Cibersegurança: Análise teórico prática sobre redes de computadores

Andrew Gonçalves[1], Sylvio André Garcia Vieira[1]

[1]Ciência da Computação – Universidade Franciscana (UFN)

Santa Maria – RS – Brasil

andrew.v.goncalves@gmail.com, Sylvio@ufn.edu.br

Abstract. *The use of the internet increases each day, and currently the technologies that make up the protection of Wi-Fi networks are susceptible to different forms of attacks, this work aims to present tools and scripts created to show vulnerabilities, as well as possible ways to protect against attacks made over Wi-Fi networks.*

Resumo. *Cada vez mais o uso da internet aumenta, e atualmente as tecnologias que compõe a proteção das redes Wi-Fi estão suscetíveis a diferentes formas de ataques, esse trabalho tem o propósito de apresentar ferramentas e scripts criados para exibir vulnerabilidades, assim como possíveis formas de se proteger de ataques realizados através de redes Wi-Fi.*

1. Introdução

O crescimento e consequente popularização da Internet nos anos recentes promoveu uma corrida ao desenvolvimento de tecnologias que facilitassem o acesso para os usuários residenciais. Desta forma cabos que interligavam computadores com os modems de acesso puderam ser opcionalmente substituídos por conexões sem fio, principalmente pela tecnologia Wi-Fi (Wireles Fidelity) [Weidman 2014]. O aumento de usuários na Internet contribuiu para uma ascendente migração de serviços que existiam basicamente em locais físicos, para os meios digitais, como comércio, contratação de serviços e sistemas financeiros. Junto a estes avanços que, além de economia de tempo, facilitaram a vida dos usuários, surgiram novas vulnerabilidades, que ora existiam apenas em situações presenciais. Muito foi feito para tentar oferecer segurança para estas transações, que antes eram realizadas por pessoas, como seguranças de lojas ou bancos. Porém, todos os protocolos desenvolvidos e utilizados para autenticação podem estar sujeitos a vulnerabilidades, inclusive o protocolo mais utilizado, o chamado de WPA2, que apresenta algumas vulnerabilidades. O protocolo mais recente apresenta novas vulnerabilidades. Por isso, é necessário a utilização de diretrizes para proteger a integridade da rede e tentar evitar invasões [Broad and Bindner 2014].

Dessa forma, muitos projetos de *Ethical Hacking* podem ser definidos como a atividade em que profissionais na área de segurança da informação, atuam dentro da lei, para identificar, explorar e corrigir vulnerabilidades em sistemas web, redes de computadores e/ou dispositivos móveis. Essas estratégias são importantes para minimizar que sejam exploradas de forma maliciosa por hackers mal-intencionados. A maioria desses projetos de *Ethical Hacking* se encontram disponíveis em plataformas de colaboração como, por exemplo, o Github e o Gitlab [Cordeiro 2020]. A utilização do sistema operacional Linux, especificamente distribuições voltadas para testes de invasão e segurança da informação, como "*Kali*" e "*Parrot*", são cruciais por incluírem uma gama

de ferramentas para a realização de testes e avaliação de invasão em protocolos como o WPA2, bem como na realização de testes forenses e desenvolvimento de ferramentas de proteção.

1.1 Objetivo Geral

O objetivo deste trabalho é apresentar as ferramentas utilizadas por profissionais da segurança da informação para realizar testes de invasão em redes Wi-Fi com WPA2, expondo vulnerabilidades e apontando as maneiras de evidenciar ataques de invasão. Além disso, serão abordadas tecnologias novas que solucionam as vulnerabilidades encontradas até o presente momento.

