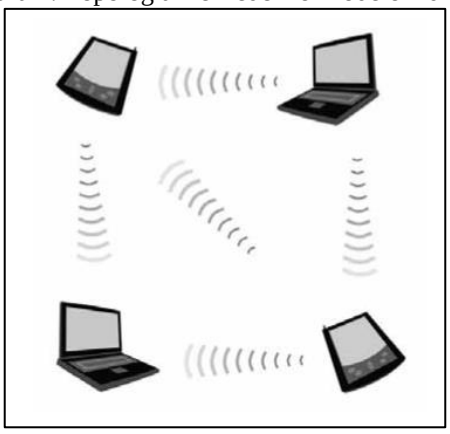
Após o cabeçalho MAC e o corpo do quadro, o *Beacon Frame* usa o *Frame Check Sequence* (FCS) para verificar se o conteúdo do quadro não foi adulterado ou danificado durante a transmissão.

2.3 Modo de operação

As WLANS em termos organizacionais, possuem dois modos de operação que são o *ad hoc* e o Infraestrutura.

A forma de funcionamento do *ad hoc*, conhecido como ponto a ponto, funciona através da comunicação entre estações, sem utilizar um AP para gerenciar a rede e oferecer os serviços (Rufino, 2015). Ela pode ser implementada utilizando técnicas de *broadcast* como mostra o modelo da Figura 2.

Figura 2: Topologia De Rede No Modelo Ad Hoc



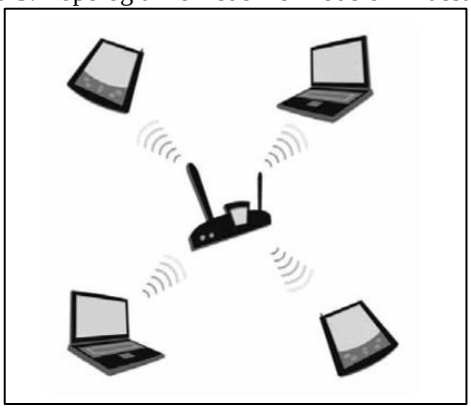
Fonte: (Rufino, 2015).

O modo de operação infraestrutura também é denominado *Basic Service Set* (BSS), ou conjunto de serviço básico em português que é composto de estações e pontos de acesso.

Qualquer dispositivo *wireless* pode ser considerado uma estação, podendo ser um computador ou celular por exemplo. Um AP é como um *hub* ou *switch* em uma rede com fio, e a estação se conecta a ele criando uma associação (conhecida como porta) com o AP (Rufino, 2015).

Este modelo é mostrado na Figura 3. Normalmente usados em aplicações comerciais, tanto para ambientes fechados como para áreas abertas.

Figura 3: Topologia De Rede No Modelo Infraestrutura



Fonte: (Rufino, 2015).

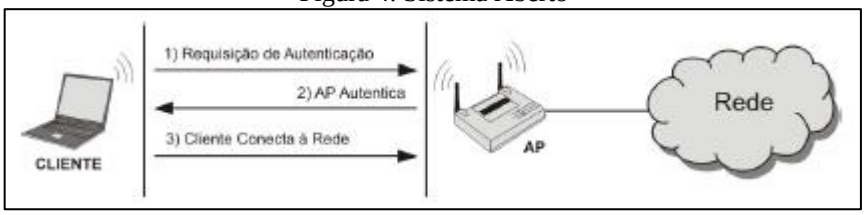
2.4 Tipos de autenticação

O padrão IEEE 802.11 utiliza duas formas de autenticação: o *Open System* e o *Shared Key*. Independente da forma que é escolhida, a autenticação deve ser realizada entre pares de estações, nunca havendo a comunicação *multicast*. Em sistemas BBS, as estações devem se autenticar e realizar a troca das informações através do AP.

2.4.1 *Open System*

O foco do desenvolvimento da autenticação de sistema aberto é verificar a rede do dispositivo sem a exigência da segurança. É uma rede que não existe qualquer proteção. Ela assume que qualquer pessoa que conheça o SSID tem liberdade para se associar a ela. Nesse caso, o usuário deve apenas solicitar a autenticação ao AP como mostra a Figura 4.

Figura 4: Sistema Aberto



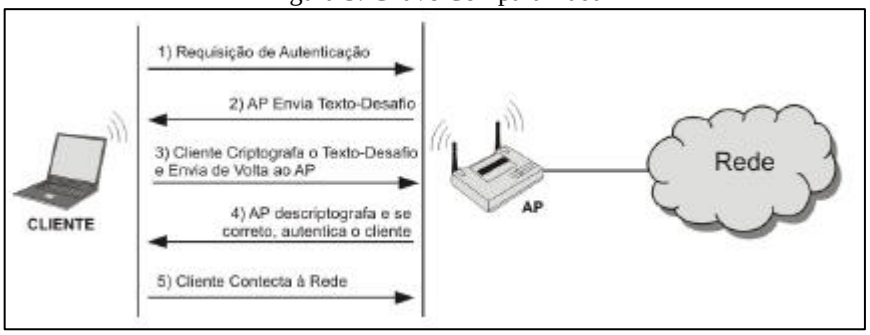
Fonte: (Linhares & Gonçalves, 2010).

2.4.2 *Shared Key*

A autenticação *shared Key* utiliza mecanismos de criptografia para concretizar a verificação dos dispositivos, que só vai realizar a autenticação do usuário se ele possuir a chave

secreta que o AP possui. A forma de se obter essa autenticação é realizada conforme é mostrado na Figura 5.

Figura 5: Chave Compartilhada



Fonte: (Linhares & Gonçalves, 2010).

Na primeira etapa, a estação a ser autenticada na rede deve enviar uma solicitação de autenticação ao AP.

Na segunda o AP responde a solicitação e remete uma mensagem contendo um desafio para a estação.

Na terceira, a estação deve provar que conhece o segredo compartilhado e deve responder à mensagem contendo o número criptografado.

Após obter a mensagem o AP compara o texto originalmente enviado com a resposta da estação. Se a criptografia foi realizada com o segredo correto e o desafio for idêntico ao original o usuário é autenticado permitindo assim o acesso (Linhares & Gonçalves, 2010).

Segundo pesquisa realizada pela Cisco em 2004, o principal problema das redes *wireless* é que elas ainda carecem de mecanismos de segurança.

A inexistência de compreensão da arquitetura de rede impede que os profissionais compreendam com precisão como as redes sem fio funcionam e como se adaptam ao ambiente existente. A qualidade da implementação da rede sem fio da empresa pode distinguir riscos gerenciáveis de riscos inaceitáveis (LINHARES e GONÇALVES, 2010).

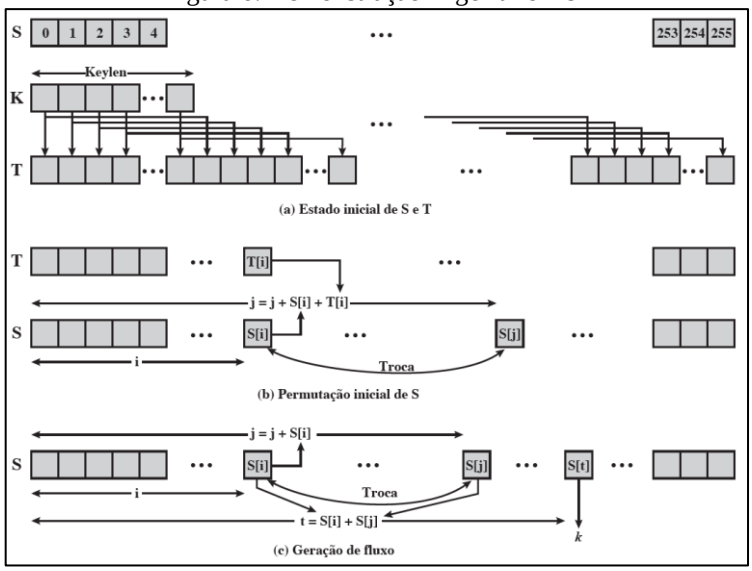
2.5 Algoritmos criptográficos

2.5.1 *Rivest Cipher 4* (RC4)

O algoritmo *Rivest Cipher 4* (RC4) é utilizado tanto pelo protocolo WEP como pelo WPA ele é um algoritmo de chave simétrica, que é segmentado em duas partes que é o *Key*

Scheduler Algorithm (KSA) e o *Pseudo Random Generation Algorithm* (PRGA) conforme apresentado na Figura 6.

Figura 6: Demonstração Algoritmo Rc4



Fonte: (Stallings, 2015).

Segundo Stallings (2015) o “S” representa o vetor de inicialização que pode ter o tamanho variável de 1 a 256 *bytes*.

O “K”, representa o *byte* gerado a partir do vetor de inicialização para fazer a encriptação e a decriptação

O “T” é um valor temporário criado à medida que cada *byte* é gerado.

O KSA consiste no processo da permutação, que consiste em inicializar o vetor de inicialização de 256 *bytes* como uma permutação de todos os números de 8 *bits* de 0 a 255. Essa permutação é condicionada a chave K que é utilizada no algoritmo, que pode variar de 1 a 256 *bytes*.

O PRGA consiste em gerar um fluxo de *bytes* contendo números pseudoaleatórios, que é utilizada para fazer a operação XOR com o fluxo de *bytes* da mensagem, para gerar a mensagem cifrada. Na prática ele é o responsável pela encriptação da mensagem.

2.5.2 *Advanced Encryption Standard* (AES)

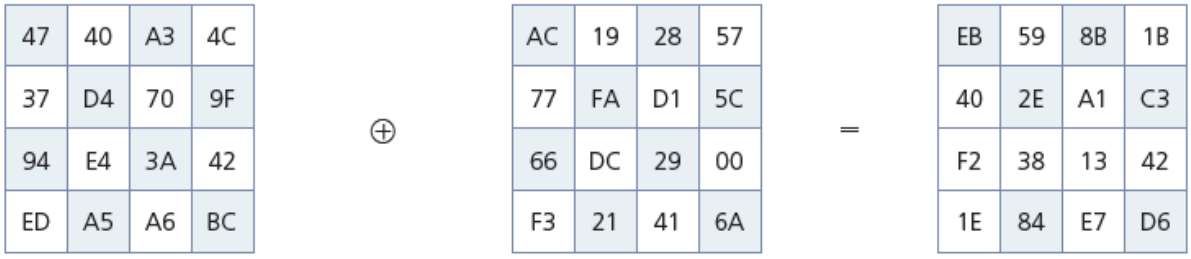
O *Advanced Encryption Standard* (AES) é um algoritmo de criptografia de chave simétrica, ou seja, a mesma chave que é utilizada para cifrar a mensagem é utilizada para decifrar (Stallings, 2015).

A única particularidade que ele tem com o RC4 é que ele tem o tamanho de bloco fixo de 128 *bits* e uma chave com tamanhos de 128, 192 ou 256 *bits*.

Ele opera sobre um arranjo bidimensional de *bits* de 4 por 4 posições, que são denominados como estado e cada pedaço do estado é chamado de subchave. Sendo que cada turno do processo de criptografia consiste em um processo de 4 estágios.

O *AddRoundKey* é o primeiro estágio onde a operação é vista como uma do tipo coluna por coluna entre os 4 bytes da coluna estado e uma *word* da chave da rodada, ela também pode ser vista como uma operação em nível de byte o qual a subchave é combinada com o estado conforme apresentado na Figura 7.

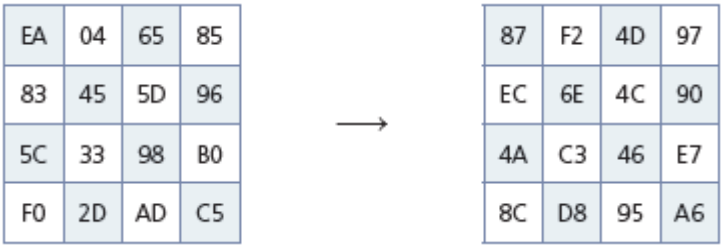
Figura 7: Add*RoundKey*



Fonte: (Stallings, 2015).

O *SubBytes* é a etapa em que cada *byte* do arranjo é atualizado utilizando uma S *box* de 8 *bits* conforme apresentado na Figura 8. A S *box* é uma combinação de uma função inversora com uma transformação que é escolhida para evitar qualquer ponto fixo.

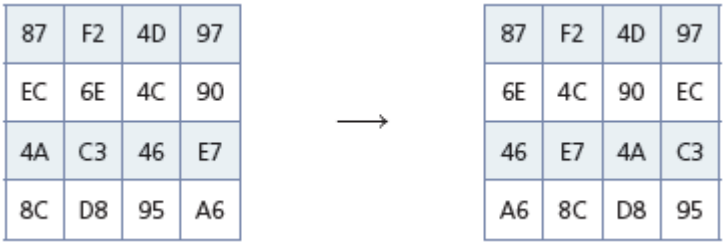
Figura 8: Sub*Bytes*



Fonte: (Stallings, 2015).

O *ShiftRows* é a etapa em que cada linha do estado é deslocada criticamente, os *bits* de um determinado número de posições conforme apresentado na Figura 9.

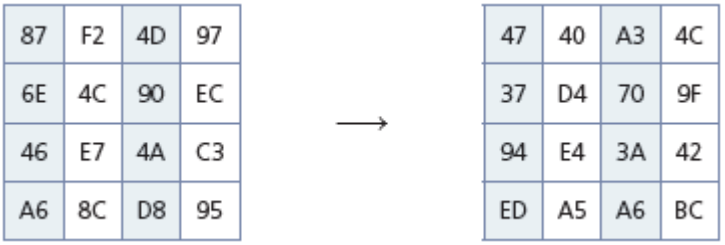
Figura 9: Shift*Rows*



Fonte: (Stallings, 2015).

O Mix*Columns* é a última etapa, no qual os 4 *bits* de cada coluna do estado são combinados utilizando uma transformação linear invertível como uma multiplicação matricial proporcionando uma difusão a cifra conforme mostrado na Figura 10.

Figura 10: Mix*Columns*



Fonte: (Stallings, 2015).

3 PROTOCOLOS DE SEGURANÇA DO IEEE 802.11

Esta seção analisará os protocolos de segurança do IEEE 802.11.

3.1 WEP

Segundo Rufino (2015), ao contrário das redes cabeadas, em que o acesso à informação requer comunicação física ou remota com os componentes da rede, as redes sem fio bastam ter uma forma de receber os sinais, ou seja, a captura da informação pode ser feita de forma passiva. Para se comunicar por meio de uma rede sem fio, apenas uma forma de recepção de sinais é necessária, ou seja, recepção passiva. Ao contrário das redes com fio, as redes com fio requerem uma conexão física entre dois componentes de rede e entre eles, o protocolo WEP é o primeiro protocolo do IEEE 802.11 que tentou solucionar esse problema além de atuar com a criptografia e autenticação entre a camada de enlace, estações e APs.

O protocolo WEP funciona na camada de enlace de dados e é baseado na criptografia RC4. Ele permite o uso de chaves compartilhadas de 64 ou 128 *bits*. Os primeiros 24 *bits* pertencem ao vetor de inicialização (IV) e não usam criptografia, o que aumenta a aleatoriedade da chave compartilhada (NAKAMURA; GEUS, 2007).

Para verificar a integridade dos dados, o protocolo WEP do remetente usa uma verificação de redundância cíclica (CRC-32) para calcular a soma de verificação da mensagem enviada, e o receptor faz o mesmo para verificar a mensagem. Da mesma forma é possível que o protocolo use um padrão mais simples, 64 *bits*, em que a chave pode ser 40 *bits* ou 24 *bits*. Portanto o modo de criptografia de dados é diferente do modo de 128 *bits*, o que garante que haja duas opções para tentar obter o nível mais baixo de segurança de rede (BAGCI, 2020).

3.1.1 Objetivo do Protocolo

O primeiro objetivo a ser alcançado é a confidencialidade, ou seja, garantir que os protocolos de segurança possam evitar que "intrusos" (qualquer pessoa não autorizada a participar das comunicações) leiam, apaguem ou insiram dados na rede.

Segundo Assunção (2013), o protocolo deve garantir a autenticidade de seus usuários e deve implementar o controle de acesso à infraestrutura *wireless* para eles. Usando o protocolo WEP, é possível descartar todos os pacotes que não estão criptografados corretamente pelo

WEP. Isso garante que apenas os usuários que possuem a chave de criptografia WEP possam participar da comunicação.

O objetivo final do protocolo é garantir a integridade da informação, de forma que a mensagem enviada possa chegar ao seu receptor sem modificação. O protocolo implementa uma função linear chamada "*checksum*" para proteger o conteúdo da mensagem transmitida permanecendo o mesmo ao longo do processo de transmissão (DRAKE, 2020).

3.1.2 Confidencialidade

A confidencialidade impede que pessoas não autorizadas obtenham informações de modo que sua implementação seja opcional. Depois de habilitado, cada *site* tem uma chave compartilhada com o AP e não há uma maneira padrão de distribuir essas senhas sendo feito manualmente em cada *site*.

A tecnologia de criptografia de chave secreta é baseada no algoritmo RC4. O algoritmo RC4 é um algoritmo de codificação de fluxo criado por Ron Rivest em 1987 para segurança RSA com comprimento de chave variável. O algoritmo é baseado no uso de permutação aleatória. Portanto, o algoritmo criptografa os dados durante a transmissão, melhorando assim seu desempenho (STALLINGS, 2015).

