**UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ**
**DEPARTAMENTO ACADÊMICO DE INFORMÁTICA**
**BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO**

**CONRADO LEITE STELLA**

# ANÁLISE DA SEGURANÇA DE REDES SEM FIO UTILIZANDO PENTEST

**TRABALHO DE CONCLUSÃO DE CURSO**

**PONTA GROSSA**

**2020**

**CONRADO LEITE STELLA**

# ANÁLISE DA SEGURANÇA DE REDES SEM FIO UTILIZANDO PENTEST

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de Bacharel em Ciência da Computação, do Departamento Acadêmico de Informática, da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Augusto Foronda

**PONTA GROSSA**

**2020**

Ministério da Educação
**Universidade Tecnológica Federal do Paraná**
Campus Ponta Grossa

Diretoria de Graduação e Educação Profissional
Departamento Acadêmico de Informática
Bacharelado em Ciência da Computação

# TERMO DE APROVAÇÃO

ANÁLISE DA SEGURANÇA DE REDES SEM FIO UTILIZANDO PENTEST

por

CONRADO LEITE STELLA

Este Trabalho de Conclusão de Curso (TCC) foi apresentado em 12 de Outubro de 2020. Como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação. O candidato foi arguido(a) pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Augusto Foronda
Orientador

_____
Prof. MSc. Geraldo Ranthum
Membro titular

_____
Prof. Dr. Richard Duarte Ribeiro
Membro titular

_____
Prof. MSc. Geraldo Ranthum
Responsável pelo Trabalho de Conclusão de Curso

_____
Profa. Dra. Mauren Louise Sguario
Coordenadora do curso

## AGRADECIMENTOS

Ao meu professor orientador, Prof. Dr. Augusto Foronda, pelo suporte, incentivo, correções e toda orientação dada.

A minha família pelo pela cobrança, apoio incondicional, amor e pela oportunidade de receber todos os meus anos de estudo.

E a todos os meus amigos e colegas que me ajudaram, direta ou indiretamente, nessa parte da minha formação. Muito obrigado.

# RESUMO

STELLA, Conrado. **Análise da Segurança de Redes Sem Fio Utilizando Pentest.** 2020. 41 p. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) - Universidade Tecnológica Federal do Paraná. Ponta Grossa, 2020.

A segurança da informação é fundamental para o funcionamento de empresas e corporações de todos os tamanhos. Realizar uma atualização nos meios de segurança de redes sem fio tem se tornado cada vez mais comum, pelo fato de que novas ameaças têm surgido frequentemente na busca da obtenção de informações protegidas. Há alguns anos, um novo profissional surgiu, o *hacker* ético, com o objetivo de realizar testes de segurança. Esse profissional tenta invadir a própria rede a fim de testar seus níveis de segurança, encontrar as falhas e corrigi-las. O pentest é muitas vezes o meio utilizado por este profissional para encontrar essas vulnerabilidades. Este trabalho teve como objetivo realizar uma análise dos principais problemas de segurança encontrados nos protocolos WEP, WPA e WPA2 através da realização do pentest em rede sem fio, com a ajuda das ferramentas contidas no sistema operacional Kali Linux. E assim, testar os mecanismos de proteção das redes sem fio já existentes em uma rede real. Por fim, realizar uma análise com os resultados obtidos para mostrar as vantagens e desvantagens dos métodos testados.

**Palavras-chave:** Pentest. Redes sem fio. Segurança da Informação. Kali Linux.

## ABSTRACT

STELLA, Conrado. **Security Analysis on Wireless Networks Using Pentest**. 2020. 41 p. Work of Conclusion Course (Graduation in Computer Science) - Federal Technology University – Paraná. Ponta Grossa, 2020.

Information security is critical to the operation of businesses and corporations of all sizes. Performing a security update on wireless networks has become increasingly common, as new threats have often emerged in the pursuit of obtaining protected information. Recently a new professional has emerged, the ethical hacker, aiming to in order to perform security testing. These professional attempts to break into the network itself to test its security levels find flaws and correct them. Pentest is often the means used by this professional to find these vulnerabilities. This paper aims to analyze the main security issues in WEP, WPA and WPA2 wireless pentest, using the intrusion tools contained in the operating system. Kali Linux. Therefore, test the protection mechanisms of existing wireless networks in a real network. Finally, perform an analysis with the results obtained to show the advantages and disadvantages of the tested methods.



**Keywords:** Pentest. Wireless Networks. Information Security. Kali Linux.

# LISTA DE ILUSTRAÇÕES

## LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

| | |
|---|---|
| AES | *Advanced Encryption Standard* |
| ARP | *Address Resolution Protocol* |
| CCMP | *Counter Mode Cipher Block Chaining Message Authentication Code Protocol* |
| CNSS | Comitê de Sistemas de Segurança Nacional |
| CPU | *Central Processing Unit* |
| CRC | *Cyclic Redundancy Check* |
| DDDS | *Direct-sequence spread spectrum* |
| DDoS | *Distributed Denial of Service* |
| DoS | *Denial of Service* |
| FMS | Fluhrer, Mantin, *and* Shamir |
| GHz | Giga-Hertz |
| GPU | Graphics Processing Unit |
| HTTPS | *Hyper Text Transfer Protocol Secure* |
| IEEE | Instituto de Engenheiros Eletricistas e Eletrônicos |
| LAN | *Local Area Network* |
| MAC | *Media Access Control* |
| MB | MegaBytes |
| Mbps | Megabit por segundo |
| MHz | Mega-Hertz |
| MIMO | *Multiple-input Multiple-output* |
| MK | *Master Key* |
| OFDM | *Orthogonal Frequency Division Multiplexing* |
| OSI | *Open System Interconnection* |
| PE | *Password Element* |
| PIN | *Personal Identification Number* |
| PMK | *Pairwise Master Key* |
| PTK | *Pairwise Transient Key* |
| RC4 | *Rivest Chipher 4* |

| | |
|---|---|
| SAE | *Simultaneous Authentication of Equals* |
| SSID | *Service Set Identifier* |
| SSL | *Secure Sockets Layer* |
| TKIP | *Temporal Key Integrity Protocol* |
| TLS | *Transport Layer Security* |
| WEP | *Wired Equivalent Privacy* |
| WPA | *Wi-Fi Protected Access* |
| WPA-PSK | *WPA-Pre-Shared Key* |
| WPA2 | *Wi-Fi Protected Access 2* |
| WPA3 | *Wi-Fi Protected Access 3* |
| WPS | *Wireless Protected Setup* |

**SUMÁRIO**

# 1 INTRODUÇÃO

Redes sem fio são populares em muitas organizações por sua facilidade de uso e flexibilidade, entretanto, elas apresentam algumas vulnerabilidades, tal como a facilidade do acesso físico a rede, que, antes das redes sem fio não era muito relevante, e ainda alguns novos tipos de ataques passaram a existir, devido a essa fragilidade conhecida nas redes sem fio (WHITEWAKER; NEWMAN, 2005).

Para combater as vulnerabilidades das redes sem fio, alguns métodos foram criados inicialmente, como *Service Set Identifier* (SSID), *Wired Equivalent Privacy* (WEP) (BONCELLA, 2002), sendo este último um protocolo de segurança.

Após o crescimento da popularidade das redes sem fio, falhas foram descobertas no WEP, pois seu método de segurança, baseado em criptografia de mensagem, pode ser quebrado facilmente com simples ataques de repetição de pacotes, por exemplo. Mesmo com outros algoritmos de segurança sendo implementados nos pontos de acesso sem fio, como *Wi-Fi Protected Access* (WPA), muitos problemas ainda persistem. Os invasores continuam tentando burlar esses sistemas de segurança, fazendo com que somente o uso da tecnologia não seja suficiente para uma proteção adequada (NAKAMURA; GEUS, 2010).

Pentest, uma abreviação de *Penetration Test*, ou em português, teste de penetração, é uma bateria de testes metodológicos, normalmente aplicado em redes de computadores, que tem como objetivo descobrir, mapear e expor todas as possíveis vulnerabilidades de uma rede (MORENO, 2015). Com a realização desse teste, procura-se melhorar a segurança na rede como um todo. Isso torna o pentest de grande importância para a segurança de uma rede sem fio, pois através da realização do pentest é possível descobrir falhas inerentes à rede testada.

Uma vez que o ambiente da segurança da informação é marcado pela evolução contínua, onde novos tipos de ataques resultam em novos métodos de proteção, levando a evolução dos tipos de ataque, que assim formam um ciclo (NAKAMURA; GEUS, 2010).

Deste modo, o presente trabalho visa realizar, além do pentest em rede sem fio para redes com protocolos WEP, WPA e WPA2, com utilização das ferramentas de invasão, realizar também uma análise de segurança com o resultado do pentest aplicado em uma rede real, procurando expor as brechas de segurança nas redes sem fio mais atuais, e tentar propor soluções de segurança mais eficientes, e assim, contribuir para a

criação de redes que venham a utilizar esses protocolos de segurança para serem mais seguras.

## 1.1 OBJETIVOS

O presente trabalho define os objetivos como objetivos gerais, estabelecidos na sessão 1.1.1 e objetivos específicos, na sessão 1.1.2.

### 1.1.1 Objetivo Geral

Este trabalho tem como objetivo geral analisar os problemas de segurança em redes sem fio, encontrados através da aplicação do pentest nos protocolos WEP, WPA e WPA2.

### 1.1.2 Objetivos Específicos

Para alcançar o objetivo geral, foram definidos os seguintes objetivos específicos:

- Analisar as principais vulnerabilidades de redes sem fio, comumente encontradas e citadas na literatura;
- Analisar as ferramentas de invasão de redes sem fio, contidas no sistema operacional *Kali Linux*, na sua versão mais recente, como *aircrack-ng* e *wireshark*;
- Analisar os mecanismos de proteção de redes sem fio através da literatura;
- Definir topologia de teste da rede sem fio, nos protocolos WEP, WPA e WPA2, com as ferramentas de invasão e proteção pesquisadas;
- Realizar uma análise dos resultados.