1.2 Objetivos Específicos

- Apresentar testes de invasão cujo alvo são redes Wi-Fi
- Identificar ataques às redes Wi-Fi em andamento
- Apresentar novas tecnologias que solucionam as vulnerabilidades analisadas

2. Referencial teórico

Na atualidade, a internet está cada vez mais presente nas nossas vidas. Uma pesquisa intitulada "Acesso à Internet e a Televisão e Posse de Telefone Móvel Celular para Uso Pessoal", realizada em 2018 pelo Instituto Brasileiro de Geografia e Estatística (IBGE), afirma que a Internet era utilizada em 74,9% dos domicílios brasileiros no ano de 2017 e este percentual subiu para 79,1% no ano seguinte (Figura 1). Muito desse tráfego se dá por meio de rede Wi-Fi (wireless fidelity), o que é evidenciado no mesmo estudo do IBGE. O equipamento mais utilizado para acessar a internet tem sido o telefone móvel, seguido imediatamente pelo microcomputador. O IBGE classifica banda larga Móvel, tanto redes Wi-Fi quanto redes de telefonia. [IBGE 2018]. Como pode ser observado na Figura 1, houve uma maior utilização da banda larga móvel em relação à fixa em todo o Brasil, com exceção do nordeste. Essa particularidade do nordeste se dá em decorrência das conexões serem prioritariamente cabeadas.

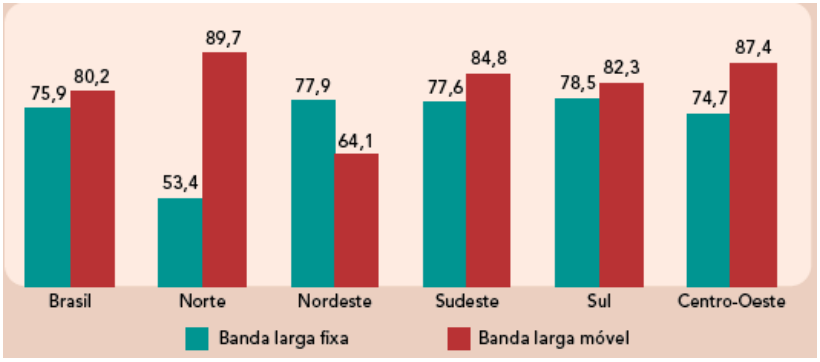

Figura 1: Utilização da internet, segundo o tipo de banda larga. Fonte: IBGE 2018

O ponto de acesso possui uma lista contendo o endereço MAC de dispositivos que podem ser autenticados. Se o endereço MAC não estiver na lista, não será possível o acesso à rede. Esse método não faz parte da especificação *IEEE* (Institute of Electrical and Electronics Engineers) 802.11, mas é disponibilizado por vários fabricantes de

equipamentos Wi-Fi para tentar aumentar o controle de acesso à rede [Linhares and Gonçalves 2009]. Nesse sentido, percebe-se a grande importância da segurança da informação, pois o padrão 802.11 do IEEE, especifica formas de segurança para operação, que os fabricantes de equipamentos com esta tecnologia devem implementar. De 1999 até os dias atuais, o IEEE estabelece padrões de proteção de dados através da rede Wi-Fi, sendo esses padrões apresentados e discutidos abaixo.

2.1 Proteção das redes sem fio

A segurança da informação é cada vez mais importante, pois a internet está sendo utilizada de maneira crescente, devido a pandemia da corona vírus (Covid-19). Segundo o Instituto de Pesquisa Econômica Aplicada [IPEA 2020], está havendo impactos significativos e ainda não completamente dimensionados sobre a sociedade. Trata-se de um evento inédito na história, dado que, no passado, epidemias parecidas se desenvolveram em um cenário de muito menor integração entre países e pessoas, divisão do trabalho e densidade populacional. Agora, é inevitavelmente a sociedade ter uma rápida adaptação às novas metodologias de trabalho, as quais se tornam cada dia mais dependentes de inovações tecnológicas. Por exemplo, a maioria das escolas e universidades aderiram o trabalho remoto. Assim sendo, a proteção de dados é muito importante porque no Brasil, segundo o [IBGE 2018], a forma mais utilizada de acesso à internet é por meio da banda larga móvel, ou seja, redes WiFi, ou de telefonia de terceira e quarta geração.