Segundo Bagci (2020), para enviar uma mensagem, a estação emissora primeiro conecta sua chave compartilhada ao vetor de inicialização. O resultado é inserido no algoritmo gerador de números pseudoaleatório (PRNG), definidos pelo RC4.

O PRNG gera uma sequência de *bits* do mesmo tamanho da informação a ser criptografada, ou seja, um quadro MAC contendo CRC. Executa o XOR (OR exclusivo) que gera quadros criptografados de fluxos de *bits*. E finalmente, o quadro e o IV são enviados ao receptor para processamento reverso.

O WEP usa um IV de 24 *bits* para proteger as chaves usadas no processo de criptografia. Para cada quadro enviado, um IV é gerado e conectado à chave, o que faz com que a chave (fluxo de chave) usada na criptografia de quadro mude a cada novo quadro. No entanto, quanto maior a capacidade da chave de criptografia, mais seguro é o processo de criptografia.

3.1.3 Integridade

O papel da integridade é garantir que o receptor obtenha os dados corretos, ou seja, garantir que o quadro enviado pelo remetente não tenha mudado ou que dados desnecessários sejam incluídos ou excluídos na transmissão. A integridade é alcançada por meio de um polinômio CRC-32, em que o *Integrity Check Value* (ICV) é adicionado a cada carga útil.

3.1.4 Autenticidade

A autenticidade visa identificar quem está realizando uma operação específica para que se possa controlar o acesso aos recursos disponíveis. Essa autenticação pode ser feita de duas maneiras.

Segundo Assunção (2013), o primeiro padrão denominado *open system*, utiliza apenas seu SSID para identificar cada AP conforme é apresentado na Figura 11.

Figura 11: Wep *Open System*

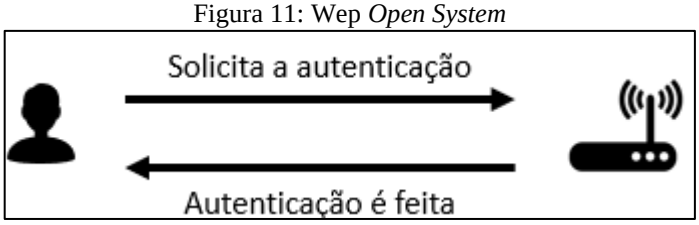


Figura adaptada do: (Linhares & Gonçalves, 2010) com o conteúdo desenvolvido pelo autor deste trabalho.

Esta opção deve ser evitada porque se a estrutura de criptografia estiver desabilitada, qualquer dispositivo é capaz de se comunicar com o AP porque o SSID é transmitido pelo próprio AP em intervalos predefinidos e pode ser capturado e usado para acesso não autorizado.

A segunda opção de autenticação WEP é baseada em um segredo compartilhado, que usa tecnologia de resposta de desafio. Entre eles, apenas o *site* é autenticado sendo necessário o AP para autenticação.

Em seguida, o AP gera um número aleatório (desafio) e o envia para a estação, que o recebe e criptografa com o algoritmo RC4 e o envia de volta (resposta). O AP decriptografa a resposta e a compara com o número enviado.

Se o resultado da comparação for positivo, o AP envia uma mensagem para a estação para confirmar que a autenticação foi bem-sucedida, conforme mostrado na Figura 12.

Figura 12: Wep *Shared Key*

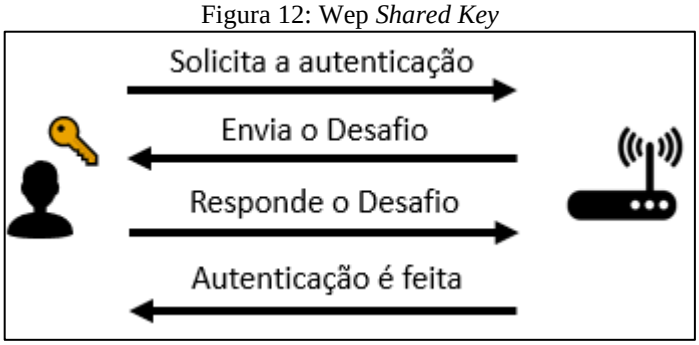


Figura adaptada do: (Linhares & Gonçalves, 2010) com o conteúdo desenvolvido pelo autor deste trabalho

3.1.5 Estrutura do WEP

Inicialmente, cada parte que deseje participar da comunicação deve possuir uma chave secreta K, que é utilizada no processo de criptografia e no processo reverso. A chave K é a mesma que a chave usada para criptografar os dados a serem transmitidos e recuperar os pacotes recebidos.

O nome desse processo é criptografia simétrica, porque as chaves de ambos os processos são exclusivas. É importante lembrar que a mudança de chaves deve ser feita com segurança, se possível, pessoalmente, para que a segurança não seja comprometida.

É mostrado posteriormente que a mesma chave K é utilizada para autenticação, o que torna o protocolo um tanto vulnerável nesse aspecto (LINHARES; GONÇALVES, 2010).

Caso um usuário queira enviar uma mensagem, que é transmitida pela WLAN usando o protocolo WEP. Em primeiro lugar, esta mensagem é criptografada que começa com a concatenação do IV com a chave conforme apresentado na Figura 13, então rodam o algoritmo KSA e o PRNG para gerar uma chave de fluxo.

Figura 13: Encriptação

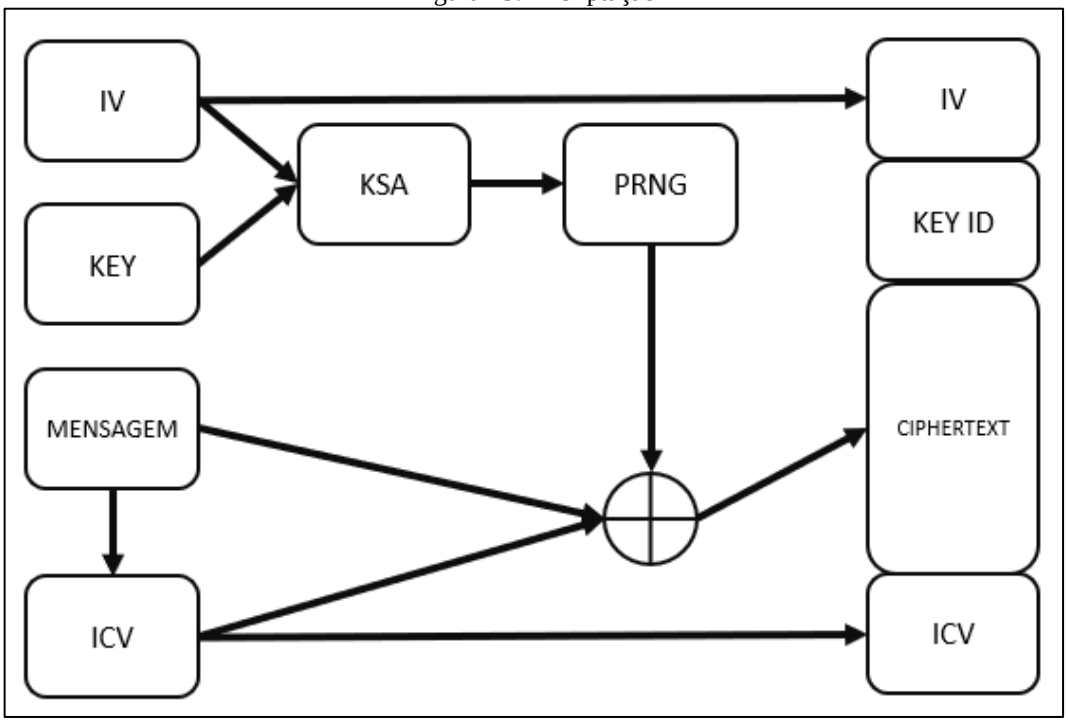


Figura adaptada do (PAIM, 2011) com o conteúdo desenvolvido pelo autor deste trabalho.

No próximo passo, o ICV é calculado e concatenado com a mensagem antes dela passar pela criptografia, só depois a mensagem para pelo XOR com a chave de fluxo e finalmente o pacote resultante é feito do IV. De uma chave ID de dois *bits*, da mensagem cifrada e do ICV.

Além do pacote de dados criptografado, o vetor de inicialização utilizado também é transmitido, para que seja realizado o processo de decriptografia reversa. A recuperação de pacotes de dados é simples. É o mesmo processo só que aplicado ao contrário. e começa com o IV e a chave que é indicada pelo ID da chave, sendo concatenados e rodam através do mesmo algoritmo KSA e PRNG para gerar uma chave de fluxo idêntica à que foi usada para criptografar.

Assim que tiver essa sequência, ele simplesmente aplica um XOR entre a sequência e o pacote de criptografia para recuperar o pacote de dados original conforme apresentado na Figura 14.

Figura 14: Decriptação

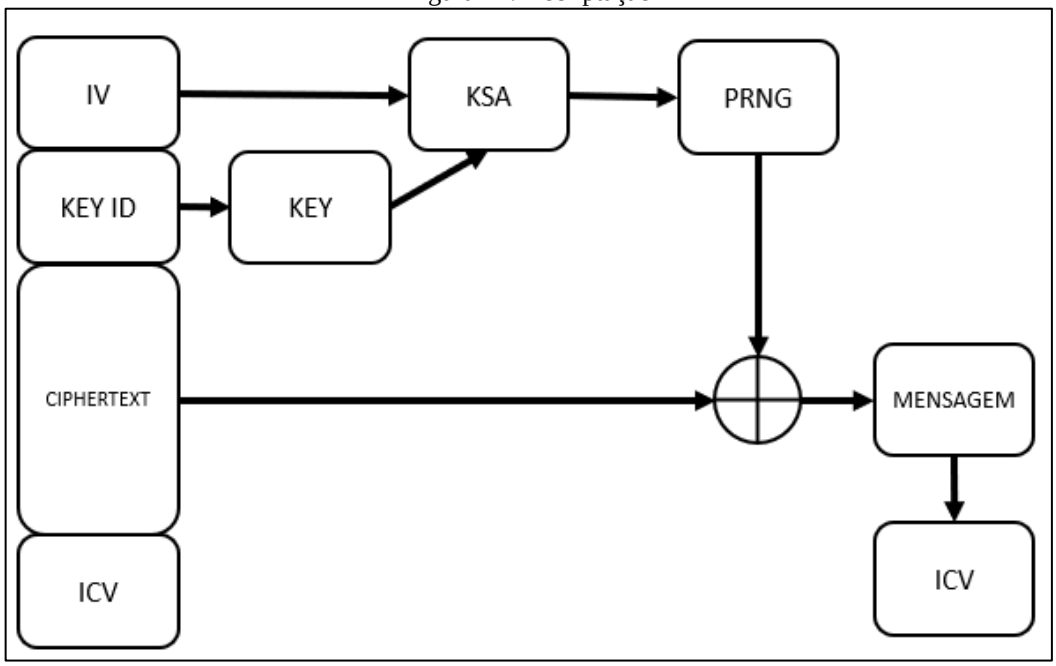


Figura adaptada do (PAIM, 2011) com o conteúdo desenvolvido pelo autor deste trabalho.

3.1.6 Vetor de Inicialização

O vetor de inicialização do WEP tem 24 *bits* e, junto a chave, é o encarregado por gerar uma sequência pseudoaleatória que criptografa o texto legível. O primeiro problema no WEP é o tamanho deste IV, que é muito pequeno.

Em casos extremos, todo pacote de dados enviado mudará este IV, partindo de zero e atingindo o valor máximo (2^{24})-1. Pode-se calcular quanto tempo esse IV levará para retornar a zero novamente: em uma conexão com uma largura de banda de 5 M*bits* / s (o valor máximo em IEEE 802.11 é 11 M*bits* / s).

$$(5\ \text{Mbits}/8)*1500 = 416\ \text{pac/s}$$

$$(2^{23}\ \text{pac}\ /416) = 40.329\ \text{seg ou 11h 12min}$$

Resumindo, no caso mais extremo, em uma conexão de 5 M*bits*/s, o IV retorna ao mesmo valor em menos de meio dia. Se a implementação assumir que o IV tem um valor aleatório, repete-se o IV em um tempo menor. É por meio deste IV repetido que o WEP pode ser quebrado. A chave K é fixa e foi definida no cliente que está se comunicando. Então, enquanto o IV for repetido, o par <K, IV> é repetido. Sempre que eles se repetem, eles geram a mesma sequência pseudoaleatória, denominada de RC4 (Stallings, 2015).

3.1.7 Vulnerabilidades

Segundo Linhares e Gonçalves (2010), uma das principais vulnerabilidades neste protocolo está relacionada à reutilização do vetor de inicialização. Embora o WEP seja usado para transformar as comunicações *wireless* mais seguras, ele também aponta muitas falhas. Conforme mencionado, o IV tem 24 *bits* e pode assumir um valor entre 0 e 16.777.215.

Por usar a mesma chave por muito tempo, o padrão WEP recomenda que o IV seja alterado toda vez que um pacote de dados for enviado, para evitar o uso repetido do fluxo de chaves. Geralmente, IV começa em 0 e aumenta em 1 com cada pacote de dados enviado.

Há dois problemas com esse mecanismo: o primeiro é que o IV mostrará o mesmo valor novamente algum dia; em segundo lugar, as pessoas frequentemente desconectam a placa de rede sem fio e conectam o computador novamente, fazendo com que o IV seja redefinido para 0 novamente, resultando em um valor baixo de IV e pacotes de dados em todos os lugares.

Outra vulnerabilidade WEP está relacionada ao CRC-32. Como seu algoritmo de garantia de integridade é linear, os pacotes de dados podem ser modificados sem serem detectados. Somente conhecendo a cadeia de valores pseudoaleatória é possível alterar o conteúdo do pacote, de modo que sua integridade não possa ser garantida.

Uma das grandes fraquezas do WEP é a inexistência de administração de chaves porque o padrão WEP não determina como as chaves devem ser distribuídas.

3.2 WPA

O WPA é o resultado dos esforços conjuntos da Wi-Fi *Alliance* e dos membros do IEEE. Em 2003, eles se comprometeram a melhorar o nível de segurança das redes sem fio para combater as vulnerabilidades no protocolo WEP. Entre eles, o *Temporary Key Exchange Protocol* (TKIP) ou em português Protocolo de Integridade de Chave Temporal que ele utiliza uma tecnologia de encriptação de chaves mais segura do que o RC4 do WEP, incluindo as funcionalidades de segurança em WPA (Rufino, 2015).

3.2.1 Autenticação

Tendo em vista as questões de segurança do protocolo WEP, o WPA propõe algumas mudanças e algumas melhorias, incluindo a autenticação que se torna necessária ao se conectar ao AP, porém a maioria dessas melhorias requerem que outros elementos sejam incluídos em

sua infraestrutura, e outros protocolos ainda devem ser usados nessa combinação como o 802.1x, ao contrário do WEP, que não oferece suporte a conexões temporárias.

Portanto, tal rede que não usa um AP não se beneficia dos mecanismos de proteção introduzidos pelo protocolo WPA em sua primeira versão (Rufino, 2015).

3.2.2 Administração da Chave do WPA

A novidade do WPA está no protocolo TKIP, responsável por gerenciar as chaves temporárias utilizadas pelos dispositivos de comunicação, e que realiza a preservação dos segredos por meio da troca constante de chaves, pois uma das vulnerabilidades do WEP advém do fato de as chaves serem estáticas para usar o protocolo WPA, as chaves de criptografia global e *unicast* precisam ser regeneradas.

Para as chaves de criptografia *unicast* o TKIP altera a chave para cada quadro, sendo as alterações sincronizadas entre o cliente e o AP. Para a chave de criptografia global, o WPA inclui uma função para o AP notificar o cliente conectado sobre a alteração da chave.

3.2.3 TKIP

Para o IEEE 802.11, a criptografia WEP é opcional. Segundo Stallings (2015) no WPA, o TKIP é necessário para a criptografia que substitui o WEP por um novo algoritmo de criptografia. Ele se utiliza do poder de computação introduzido no equipamento existente para executar operações de criptografia.

É o protocolo utilizado pelo WPA para criptografar e transmitir mensagens. Que utiliza o algoritmo RC4, bem como WEP, mas toma algumas medidas de precaução para evitar ataques, como não enviar a chave "em claro" e usar uma estratégia de vetor de inicialização mais inteligente.

O WPA trabalha com uma chave de 32 a 512 *bits* chamada *Pairwise Master Key* (PMK) ou em português Chave Mestra Dupla, que gera uma *Pairwise Transient Key* (PTK) em português chave transitória dupla, com base em alguns parâmetros obtidos durante a conexão. Ele é compartilhado entre o computador e o AP, que é composta por 512 *bits*, que podem ser divididos em quatro outras chaves de 128 *bits* – Chave de Confirmação de Chave (KCK), Chave de Criptografia de Chave (KEK), Protocolo de integridade de chave (TEK), Chave de integridade de dados (TMK) - para diferentes processos deste protocolo.

3.2.4 Michael

Segundo Linhares e Gonçalves (2010), para o IEEE 802.11 e o WEP, a integridade dos dados é fornecida por um IV de 32 *bits*, que aparece com a carga IEEE 802.11 que utiliza a criptografia WEP. Embora o ICV seja criptografado, é possível alterar os *bits* na carga criptografada e atualizar o ICV criptografado sem ser detectado pelo receptor.

No WPA, o TKIP usa o Michael (MIC) que representa o ICV para evitar que isso ocorra. Esta função usa metade da chave temporária TMK do MIC (em termos de dígitos) para "embaralhar" os dados da mensagem original, adicionar os endereços MAC de origem e de destino, organizar e deslocar e retornar um valor de 8 *bytes* e o OU-Exclusivo.