## 1.2 JUSTIFICATIVA

Em uma rede sem fio, a segurança da informação é um quesito muito importante, e este ambiente digital está sempre em evolução, ou seja, novos métodos de invasão continuam aparecendo. Portanto, é fundamental analisar esses novos tipos de invasão e como as redes se comportam a esses ataques, utilizando as ferramentas e métodos mais atuais, com objetivo de melhorar e atualizar seu nível de segurança.

## 1.3 ORGANIZAÇÃO DO TRABALHO

Este trabalho divide-se em cinco capítulos. O capítulo 2 aborda sobre o referencial teórico, com os conceitos e técnicas referentes a segurança de redes sem fio, a teoria e aplicação do pentest, bem como trabalhos relacionados.

O capítulo 3 mostra o desenvolvimento dos mais conhecidos métodos de invasão nos protocolos WEP, WPA e WPA2 para efeito de demonstração de um ataque em uma rede real e possibilidade de comparação entre tipos de ataques.

No capítulo 4, os resultados dos testes realizados no capítulo 3 são avaliados e explicados. Assim como a comparação com ataques equivalentes nos mesmos protocolos. Mostrando uma análise atual e detalhada dos pontos fortes e pontos fracos da utilização dos protocolos WEP, WPA, WPA2 e WPA3 nos dias de hoje.

Por fim, o capítulo 5 relata a conclusão dos esforços empregados nesse trabalho, mostrando, resumidamente, o cenário atual dos protocolos abordados, e indicando possíveis trabalhos futuros para continuação do mesmo. Em seguida estão as referências utilizadas no estudo.

# 2 REFERENCIAL TEÓRICO

Neste capítulo são apresentados os conceitos básicos para a compreensão do trabalho e está divido da seguinte forma: Na sessão 2.1 será apresentado a concepção sobre segurança da informação, assim como as ameaças, vulnerabilidades e os ataques em redes sem fio. A sessão 2.2 abordará alguns padrões 802.11 do *Institute of Electrical and Electronics Engineers* (IEEE) e suas evoluções. A sessão 2.3 apresentará os principais protocolos de segurança utilizados por esses padrões, bem como suas vulnerabilidades e alguns ataques por eles sofrido. A sessão 2.4 irá abordar o conceito de pentest, sua teoria, o ambiente para realização do teste e as principais ferramentas utilizadas.

## 2.1 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é fundamental para uma empresa. Com o objetivo de proteger a confidencialidade, integridade e a disponibilidade dos meios de informação, em qualquer que seja o seu uso, armazenamento, processamento ou transmissão, são aplicados: políticas, educação, treino com consistência e também da tecnologia (WHITMAN; MATTORD, 2011).

O Comitê de Sistemas de Segurança Nacional (CNSS), uma organização intergovernamental norte-americana, responsável por definir políticas para segurança de sistemas nos Estados Unidos, define segurança da informação como a proteção da informação e seus elementos críticos, incluindo os sistemas e equipamentos que utilizam, guardam e transmitem as informações.

A rede, seja em ambientes coorporativos ou em ambientes domésticos, é uma das formas mais utilizadas para compartilhar informações, trazendo flexibilidade e facilidade, resultando em maior produtividade e novas possibilidades dentro de uma organização. Sendo assim, uma estrutura de rede é essencial para corporações de todos os tamanhos, logo, esta rede precisa ser confiável e para que isso ocorra, ela precisa ser protegida corretamente. Isso significa que a informação deve chegar de forma integra a todos os usuários desta rede.

### 2.1.1 Ameaças e Vulnerabilidades

Novas vulnerabilidades são encontradas ao longo do tempo. Como por exemplo as redes sem fio, ao mesmo tempo que trouxeram muitas facilidades para seus usuários, abriram brechas de segurança. Novas preocupações apareceram, tal como o acesso físico a rede, que, antes das redes sem fio não era muito relevante. A medida que aumenta a vulnerabilidade da segurança da informação, aumenta também o risco das ameaças (NAKAMURA; GEUS, 2010).

O cenário de redes sem fio já é uma realidade nas instituições e empresas, devido, em grande parte, a facilidade e praticidade na hora de implementação e utilização desse tipo de tecnologia, mas por outro lado, como citado anteriormente, essas redes trazem novas vulnerabilidades, e novas vulnerabilidades exigem novas medidas de segurança, que serão abordados a seguir.

### 2.1.2 Ataques a Redes Sem Fio

Como o armazenamento de informação é um recurso fundamental para organizações, pessoas maliciosas tentam obter acesso a este tipo de informação. Estas pessoas que tentam explorar essas vulnerabilidades dos sistemas de segurança são conhecidas como *hackers*, se aproveitam de brechas conhecidas e buscam também novos meios de invadir os sistemas para manipular as informações.

Embora vários tipos de ataques já sejam conhecidos, muitos sistemas ainda não estão preparados para ataques em potencial, por isso, os *hackers* continuam suas investidas com intuito de invadir um sistema. Dentre os ataques nas redes sem fio, os mais comuns são:

- *Evil Twin*, conhecido também como associação maliciosa, é um ataque do tipo *Man in the Middle* (homem no meio), caracterizado pela tentativa de obter as credenciais de acesso à rede da vítima através da cópia do ponto de acesso. Enquanto a vítima acredita estar conectando na própria rede, ela envia os pacotes de procura do ponto de acesso, o atacante responde, se passando pelo ponto de acesso. Quando a vítima informa as credenciais de entrada na rede, o invasor obtém essa informação e assim consegue entrar na rede alvo.
- *Denial of Service* (DOS) ou negação de serviços, é um ataque que tem como objetivo comprometer a disponibilidade do sistema através do impedimento do

uso dos recursos pelo usuário legítimo e não obrigatoriamente um ataque para conseguir informações. Uma variação deste tipo de ataque é o *Distributed Denial of Service* (DDoS) ou negação de serviços distribuído. Este necessita de uma rede de computadores que possam ser controlados pelo atacante, geralmente computadores infectados. Utilizando mais computadores a efetividade do ataque é multiplicada, com objetivo de causar uma sobrecarga no sistema da vítima, e assim causar a indisponibilidade de serviços.

- O *MAC Spoofing*, ou falsificação do MAC, é uma técnica que tem como alvo usuários cuja rede utiliza lista de acesso baseada no endereço MAC, fazendo que, somente os endereços contidos na lista ganhem acesso à rede sem fio. Neste tipo de ataque, o invasor tenta capturar um endereço válido contido na lista, trocar seu endereço para o obtido e assim conseguir acesso à rede (BONCELLA, 2002).
- *WiFi Sniffers,* é o tipo de ataque em que todos os pacotes possíveis são observados pelo atacante. Nesse tipo de abordagem, o invasor fica ao alcance do ponto de acesso para receber todos os pacotes transmitidos pelo ponto, até mesmo os que não são endereçados a ele. Com esses pacotes capturados, é possível ler os dados, modificá-los e até retransmitir esses pacotes modificados em algumas situações. Existem métodos que criptografam esses pacotes, a fim de proteger os mesmos, como servidores que usam protocolo *HTTPS*. Neste caso os pacotes são protegidos pelas criptografias *SSL* e *TLS*, mas isto não impede, necessariamente, que eles possam ser lidos e modificados.

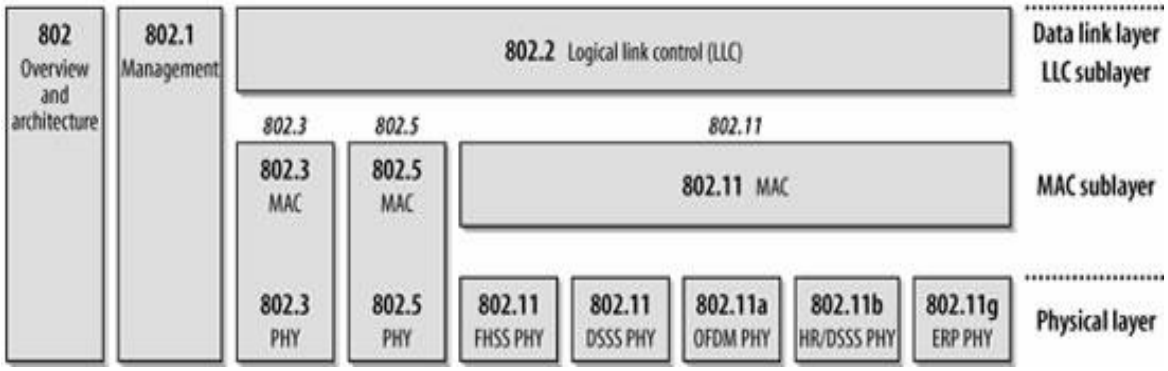
## 2.2 PADRÕES IEEE 802.11

As especificações do modelo 802 do *Institute of Electrical and Electronics Engineers* (IEEE), ou Instituto de Engenheiros Eletricistas e Eletrônicos, tem seu foco nas duas camadas mais baixas do modelo OSI, incorporando as camadas física e de enlace de dados, como mostra a Figura 01, embora esta não demonstre os mais atuais padrões da IEEE, já serve para exemplificar o foco do padrão no modelo OSI.

As especificações individuais da série 802 são identificadas por um segundo número, como por exemplo 802.5, que é uma especificação para o protocolo *Token Ring* (GAST, 2005). No caso do 802.11, publicada em 1997 na sua versão inicial, define

uma série de padrões de transmissões e codificações para comunicações sem fio. Trabalhava apenas na frequência 2,4GHz, e surgiu para atender as necessidades de redes domesticas e corporativas, como possuía uma taxa de transferência máxima de apenas 2 Mbps, logo surgiu uma necessidade de padrões com velocidade maior, como resultado, surgiram várias extensões do padrão 802.11.