É importante desenvolver o conceito de criptografia, pois é como se dá a proteção das redes sem fio. Linhares and Gonçalves, (2009) descrevem criptografia como uma forma de incrementar a segurança dos dados cujo intuito é permitir que somente pessoas ou dispositivos autorizados tenham acesso aos dados que estão ou serão encriptados. O processo utilizado por essas pessoas ou dispositivos para acessarem os dados se chama decodificação ou descriptografia.

O primeiro protocolo de segurança lançado pela IEEE 802.11 foi o WEP (Wired Equivalence Privacy) em 1999 (Figura 2). Esse protocolo se mostrou muito vulnerável a ataques de negação de serviço e ataques de força bruta devido à chave de criptografia ser reduzida, reutilizada e estática. Em 2003, houve a primeira atualização na ementa de segurança do IEEE 802.11, ano em que foi implantado o protocolo WPA (Wifi Protected Access) apenas como solução temporária, enquanto o desenvolvimento da nova ementa era finalizado. Em 2004 foi lançado o protocolo de segurança IEEE 802.11i, o qual trouxe melhorias relevantes para a segurança dos dados, porém continuou não fornecendo proteção aos quadros de gerenciamento e controle [Linhares and Gonçalves, 2009].

A proteção dos pontos de acesso pode ocorrer de diversas formas. Atualmente, existem quatro formas principais de realizar a autenticação em pontos de acesso, e cada uma delas possui vulnerabilidades diferentes (Figura 2). No entanto, como o objeto de estudo deste trabalho é a autenticação WPA2, as vulnerabilidades dessa forma de autenticação se dão por meio de ataque de negação de serviço, seguido de captura de chaves de autenticação de 4 fatores. Os padrões de segurança que foram desenvolvidos até o presente momento são os seguintes:

- ***WEP (Wired Equivalent Privacy)*** –é um padrão de segurança que não suporta autenticação e criptografia seguras, seu único objetivo é proteger os dados de possíveis vazamentos de informação de forma passiva [da Silva Gonçalves e DAmbrosio, 2009]. O algoritmo WEP se baseia em uma chave secreta utilizada para codificar todas a informações que circulam pela rede. A chave secreta compartilhada pode ser de 64, 128 ou 256 bits.

- ***WPA (Acesso Protegido Wi-Fi–Pessoal)*** **-** o WPA é um método de segurança sem fio que fornece proteção forte dos dados, evitando o acesso não autorizado às redes de tamanho pequenas [da Silva Gonçalves e DAmbrosio, 2009]. Utilizando uma criptografia baseada em data e tempo de solicitação da autenticação, a WPA pode conter, ou não, uma chave pré compartilhada (PSK), que é caracterizada por uma chave de autenticação própria de um ponto de acesso. A variação que possui PSK se chama *WPA Personal*. A outra variante, que não possui PSK, denomina-se *WPA Enterprise.*

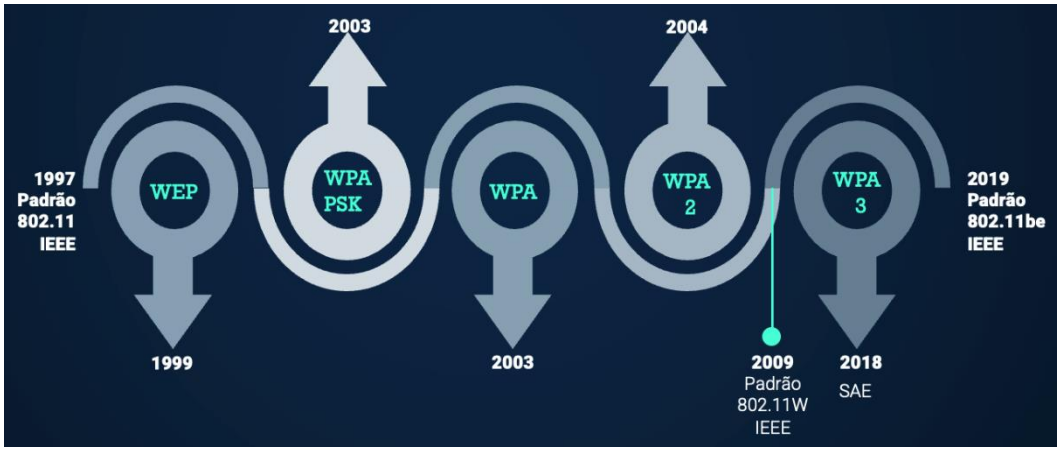

Figura 2: Padrões de proteção das redes Wi-Fi ao longo dos anos. [Dos Autores 2021].