Figura 15: Código De Integridade De Mensagem

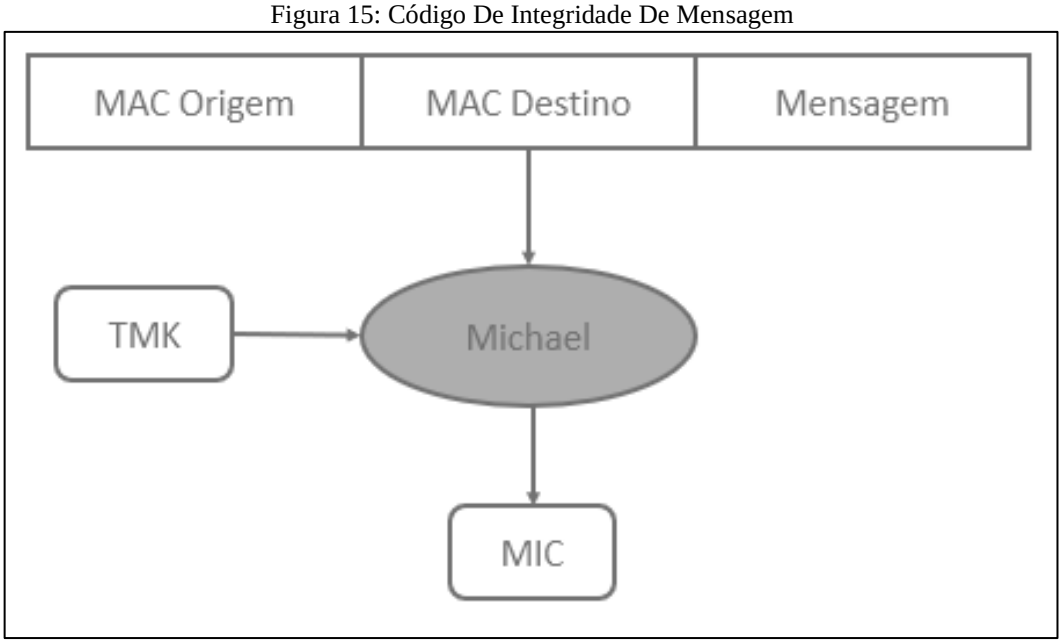


Figura adaptada do: (Paim, 2011) com o conteúdo desenvolvido pelo autor deste trabalho.

O processo simplificado é apresentado na Figura 15. A vantagem do MIC é que seu produto não tem nada a ver com o vetor de inicialização, portanto, qualquer tentativa de ataque é limitada à quebra de força bruta.

Outro ponto fraco do WEP é que terceiros podem capturar pacotes e ré enviá-los indefinidamente. A estratégia adotada pelo WPA é muito simples, incluindo o uso de um vetor de inicialização de 48 *bits* como identificador de pacote: o cliente da rede e o AP redefinem o vetor de inicialização para comunicação entre eles no início, e o aumenta a cada novo envio.

Se algum pacote chegar com um valor IV inferior ao do último pacote recebido, isso é um sinal de uma tentativa de ataques de repetição e é ignorado.

Por fim, no processo de troca de mensagens, os dois estágios de TEK ou chave de criptografia temporária são combinados com o vetor de inicialização, o que aumenta a complexidade de obtenção do primeiro estágio.

No primeiro estágio, os 32 *bits* mais altos do vetor de inicialização, o TEK e o endereço MAC da pessoa que está transmitindo a mensagem são inseridos como parâmetros da função *digest* (fase 1), que retorna um valor de 80 *bits*.

Este valor e os 16 *bits* mais baixos do vetor de inicialização são enviados para uma nova função de resumo (fase 2), que retorna um valor de 128 *bits*: os primeiros 24 *bits* correspondem ao vetor de inicialização usado pelo RC4, e os outros 104 *bits* correspondem para a chave (Linhares & Gonçalves, 2010). A Figura 16 mostra o esquema geral do algoritmo de codificação de chave.

Figura 16: Algoritmo De Mistura De Chaves

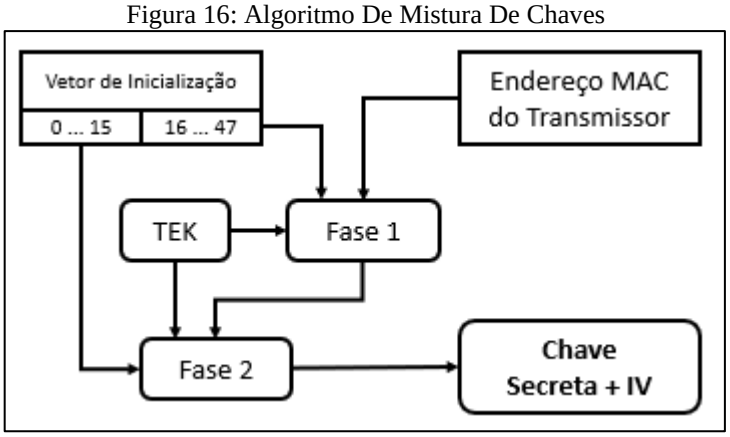


Figura adaptada do: (Paim, 2011) com o conteúdo desenvolvido pelo autor deste trabalho.

3.2.5 Vulnerabilidades

Uma pesquisa mencionada pelo laboratório da empresa especializada em segurança ICSA Labs descobriu que, sob certas condições, o padrão WPA não é tão seguro quanto seu predecessor, WEP (KOHLIOS e HAYAJNEH, 2018).

Segundo Moskowitz (2003), acerca de um estudo intitulado "*Breaking Weakness in WPA Interface Selection*", o diretor técnico sênior do ICSA Lab da TruSecure, Robert Moskowitz, descreveu muitas das falhas que o WPA possui, uma delas é a ausência de obstáculos que os atacantes têm em capturar informações de tráfego de rede sem fio, graças a obtenção de senhas através da análise dos dados capturados.

Moskowitz (2013), disse que os problemas do WPA estão na utilização de chaves pré-compartilhadas (PSK), que é uma ferramenta de autenticação alternativa projetada para

pequenas empresas e usuários que não queiram utilizar um servidor de autenticação separado e infraestrutura 802.1x (MOSKOWITZ, 2003).

Moskowitz, foi um dos integrantes da *Alliance* que ajudou no projeto dos padrões de segurança sem fio IEEE 802.11i e WPA, que relatou o método pelo qual os dispositivos WPA trocam informações de criptografia de dados, uma vez que o protocolo permite que os invasores usem "ataques de dicionário" para adivinhar as senhas PSK (MOSKOWITZ, 2003).

No "ataque de dicionário", o invasor faz a captura de dados da rede sem fio que é transmitido entre o AP e a estação de trabalho e utiliza um programa específico para adivinhar a senha. Outros padrões de segurança sem fio também são frágeis.

As vulnerabilidades WEP são conhecidas há muito tempo, mas o protocolo de segurança *Lightweight Extensible Authentication Protocol* (LEAP) da Cisco se mostrou vulnerável a essas invasões.

O maior problema é que nos padrões WEP e LEAP, o invasor precisa obter muitas informações da rede, enquanto no padrão WPA, apenas quatro pacotes de dados específicos precisam ser capturados para descriptografar a senha. Segundo Moskowitz (2003), não é recomendado o uso de senhas com menos de 20 caracteres. Mas, segundo ele, uma solução é usar uma senha de pelo menos 17 caracteres (MOSKOWITZ, 2003).

Moskowitz afirma que o padrão WPA é muito mais seguro do que o WEP, embora pesquisas recentes tenham revelado essas falhas. No entanto, Moskowitz relatou que o problema está nos fabricantes de dispositivos e implementadores de WPA. Na pressa para fornecer o padrão WPA em seus produtos, fabricantes como o Linksys Group (agora conhecido como Cisco) fizeram pouco para evitar os defeitos conhecidos relatados no documento oficial do padrão IEEE 802.11i (MOSKOWITZ, 2003).

3.3 WPA2

Em 2004 o padrão WPA2 foi aprovado com o objetivo de aprimorar a proteção da comunicação já que o protocolo WPA utilizado na época, possuía várias fragilidades.

A nova estrutura de criptografia utilizada requer mais poder de computação da *Network Interface Card* (NIC) durante o processo de codificação/decodificação, portanto, não é possível atualizar apenas o *firmware*. Alguns mecanismos introduzidos no WPA são usados no WPA2, porque o WPA é baseado no rascunho do WPA2. O principal avanço do WPA2 sobre o WPA são os novos algoritmos de criptografia e integridade (LINHARES e GONÇALVES, 2010).

3.3.1 Autenticação

A autenticação do WPA2 é idêntica ao WPA. O grande progresso foi na verificação de identidade é o foco em *roaming*, fazendo com que quando o usuário for autenticado, uma sucessão de mensagens seja trocada entre o AP e o cliente.

Esse envio de mensagens resulta em uma demora no andamento da conexão. Caso um cliente mude de um AP para outro AP, o atraso pode acarretar desconexões, principalmente no tráfego de áudio e vídeo. Para minimizar esse atraso associado, o dispositivo pode oferecer suporte a *cache* PMK e pré-autenticação.

O *cache* PMK é composto de APs que armazenam os resultados da verificação do cliente. Se o cliente se reassociar ao AP, esta informação armazenada é usada para reduzir o número de mensagens trocadas durante a reautenticação.

Na *preauthentication*, quando um cliente se conecta ao AP principal, ele estabelece associações com outros Aps cujos sinais o alcançam. Desta forma, quando o AP muda, nenhum tempo é perdido para autenticação (ASSUNÇÃO, 2013).

3.3.2 Integridade

O protocolo *Counter Mode with Cipher Block Chaining Message Authentication Code* (CCMP) é encarregado pela integridade e confidencialidade do WPA2, que se beneficia do algoritmo AES para fazer a encriptação das mensagens transmitidas (LINHARES e GONÇALVES, 2010).

Ele usa a combinação entre o bloco de dados e a chave de criptografia, de forma que toda a nova combinação dependa apenas do resultado de seus antecedentes. Portanto, é difícil obter a chave e o intervalo de combinação do vetor de inicialização é maior. Assim como o TKIP, ele foi desenvolvido para solucionar a ineficiência do WEP, que é considerada uma solução de longo prazo e mais segura em relação ao TKIP. O seu funcionamento é mostrado na Figura 17.

Figura 17: Integridade Wpa2

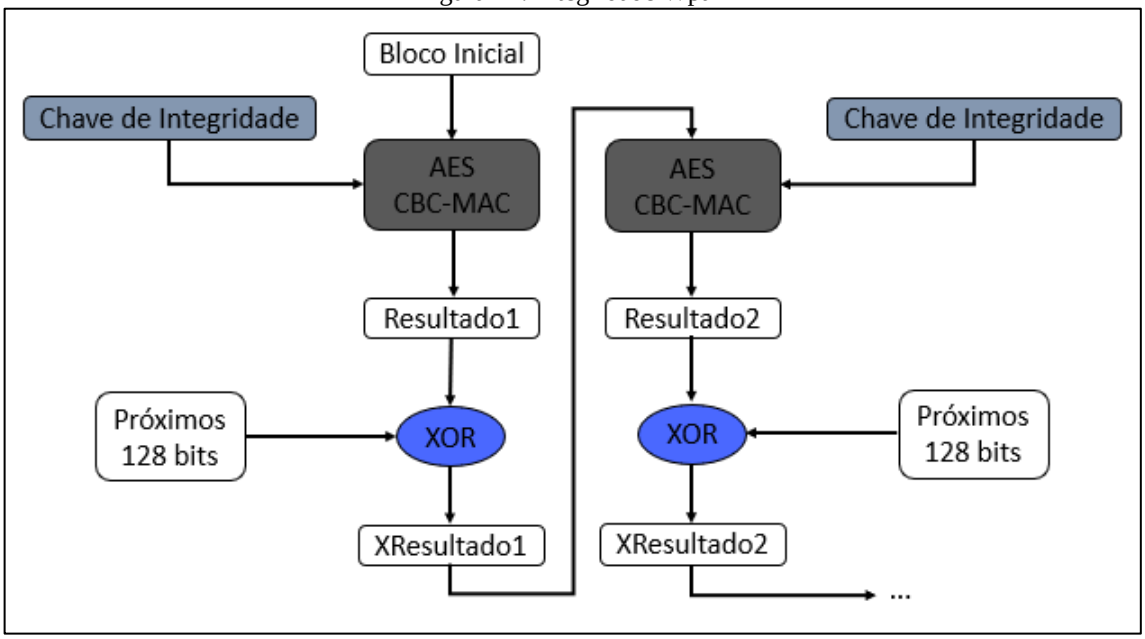


Figura adaptada do: (Linhares & Gonçalves, 2010) com o conteúdo desenvolvido pelo autor deste trabalho.

O bloco inicial diz respeito aos primeiros 128 *bits* do campo de dados que são atribuídos para o *Cipher Block Chaining Message Authentication Code* (CBC-MAC) em português código de autenticação de mensagens de encadeamento de bloco de cifra do modo de contador, sendo o CBC-MAC o encarregado pela integridade do quadro e da chave de integridade. Depois disso, outros 128 *bits* são gerados e exibidos como “Resultado1”.

Após isso, é feito o XOR entre o “Resultado 1” e o próximo bloco. Após passar pelo o XOR, passa novamente para o CBC-MAC que gera assim o “Resultado 2” e repete o processo até o último bloco do campo de dados do pacote sendo que dos 128 *bits*, apenas os 64 *bits* mais importantes que vão para o MIC no final.

3.3.3 Confidencialidade

Segundo Linhares e Gonçalves (2010), o CCMP se baseia na ideia de chaves temporárias, do mesmo modo que o TKIP no WPA. Consequentemente há uma classificação de chave no WPA2, em que a PMK deriva uma chave provisória para criptografia e integridade.

O algoritmo encarregado pela criptografia de quadros é o AES (CTR). A chave de criptografia de dados é simétrica e possui o tamanho de 128 *bits*, sendo que o IV permanece com apenas 48 *bits* de comprimento (PAIM, 2011).

3.3.4 Vulnerabilidades

Embora o WPA2 seja um dos protocolos mais seguros, ele ainda tem algumas vulnerabilidades, a mais famosa delas é a negação de serviço. E como utiliza uma estrutura de gestão e controle de proteção, isso torna possível forçar uma estrutura de gerenciamento de tipo de desautenticação. Ataques de força bruta a sua PSK com menos 20 caracteres continuam sendo susceptíveis a ataques (LINHARES e GONÇALVES, 2010).

3.4 WPA3

Segundo a Wi-Fi *Alliance* o WPA3 é uma nova geração de protocolo de segurança do IEEE 802.11, que adiciona novos recursos para simplificar a segurança da rede sem fio, a fim de se obter uma autenticação mais forte, fornecer maior força de criptografia para o mercado de dados altamente confidenciais e manter a flexibilidade das redes de missão crítica.

Todas as redes WPA3 utilizam os métodos de segurança mais recentes, proíbem protocolos legados e exigem o uso de uma estrutura de gerenciamento protegida chamada *Protected Management Frames* (PMF). Como as redes Wi-Fi têm finalidades e requisitos de segurança diferentes, o WPA3 inclui recursos adicionais especificamente para redes pessoais e corporativas.

Os usuários WPA3-*Personal* podem obter melhor proteção contra adivinhação de senha e os usuários WPA3-*Enterprise* agora podem aproveitar os protocolos de segurança avançados para redes de dados confidenciais. O WPA3 mantém a interoperabilidade com dispositivos WPA2 e é uma certificação obrigatória para dispositivos Wi-Fi (MYERSON, 2018).

3.4.1 WPA3-Personal

O WPA3-*Personal* fornece melhor proteção para usuários individuais e fornece autenticação mais forte com base na senha. Mesmo que a senha escolhida pelo usuário não atenda às recomendações de complexidade típicas o recurso é habilitado por meio da *Simultaneous Authentication of Equals* (SAE), que substitui a PSK do WPA2-Personal (ALLIANCE, 2018).

Essa tecnologia pode resistir a ataques de dicionário *offline*, nos quais os invasores tentam determinar as senhas da rede tentando senhas potenciais sem interação adicional com a rede, o que permite que os usuários escolham uma senha que seja mais fácil de lembrar. Oferece

proteção aprimorada sem alterar a maneira como os usuários se conectam à rede. E mesmo se a senha vazar após a transmissão de dados, ele pode proteger o tráfego de dados (ALLIANCE, 2018).

3.4.2 WPA3-Enterprise

O WPA3-*Enterprise* pode fornecer maior segurança para empresas, governos e instituições financeiras. O WPA3-*Enterprise* é construído sobre o WPA2 para garantir a aplicação consistente de protocolos de segurança em toda a rede.

Fornece um modo opcional usando protocolos de segurança de 192 *bits* de menor força e ferramentas de criptografia para proteger melhor os dados confidenciais:

Para a criptografia da autenticação utiliza o *Galois/Counter Mode Protocol* 256-*bit* (GCMP-256).

Para a derivação e confirmação da chave, o WPA3 utiliza o *Hashed Message Authentication Mode* (HMAC) e o *Hashed Message Authentication Mode Secure Hash Algorithm* (HMAC-SHA384).

Para o estabelecimento e autenticação de chave, o WPA3 usa o *Elliptic Curve Diffie-Hellman* (ECDH) e o *Exchange and Elliptic Curve Digital Signature Algorithm* (ECDSA) usando uma curva elíptica de 384 *bits* (ALLIANCE, 2018).