**Figura 1 – Relação do padrão IEEE 802.11 e o modelo OSI**




**Fonte: 802.11 Wireless Networks: The Definitive Guide**

### 2.2.1 802.11a

A alteração da versão de padrão 802.11a, em relação versão original 802.11 foi retificada em 1999. Entre as principais alterações estavam a banda de frequência de operação do padrão, ao invés de utilizar a largura de banda de 2,4GHz, como no seu antecedente, o padrão 802.11a passou a utilizar 5GHz como frequência de sua operação. Outra grande mudança foi a velocidade, ao adotar a técnica de codificação OFDM (*Orthogonal Frequency Division Multiplexing*), utilizando cinquenta e duas sub-bandas, chega a uma velocidade de transmissão total de 54Mbps (LAMICHHANE, 2016).

O padrão 802.11a foi aprovado rapidamente nos Estados Unidos e no Japão, mas em outras regiões, como na União Europeia, sua aprovação foi mais demorada devido aos órgãos regulamentadores dessas regiões, causando uma menor popularidade do padrão 802.11a, uma vez que o padrão 802.11b já estava sendo utilizado em mais regiões, mesmo sendo projetado depois do 802.11a, o 802.11b foi implementado em massa antes, aumentando assim, o número de usuários (LAMICHHANE, 2016).

### 2.2.2 802.11b

Aprovado em julho de 1999, o padrão 802.11b contava com uma largura de banda de 22MHz e atuava na frequência de 2,4GHz, gerando alguns problemas por conta da interferência causada nesta faixa de sinal. Porém, este padrão ficou conhecido pela sua compatibilidade, tornando-se um padrão muito popular.

Utiliza um método de controle de comunicação igual ao do padrão 802.11 e conta com um alcance médio de sinal de trinta metros. Sua velocidade era inferior, se comparado ao padrão 802.11a, podendo alcançar, em média, 11Mbps de transmissão. Um dos fatores causadores desta velocidade relativamente baixa é o fato de que o padrão 802.11b utiliza a técnica DSSS (*Direct-sequence spread spectrum*), ou em português, sequência direta de espalhamento de espectro, para fazer a modulação da onda de sinal, porém, este tipo de modulação tem um envio de informações redundante, causando um pequeno desperdício de espectro na frequência da largura de banda.

### 2.2.3 802.11g

O terceiro padrão publicado foi o 802.11g, em junho de 2003. Assim como o padrão 802.11b, utiliza a frequência de 2,4GHz, mas tem uma velocidade de transmissão superior, chegando a 54Mbps, para isso, o padrão 802.11g utiliza tanto a modulação DSSS, vista no 802.11b, quando a OFDM, vista no padrão 802.11a, e ainda pode utilizar as duas combinadas, tornando assim, este padrão, um dos mais completos da família de padrões 802.11.

### 2.2.4 802.11n

O padrão 802.11n, lançado em outubro de 2009, veio com a novidade das antenas *multiple-input multiple-output* (MIMO), o que possibilitou que a transmissão de dados chegasse a uma velocidade máxima de 600Mbps. A taxa de transferência deste padrão teve um aumento significativo em relação aos outros padrões publicados até então, o 802.11n mostrou um grande avanço para a rede de comunicação sem fio.

### 2.2.5 802.11ac

O lançamento do padrão 802.11ac aconteceu em dezembro de 2013. Este padrão atua na frequência de 5GHz, o que resulta em um alcance de sinal menor, porém, pode trabalhar com menos interferências do que na frequência de 2,4GHz, utilizada por outros padrões. Tem um potencial de velocidade de 1.300Mpbs e tem uma largura de banda de até 160MHz. Assim como o 802.11n, o 802.11ac utiliza antenas MIMO e modulação OFDM, este padrão é compatível com todos os padrões da 802.11 da IEEE lançados antes dele.

## 2.3 PROTOCOLOS DE SEGURANÇA EM REDES SEM FIO

Redes sem fio têm diversas vantagens em relação a redes cabeadas, como por exemplo, a facilidade de implementação e uso, mas também existem desvantagens. As redes sem fio são mais vulneráveis para potenciais invasores. Tentando combater uma entrada não permitida na rede, os padrões 802.11 da IEEE são implementados com protocolos responsáveis pela segurança da rede. Nesta seção serão abordados os principais protocolos de segurança utilizados nos padrões de rede 802.11.

### 2.3.1 Protocolo WEP

O protocolo WEP (*Wired Equivalent Privacy*), é descrito no padrão 802.11 da IEEE. No início das redes sem fio, acreditava-se que o protocolo WEP era resistente a ataques de invasores, mas com a crescente popularidade do meio de comunicação sem fio, vários analistas e pesquisadores encontraram diversas falhas no projeto do protocolo original, mas, como era a única solução de segurança até o momento, era mais eficiente do que uma rede aberta (VIBHUTI, 2005).

A segurança do protocolo WEP é composta por duas fases, a fase de autenticação e a fase de criptografia. A autenticação é usada quando um novo dispositivo tenta acessar a LAN, *Local Area Network,* ou em português, rede local, pela primeira vez, este processo pode ser realizado de dois modos, o de sistema aberto, no qual o cliente consegue entrar na rede sem credenciais, e o sistema de chave compartilhada.

No processo de autenticação do protocolo WEP por chave compartilhada, o dispositivo que tenta se conectar envia um requerimento ao ponto de acesso, então, o ponto de acesso responde, enviando o que na literatura é chamado de "*challenge",* o desafio é uma série de números aleatórios sem criptografia, então o dispositivo deve responder ao desafio, enviando uma resposta com este número criptografado de acordo com a chave compartilhada. O ponto de acesso realiza a descriptografação, se as chaves se coincidirem, o acesso à rede é liberado e o cliente é informado. Na fase de criptografia, o protocolo WEP utiliza o algoritmo RC4 (*Rivest Chipher 4*) para fazer a criptografia e o método de detecção de erros CRC (*Cyclic Redundancy Check*) para garantir a integridade.

Alguns ataques exploram as vulnerabilidades do RC4, como por exemplo, conforme (Tews, 2007):

- *Packet Injection,* é o termo dado ao ataque em que o invasor captura um pacote em uma rede WEP, para depois reenviar este mesmo pacote, e ele ainda será aceito pela rede. O protocolo WEP não tem nenhum mecanismo de defesa contra este tipo de ataque, uma vez que o invasor intercepte um pacote, este pode ser injetado novamente na rede, desde que a senha não seja alterada e a estação que enviou o pacote originalmente ainda esteja conectada na rede. Caso a estação que tenha enviado não esteja mais na rede, o endereço pode ser alterado, uma vez que estes campos de cabeçalho não estão protegidos pelo IPV (*Integrity protection value*), um método de garantir a integridade dos pacotes no protocolo WEP.
- No ataque de Autenticação Falsa, o invasor consegue entrar na rede protegida por WEP que suporta o método de autenticação de sistema aberto, sem conhecer a senha compartilhada. E também consegue acessar a rede que utiliza autenticação por chave compartilhada, caso consiga capturar completamente esta chave entre a estação e o ponto de acesso. Quando um cliente realiza a conexão, o atacante tenta capturar este pacote, e como alguns bits enviados pelo protocolo WEP são constantes e já conhecidos pelo atacante, o desafio é transmitido em um *frame* (pedaço da mensagem) e não é criptografado, logo, também é conhecido pelo invasor. Assim este consegue encontrar a chave de compartilhamento, que está em outro *frame.* Deste modo, o invasor inicia o processo de autenticação com

o ponto de acesso, recebendo um desafio, então, o atacante constrói um *frame* utilizando a chave de compartilhamento recuperada, conseguindo assim a autenticação pelo ponto de acesso.

Vários ataques utilizam da simplicidade do algoritmo RC4 para conseguir um acesso, usando modelos matemáticos. Ainda de acordo com Tews (2007), os mais conhecidos são, o ataque FMS (Fluhrer, Mantin *and* Shamir), que, em 2001, definiram, teoricamente, um modelo matemático capaz de realizar uma descoberta da senha, testado em uma simulação, conseguindo uma taxa de 50% de sucesso e com pequeno custo computacional. Após o FMS, outros ataques vieram, alguns derivados dele, como por exemplo o ataque *KoreK,* que obteve um sucesso muito maior e com menor tempo computacional.

O ataque PTW (Pyshkin, Tews, Weinmann) se mostrou ainda mais eficiente ao invadir o protocolo WEP. Enquanto o ataque *KoreK* demorava em torno de 10 minutos para descobrir a senha, em alguns casos, dependendo da qualidade de sinal, o ataque PTW conseguia em menos de 60 segundos, provando que o protocolo WEP mostrava várias falhas de projeto, assim, a IEEE começou a desenvolver novos protocolos de segurança para seus padrões.

### 2.3.2 Protocolo WPA

O protocolo WPA (*Wi-Fi Protected Access*), introduzido em 2003 pela Wi-Fi Alliance, foi criado com objetivo de substituir o protocolo WEP como uma solução rápida, devido as suas vulnerabilidades já conhecidas.

O método de criptografia que o protocolo WPA usa é o *Temporal Key Integrity Protocol (TKIP).* Embora o TKIP também use o algoritmo RC4, assim como o protocolo WEP, ele conta com algumas importantes melhorias, como por exemplo, uma mudança dinâmica de chaves compartilhadas durante a comunicação e também um IV (*Initialization Vetor*), ou vetor de inicialização, de 48 bits, muito maior do que o encontrado no protocolo WEP. Uma função para embaralhar as chaves é usada para cada sessão. E, para garantir a integridade dos dados das mensagens, um novo algoritmo, chamado Michael, foi utilizado (KUMKAR et al., 2012).

Para a autenticação, o WPA apresentou algumas novas soluções. O *WPA-Pre-Shared Key* (WPA-PSK) ou *WPA-Personal,* é uma chave estática, criada para iniciar a comunicação entre dois usuários. Chamada de chave mestra de emparelhamento,

*Pairwise Master Key* (PMK), deve estar pronta no TKIP antes da associação ser feita. Esta autenticação é indicada para pequenas redes, como redes domésticas ou pequenos escritórios, e utiliza uma chave de 256 *bits* para criptografia. E o WPA-Enterprise, criado para grandes redes, provém um método de autenticação mais robusto, utilizando as definições 802.1x, um padrão de autenticação para acesso a portas de rede, e o EAP (*Extensible Authentication Protocol*), que é um protocolo para autenticação em um servidor específico.