2.2 Autenticação de 4 fatores

Toda autenticação WPA possui uma autenticação de 4 fatores, também chamada de *4-Way-Hadshake.* Nessa autenticação, o ponto de acesso e o dispositivo que pretende se conectar trocam 4 pacotes de dados, os quais servem para que o ponto de acesso verifique a senha digitada no dispositivo com a PSK ou MSK.

O *4-way handshake* faz parte de um processo de autenticação, cuja função é legitimar que o usuário tenha acesso à rede em que está tentando se conectar [de Souza and da Silva Gonçalves 2010]. O processo se dá através do contato inicial com a rede pelo cliente que gostaria de realizar a conexão. Então, para isso, é gerada uma chave temporal (ou seja, sua derivação parte do tempo, assegurando uma criptografia diferente, todas as vezes que essa chave é gerada), chamada PTK. Essa chave é enviada para o PA, que por sua vez cria uma chave temporal própria (GTK) derivada da senha original (MSK). As duas chaves retornam ao cliente para esse então gerar uma chave "mestre" que é derivada da senha que o usuário digitou na hora de autenticação (PMK). Assim, o cliente envia esse resultado para o PA, de forma que ele possui todas as chaves necessárias

para realizar a verificação, confirmando se a senha digitada no cliente está correta ou não. Caso esteja correta, o cliente conseguirá realizar a conexão (Figura 3).

É importante ressaltar que todo esse processo se dá para assegurar a proteção da rede. Em momento algum a transferência de pacotes de senha em texto simples para realizar a checagem de integridade. Ao invés disso, o protocolo criptografa a senha original (MSK) quatro vezes, utilizando quatro algoritmos diferentes, sendo dois deles baseados no tempo, para garantir uma segurança ainda mais robusta. Só após esse processo ser efetuado corretamente, a conexão for estabelecida na rede WPA e WPA2.