O WPA 3 utiliza para a proteção de quadro de gerenciamento o 256-*bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code* (BIP-GMAC-256).

Segundo a Wi-Fi Alliance (2018), o modo de segurança de 192 *bits* fornecido pelo WPA3-*Enterprise* garante que a combinação correta de ferramentas de criptografia seja usada e uma linha de base de segurança consistente seja definida em toda a rede WPA3.

3.4.3 Redes Abertas

Os usuários acessam redes *Wi-Fi* em qualquer lugar: em casa, no escritório, em hotéis, *Shopping Center*s, centros de transporte e locais municipais. Acessar redes não seguras nesses locais apresentam um risco de alguém adquirir os dados pessoais, razão pela qual a Wi-Fi *Alliance* recomenda que os usuários acessem apenas redes autenticadas e seguras sempre que possível. No entanto, existem situações em que uma rede Wi-Fi aberta é a única opção viável.

Embora muitos consumidores em todo o mundo utilizem redes abertas sem nenhum problema, é importante estar ciente do risco que uma rede aberta apresenta e ser diligente na proteção dos dados do usuário (ALLIANCE, 2018).

Para lidar com esses riscos, a Wi-Fi *Alliance* desenvolveu uma solução para beneficiar os usuários de redes Wi-Fi abertas que veio com o WPA3.

O Wi-Fi *CERTIFIED Enhanced Open* que é uma certificação da Wi-Fi *Alliance* que preserva a conveniência das redes abertas, enquanto reduz alguns dos riscos associados ao acesso a uma rede não segura. As redes *Wi-Fi Enhanced Open* fornecem criptografia de dados não autenticada aos usuários, uma melhoria em relação às redes abertas tradicionais sem nenhuma proteção (ALLIANCE, 2018).

Essas proteções são transparentes para o usuário. Com base em *Opportunistic Wireless Encryption* (OWE) definido na especificação RFC8110 do *Internet Engineering Task Force* (IETF) e na especificação *Wi-Fi Alliance Opportunistic Wireless Encryption, Wi-Fi Enhanced Open* que beneficia os usuários ao fornecer criptografia de dados que mantém a facilidade do uso de redes abertas e beneficia os provedores da rede porque não há senhas públicas para manter, compartilhar ou gerenciar (ALLIANCE, 2018).

Como o *Wi-Fi Enhanced Open* é um programa *Wi-Fi CERTIFIED*, a tecnologia é interoperável com redes legadas, mesmo aquelas que usam um portal cativo. Os operadores de rede que desejem implantar autenticação completa e solução de provisionamento de dispositivos devem considerar abordagens como Wi-Fi *CERTIFIED Passpoint* (ALLIANCE, 2018).

3.4.4 Vulnerabilidades

Embora a *Wi-Fi Alliance* alegue que, devido à essa função de *handshake* do *Dragonfly*, o WPA3 não pode ser usado para quebrar senhas de rede, a Universidade de Tel Aviv e os pesquisadores da KU descobriram uma vulnerabilidade chamada *Dragonblood*, que provou que a Wi-Fi *Alliance* estava errada. Essa vulnerabilidade foi descoberta em abril de 2019 (KHANDELWAL, 2019).

Depois de descobrir essas falhas, a Wi-Fi *Alliance* lançou *patches* para resolver esses problemas e criou recomendações de segurança para mitigar os ataques iniciais de *Dragonblood*.

No entanto, essas recomendações de segurança foram criadas de forma privada, sem colaboração com pesquisadores, e não foram suficientes para proteger os usuários de ataques *Dragonblood*. Pelo contrário, ele abre dois novos ataques de canal lateral. Mesmo que esteja usando a versão mais recente do protocolo *Wi-Fi*, permite que um invasor roube sua senha *Wi-Fi* (LAKSHMANAN, 2021).

Três meses após a descoberta do sangue de dragão, os pesquisadores Mathy Vanhoef e Eyal Ronen descobriram uma nova falha no aperto de mão do WPA3 *Dragonfly* relacionada ao segundo tipo de vazamento do canal lateral (VANHOEF e RONEN, 2019).

Embora a Wi-Fi *Alliance* afirme mais uma vez que é completamente impossível usar uma rede Wi-Fi protegida por WPA3 para quebrar a senha, os pesquisadores mais uma vez provaram que essa afirmação estava errada e falaram sobre diferentes falhas de design no protocolo WPA3 (*Downgrade attack, Side-channels leaks*) (KHANDELWAL, 2019).

Essa lacuna séria no protocolo WPA3 permite que os cibercriminosos quebrem as senhas e acessem o tráfego criptografado para roubar dados confidenciais transmitidos, como números de cartão de crédito, senhas, mensagens de bate-papo e *e-mails*.

A primeira vulnerabilidade foi identificada como CVE-2019-13377 que os pesquisadores relatam um novo vazamento no tubo lateral. Esta é a primeira vulnerabilidade no algoritmo de criptografia de senha quando o *Dragonfly* usa a curva *Brainpool* para apertar a mão do WPA3 (KHANDELWAL, 2019)

Durante o algoritmo *Dragonfly*, ele tentou encontrar a saída de *hash* usando a curva de *Brainpool*. Pode levar várias iterações antes de encontrar uma saída *hash* menor do que a primeira saída *hash*, mas o número de iterações sem esta saída *hash* válida depende da senha usada e do endereço MAC do cliente do terminal.

A segunda vulnerabilidade, identificada como CVE-2019-13456, é um erro de divulgação de informações que existe na implementação do *Extensible Authentication Protocol Password* (EAP-pwd) do FreeRADIUS (um dos servidores de serviço de usuário discado com autenticação remota (RADIUS), de código aberto usado pela empresa como centro de banco de dados) para verificar o usuário de autenticação remota.

Mathy Vanhoef, uma das duas pesquisadoras que descobriram a vulnerabilidade *Dragonblood*, disse à *Hacker News* que um invasor pode iniciar múltiplos *handshake* EAP-pwd para vazar informações, e essas informações podem ser usadas para recuperar a senha *Wi-Fi* do usuário durante ataques de dicionário e *cracking* (LAKSHMANAN, 2021).

De acordo com os pesquisadores, é muito difícil implementar algoritmos *Dragonfly* e WPA3 sem vazamento de canal lateral, e contramedidas compatíveis com versões anteriores contra esses ataques são muito caras para dispositivos leves.

Os pesquisadores compartilharam suas novas descobertas com a *Wi-Fi Alliance* e relataram que o padrão *Wi-Fi* está sendo atualizado para fornecer defesa adequada, o que pode levar ao WPA 3.1, mas, a nova defesa é compatível com a versão inicial do WPA3 compatível. Suportado.

Mathy Vanhoef também disse ao *The Hacker News* que, a *Wi-Fi Alliance* desenvolveu secretamente suas diretrizes de segurança. Se fizerem isso publicamente, podem evitar esses novos problemas. Mesmo a autenticação WPA3 inicial é parcialmente confidencial, o que não é ideal (LAKSHMANAN, 2021).

4 AMBIENTE DE TESTES

Este capítulo apresenta o cenário e as ferramentas que foram utilizadas para a simulação do ataque a uma rede aberta.

4.1 Cenário

O cenário foi montado com a intenção de simular um local de acesso público a *Internet*, como por exemplo um *Shopping Center* ou uma cafeteria. O objetivo é se aproveitar do acesso público, para gerar um ataque que possibilite a captura de tráfego gerado pelos usuários.

Para tanto foi criado uma rede que simula essa situação, no qual foram utilizados os equipamentos listados no Quadro 1.

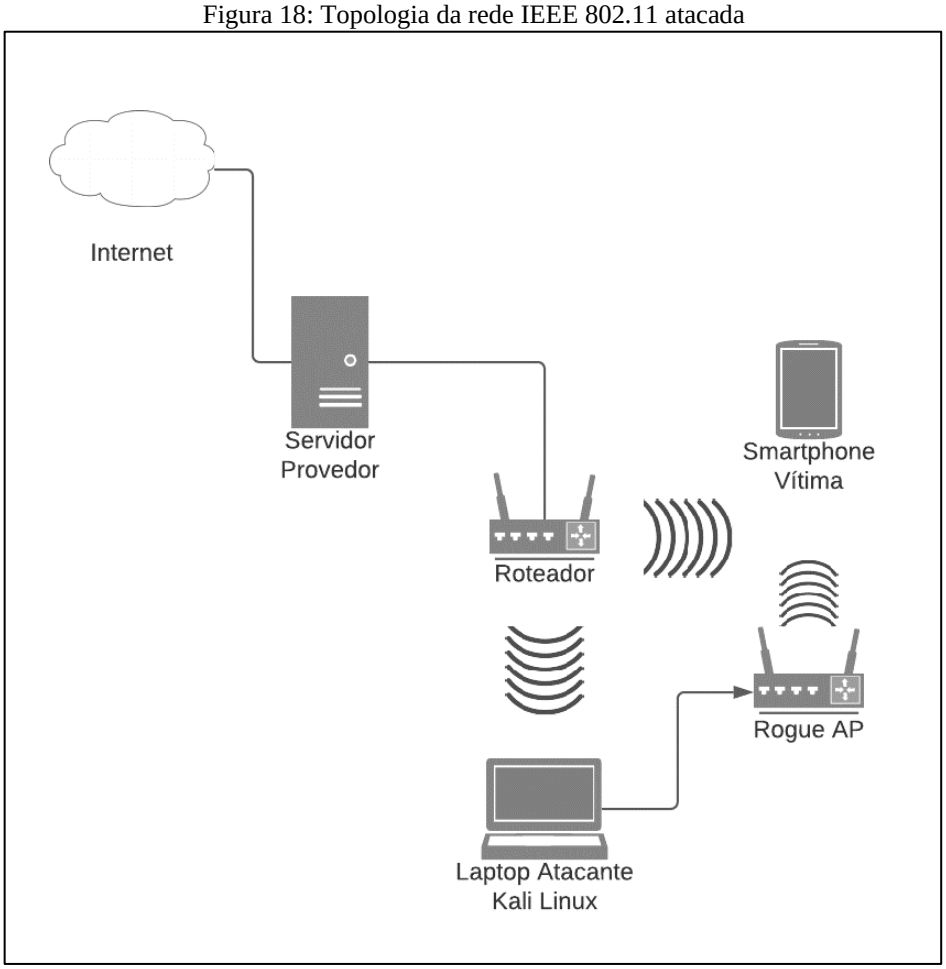
Quadro 1 - Equipamentos utilizados

Quantidade	**Equipamentos**
1	roteador *Wireless* Intelbras modelo W4-300F
1	adaptador USB IEEE 802.11 n/g/b modelo TL-WN 722N
1	*smartfone* sistema operacional Android versão 9.0
1	computador AMD Ryzen 7, 2.30 GHz, 8 GB de RAM

Fonte: Autoria própria.

O cenário foi dividido entre cliente, servidor e atacante. No cliente foi utilizado um *smartfone*, sistema operacional Android, versão 9.0 que representou o papel da vítima que já está conectado no AP. No servidor foi utilizado o roteador *wireless* Intelbras modelo W4-300F simulando a rede aberta com acesso à *Internet*. E o atacante foi simulado através de uma máquina virtual (*Virtual Machine* – VM) o VMware, no qual foi instalado o sistema operacional Kali Linux, versão 2021-3 além de ser utilizado o adaptador USB IEEE 802.11 n/g/b para que possibilitasse que a VM tenha uma placa de rede *wireless* que foi utilizado o modelo TL-WN 722N. A Figura 18 mostra o cenário de todas as simulações.

Figura 18: Topologia da rede IEEE 802.11 atacada



Fonte: Elaborado pelo autor.

4.2 Ferramentas

Nesta seção, são descritas as ferramentas que foram utilizadas nos ataques que são detalhadamente expostos no capítulo 5.

4.2.1 Kali Linux

O Kali Linux é um sistema operacional Linux que possui um conjunto de ferramentas de intrusão, o objetivo principal é realizar testes de invasão, *hacking* ético e avaliação de segurança da rede e é composto por mais de 300 ferramentas diferentes. A distribuição Kali é totalmente *open source* e qualquer usuário consegue visualizar facilmente todos os seus códigos.

Todas as ferramentas pertencentes ao sistema operacional foram avaliadas quanto à sua aplicabilidade e eficácia antes de serem incluídas, que inclui o *metasploit* para teste de invasão de rede, a network mapper (NMAP) em português mapeador de rede, para varredura de portas

e vulnerabilidades, *Wireshark* para monitoramento de tráfego de rede e Aircrack-ng para teste de segurança de rede sem fio. Estas são algumas das ferramentas do Kali Linux (Kali Linux, 2021).

4.2.2 Aircrack-ng

O Aircrack-ng é um conjunto de ferramentas para auditoria de redes sem fio, capaz de detectar redes e fazer a análise delas, como o airmon-ng, airodump-ng e aireplay-ng que foram utilizadas nos testes. Todas suas ferramentas são utilizadas em linhas de comando e o seu principal uso é um ambiente Linux, porém ele também pode ser executado em diferentes sistemas operacionais (Moreno, 2016).

O aircrack-ng foca em diferentes áreas de segurança em redes *wireless*, entre elas estão o monitoramento, que faz a captura de pacotes e exportação de dados para arquivos texto para processamento futuro por ferramentas de terceiros o ataque, que permite ataques de repetição, desautenticação, pontos de acesso falsos e outros via injeção de pacotes, o teste que serve para fazer a verificação de placas Wi-Fi e recursos de *driver*s como captura e injeção e *cracking*. As ferramentas que foram utilizadas nos testes estão descritas no Quadro 2.

Quadro 2 - Ferramentas utilizadas da suíte de ferramentas aircrack-ng

Ferramenta	**Função**
airmon-ng	Habilita a o modo monitor da *interface wireless.*
airodump-ng	Monitora os pacotes 802.11.
aireplay-ng	Injeta pacotes na rede.

Fonte: Autoria própria.

4.2.2.1 Airmon-ng

O Airmon-ng é usado para criar ou finalizar *interface*s em modo monitor. Também checa e finaliza processos que atrapalham a *suíte* aircrack-ng.

O Airmon-ng é uma das ferramentas da *suíte* aircrack-ng, ele é utilizado para checar e finalizar processos que podem atrapalhar a execução do programa, ele também é utilizado para transformar *interface*s *wireless* em *interface*s de monitoramento, de forma que essas *interface*s capturam pacotes de APs. (Moreno, 2016)

4.2.2.2 Airodump-ng

O Airodump-ng é uma ferramenta utilizada para a captura de pacotes de uma rede *wireless*, que tem como principal função a captura de IV's, sendo capaz de capturar todos os pacotes e *frames* trafegados na rede. Com os pacotes capturados, pode-se visualizar diversas informações valiosas das redes, como o endereço MAC do AP, qual método de criptografia utilizado pelo AP, canal de operação, se as redes estão sendo utilizadas ou não, número de pessoas conectadas às redes, velocidade máxima de transmissão de dados, entre outros (Moreno, 2016).

Ela contém recursos e configurações para a análise da rede sem fio além das convencionais, como descobrir o nome de uma rede oculta além de mostrar as *request* de clientes procurando por redes.

4.2.2.3 Aireplay-ng

O Aireplay-ng é uma ferramenta de ataque, que contém múltiplos vetores de ataques que podem ser combinadas com outras ferramentas, como o Packetforge-ng e o Aircrack-ng. Os principais métodos de ataque utilizados pelo Aireplay-ng são os, Testes de injeção, Death, Fake Auth, Modo Interativo, *Address Resolution Protocol* (ARP) Replay, Chop Chop, Fragmentação (Moreno, 2016).

4.2.3 Wifipumpkin3

O Wifipumpkin3 é uma estrutura para o *rogue* AP, escrito em Python, que permite e oferece a pesquisadores de segurança, *redteams* e engenheiros reversos a montagem de uma rede sem fio para conduzir um ataque o *Man-in-the-middle* (MITM).

O Wifipumpkin3 é uma ferramenta utilizada para fazer a ponto de uma conexão *Ethernet* ou Wi-Fi existente fornecer acesso à *Internet* para qualquer pessoa que queira se conectar a uma rede aberta sem fazer muitas perguntas, que possui uma grande quantidade de recursos incluído pontos de acesso Wi-Fi desonestos, ataques de desautorização em APs clientes, uma solicitação de sondagem e monitor de credenciais, *proxy* transparente, ataque de atualização do Windows, gerenciador de *phishing*, envenenamento de ARP, falsificação de DNS, Pumpkin-Proxy e captura de imagem no vôo.

4.2.4 Wireshark

O Wireshark é o analisador de protocolo de rede mais importante e amplamente utilizado no mundo. Ele permite a visualização do que está acontecendo na rede em um nível micro e é o padrão mais comumente utilizado em empresas comerciais e sem fins lucrativos (Combs, 2021).

Além de ser um *software* livre, também pode encontrar versões adequadas para as plataformas Windows, Mac OS X, Linux e Unix. O Wireshark é um analisador de protocolos de rede com função *sniffer*, que permite capturar pacotes de dados em tempo real diretamente na ferramenta para análise posterior.

A principal vantagem de se usar o Wireshark como *sniffer* e analisador de pacotes é que os pacotes capturados podem ser monitorados em tempo real em sua *interface* gráfica, e a ferramenta mostra esses pacotes em detalhes. Além disso, ele também possui várias funções, incluindo verificação detalhada do protocolo, captura em tempo real e outros fatores.