Em relação aos problemas encontrados no protocolo WEP, o protocolo WPA teve excelentes resultados, apenas com uma atualização de software. Este protocolo corrigiu a maioria das falhas de segurança conhecidas ou ignoradas pelo WEP.

Os ataques mais comuns ao protocolo WPA se devem a vulnerabilidades da criptografia TKIP. Alguns desses ataques são descritos por Vanhoef e Piessens (2013), como o ataque *Denial of Service* (DoS), em que partes do cabeçalho dos pacotes são alterados propositalmente para causar erro no algoritmo de integridade, com esses erros o ponto de acesso desliga todo os tráfegos do TKIP por 1 minuto, repetindo esse processo o DoS é causado. Outro tipo de ataque possível é o *Portscan*, ou em português, varredura de portas, este ataque procura injetar pacotes em todas as portas dos clientes no ponto de acesso. O último ataque citado tem como objetivo dar um *reset* no algoritmo Michael, causando inconsistência no seu funcionamento.

### 2.3.3 Protocolo WPA2

O protocolo WPA2 (*Wi-Fi Protected Access 2*), retificado em 2004 como uma melhoria do protocolo WPA, devido as vulnerabilidades encontradas no mesmo. A principal mudança em relação a sua versão anterior foi a utilização do algoritmo de criptografia AES (*Advanced Encryption Standard*), embora o TKIP ainda continuasse disponível. Embora o algoritmo AES fosse muito mais eficiente, ele exigia um processamento maior, e não era compatível com todos os *hardwares* de ponto de acesso sem fio, era necessário trocar o equipamento.

A segurança da comunicação é estabelecida em quatro partes no protocolo WPA2, segundo Arana (2006). Na primeira parte, tanto cliente quanto o ponto de acesso entram em acordo sobre as políticas de segurança, incluindo método de autenticação, protocolos de tráfego, entre outros. Na segunda fase, aplicado apenas no modo *Enterprise*, a autenticação é iniciada entre o ponto de acesso e o cliente, gerando uma

MK (*Master Key*). Na terceira fase, após o sucesso da autenticação, chaves temporárias são criadas e renovadas regularmente. Por fim, na quarta fase, todas as chaves geradas no passo anterior são usadas pelo CCMP (*Counter Mode Cipher Block Chaining Message Authentication Code Protocol*), em português, Protocolo de Código de Autenticação de Mensagens em Cadeia de Blocos de Cifra no Modo Contador, protocolo este, que faz uso do AES para prover a confidencialidade e integridade dos dados transmitidos.

Entre os principais benefícios do WPA2, junto com o WPA, foi a resolução das vulnerabilidades do protocolo WEP. Um algoritmo de criptografia mais eficiente do que o WPA utiliza, e ainda melhorias aos clientes do ponto de acesso, como um método de reconexão de clientes e um suporte a pré-autenticação, permitindo que o cliente continue conectado enquanto ele se afasta do ponto de acesso.

Durante o *handshake*, processo de “aperto de mãos”, que é o método de reconhecimento entre cliente e ponto de acesso, cada estação precisa de uma chave chamada *Pairwise Transient Key* (PTK) para proteger esta comunicação individual. Esta chave é derivada da PMK (*Pairwise Master Key*), uma *string* fixa, derivada da concatenação da senha, do SSID, do tamanho do SSID e do número usado uma vez em cada sessão. Então, um *hash* é realizado com essa *string* 4096 vezes, gerando um valor de 256 *bit*. Quando esta *string* é capturada, um ataque do tipo *dictionary attack* se torna possível, este ataque consiste em tentar entrar no ponto de acesso utilizando todas as possibilidades encontradas no dicionário (MYLONAS et al., 2011).

Em dezembro de 2011, uma falha na segurança do WPS (*Wireless Protected Setup*), tecnologia implementada no WPA2 para facilitar a conexão do cliente no ponto de acesso, foi descoberta. O código PIN (*Personal Identification Number*) pode ser facilmente revelado através de um ataque de força bruta, e sabendo o código PIN, o invasor consegue entrar no ponto de acesso (ZISIADIS et al., 2013).

### 2.3.4 Protocolo WPA3

O protocolo WPA3 (*Wi-Fi Protected Access 3*), foi lançado em junho de 2018, sendo o sistema de segurança de redes sem fio mais atual. Criado com intuito de cobrir as falhas das suas versões prévias, o WPA3 usa o SAE (*Simultaneous Authentication of Equals*) como técnica para autenticar o cliente no ponto de acesso. O modo como é feito o *handshake* foi mudado, chamado de *dragonfly handshake,* ou somente *dragonfly,*

substitui o *handshake* de quatro etapas utilizado pelo WPA2. O *dragonfly* utiliza um PE (*password element*) ao invés de senhas para chaves computacionais, como nas versões anteriores. A PE determina um tempo de sessão, utilizando parâmetros através de cálculos matemáticos (KOHLIOS; HAYAJNEH, 2018).

Embora o protocolo WPA3 tenha conseguido resolver a maioria das vulnerabilidades encontradas no WPA2, algumas falhas ainda continuaram. Conforme Vanhoef e Ronen (2019), ao realizar os ataques, falhas foram encontradas no processo do *dragonfly handshake*, mas mesmo assim, ainda o consideram um grande avanço em relação ao WPA2.

## 2.4 PENTEST

Testes de penetração, ou pentest, são testes realizados com objetivo de descobrir falhas, aberturas, em um sistema, realizando uma auditoria completa. Esses testes são realizados por métodos padrões e seguem normas. O pentest pode ser definido em três estratégias. O Teste Caixa Preta, em que o profissional responsável pela realização do pentest não recebe nenhuma informação da rede em que o teste ocorrerá, colocando em condições reais de um possível invasor externo. O Teste Caixa Branca, várias informações sobre a rede são passadas ao aplicador, simulando um ataque interno, onde se tem conhecimento sobre a rede. E o Teste Caixa Cinza apenas algumas informações são passadas, com o objetivo de economizar tempo e analisar a efetividade do teste (FIGUEIREDO, 2015).

### 2.4.1 Kali Linux

O Kali Linux é uma distribuição do Linux, baseada em Debian, desenvolvida com o foco em realização de pentest. Lançada em março de 2012, tem como principais características um grande suporte a adaptadores de rede sem fio, *kernel* customizado para injetar pacotes, e conta com várias ferramentas já instaladas, para auxiliar no pentest (ALLEN; HERIYANTO; ALI, 2014).

Dentre as principais e mais utilizadas ferramentas do Kali Linux, para auxílio do pentest, podemos citar:

- Metasploit Framework*,* é um *framework* completo para testes de penetração e é organizado por módulos, estes módulos contém outros programas

maliciosos para realizar um ataque. O objetivo desta ferramenta é criar um ambiente completo para explorar vulnerabilidades que levam à brechas na segurança de um sistema.

- O Wireshark é o analisador de protocolos mais usado no mundo. Esta ferramenta consegue mostrar tudo que está acontecendo na rede de forma detalhada. Possui interface gráfica para melhor visualização dos dados, utilizando cores diferentes para identificar os tipos de pacotes transmitidos na rede em tempo real.
- A ferramenta Aircrack-ng conta com várias ferramentas em uma só, sendo possível realizar um monitoramento, ataques, testes em adaptadores de redes, medindo suas capacidades e ainda realiza quebra de protocolos WEP, WPA e WPA2.
- O *Network Mapper,* conhecido como Nmap é um software que realiza um escaneamento completo de portas, possui uma versão com interface gráfica e é conhecido pela sua eficiência e velocidade. Com esta ferramenta é possível encontrar portas abertas na rede alvo, permitindo assim, a realização de algum tipo de ataque.

Estes são apenas alguns exemplos de ferramentas utilizadas em um pentest. Sua utilização leva em conta fatores como, a disposição da rede, como ela está configurada, quais protocolos utiliza, e também os objetivos específicos do teste a ser realizado.

# 3 DESENVOLVIMENTO

Neste capítulo é apresentado a preparação do ambiente para realização de alguns testes práticos de invasão, em redes reais que utilizam os protocolos WEP, WPA e WPA2.

## 3.1 PREPARAÇÃO DO AMBIENTE DE TESTES

Para a realização do pentest em redes sem fio, nas redes WEP, WPA e WPA2, alguns preparos foram feitos. Primeiramente, uma máquina virtual, utilizando o *software* VMWare, com Kali Linux foi criada com a versão 5.2.0 do *kernel*, com drivers disponíveis para o adaptador externo utilizado, para este trabalho, o modelo TL-WN722N da fabricante TP-Link foi utilizado, ilustrado na Figura 02.