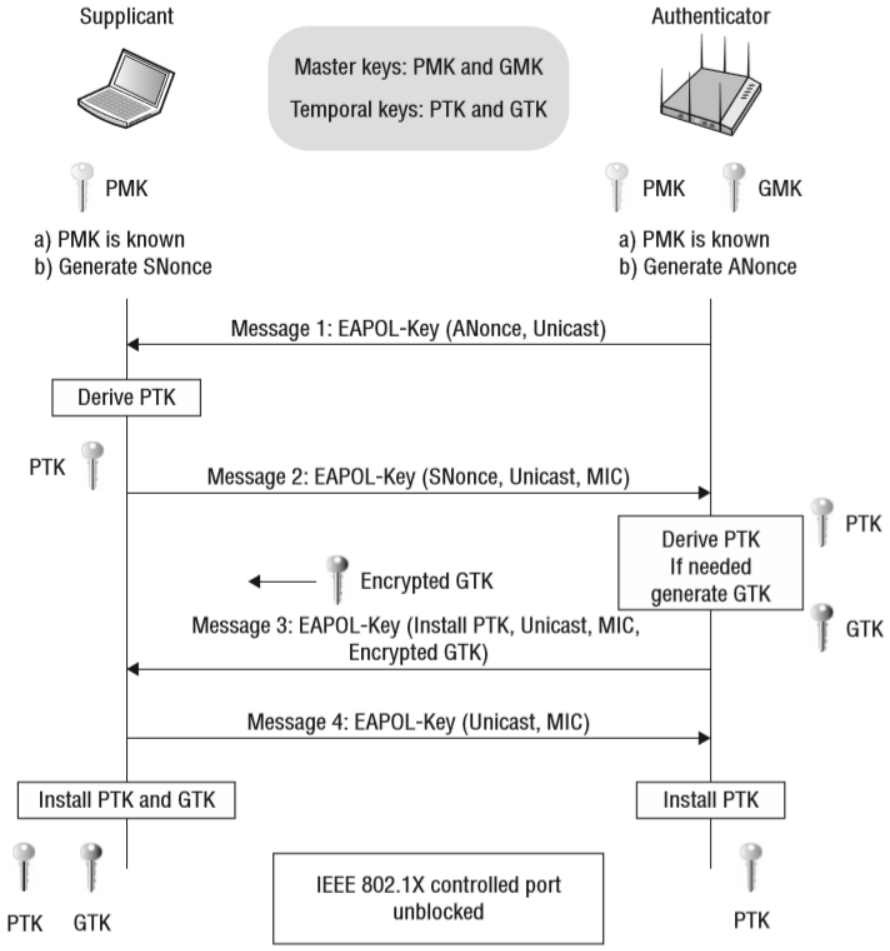

Figura 3: Autenticação de 4 fatores no protocolo WPA2. [4-way handshake 2019]

2.3 Ataque de desautenticação

Ataques de desautenticação ocorrem quando um dispositivo capaz de monitorar e injetar pacotes, consegue tirar um dispositivo conectado à rede vítima, forçando uma nova autenticação. Essa é uma vulnerabilidade tanto do protocolo WPA quanto do WPA2, sendo um ataque de negação de serviço, onde o MIC (Message Integrity Check), possui um mecanismo de proteção para evitar ataques de força bruta. Em decorrência desse mecanismo é que acarreta um ataque de negação de serviço (DoS). [Linhares and Gonçalves, 2009]. Quando dois erros de MIC são detectados em menos de um minuto, o PA cancela a conexão por 60 segundos e altera a chave de integridade. Portanto, com uma

simples injeção de pacotes malformados é possível fazer um ataque de negação de serviço.

Através do protocolo IEEE 802.11w alguns dispositivos mais modernos conseguem identificar ataques de desautenticação e negação de serviço e protegem o usuário. Isso se dá pois, segundo Ahmad and Tadakamadla, (2011), esta tecnologia permite que o ponto de acesso tenha controle sobre os quadros de gestão e controle (*management and controll frames*). Então, quando ele detecta uma atividade suspeita, como por exemplo, 5 quadros de tentativa de autenticação diferentes, ele consegue proteger o usuário de ser desautenticado, pois esse protocolo possui "*Robust Management frames*". Esses quadros de gestão robusta possuem uma formatação diferente dos quadros de desautenticação e autenticação. Sem essa tecnologia, o ataque de desautenticação se torna muito difícil de ser realizada no cliente protegido por esse ponto de acesso. Mas, mesmo a última atualização do protocolo com um sistema mais robusto de gerência e controle de frames, o WPA2 é vulnerável à ataques de DDoS (Ataque de negação de serviço), que tem como alvo o próprio ponto de acesso. Nesse sentido, um atacante pode fazer um ataque conhecido como "*probe attack*", onde um dispositivo manda muitos pacotes de autenticação diferentes, com a intensão de sobrecarregar o ponto de acesso vítima do ataque, de modo a forçar uma reinicialização do dispositivo.

2.4 WPA2

Este trabalho terá o foco em redes protegidas com autenticação WPA2, pois esta é uma das tecnologias mais atuais no momento. A proteção de redes WPA2 se dá por meio de melhorias em uma série de padrões de segurança que apareceram recentemente. Os padrões WPA2-Pessoal (com PSK) e WPA2-Enterprise (sem PSK) aperfeiçoam as medidas de segurança correspondentes à proteção dos dados, aos acessos e à autenticação dos usuários em relação aos padrões WEP e WPA. O WPA2 utiliza o algoritmo de criptografia denominado *AES* (Advanced Encription Standard, ou Padrão Avançado de Criptografia).

Atualmente, alguns pontos de acesso, por meio do protocolo IEEE 802.11w (introduzido em 2009), conseguem se proteger de ataques de desautenticação e negação de serviço. No entanto, existem ataques feitos para desarmar essa proteção. Os ataques conhecidos como "*beacon attack*" e "*probe attack*".