5 DESCRIÇÃO DO EXPERIMENTO

Neste capítulo é descrita a simulação dos testes de invasão a redes sem fio IEEE 802.11, que foi subdividido em três partes, iniciando com o ataque de desautenticação, em seguida o do *rogue* AP e posteriormente o MITM.

5.1 Ataque de desautenticação

O ataque de desautenticação é um ataque MITM cujo objetivo é a comunicação entre o roteador e o dispositivo, desabilitando efetivamente o Wi-Fi no dispositivo. Nesse tipo de ataque, o cliente pode ser desautenticado da rede até que o invasor decida quando parar.

O ataque de desautenticação tem várias finalidades, como deixar o usuário em um estado *Denial of Service* (DoS), em português negação de serviço, apenas para desconectar o usuário, ou pode ser combinado com DoS Evil Twin / *honeyspot*, uma falsa rede com o mesmo nome, permitindo que os usuários se conectem a esta rede, para que ele possa obter dados da rede real. Outro método de usar o ataque de desautenticação é para ataques criptográficos, capturando o fluxo de chaves ou *handshake* de quatro vias e gerando uma solicitação *address resolution protocol* (ARP) em português protocolo de resolução de endereços. Para demonstrar o ataque de desautenticação, foram utilizadas as ferramentas airmon-ng e aireplay-ng da *suíte* de ferramentas aircrack-ng (MORENO, 2016).

5.1.1 Método de Ataque

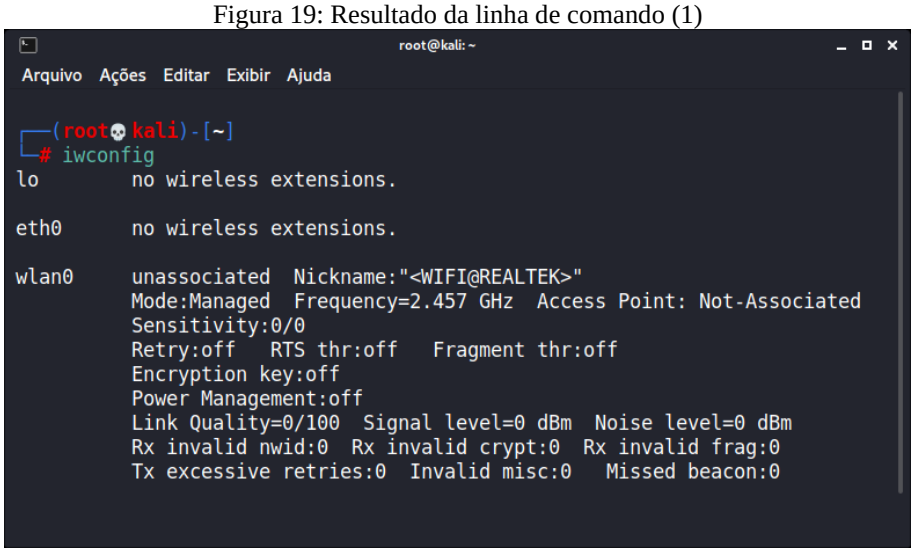
Para a demonstração do ataque de desautenticação, as ferramentas airmon-ng e aireplay-ng do *kit* de ferramentas aircrack-ng foram utilizadas para a realização do ataque, que é necessário que o invasor esteja no modo *root* no Kali Linux para que as ferramentas possam ser utilizadas através da linha de comando no terminal. A partir de ambas as ferramentas é possível descobrir todas as redes mesmo que ocultas, monitorar, capturar e fazer a injeção de pacotes.

Para isso é necessário um adaptador *wireless* ativo no ambiente virtualizado, que para esse trabalho foi utilizado o VMware e após estar conectado a primeira coisa a se fazer é identificar o nome da *interface* de rede que também pode ser utilizado para configurar o dispositivo em modo promíscuo e modo monitor, trabalhar em um canal específico e criar *interface*s virtuais. Sendo esse representado pelo comando (1).

```
# iwconfig                                                    (1)
```

A Figura 19 mostra o resultado da linha de comando (1). Com ele é possível ver todos os dispositivos de rede encontrados pelo sistema operacional no computador.

Figura 19: Resultado da linha de comando (1)

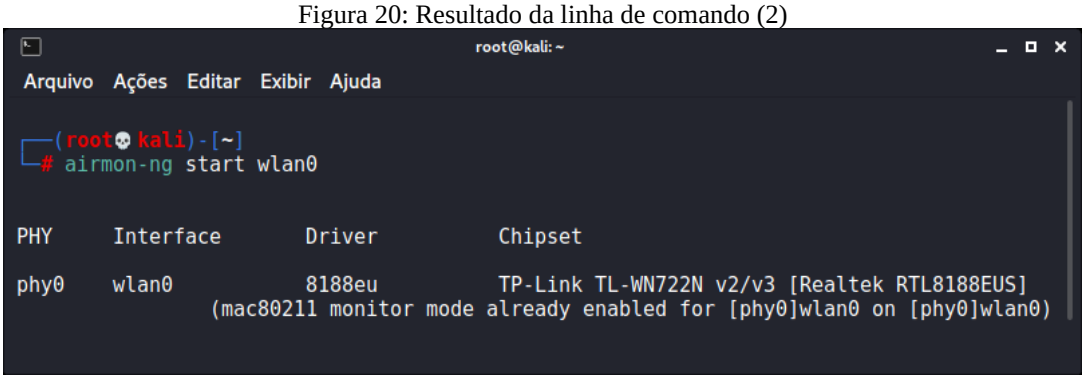


Fonte: Tela capturada pelo autor deste trabalho.

Após a identificação da *interface* de rede é necessário iniciar a placa em modo monitor e para isso foi utilizado o comando (2) que é apresentado na Figura 20.

airmon-ng start wlan0 (2)

Figura 20: Resultado da linha de comando (2)

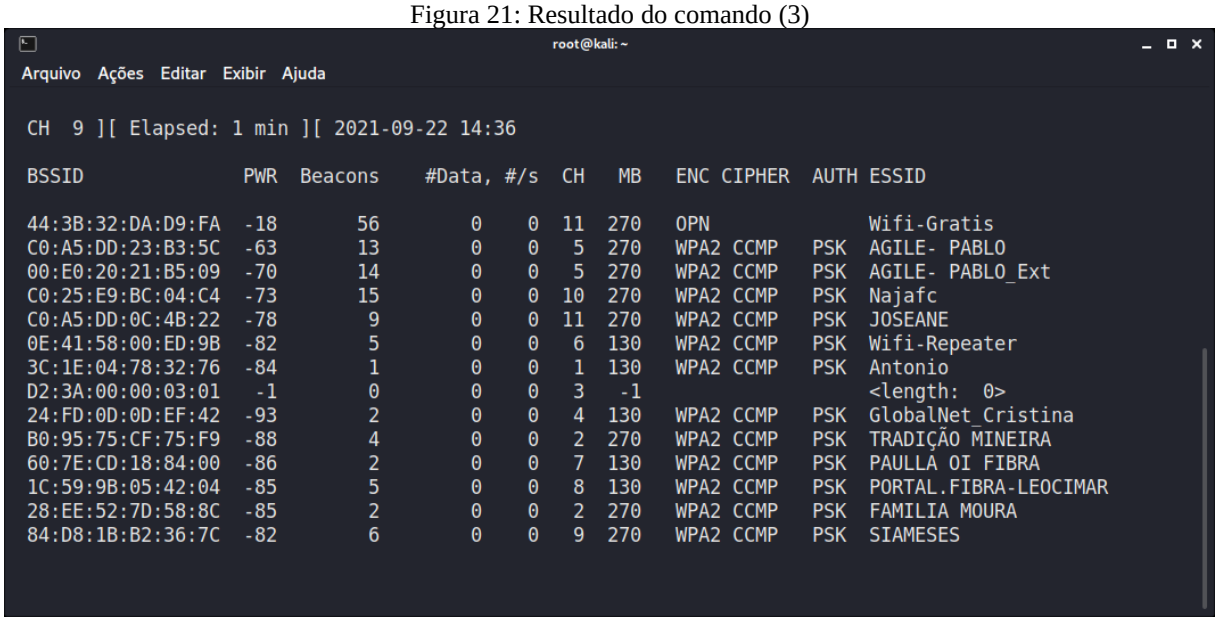


Fonte: Tela de captura do *software* (Airmon-ng, 2021) pelo autor deste trabalho.

Após a ativação do modo monitor é utilizado a segunda ferramenta para a realização do ataque que é o airodump-ng para visualizar as informações sobre as redes, que para ser utilizado foi usado a linha de comando (3).

airodump-ng wlan0 (3)

Figura 21: Resultado do comando (3)



Fonte: Tela de captura do *software* (Airodump-ng, 2021) pelo autor deste trabalho.

O resultado da linha de comando (3) é uma lista com todos os APs ao alcance, identificando todas as informações dos AP disponíveis conforme mostrado na Figura 21 e descritas no Quadro 3.

Quadro 3 - Descrição das informações obtidas pela linha de comando (3)

Campo	Descrição
BSSID	Endereço MAC do AP.
PWR	Nível de sinal apresentado pela placa. Seu significado depende do *driver*, mas quanto maior o sinal mais perto do AP ou estação. Se o *basic service set identifier* (BSSID) em português identificador de conjunto de serviço básico PWR for -1, então o *driver* não suporta relatório do nível de sinal. Se o PWR for -1 para um número limitado de estações, então isso é para um pacote que veio de um AP para o cliente, mas as transmissões do cliente estão fora do alcance da placa. O que significa que está escutando somente metade da comunicação. Se todos os clientes tiverem PWR como -1, então o *driver* não suporta relatório do nível de sinal.
BEACONS	Número de pacotes de aviso enviados pelo AP. Cada AP manda por volta de 10 *beacon*s por segundo na velocidade mais baixa (1Mbps), então geralmente eles podem ser pegos de bem longe.

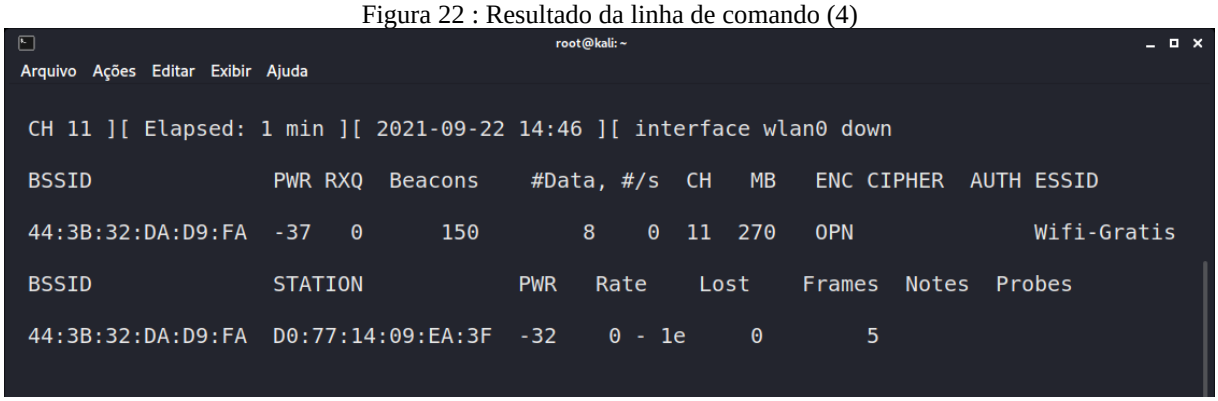
#Data	Número de pacotes de dados capturados (se WEP, contagem única de IVs), incluindo pacotes de difusão de dados.
#S	Número de pacotes de dados por segundo medidos nos últimos 10 segundos.
CH	Número do Canal (capturados a partir dos pacotes *beacon*). Às vezes pacotes de outros canais são capturados mesmo se o airodump-ng não estiver saltando canais, por causa da interferência de rádio.
MB	Velocidade máxima suportada pelo AP. Se MB = 11, é IEEE 802.11b; se MB = 22 é IEEE 802.11b+ e velocidades maiores são IEEE 802.11g. O ponto (após 54 acima) indica que preâmbulo curto - *short preamble* - é suportado.
ENC	Algoritmo de criptografia em uso. OPN = sem criptografia, "WEP?" = WEP ou maior (não há dados suficientes para escolher entre WEP e WPA/WPA2), WEP (sem o ponto de interrogação) indica WEP estático ou dinâmico, e WPA ou WPA2 se TKIP ou CCMP estiver presente.
CIMPHER	A cifra detectada. Um desses: CCMP, WRAP, TKIP, WEP, WEP40 ou WEP104. Não é regra, mas o TKIP é tipicamente usado com WPA e o CCMP é tipicamente usado com WPA2. WEP40 é mostrado quando o índice da chave é maior que 0. O padrão define que o índice pode ser 0-3 para 40 *bits* e deve ser 0 para 104 *bits*.
AUTH	O protocolo de autenticação usado e po de ser: MGT (WPA/WPA2 usando um servidor de autenticação separado), SKA (Chave compartilhada para WEP), PSK (Chave pré-compartilhada para WPA/WPA2), ou OPN (Aberto para WEP).
ESSID	O SSID, que pode estar vazio, se o esconder SSID estiver ativado. Nesse caso, airodump-ng tenta recuperar o SSID de respostas de sondagem (*probe responses*) e pedidos de associação (*association requests*).

(SMITH, 2008)

Após a identificação e informação de todos os APs, é necessário pegar dois dados do AP que é a vítima deste ataque, que são o BSSID e o CH que é o canal utilizado pelo AP. Com essas informações é utilizado novamente a ferramenta Airodump-ng só que agora informando o canal, o endereço MAC do AP e a *interface* de rede utilizada que é a wlan0 descrita no comando (4) e a sua saída na Figura 22.

```
# airodump-ng -c11 -bssd 44:3B:32:DA:D9:FA wlan0
```
(4)

Figura 22 : Resultado da linha de comando (4)



Fonte: Tela de captura do *software* (Airodump-ng, 2021) pelo autor deste trabalho.

Após obter todas as informações do AP, foi utilizado a ferramenta aireplay-ng para solicitar a injeção de pacotes sobrecarregando assim o AP, forçando a desautenticação de todos os dispositivos conectados a ele. O Quadro 4 mostra todas as opções do aireplay-ng.

Quadro 4 - Ferramentas utilizadas da suíte de ferramentas aireplay-ng

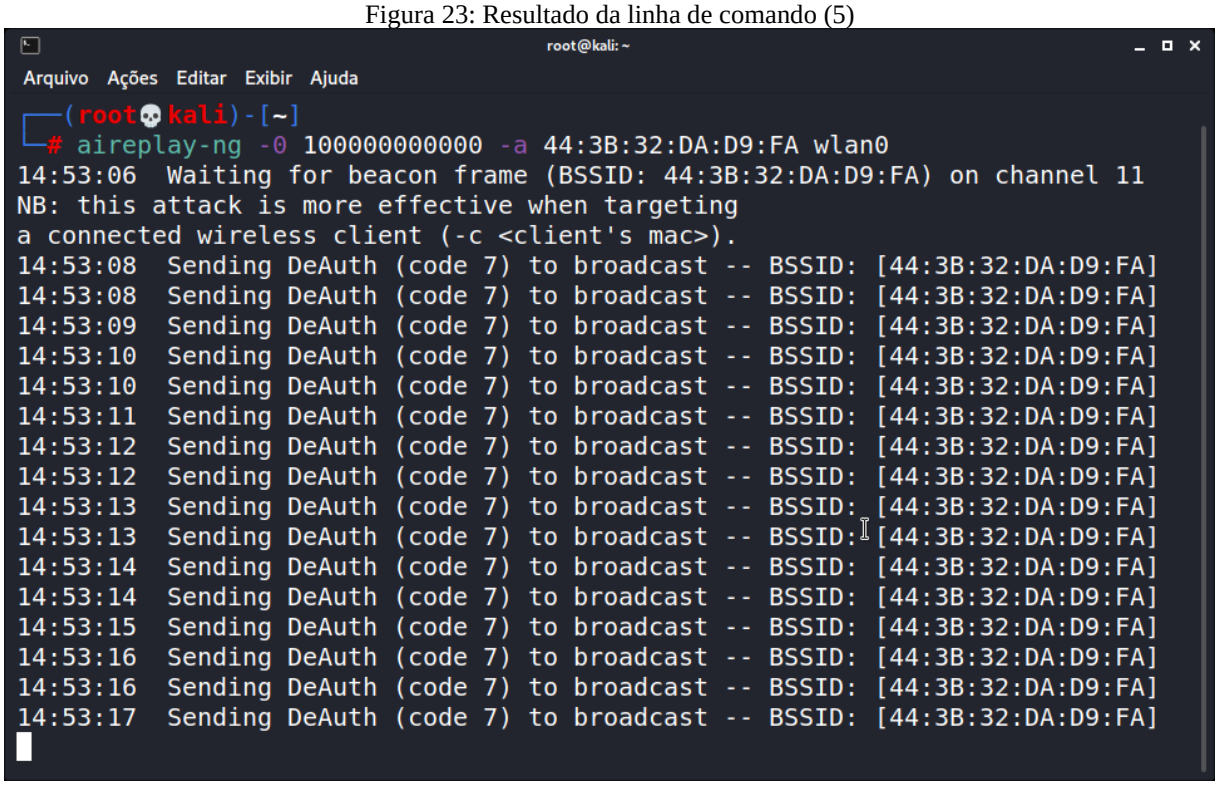
Ataque	**Modos de Ataque**
-0	Desautenticação
1	Autenticação falsa
2	Repetição de pacotes interativos
3	Repetição de ARP *Request*
4	Ataque Korek chopchop
5	Ataque de fragmentação
9	Teste de injeção.