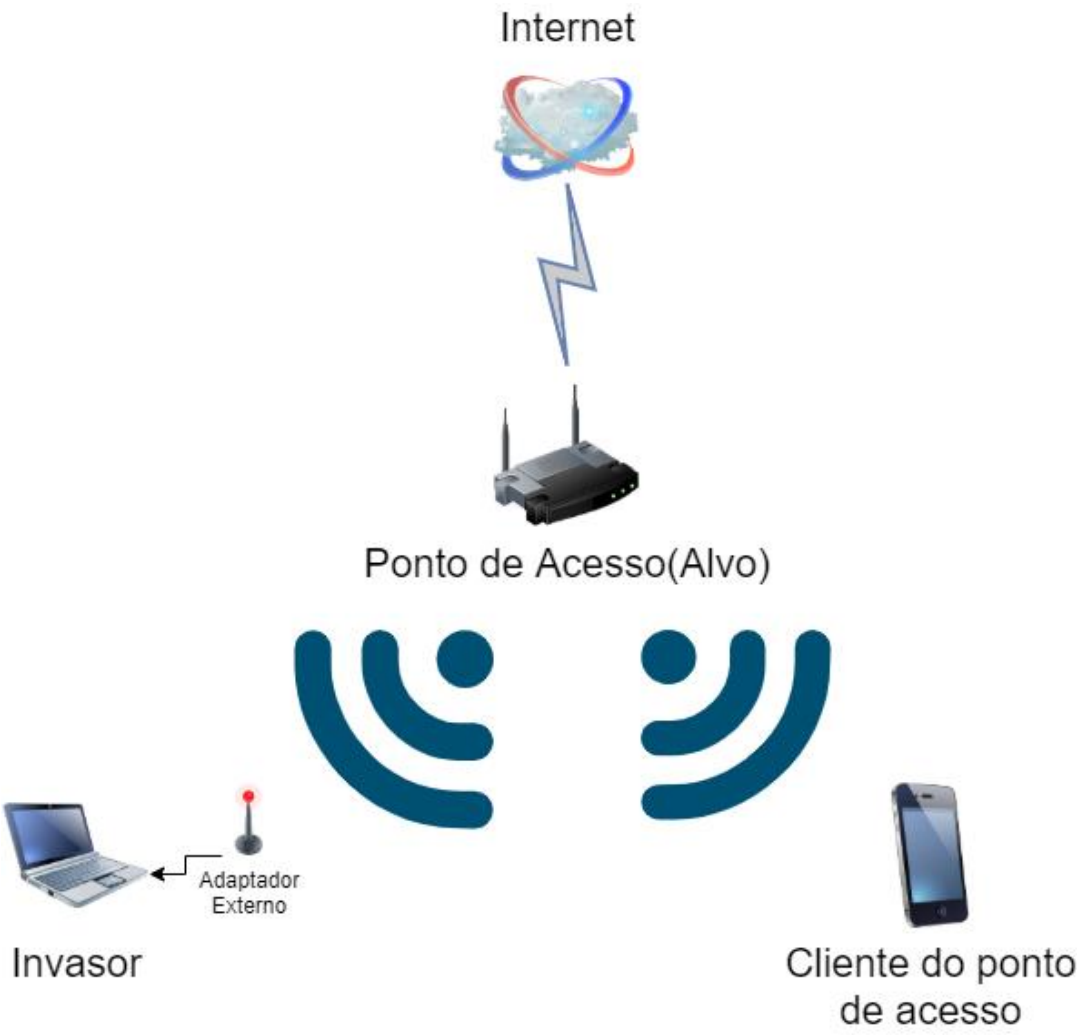
**Figura 2 – Adaptador de rede TL-WN722N**


**Fonte: TL-WN722N, 2020.**

Um resumo simplificado da topologia da rede é mostrado na Figura 03, para ajudar a entender a disponibilidade da rede de testes, onde o invasor é representado no

alcance do sinal do ponto de acesso. Também está representado um cliente já conectado do ponto de acesso, que é necessário para alguns tipos de teste.

**Figura 3 – Topologia da rede de testes**




**Fonte: Autoria própria**

Após a instalação dos drivers do adaptador externo no sistema operacional, a máquina para os testes está pronta. O primeiro teste a ser feito, é colocar o adaptador externo no modo monitor.

## 3.2 MODO MONITOR

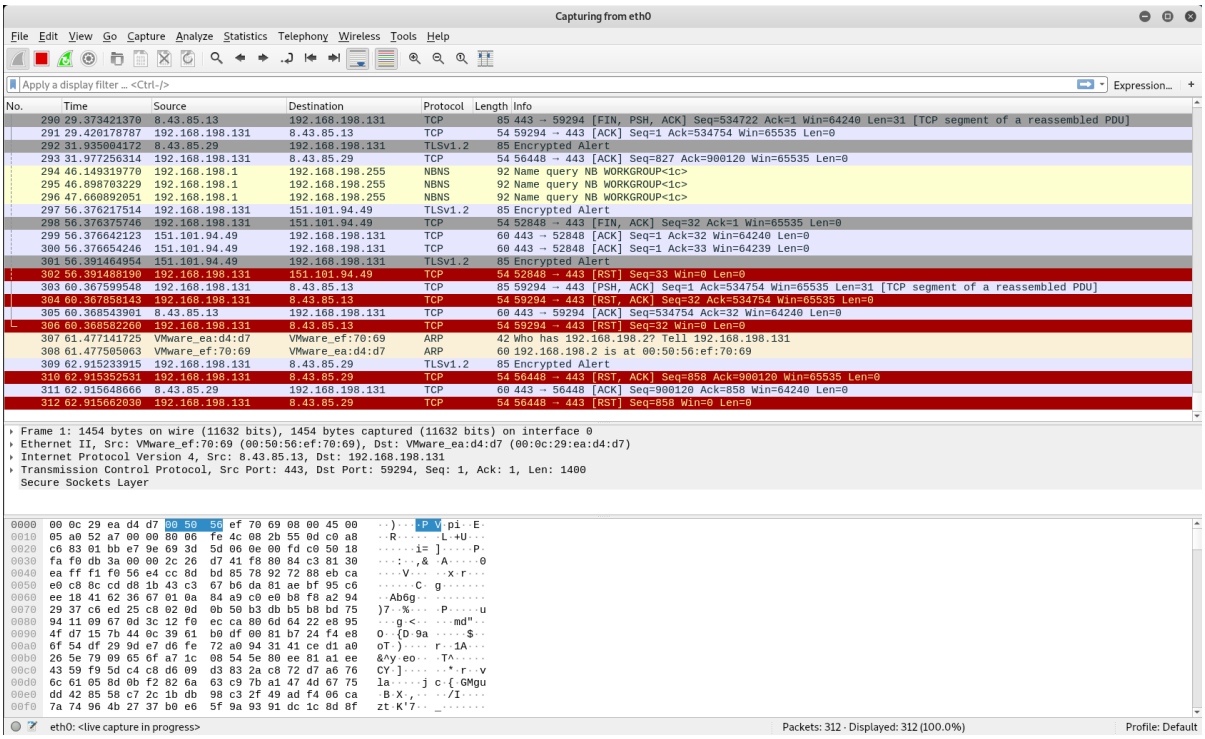
Para iniciar os testes, algumas configurações devem ser previamente estabelecidas, a primeira delas é colocar o adaptador externo no modo de

monitoramento, ou modo monitor. Deste modo, o adaptador não descartará pacotes que não sejam a ele destinado, ou seja, ele irá aceitar todos os pacotes.

Para este passo, é fundamental um adaptador externo para redes sem fio. Um adaptador interno de notebook dificilmente irá conseguir entrar em modo de monitoramento e receber os pacotes necessários para os ataques aplicados nesse trabalho.

Para demonstrar essa diferença, a ferramenta WireShark, um analisador de tráfego de rede, pode realizar uma listagem de todos os pacotes que passam pelo alcance da placa de rede enquanto está sendo executado. A Figura 04, mostra a placa interna de rede do notebook, que não está no modo monitor, operando através da máquina virtual pela interface eth0.

**Figura 4 – Analisando tráfego de rede com o adaptador interno**

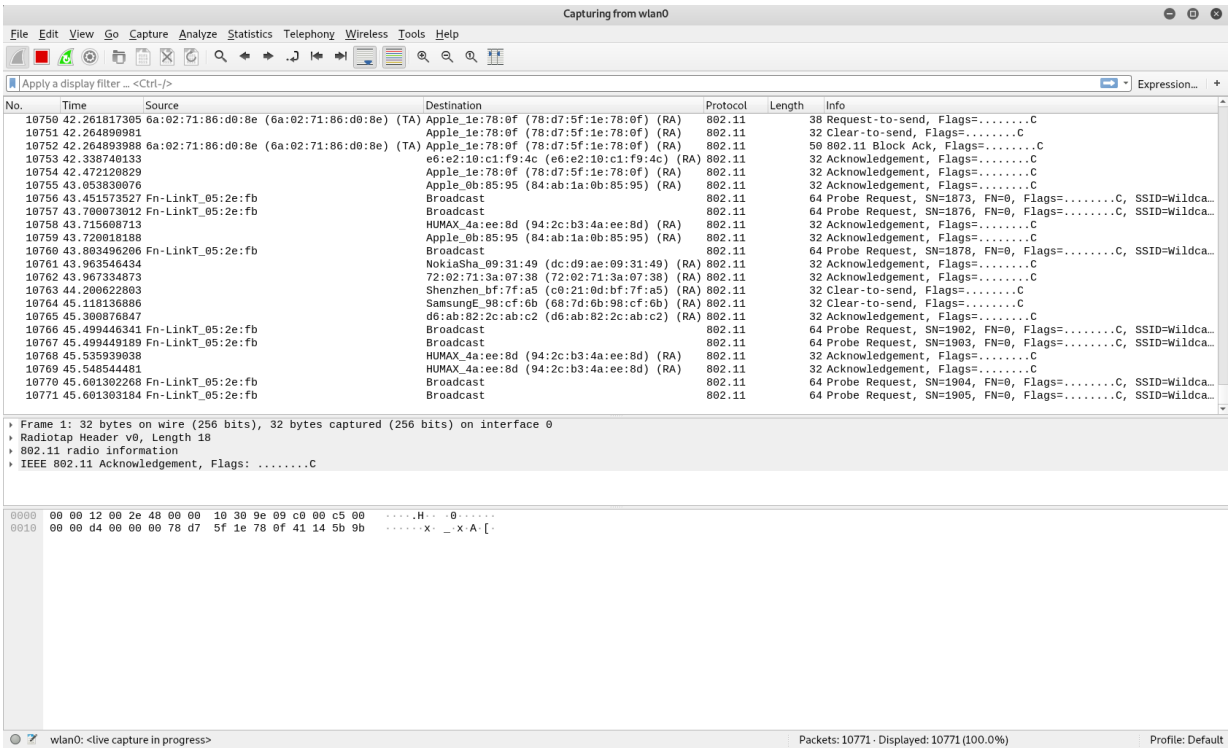



**Fonte: Autoria própria**

É possível perceber que os pacotes têm origem (*Source)* ou destino (*Destination)* em sua grande maioria, nos mesmos endereços. Ou seja, a placa apenas reage a pacotes que envia ou que recebe.

Já com o adaptador externo, em modo monitor, é possível notar uma grande diferença, na quantidade e endereços dos pacotes enviados e recebidos, como mostra a Figura 05.

**Figura 5 – Analisando tráfego de rede com o adaptador externo, em modo monitor**



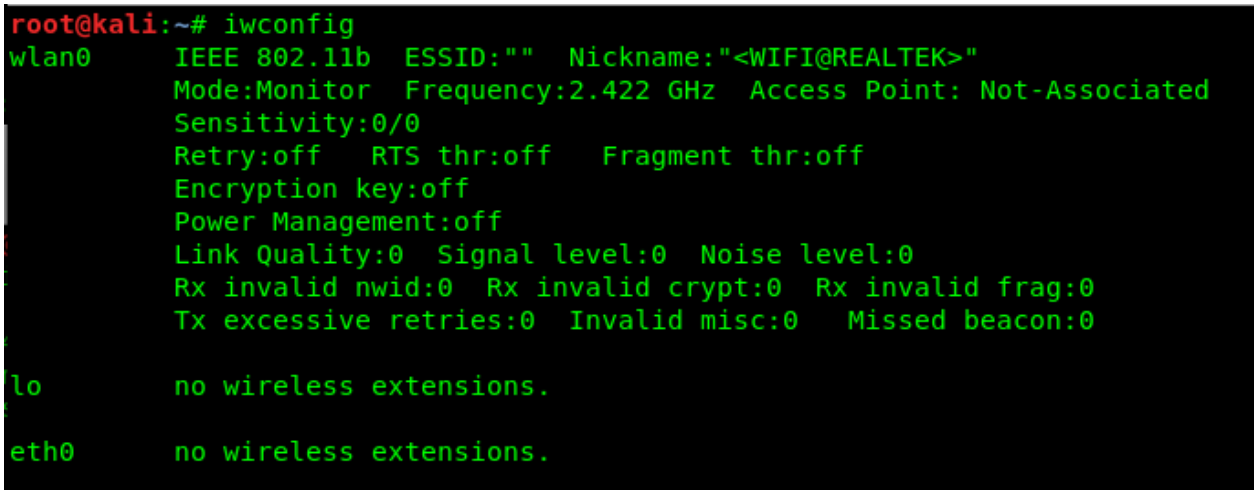

**Fonte: Autoria própria**

Para colocar o adaptador no modo monitor, os seguintes comandos são utilizados. É importante ressaltar que os comandos utilizados para ativar o modo monitor podem ser diferentes de adaptador para adaptador, variando conforme fabricante, modelo e driver utilizado.

*ifconfig wlan0 down*
*iwconfig wlan0 mode monitor channel “X”*
*ifconfig wlan0 up*

Onde, *wlan0* é o nome da interface de rede utilizada pelo adaptador externo. O parâmetro “X” representa o canal de operação enquanto o adaptador estiver no modo monitor, este é um parâmetro opcional. A Figura 06 mostra que o adaptador foi colocado com sucesso no modo monitor.

**Figura 6 – Verificando o estado do adaptador externo**




**Fonte: Autoria própria**

A frequência (*Frequency)*, é dada pelo canal em que a interface está operando, no padrão de 2.4GHz, o canal 1 começa em 2.412GHz e escala em intervalos de 5MHz. No exemplo acima, o adaptador está operando no canal 3. É válido observar também, o protocolo do padrão IEEE 802.11b sendo utilizado nesse teste.

O próximo pentest é o da quebra do protocolo WEP, tentar entrar na rede protegida por este protocolo, sem conhecer a chave acesso.

## 3.3 PENTEST EM PROTOCOLO WEP

Com o adaptador externo em modo de monitoração, é possível dar sequência aos testes de invasão. O primeiro teste será quebrar a chave de acesso do protocolo WEP. Este teste será composto pelos seguintes passos.

1. Colocar o adaptador externo no modo monitor;
2. Realizar o teste de injeção de pacotes. Este passo não é necessário, mas é útil para verificar se o adaptador tem capacidade de realizar a invasão;
3. Capturar dos Vetores de Inicialização;
4. Realizar uma falsa autenticação;
5. Retransmitir dos pacotes ARP;
6. Quebrar a chave de acesso.

O próximo passo é realizar um teste de injeção de pacotes, para verificar se o adaptador está apto e pronto para realizar os testes. O *Packet Injection,* é o processo de criar pacotes e inseri-los na rede, com o objetivo de interferir na comunicação de outros dispositivos, e até mesmo do ponto de acesso. Assim, inúmeras janelas de opções se tornam possíveis, como por exemplo, se passar por outro dispositivo. Para executar um teste de injeção de pacotes, é aplicado o seguinte comando.

*aireplay-ng -9 -e teste -a E8:94:F6:05:BF:B8 wlan0*

Onde, *-9* é o parâmetro do *aireplay-ng* para teste de injeção de pacotes, *-e teste* indica nome da rede sem fio e *-a E8:94:F6:05:BF:B8* indica o endereço MAC do ponto de acesso. O comando retorna como saída o resultado do teste de injeção de pacotes, como mostra a Figura 07.

**Figura 7 – Resultado do teste de injeção**


**Fonte: Autoria própria**

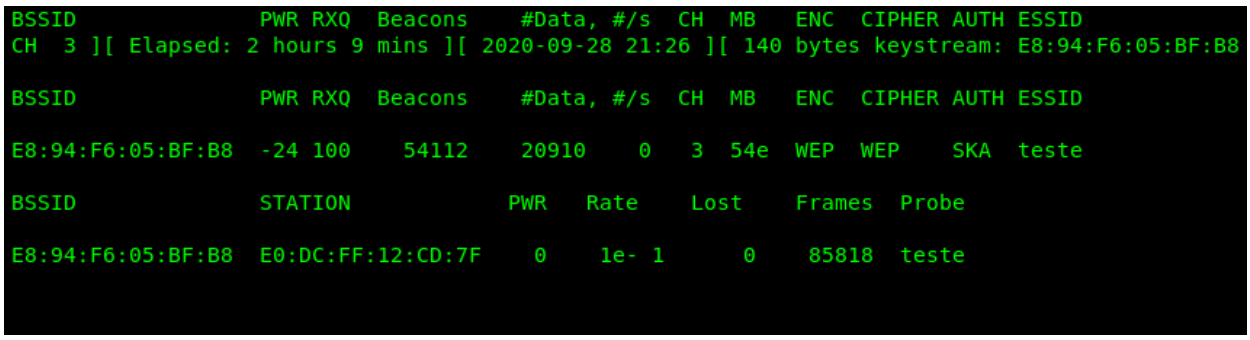
Um dado importante de se observar é a taxa de porcentagem dos dados de resposta obtidos, mostrados na última linha da Figura 07, é necessária uma taxa próxima a 100% para se obter sucesso nesse teste. Com o teste de injeção funcionando, é possível capturar os Vetores de Inicialização, *IV's.* Para isto, é utilizado o seguinte comando, e assim, verificar os pacotes de injeção que chegam na rede alvo.

*airodump-ng -c 3 --bssid E8:94:F6:05:BF:B8 -w output wlan0*

Onde *-c 3* representa o canal a ser monitorado, *--bssid E8:94:F6:05:BF:B8* define o endereço MAC da rede alvo, para filtrar os resultados e *-w* indica o filtro dos pacotes que contêm os *IV's.* É recebido um resultado semelhante ao da Figura 08. Na parte

inferior, os pacotes com os filtros aplicados são mostrados. Um pouco acima, o campo "*#s"* define os IV's que chegam por segundo. E onde está escrito *140 bytes keystream*, indica que Vetores de Inicialização já foram encontrados. Para realizar isso no teste, um outro dispositivo foi intencionalmente conectado. Como era uma rede sem tráfego, poderia não ser possível encontrar um pacote com IV.

**Figura 8 – Resultado da captura dos Vetores de Inicialização**



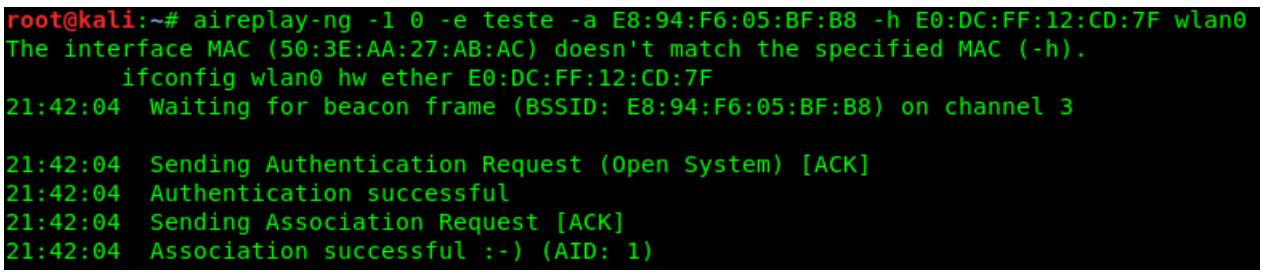

**Fonte: Autoria própria**

A seguir, será realizar a falsa autenticação com o ponto de acesso. Para isso, é preciso utilizar um endereço MAC que já tenha sido associado previamente com o ponto de acesso, caso contrário será rejeitado. É executado o seguinte comando.

*aireplay-ng -1 0 -e teste -a E8:94:F6:05:BF:B8 -h E0:DC:FF:12:CD:7F wlan0*

O parâmetro *-1* representa a tentativa de falsa autenticação, *0* é o tempo em segundos para tentar uma reassociação, caso necessário, *-h* indica o endereço MAC que será usado ao invés do endereço do nosso adaptador externo, pois este já é associado ao ponto de acesso. A Figura 09 mostra o resultado da falsa autenticação.