Fonte: (AIRCRACK-NG, 2019)

Para a realização do ataque de desautenticação foi utilizado o módulo de ataque 0 também conhecido como ataque de desautenticação, descrito no Quadro 4 que foi utilizado no comando da linha (5) informado o nome da ferramenta. A opção -0 identifica o ataque é o de desautenticação. Após isso, foi informado a quantidade de pacotes de desautenticação que foi definido como (100000000000). Depois é acrescentado a opção -a que funciona como um atalho informando que o próximo dado a ser inserido é o endereço MAC do AP. Após a inserção do MAC do AP o comando da linha (5) é executado. Sua saída é apresentada na Figura 23.

aireplay-ng -0 100000000000 -a 44:3B:32:DA:D9:FA wlan0 (5)

Figura 23: Resultado da linha de comando (5)



Fonte: Tela de captura do *software* (Aireplay-ng, 2021) pelo autor deste trabalho

5.1.2 Método de Defesa

Como o ataque de desautenticação utiliza as funções definidas na especificação IEEE 802.11, não é possível reduzir completamente o risco de tal ataque, mantendo a conformidade com o padrão. Nesse sentido, de acordo com (McClure, Scambray, & Kurtz, 2014), fez com que alguns clientes corporativos criassem drives personalizados para minimizar os danos.

Assim que o adaptador de rede sem fio do cliente identifica o quadro de desautenticação e se reconecta rapidamente em um AP corporativo completamente diferente, o adaptador de rede sem fio do cliente desconecta tanto o intruso como o alvo. Após ser descoberta essa forma de defesa, foram lançadas ferramentas que observam esse comportamento e tentam automatizar o monitoramento do cliente à medida que ele se move para cada AP, pondo-o para fora assim que o descobrem.

5.1.3 Resultados Obtidos

O resultado do ataque se mostrou eficaz, mesmo existindo a proteção de ataque ARP nos APs e embora o roteador utilizado na simulação possua esta função, ela foi completamente inválida utilizando o aireplay-ng.

De modo que foi possível enviar uma grande quantidade de pacotes ARP para o cliente do MAC 44:3B:32:DA:FA forçando assim a desautenticação de todos os dispositivos conectadas a ela.

5.2 Ataque *Rogue* Ap

Ataques *Rogue* AP são um dos ataques de ponta mais eficazes e potenciais em clientes de uma WLAN, que envolve o uso de pontos de acesso falsos, chamados *Rogue* AP, que são projetados para falsificar dispositivos maliciosos para que se façam passar por APs e enganar os usuários para que ingressem em redes falsas (Vale, 2010).

Segundo Vale (2010), seu objetivo é monitorar o tráfego da rede da vítima, que inevitavelmente passa por dispositivos maliciosos. Este tipo de ataque geralmente ocorre em um determinado local, em que o sinal de uma determinada rede sem fio é enfraquecido e então o invasor cria uma rede sem fio com o mesmo SSID e BSSID, além de compartilhar a conexão com a *Internet* através da *interface wireless*, até que a rede seja pirateada, sendo necessário a utilização de uma antena de maior ganho para chegar ao sinal e depois distribuí-lo.

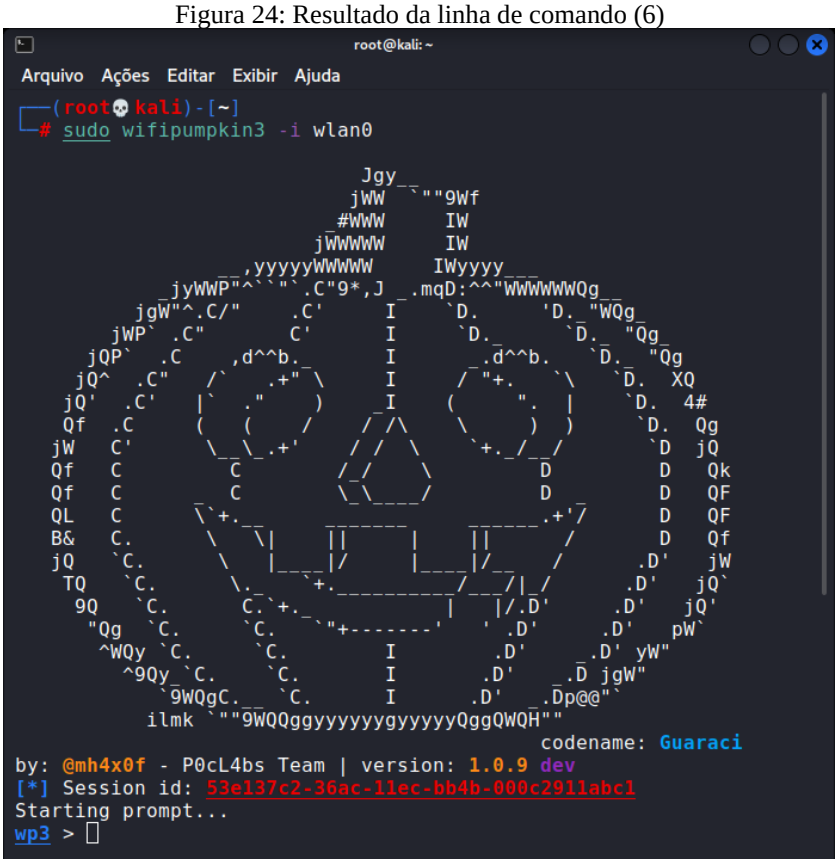
5.2.1 Método de Ataque

Para efetuar o ataque *rogue* AP, foi utilizado o *software* Wifipumpkin3 que é um *software* que possui uma estrutura para o ataque de *rogue* AP que é escrito em *Python* e descrito na seção 4.2.3 que não é nativo do Kali Linux sendo necessário à sua instalação conforme os parâmetros encontrados no Apêndice A.

Para construir um *rogue* AP, é necessário criar uma ponte entre a rede falsa criada com o Wifipumpkin3 e a rede legítima. Inicialmente foi informada a ferramenta que seria utilizada para a mesma a *interface* do adaptador de rede que seria o *rogue* AP o qual está identificado como wlan0 comando (6) e apresentado na Figura 24.

```
# sudo Wifipumpkin3 -i wlan0                                    (6)
```

Figura 24: Resultado da linha de comando (6)



Fonte: Tela de captura do *software* (Wifipumpkin3, 2021) pelo autor deste trabalho

Após a inicialização da ferramenta foi utilizado o comando (7) para verificar quais dados estavam setados na configuração do *rogue* AP antes da sua inicialização, e todos os dados que podem ser alterados. São eles: o BSSID, o SSID, o *Channel*, a *Interface*, o *Status* e o *Security* descritos no Quadro 5, apresentados no Quadro 5 e na Figura 25.

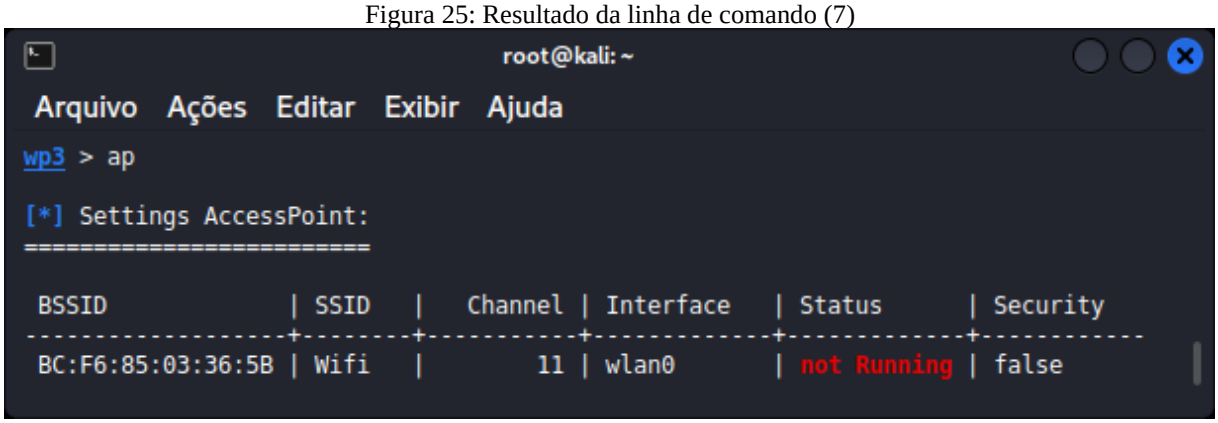
wp3 > ap (7)

Quadro 5 - Descrição das configurações *rogue* AP

Configurações do *rogue* AP	**Descrição**
BSSID	Endereço MAC do *rogue* AP.
SSID	Nome do *rogue* AP.
CHANEL	Canal utilizado pelo *rogue* AP.
INTERFACE	Interface utilizada pelo
STATUS	Status do *rogue* AP
SECURITY	Tipo de segurança utilizada para se autenticar na *rogue* AP.

Fonte: Elaborado pelo autor.

Figura 25: Resultado da linha de comando (7)



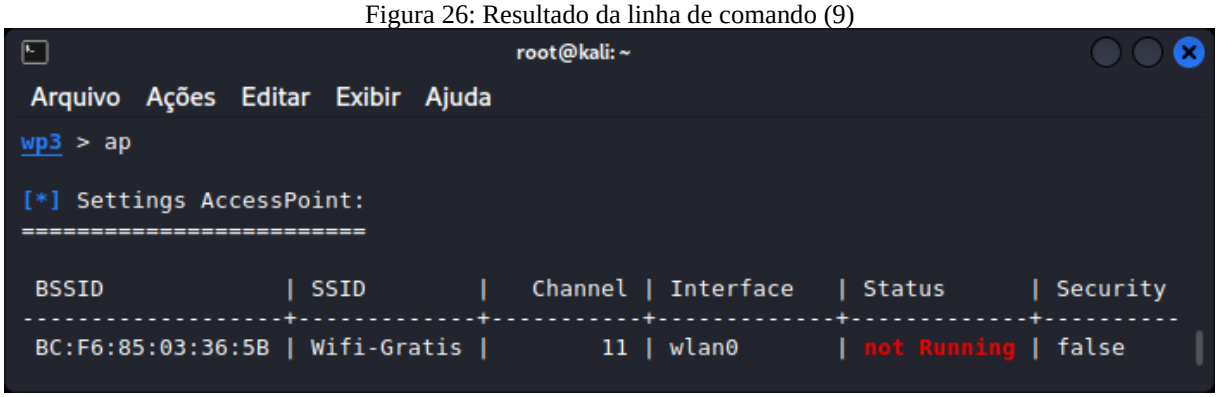
Fonte: Tela de captura do *software* (Wifipumpkin3, 2021) pelo autor deste trabalho

Após a verificação foi visto que apenas o SSID estava com o dado diferente dos dados obtidos pelo Airodump-ng do ataque descrito na seção 5.1 desse trabalho. Foi configurado nas configurações do *rogue* AP o mesmo SSID que é "Wifi-Gratis" comando (8).

wp3 > set ssid Wifi-Gratis (8)

Em seguida foi utilizado o comando da linha (7) para verificar novamente se o SSID está correto conforme demonstrado na Figura 26.

Figura 26: Resultado da linha de comando (9)



Fonte: Tela de captura do *software* (Wifipumpkin3, 2021) pelo autor deste trabalho

Posteriormente foi utilizado o comando (9) para iniciar o *rogue* AP.

wp3 > start (9)

Após a inicialização do ataque *rogue* AP o ataque 5.3 é executado.

5.2.2 Método de Defesa

Não há como o usuário ou seu dispositivo distinguir entre os APs legítimos e falsos. Contudo, dentre os diversos métodos de controle de acesso, o mais indicado é a estrutura

analítica do projeto (EAP), utilizado pelo padrão IEEE 802.1x, pois permite validar o certificado digital do servidor de autenticação da rede e usar criptografia.

No entanto, se o *rogue* AP usar um certificado digital emitido por uma autoridade certificadora (AC) legítima, o dispositivo aceitará o certificado sem contestar. Na verdade, apenas o provedor de serviço pode detectar e reagir contra os *rogue* APs.

Contudo, essa ação requer uma infraestrutura de rede que implica em um significativo investimento, como a utilização de APs especiais e sistemas de monitoramento e de contra-ataque, conhecidos como *Wireless Intrusion Prevention System* (WIPS). Outra forma de tentar mitigar o problema é sempre utilizar comunicação segura, *Hyper-Text Transfer Protocol Secure* (HTTPS), entre o cliente e o servidor (DIAS, 2019).

5.2.3 Resultados Obtidos

O resultado do ataque foi satisfatório. Ao levantar o serviço da rede do *rogue* AP para a captura de dados de estações simulando um local público, um dispositivo além do que foi utilizado para simulação, tentou se autenticar na rede o que mostrou que o ataque é efetivo. Mas como o trabalho foi para fins de estudo e apenas simulação, para a segurança da vítima o ataque foi interrompido e realizado em outro horário.

5.3 Ataque Man-in-The-Middle

O ataque MITM é uma forma de ataque em que os dados entre duas partes são de alguma forma interceptados, registrados e possivelmente alterados pelo atacante sem que as vítimas percebam. É um ataque que o atacante consegue ficar no meio da conexão entre o cliente o seu destino, capturando toda a conexão.

Os ataques de MITM em redes sem fio podem ser efetuados com o intuito de capturar credenciais de usuários. Este tipo de ataque é possível mediante a utilização de um processo denominado ARP *spoofing*. Este processo é efetuado da seguinte forma: o ARP identifica o endereço MAC para um determinado endereço IP. Sempre que um dispositivo pretende comunicar com o seu par numa rede IP, envia um pedido ARP por difusão na rede solicitando o endereço MAC do IP do interlocutor. Um atacante pode responder com o endereço MAC do seu dispositivo que identifica o endereço IP do pedido. A partir desse momento, todas as comunicações entre os dispositivos são primeiro encaminhadas para o dispositivo do atacante, permitindo o recolhimento, manipulação ou eliminação da informação.

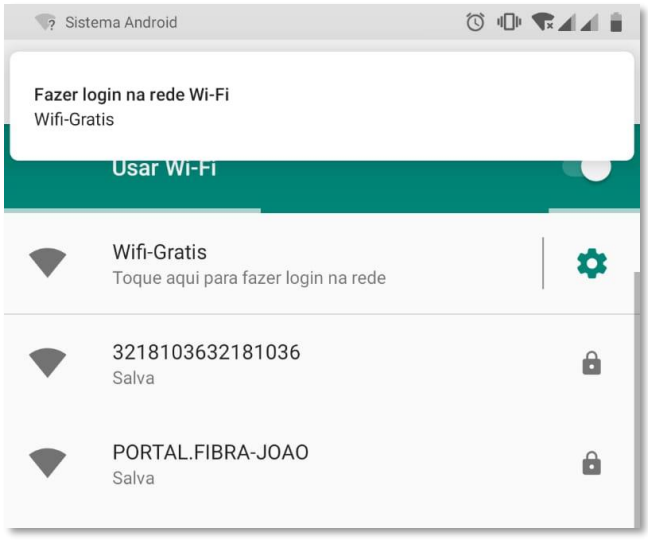
5.3.1 Método de Ataque

O objetivo do ataque foi obter as credenciais de login e senha do *Facebook* assim como fazer a captura de todo o tráfego a partir da autenticação do mesmo no *rogue* AP. Para a realização do ataque MITM foi utilizado o Wifipumpkin3 do ataque do *rogue* AP em conjunto com o Wireshark descrito na seção 4.2.4 que não é nativo do Kali Linux sendo necessário à sua instalação, para fazer a análise do tráfego da rede.

O ataque funciona da seguinte forma: primeiramente é necessário o atacante fazer a verificação para saber se o *rogue* AP está ativo, ele estando ativo e o ataque de desautenticação também o ataque pode ser feito.

O ataque começa com vítima tentando se conectar em algum AP, que ao fazer a busca aparecerá o AP do ataque do *rogue* AP e ao tentar se conectar a ela aparece na de tela de autenticação conforme apresentado na Figura 28.

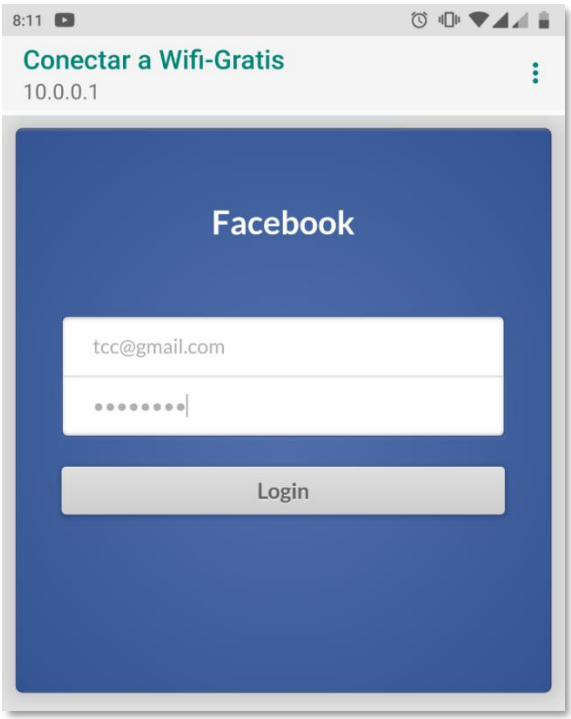
Figura 27: *Print* da tela da vítima



Fonte: Elaborado pelo autor.