**Figura 9 – Resultado da falsa autenticação**



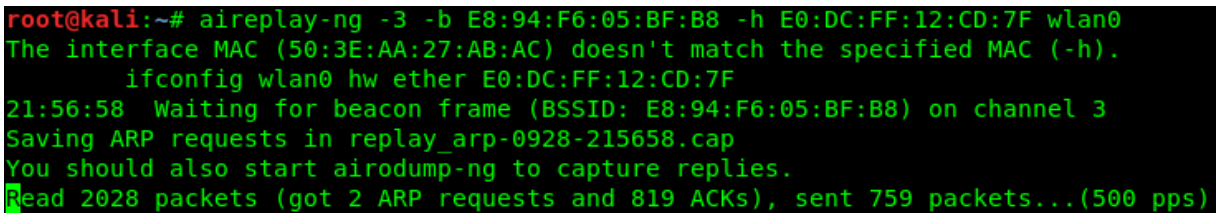

**Fonte: Autoria própria**

O passo seguinte, consiste em capturar pacotes do tipo ARP, *Address Resolution Protocol,* que são pacotes de comunicação. O objetivo deste passo é apenas redirecionar novamente estes pacotes na rede, pois o ponto de acesso cria novas IV's toda vez que estes pacotes são retransmitidos. Quanto maior o número de IV's obtidas, maior a chance e rapidez na hora da quebra do passe de acesso do ponto. Para isso, é aplicado o seguinte comando.

*aireplay-ng -3 -b E8:94:F6:05:BF:B8 –h E0:DC:FF:12:CD:7F wlan0*

O -3 indica o modo de requerimento dos pacotes ARP da ferramenta *aireplay-ng*. A Figura 10 ilustra o resultado do procedimento.

**Figura 10 – Resultado do requerimento de pacotes ARP**




**Fonte: Autoria própria**

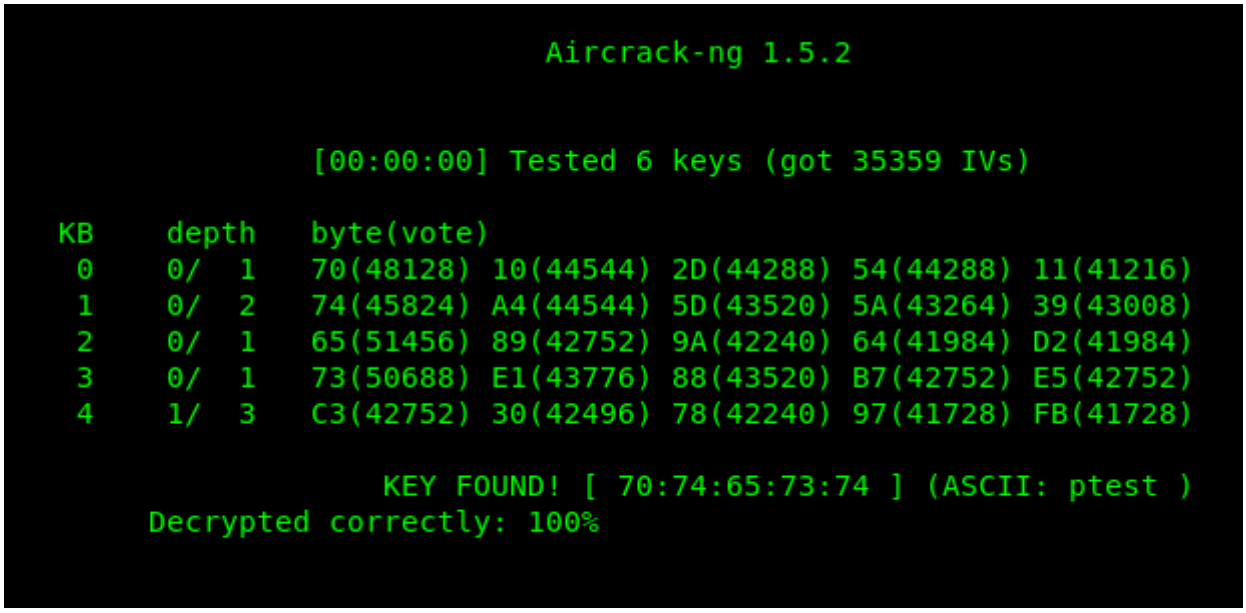
Para uma maior chance de sucesso na quebra da chave de acesso, é necessária uma maior quantidade de pacotes ARP, porém, como é uma rede de testes, sem tráfego, o número de pacotes ARP retransmitido é baixo.

Com as *IV's* obtidas, a chave do protocolo WEP está próxima de ser quebrada. É utilizada a ferramenta *aircrack-ng*, do seguinte modo.

*aircrack-ng -b E8:94:F6:05:BF:B8 output*.cap*

O indicador *-b* seleciona apenas o ponto de acesso alvo, enquanto o outro parâmetro indica que uma busca deve ser feita em todos os arquivos criados, iniciados com *output* e terminados em *.cap*, que foram os arquivos criados pelos métodos anteriores, durante a captura dos Vetores de Inicialização. No final, temos a saída do *aircrack-ng* indicando os resultados obtidos, como mostra a Figura 11, a senha "ptest" foi corretamente encontrada.

**Figura 11 – Resultado final do procedimento de quebra do protocolo WEP**




**Fonte: Autoria própria**

O resultado foi obtido em frações de segundos, visto que o WEP é um protocolo ultrapassado e com uma chave de acesso muito fraca, este teste serve como aprendizado para aplicações em outros protocolos e em outros tipos de teste.

## 3.4 PENTEST EM PROTOCOLO WPA/WPA2

Pode-se realizar a tentativa de quebra dos protocolos WPA e WPA2 com o mesmo conjunto de procedimentos. O primeiro passo é igual ao do procedimento de quebra do protocolo WEP, colocar o adaptador externo em modo monitor, no canal em que a rede alvo está operando. Com o adaptador já em modo monitor, é possível iniciar o ataque. Os passos realizados nesse teste são os seguintes.

1. Colocar o adaptador externo no modo monitor;
2. Realizar a captura de um *handshake* com um cliente já autorizado;
3. Desautenticar um cliente, passo opcional, utilizado para acelerar o passo 2;
4. Quebra da chave de acesso.

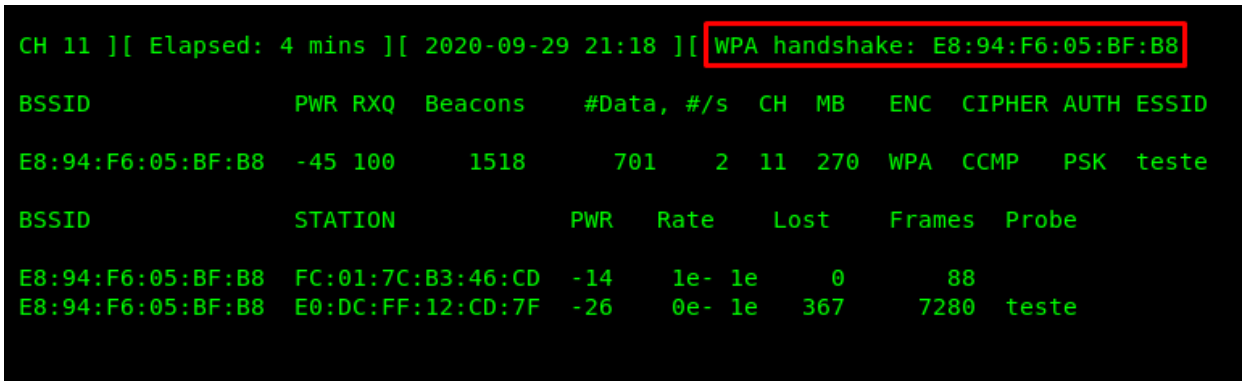
O passo seguinte consiste em encontrar um *handshake* com um cliente autorizado na rede. Para isso, o *scanner* de pacotes *airodump-ng* é utilizado para procurar pelos pacotes com prefixo “psk”, que são os arquivos que contêm os Vetores

de Inicialização, mas somente eles não são suficientes para quebrar os protocolos WPA e WPA2, uma vez que estes *IV's* são dinâmicos e alterados de tempo em tempo. É então executado o seguinte comando:

*airodump-ng -c 11 --bssid E8:94:F6:05:BF:B8 -w psk wlan0*

Onde *-c* indica o canal de operação, *--bssid* representa o endereço do alvo a ser observado, *-w* é o filtro para selecionar o tipo específico de pacotes pelo prefixo e *wlan0* a interface utilizada. A Figura 12 ilustra uma captura que obteve sucesso em encontrar um *handshake,* destacado em vermelho no canto superior direito.

**Figura 12 – *Handshake* capturado com sucesso**



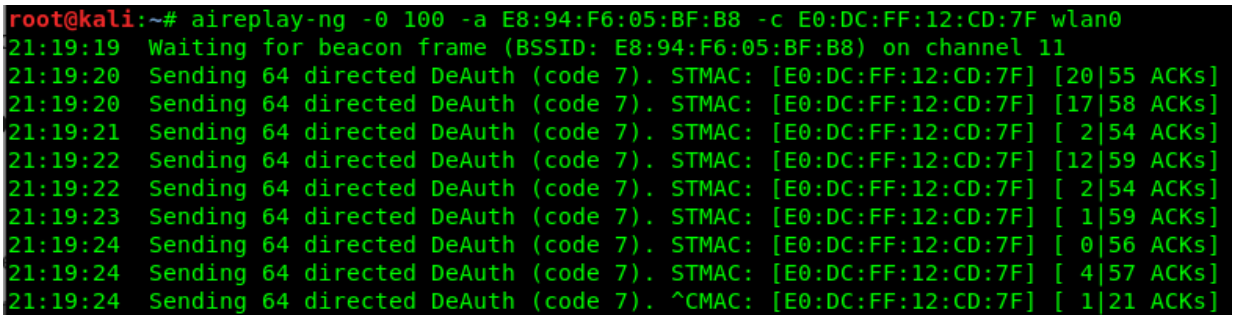

**Fonte: Autoria própria**

Conseguir um *handshake* pode ser um processo muito demorado, uma vez que é necessário que algum cliente se conecte ao ponto de acesso. Caso o cliente já esteja conectado, um novo *handshake* não acontecerá até que ele se desconecte e então volte a se conectar. Uma abordagem mais agressiva pode ser executada para evitar essa espera. É possível tentar uma desconexão forçada a um cliente já dentro da rede, e assim, capturar o pacote contendo o Vetor de Inicialização. Para isso, quando o mesmo se reconectar, é possível utilizar a ferramenta *aireplay-ng,* que possui um método de desautenticação de cliente para cliente, apenas enviando uma mensagem dizendo que o alvo não está mais conectado ao ponto de acesso, utilizando o seguinte comando.

*aireplay-ng -0 100 -a E8:94:F6:05:BF:B8 -c E0:DC:FF:12:CD:7F wlan0*

Onde *-0* indica o ataque de desautenticação, “100” é o parâmetro para quantidade de pacotes enviado, *-a* é o ponto de acesso e *-c* o cliente alvo. Com um pouco de sorte, o alvo será desconectado. Alguns fatores podem ser decisivos para o sucesso ou não do procedimento, como, a distância entre o atacante e o alvo, e a quantidade de pacotes enviados, já que muitos pacotes podem fazer o cliente não se reconectar, e poucos podem fazer com que ele não se desconecte. A Figura 13 mostra um ataque de desconexão bem-sucedido. Os valores para “ACKs” mostradas no final de cada resultado significam que os pacotes foram entregues corretamente, ou seja, que o cliente recebeu os pacotes.

**Figura 13 – Processo de desautenticação do *aireplay-ng***




**Fonte: Autoria própria**

Com o *handshake* obtido, é possível utilizar novamente a ferramenta *aircrack-ng* para tentar a quebra dos protocolos WPA e WPA2. Durante esse passo, será necessária a utilização de uma lista de palavras com possíveis senhas para comparação, a ferramenta disponibiliza uma pequena lista para testes, mas não é viável em aplicações reais. É importante ressaltar que, este método pode demorar muito tempo, dependendo da força da senha, capacidade de processamento da CPU e do banco de palavras utilizado. Pode-se utilizar a ferramenta com o seguinte comando.

*aircrack-ng -w /root/Desktop/passlst -b E8:94:F6:05:BF:B8 psk*.cap*

Onde *-w* indica o arquivo da lista de palavras, *-b* é a rede alvo e *psk*.cap* indica que está sendo buscado em todos os arquivos iniciados por *psk* e terminados em *.cap*, que são os arquivos de *handshake* capturados nos passos anteriores. Se a ferramenta conseguir encontrar com sucesso a chave de acesso, a resposta será similar à mostrada pela Figura 14.

**Figura 14 – Resultado positivo pelo *aircrack-ng* para quebra de protocolo WPA e WPA2**


**Fonte: Autoria própria**

Mesmo utilizando uma base extremamente pequena, em um ambiente de testes, percebe-se uma maior dificuldade de invasão nos protocolos WPA e WPA2, comparados ao seu antecessor WEP, principalmente pelo tempo de quebra da chave e do consumo de processamento. Analisando mais profundamente, embora o WPA tenha menos passos nesse procedimento equivalente, a demora para realiza-los é muito maior, visto também, que, ainda precisa de outro cliente para conseguir quebrar a chave de acesso.

Os métodos apresentados neste trabalho, para encontrar a chave de acesso dos protocolos WEP, WPA e WPA2, podem se tornar extremamente lentos e com baixa chance de sucesso para uma senha forte, com vários caracteres e caracteres especiais, por exemplo. Tornando assim, muito difíceis de serem aplicados em ambientes reais.

Com o passar do tempo, novas ferramentas surgiram, utilizando algoritmos mais eficientes, aproveitando a capacidade de processamento dos *hardwares* mais atuais, recorrendo a GPU para quebrar os variados tipos de criptografia contidos nas senhas utilizados pelos protocolos, trazendo assim, uma variedade muito ampla de métodos para invasões em redes sem fio.

É válido ressaltar, que, o protocolo WEP já não é mais utilizado nos dias atuais, visto que, seus mecanismos de segurança já se mostraram completamente vulneráveis

a invasores. O protocolo de segurança mais utilizado atualmente, nas redes sem fio é o WPA2. Embora existam diversas maneiras de ser invadido, ainda não foi substituído em massa pelo seu sucessor, o WPA3, que promete corrigir as suas falhas. Mesmo assim, o WPA2 se mostra bastante confiável, quando utilizado da maneira correta, com senhas fortes, trocadas de tempo em tempo, controle de acesso por endereço MAC, limitação da propagação do sinal, entre outros.

# 4 CONCLUSÃO

O propósito de um *hacker* ético é, principalmente, executar testes, denominado de *pentest* a fim de encontrar falhas em sistemas de tecnologia de informação. Este trabalho é voltado a uma pequena parte desses testes, quando aplicados em redes sem fio. Mais especificamente, nos protocolos de segurança WEP, WPA e WPA2.

Assim sendo, primeiramente, no capítulo 2, uma abordagem sobre os principais focos na área de segurança em redes sem fio feita, como caracterizados nos três primeiros objetivos específicos, análise das principais vulnerabilidades, das ferramentas de invasão, e dos mecanismos de proteção de redes sem fio, encontradas e citadas na literatura.

No capítulo 3, o desenvolvimento, os objetivos específicos restantes foram representados, através da realização do pentest praticado em redes sem fio, nos protocolos WEP, WPA e WPA2, definidos na topologia da rede de testes criada especificamente para este propósito. Também neste capítulo foi tratado dos resultados, para cada protocolo testado, assim como uma comparação breve entre eles. E, comentado como está atualmente o cenário da segurança em redes sem fio.

Desse modo, o principal objetivo, de realizar uma análise da segurança em redes sem fio, utilizando pentest, nos protocolos WEP, WPA e WPA2, foi cumprido. Como sugestão de trabalhos futuros, seria interessante uma abordagem desse tipo de ataque no protocolo WPA3, se disponível, além de ataques com abordagens diferentes, e também ataques utilizando outros adaptadores externos, com outros drivers, ferramentas similares, para comparações de desempenho.

## REFERÊNCIAS

ALLEN, Lee; HERIYANTO, Tedi; ALI, Shakeel. **Kali Linux – Assuring Security by Penetration Testing**. Birmingham B3 2PB, UK: Packt Publishing Ltd, 2014. 541 p. ISBN 978-1-84951-948-9.

ARANA, Paul Albert R. Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2). **INFS 612**, [*s. l.*], 2006.

BONCELLA, Robert J. **Wireless Security: An Overview. Communications of the Association for Information Systems, Washburn University**, v. 9, p. 269-282, 8 out. 2002. DOI 10.17705/1CAIS.00915. Disponível em: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=2750&context=cais. Acesso em: 6 set. 2019.

FIGUEIREDO, Davis Anderson. **Análise da Segurança de Redes Wi-Fi Através de Teste de Penetração em Instituições de Ensino Superior de Belo Horizonte**. Orientador: Prof. Dr. Rodrigo Moreno Marques. 2015. Tese de Mestrado (Sistemas de Informação e Gestão do Conhecimento) - Universidade FUMEC, Belo Horizonte, 2015.

GAST, Matthew S. **802.11 Wireless Networks: The Definitive Guide**. 2. ed. [S. l.]: O'Reilly Media, 2005. 672 p. ISBN 978-0-596-10052-0.

KOHLIOS, Christopher P.; HAYAJNEH, Thaier. A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. **Electronics 2018**, Fordham University, New York, NY 10023, USA, p. 284-312, 30 out. 2018.

KUMKAR, Vishal *et al*. Vulnerabilities of Wireless Security protocols (WEP and WPA2). **International Journal of Advanced Research in Computer Engineering & Technology**, [*s. l.*], v. 1, ed. 2, abril 2012.

LAMICHHANE, Shree Krishna. **Penetration Testing in Wireless Networks**. Orientador: Kimmo Sauren, Senior Lecturer. 2016. 41 p. Thesis (Bachelor's Degree in Information Technology) - Helsinki Metropolia University of Applied Sciences, [*S. l.*], 2016.

MORENO, Daniel. **Introdução ao Pentest**. 1. ed. [S. l.]: NOVATEC, 2015. 296 p. ISBN 978-85-7522-431-1.

MYLONAS, Phivos *et al*. Real-life paradigms of wireless network security attacks. **15th Panhellenic Conference on Informatics**, Kastonia, Greece, 3 nov. 2011.

NAKAMURA, Emilio Tissato; GEUS, Paulo Licio. **Segurança de Redes em Ambientes Cooperativos**. 2. ed. [S. l.]: NOVATEC, 2007. 482 p.

TEWS, Erik. **Attacks on the WEP protocol**. Orientador: Prof. Dr. Dr. h. c. Johannes Buchmann. 2007. Diploma thesis (Fachbereich Informatik) - TU Darmstadt, [*S. l.*], 2007.

TL-WN722N. **TP-LINK.** Adaptador USB Wireless N de Alto Ganho de 150Mbps. Disponível em <https://www.tp-link.com/br/home-networking/adapter/tl-wn722n/>. Acesso em: 28 de set. de 2020.

VANHOEF, Mathy; PIESSENS, Frank. Practical Verification of WPA-TKIP Vulnerabilities. **ASIA CCS '13**, [*S. l.*], p. 427-436, 8 de maio de 2013.

VANHOEF, Mathy; RONEN, Eyal. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. **ANRW**, Montreal, Canada, 22 jul. 2019.

VIBHUTI, Shivaputrappa. IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability. **CS265 Spring 2005**, San Jose State University, CA, USA, 2005.

WHITEWAKER, Andrew; NEWMAN, Daniel P. **Penetration Testing and Network Defense: The pratical guide to simulating, detecting, and responding to network attacks**. 1. ed. Indianapolis, IN 46240 USA: Cisco Press, 2005. 624 p. ISBN 1-58705-208-3.

WHITMAN, Michael E.; MATTORD, Herbert J. **Principles of Information Security**. 4. ed. [S. l.]: Cengage Learning, 2011. 656 p. ISBN 978-1-111-13821-9.

ZISIADIS, Dimitris *et al*. Enhancing WPS Security. **IFIP Wireless Days**, Dublin, Ireland, 7 jan. 2013.