Assim que a vítima clica no AP para se conectar ao AP, aparece a opção para ela se autenticar antes de ter acesso à *Internet* liberado e é apresentada uma tela de autenticação *fake* do *Facebook*, no qual é solicitado as credenciais para que a conexão seja autorizada conforme apresentado na Figura 29.

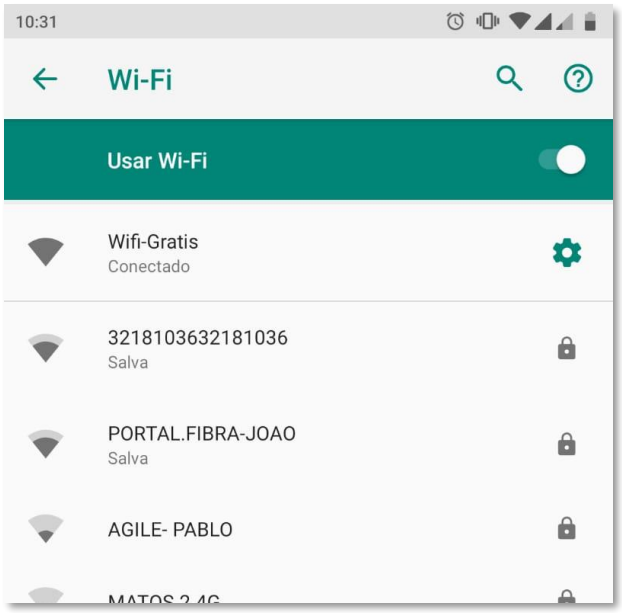
Figura 28: *Print* tela de login da vítima



Fonte: Elaborado pelo autor.

Na Figura 29 é mostrado o *print* da tela da vítima após a informação das credenciais no qual o acesso à *Internet* é autorizado para a vítima.

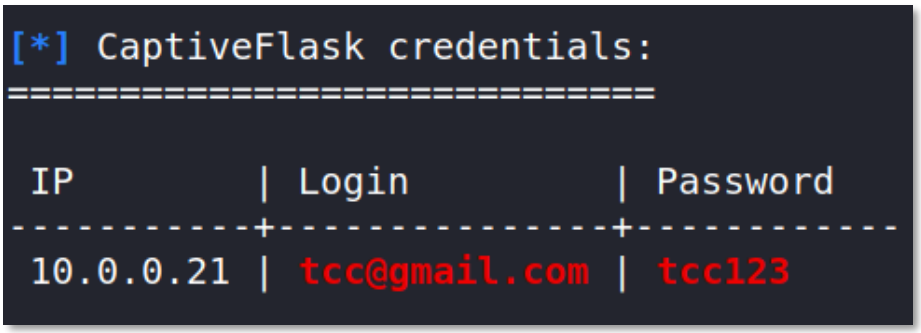
Figura 29: *Print* após o login da vítima



Fonte: Elaborado pelo autor.

E a partir desse momento o atacante obtém o acesso total a todo o tráfego da rede assim como a credencial que a vítima digitou para se autenticar no AP sendo essa mostrada no terminal do Wifipumpkin3 conforme pode ser visto na Figura 31.

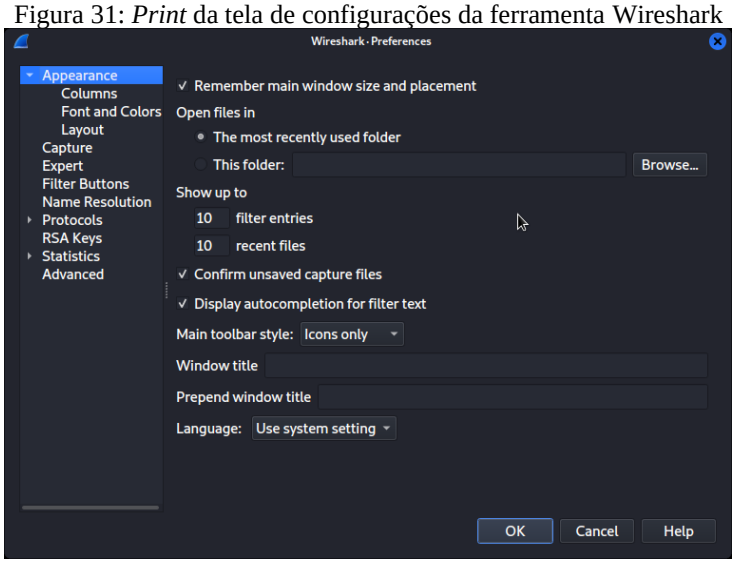
Figura 30: *Print* da tela da ferramenta Wifipumpkin3 após o usuário fazer o login



Fonte: Tela de captura do *software* (Wifipumpkin3, 2021) pelo autor deste trabalho

Para ser feito a captura do tráfego foi utilizado o Wireshark o qual após a sua inicialização foi feita algumas configurações na ferramenta, a fim de ser salvo todos os pacotes capturados em um arquivo *log* que foi criado no *Desktop* nomeado como sslkeylogfile.log. Para se ter acesso a aba de configurações foi utilizado as teclas de atalho Ctrl + Shift + P. Após ser digitado foi mostrada a tela de configurações conforme mostrado a Figura 32.

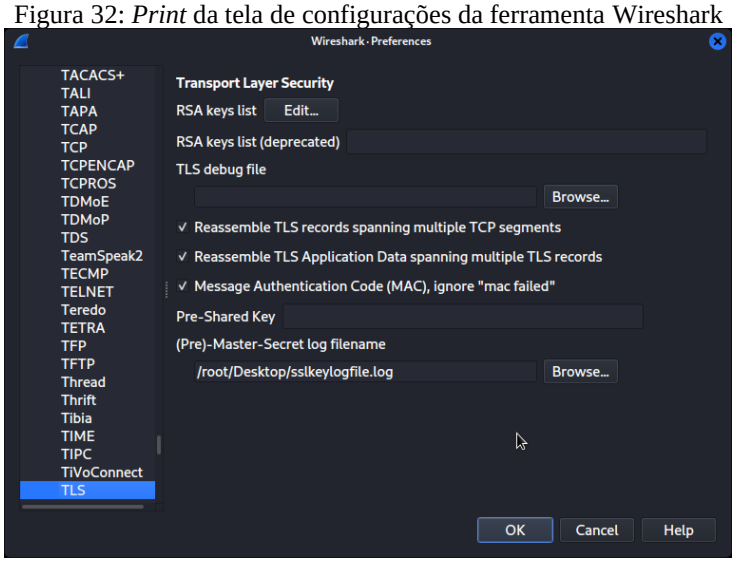
Figura 31: *Print* da tela de configurações da ferramenta Wireshark



Fonte: Tela de captura do *software* (Wireshark, 2021) pelo autor deste trabalho

Após foi selecionado a opção *Protocols* da Figura 31 é selecionado o protocolo *Transport Layer Security* (TLS) demostrado na Figura 32. Após a seleção do protocolo na opção *(Pre)-Master-Secret log filename* é selecionado o arquivo log que foi criado no *Desktop* e salvo as configurações.

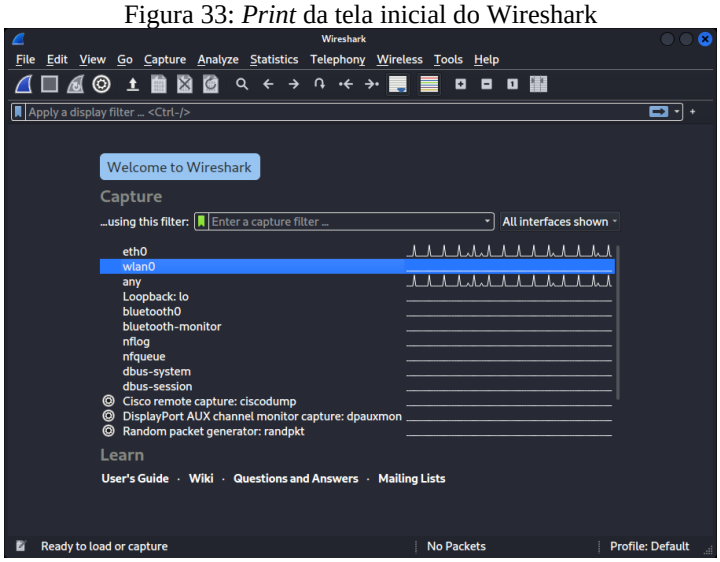
Figura 32: *Print* da tela de configurações da ferramenta Wireshark



Fonte: Tela de captura do *software* (Wireshark, 2021) pelo autor deste trabalho

Logo em seguida, volta novamente na tela inicial da ferramenta e seleciona a *interface* de rede que foi utilizada para o *rogue* AP que é a Wlan0 conforme demostrado na Figura 33.

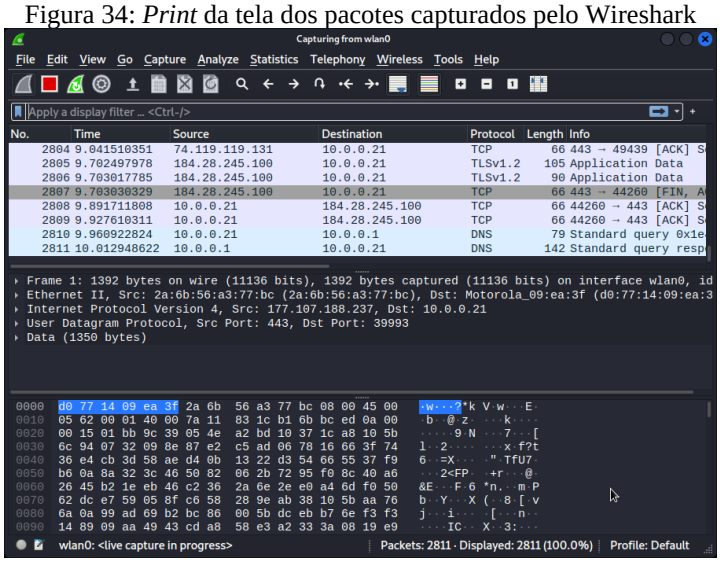
Figura 33: *Print* da tela inicial do Wireshark



Fonte: Tela de captura do *software* (Wireshark, 2021) pelo autor deste trabalho

Após ser selecionada a *interface* os pacotes capturados pelo Wireshark apresentados na Figura 34, são salvos no arquivo log que foi criado no *Desktop*.

Figura 34: *Print* da tela dos pacotes capturados pelo Wireshark



Fonte: Tela de captura do *software* (Wireshark, 2021) pelo autor deste trabalho

Posteriormente, depois de algum tempo é aberto o arquivo sslkeylogfile.log apresentado na Figura 35, para verificar se os pacotes capturados pelo o Wireshark estão nele, para que possa ser feita uma análise desses dados em outro momento, finalizando assim a parte de captura do tráfego finalizando assim o ataque MITM.

5.3.2 Método de Defesa

Existem muitas maneiras de se defender contra-ataques MITM, mas a maioria delas deve ser instalada no roteador/servidor e não é 100% segura. Também existe uma técnica que impõe criptografia complexa entre o cliente e o servidor.

Nesse caso, o servidor pode se identificar fornecendo um certificado digital para que o cliente possa estabelecer uma conexão criptografada e enviar informações confidenciais por meio dela. Mas a possibilidade dessa defesa depende de os dois servidores possuírem essa criptografia habilitada.

Por outro lado, os usuários podem se proteger de ataques MITM evitando conectar-se a Wi-Fi gratuito ou instalando *plug-ins* como HTTPS *Everywhere* ou ForceTLS no navegador. Esses programas só escolherão uma conexão segura enquanto estiverem disponíveis. Em qualquer caso, todas as estratégias de defesa têm limitações e há evidências de que vírus como SSLStrip ou SSLSniff podem contornar a segurança das conexões SSL.

5.3.3 Resultados Obtidos

O exemplo apresentado neste trabalho, utiliza uma rede falsa criada com o ataque *rogue* AP, apenas para que o ataque MITM possa ser feito possibilitando que a captura da senha de autenticação da rede com o *login* e senha do Facebook possa ser capturada e posteriormente que todos os pacotes também possam ser capturados e armazenados em um arquivo de *log* para serem analisados em outro momento. Portanto o ataque foi satisfatório já que foi feita a captura de senha utilizando o Wifipumpkin3 e a captura dos pacotes utilizando o Wireshark que ficou faltando a parte da análise desses dados capturados.

6 CONCLUSÃO

Por meio desse estudo, foram realizados ataques bem-sucedidos nesse tipo de rede, pode-se perceber que as redes IEEE 802.11 estão longe de serem seguras, já que estão constantemente sob ataques, que visam explorar suas vulnerabilidades.

Com o avanço dos protocolos de segurança, grandes melhorias ocorreram. Conforme foi visto no capítulo 3 desse estudo, novos métodos foram projetados para lidar com as vulnerabilidades de protocolos anteriores. De modo que, considerando o ano de 2021, se o WPA2 for configurado corretamente, ele supre bem a essa demanda.

Durante o processo de pesquisa, foi feita a análise das vulnerabilidades dos protocolos WEP, WPA, WPA2 e WPA3. Foi apresentado um estudo de caso, no qual foram obtidas credenciais de autenticação através de falhas contidas nesses protocolos de segurança. Além disso, foram mostrados métodos de defesa para se prefinir dos ataques realizados.

Em relação ao protocolo WEP, pode-se analisar seu funcionamento e apontar suas lacunas e falhas de segurança. Percebe-se que um dos seus grandes problemas é a repetição do IV, portanto, o seu não reaproveitamento deve ser controlado de uma forma mais rígida.

Outro ponto levantado é o tamanho da sua chave de criptografia, que era de 40 *bits* no WEP que foi aumentada para 104 *bits* na versão atualizada. Esse aumento no tamanho da chave mostrou-se eficaz, dificultando a sua detecção mais rápida.

Apesar do aumento do tamanho das chaves ainda existia uma outra fraqueza que é a inexistência de administração de chaves, o padrão não determina como elas devem ser distribuídas. Essas conclusões foram descritas detalhadamente na seção 3.1.

O protocolo WPA, surgiu com o propósito de melhorar o nível de segurança da rede sem fio a fim de combater as vulnerabilidades existentes no protocolo WEP, utilizando uma tecnologia de encriptação de chaves mais segura do que o RC4 do WEP conforme foi descrito na seção 3.2.

Por outro lado, o protocolo WPA2 é uma versão melhorada do WPA, que foi feita a inclusão de novos algoritmos de criptografia e integridade. Sendo a maioria dos equipamentos fornecidos pelos provedores de serviço de *Internet*, configurados com este padrão ao sair de fábrica, ajudando assim a melhorar a segurança da rede sem fio. Mesmo assim, ele possui algumas vulnerabilidades, sendo a mais famosa o DoS. Devido ao fato de o WPA2 utilizar uma estrutura de gerenciamento e controle de proteção, torna-se possível forçar uma estrutura de

gerenciamento de tipo de desautenticação. Portanto, ataques de força bruta em PSKs com menos de 20 caracteres ainda continuam vulneráveis conforme foi descrito na seção 3.3.

Com o avanço da tecnologia e a descoberta de vulnerabilidades no protocolo WPA2, surgiu o protocolo WPA3 que, de acordo com os resultados e discussões da seção 3.4, trouxe novos recursos para se obter uma autenticação mais forte além de trazer consigo novas vulnerabilidades, até mesmo algumas herdadas de seu protocolo predecessor WPA2.

Na parte experimental dessa monografia foram realizados três ataques, são eles o de desautenticação, *rogue* AP e MITM. Optou-se pela realização de mais de um ataque para mostrar o comportamento dos ataques diante de vários tipos de vulnerabilidades dos protocolos WPA e WPA2 deste o caso mais simples ao mais sofisticado.

De modo que, por meio da parte experimental do capítulo 5, os ataques podem ser realizados utilizando ferramentas totalmente gratuitas que podem ser utilizadas por qualquer pessoa mediante a um estudo dessas vulnerabilidades.

O primeiro ataque implementado para testes neste trabalho, foi o de desautenticação, descrito na seção 5.1 que consistiu em desabilitar a comunicação entre o roteador e a vítima, desabilitando efetivamente o Wi-Fi do dispositivo possibilitando assim um ambiente propício para o segundo ataque.

O segundo ataque implementado foi o *rogue* AP, que se aproveita das falhas dos sistemas operacionais e da falta de atenção do usuário. Segundo Vale (2010), é considerado como um dos ataques de ponta mais eficazes e potenciais e são projetados para falsificar dispositivos maliciosos, enganando assim os usuários e permitindo que o terceiro ataque possa ser efetuado conforme foi descrito na seção 5.2.

O terceiro ataque MITM descrito na seção 5.3 foi realizado em conjunto com o *rogue* AP. Nele são possíveis a interceptação e a alteração de pacotes de todo o tráfego feito pela vítima, permitindo com que o atacante fique no meio da conexão entre o cliente e destino, capturando todos os pacotes. Esse ataque depende muito da falta de informação por parte da vítima, já que o ataque foi feito utilizando uma página de autenticação *fake* do Facebook. Destaca-se que, essa página de autenticação não possui certificado digital o que dificulta o ataque já que a maioria dos navegadores expõem isso.

Os resultados obtidos nos ataques feitos foram satisfatórios. Foi possível explorar as falhas de segurança apresentadas no referencial teórico. Dessa forma, por meio dessa pesquisa, pode-se concluir que o maior problema no campo da segurança de redes sem fio é a falta de

familiarização por parte dos usuários com tópicos relacionados à segurança, como a escolha de senhas fáceis que podem ser facilmente descobertas.

Por meio dessa pesquisa foi observado que as medidas corretivas são simples de serem implementadas caso as orientações descritas na seção 5.1.2, 5.2.2 e 5.3.2 sejam seguidas. Conclui-se que a segurança das redes Wi-Fi exige que os usuários, sejam eles residenciais ou comerciais, que compreendam sobre a melhor forma de configuração dos seus dispositivos, para assim prevenir possíveis ataques. Em suma, divulgar ao público informações sobre o correto processo de configuração da rede Wi-Fi é fundamental, ressaltando a importância de ferramentas que garantam a segurança adequada da rede.

A metodologia adotada nesse trabalho foi adequada uma vez que todos os ataques foram realizados em um ambiente simulado não ocorrendo nenhum dano a qualquer pessoa ou organização, mas apesar de ser feito em um ambiente simulado foi possível reproduzir uma situação semelhante a que se tem na vida real.

Conclui-se que os objetivos propostos inicialmente cumpriram o esperado, já que foi identificado todos os protocolos de segurança do IEEE 802.11, por conseguinte a criptografia e a análise das fragilidades de cada um dos protocolos, junto com a demonstração de ataques e modos de proteção.

Apesar de existir vulnerabilidades severas nos protocolos de segurança, é importante enfatizar que a partir do momento que o usuário estuda e adota certos procedimentos descritos nas seções 5.1.2, 5.2.2 e 5.3.2 o risco pode ser minimizado ou até mesmo eliminado.

6.1 Sugestões de trabalhos futuros

Conforme foi descrito na conclusão, a parte prática deste trabalho focou na demonstração de algumas das vulnerabilidades dos protocolos WPA e WPA2 das redes IEEE 802.11. Descrevendo três diferentes tipos de ataques.

Em função disto, são dadas as seguintes sugestões de trabalhos futuros:

- Demonstração da análise dos dados capturados pelo Wireshark do ataque MITM;
- Implementação de uma rede *mesh* utilizando o protocolo WPA3 que seja segura, simulando um ambiente de um *Shopping Center* ou cafeteria ou outro local de acesso público ao Wi-Fi;
- Demonstração de um ataque a uma rede configurada com protocolo WPA3.

7 REFERÊNCIAS

AIRCRACK-NG. **Aircrack-ng**, 2019. Disponivel em: <https://www.aircrack-ng.org/doku.php?id=aireplay-ng>. Acesso em: 14 Outubro 2021.

ALLIANCE. Wi-Fi Org. **Wifi Alliance**, 2018. Disponivel em: <https://www.wi-fi.org/discover-wi-fi/security>. Acesso em: 7 Julho 2021.

ASSUNÇÃO, M. **Wireless Hacking - Ataque e segurança de redes sem fio WI-FI**. [S.l.]: [s.n.], 2013. ISBN 978-8575022825.

BARROS, E. Acesso sem controle a internet: Uma abordagem com engenharia social através de wireless fidelity (Wi-fi). **Revista UniBF**, Paraná, p. 1-5, Março 2021. Disponivel em: <https://revistaunibf.emnuvens.com.br/monumenta/article/view/41/23>. Acesso em: 20 abril 2021.

BOMFIM, M. **Wifipumpkin3**, 29 Setembro 2021. Disponivel em: <https://wifipumpkin3.github.io>. Acesso em: 12 Outubro 2021.

COMBS, G. **WireShark**, 2021. Disponivel em: <wireshark.org>. Acesso em: 12 Outubro 2021.

DIAS, D. Wireless Aruba – Rogue Containment (WIPS). **Comutadores**, 2019. Disponivel em: <https://www.comutadores.com.br/tag/wips/>. Acesso em: 10 Outubro 2021.

GIL, A. C. **Como elaborar projetos de pesquisa**. 6ª. ed. São Paulo: Atlas Ltda, 2017. ISBN 978-85-97-01292-7.

GIMENES, E. **Segurança de Redes Wireless**. FATEC. São Paulo, p. 58. 2005.

JUNIOR, A.; MORENO, E. Segurança em infraestrutura para internet das coisas, Pernanbuco, 9 maio 2016. 370-380. Disponivel em: <https://doaj.org/article/c89df05024004589997e01f06df279c8>. Acesso em: 9 Abril 2021.

KALI Linux. **Kali Linux**, 14 out. 2021. Disponivel em: <http://kali.org/>. Acesso em: 21 abr. 2021.

KHANDELWAL, S. Researchers Discover New Ways to Hack WPA3 Protected WiFi Passwords. **The Hacker News**, 3 Agosto 2019. Disponivel em: <https://thehackernews.com/2019/08/hack-wpa3-wifi-password.html>. Acesso em: 04 ago. 2021.

KOHLIOS, C.; HAYAJNEH, T. A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. **MDPI**, New York, 30 Outubro 2018. Disponivel em: <https://www.mdpi.com/2079-9292/7/11/284>. Acesso em: 15 Setembro 2021.

KUROSE, J.; ROSS, K. **Redes de computadores e a internet uma abordagem top-down**. 6ª. ed. São Paulo: Pearson Education do Brasil, 2014. 658 p.

KURYU, J. **Share Technote**. Disponivel em: <http://www.sharetechnote.com/html/WLAN_FrameStructure.html>.

LAKSHMANAN, R. Nearly All Wi-Fi Devices Are Vulnerable to New FragAttacks. **The Hacker News**, 12 Maio 2021. Disponivel em: <https://thehackernews.com/2021/05/nearly-all-wifi-devices-are-vulnerable.html>. Acesso em: 15 Outubro 2021.

LINHARES, A.; GONÇALVES, P. **Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w∗**, Recife – PE, 2010. 1-17.

MCCLURE, S.; SCAMBRAY, J.; KURTZ, G. **Hackers Expostos**. 7ª. ed. [S.l.]: Bookman, 2014.

MORENO, D. **Penteste em redes sem fio**. São Paulo: Novatec Editora Ltda., 2016.

MOSKOWITZ, R. Weakness in Passphrase Choice in WPA Interface. **wifinetnews**, Novembro 2003. Disponivel em: <https://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html>. Acesso em: 22 Setembro 2021.

MYERSON, J. WPA3 protocol: Should enterprises implement the changes? **Techtarget**, Setembro 2018. Disponivel em: <https://www.techtarget.com/searchsecurity/answer/WPA3-protocol-Should-enterprises-implement-the-changes>. Acesso em: 23 Setembro 2021.

NAKAMURA, E.; GEUS, P. **Segurança de Redes em Ambientes Cooperativos**. [S.l.]: Novatec, 2007. 482 p. ISBN 978-85-7522-136-5.

PAIM, R. Grupo de Teleinformática e automação UFRJ, 2011. Disponivel em: <https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/index.html>.

RUFINO, N. M. D. O. **Segurança em Redes sem fio:** Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth. 4ª. ed. [S.l.]: Novatec, 2015. 288 p.

SANTANA. [S.l.]: [s.n.]. ISBN 978-8575022825.

SMITH, J. Airodump-ng. **Aircrack-ng**, 25 mar. 2008. Disponivel em: <https://www.aircrack-ng.org/doku.php?id=pt-br:airodump-ng>. Acesso em: 15 out. 2021.

STALLINGS, W. **Criptografia e Segurança de Redes Principios e Práticas**. 6º. ed. São Paulo – SP – Brasil: Pearson Education do Brasil, 2015. 558 p. ISBN 978-85-430-0589-8.

VALE, D. Ataque de Rougue AP com AIRBASE-NG, 30 nov. 2010. Disponivel em: <https://www.vivaolinux.com.br/artigo/Ataque-de-Rougue-AP-com-AIRBASENG>.

VANHOEF, M.; RONEN, E. Dragonblood: Analyzing the Dragonfly. **Analysing WPA3's Dragonfly Handshake**, Abril 2019. 17.

VASCONCELLOS, R. **Segurança em Redes sem Fio**. Rio de Janeiro: Rede Nacional de Ensino e Pesquisa – RNP, 2013. 182 p. ISBN 978-85-63630-30-8.

WAZLAWICK, R. **Metodologia de pesquisa para ciência da computação**. 2ª. ed. Rio de Janeiro: Elsevier Editora Ltda, 2014. 146 p. ISBN 978-85-352-7782-1.

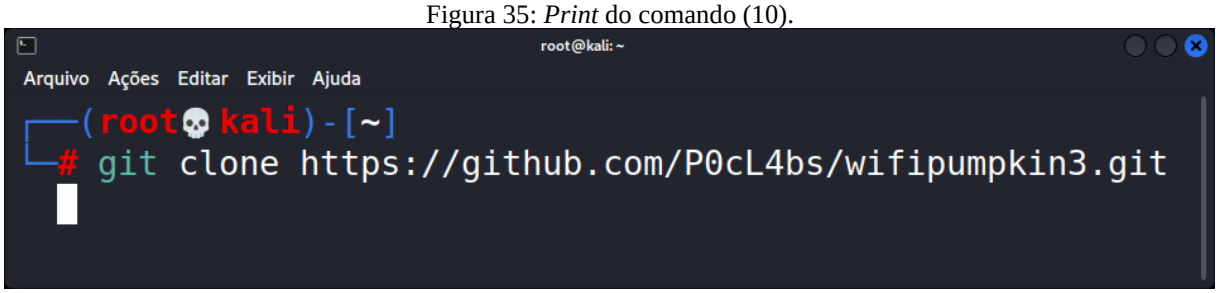
APÊNDICE A – INSTALAÇÃO DO WIFIPUMPKIN3

Descreve-se nesse apêndice as etapas que foram realizadas na instalação do Wifipumpkin3.

(1) A partir do terminal do Kali Linux, foi digitado o comando apresentado na Figura 35 que clona o Wifipumpkin3 proveniente do repositório

git clone https://github.com/P0cL4bs/Wifipumpkin3

Figura 35: *Print* do comando (10).

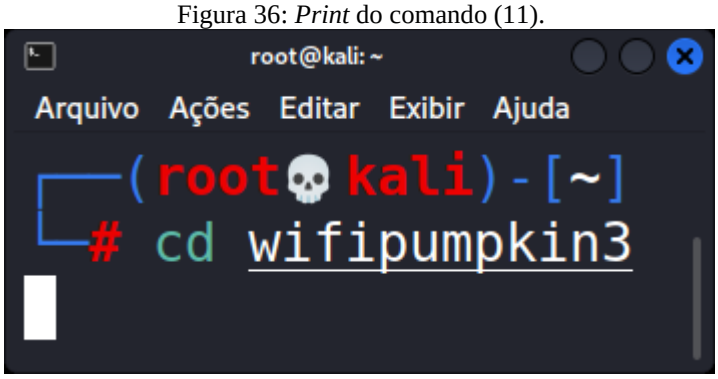


Fonte: Elaborado pelo autor.

(2) Usando o Terminal, abra a pasta Wifipumpkin3 utilizando o comando 11.

cd Wifipumpkin3 (11)

Figura 36: *Print* do comando (11).

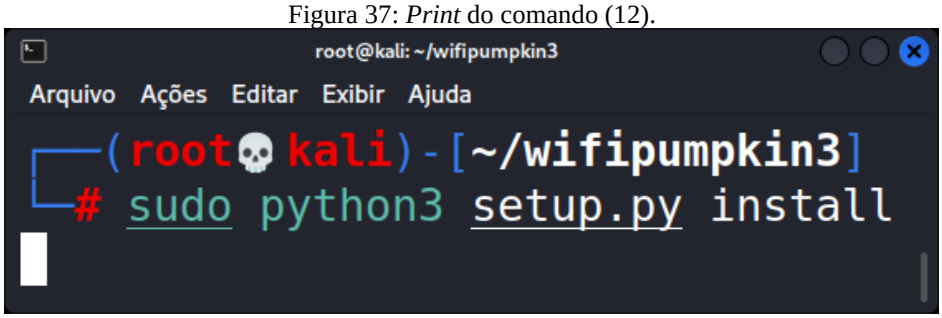


Fonte: Elaborado pelo autor.

(3) Instalar o arquivo setup.py usando o seguinte comando:

sudo python3 setup.py install (12)

Figura 37: *Print* do comando (12).



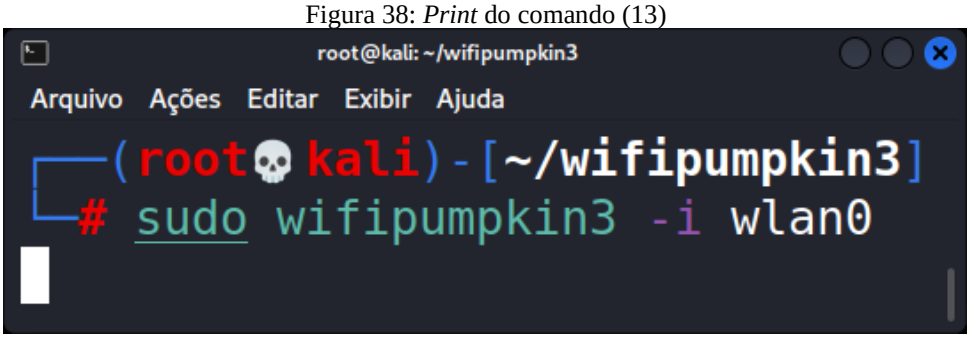
Fonte: Elaborado pelo autor.

(4) Assim que tiver instalado com sucesso o arquivo setup.py. Digite o comando abaixo para iniciar o Wifipumpkin3:

sudo Wifipumpkin3 -i <interface_name> // *interface* deve estar no modo gerenciado. No meu caso, o wlan0 está no modo gerenciado.

sudo Wifipumpkin3 -i wlan0 (13)

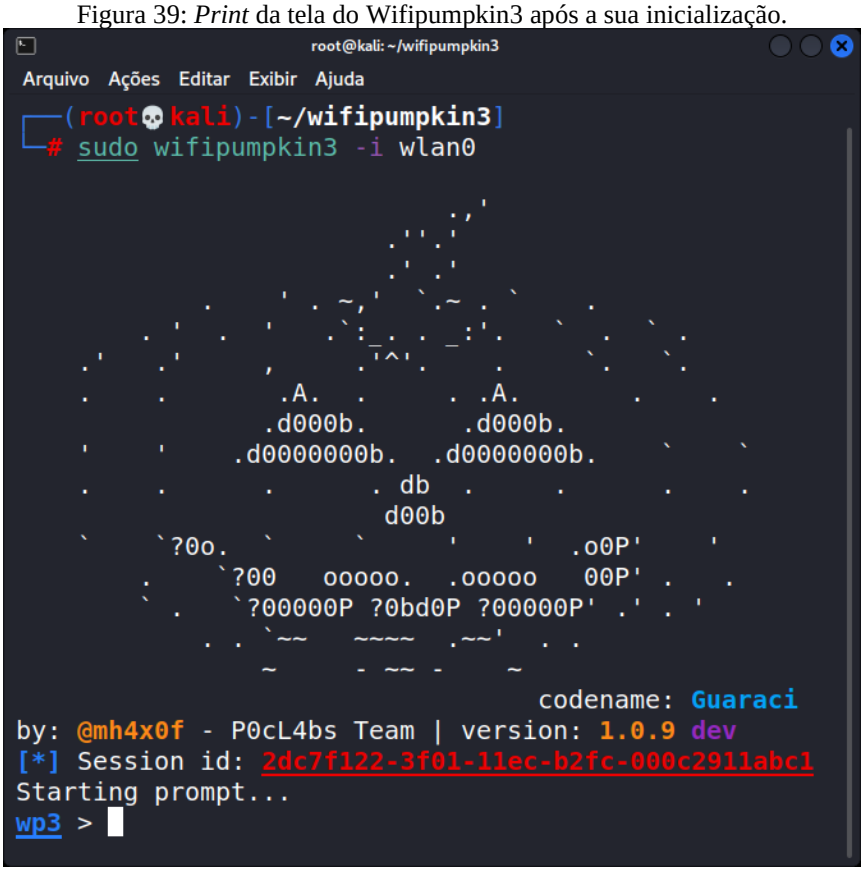
Figura 38: *Print* do comando (13)



Fonte: Elaborado pelo autor.

(5) Assim que o programa inicializar com conforme a figura 31 a instalação foi feita com sucesso.

Figura 39: *Print* da tela do Wifipumpkin3 após a sua inicialização.



Fonte: Elaborado pelo autor.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR

Av. Universitária, 1069 ● Setor Universitário
Caixa Postal 86 ● CEP 74605-010
Goiânia ● Goiás ● Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br ● reitoria@pucgoias.edu.br

RESOLUÇÃO n° 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O(A) estudante João Alves Da Silva Neto
do Curso de Ciencia Da Computação, matrícula 2013290280040-7,
telefone: 62 99686-8099 e-mail joaoauvs@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado Segurança em Redes Wireless IEEE 802.11 e Suas Vulnerabilidades, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 15 de Dezembro de 2021.

Assinatura do(s) autor(es): João Alves Da Silva Neto

Nome completo do autor: João Alves Da Silva Neto

Assinatura do professor-orientador: _____

Nome completo do professor-orientador: _____