Quando um usuário se autentica, há uma série de mensagens trocadas entre o ponto de acesso (PA) e o cliente. Essa troca de mensagens introduz um atraso no processo de conexão. Quando um cliente se desloca de um PA para outro, o atraso para estabelecer a associação pode causar uma interrupção notória da conexão, principalmente em tráfego de voz e vídeo. Para minimizar esse atraso de associação, o equipamento pode dar suporte a PMK Caching, o que consiste em guardar os resultados das autenticações dos clientes. Se o cliente voltar a se associar com o PA, essas informações guardadas são utilizadas para diminuir o número de mensagens trocadas na re-autenticação. Já em um processo denominado Preauthentication, enquanto o cliente está conectado a um PA principal, ele faz associações com outros PAs cujo sinal é repetido ao usuário. Desta forma, quando há

uma mudança de PA, não há perda de tempo com a autenticação (Figura 4). [Linhares and Gonçalves, 2009]

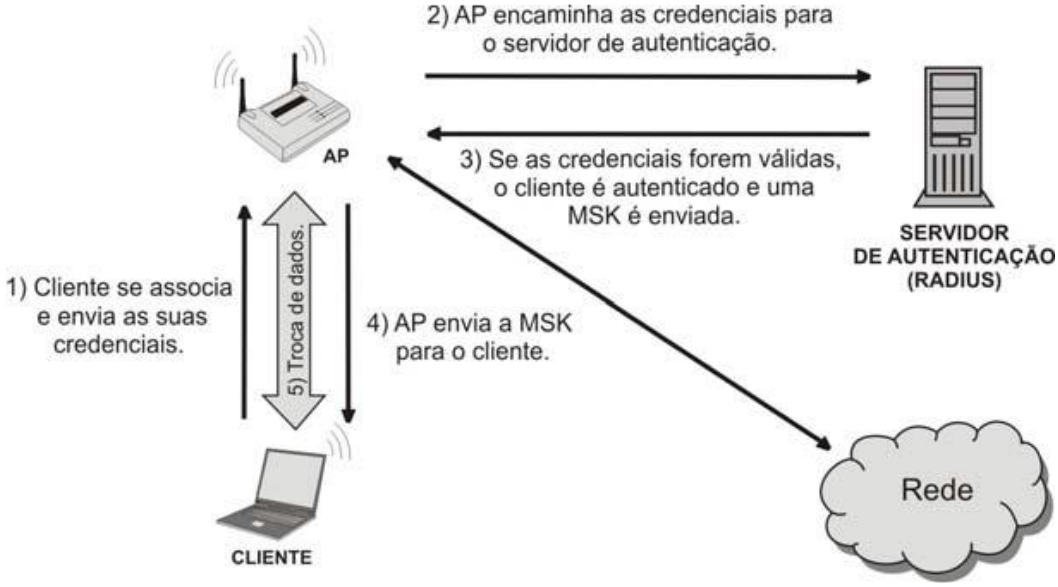

Figura 4. Autenticação 802.1x/EAP [Linhares and Gonçalves 2009]

Após a autenticação, inicia-se o processo de derivação da PMK, onde as chaves serão estabelecidas. Esse processo é chamado de 4-Way-Hadshake, ou seja, autenticação de 4 fatores. Se a autenticação foi baseada no modo PSK, a chave PMK é a própria PSK. Se não, a PMK é derivada a partir da MSK, a qual foi compartilhada durante o processo de autenticação 802.1x/EAP. A PMK nunca é usada para encriptação ou integridade, mas é usada para gerar chaves temporárias (Pariwise Transient Key - PTK). A PTK é um conjunto de chaves, entre elas a chave de criptografia de dados (Temporal Encryption Key – TEK) e a chave de integridade de dados (Temporal MIC Key - TMK). Ao final da autenticação de 4 fatores, é garantido que tanto o cliente quanto o PA possuem a mesma PTK, estando prontos para a troca de dados. [Linhares and Gonçalves, 2009]. Essa hierarquia de chaves de autenticação pode ser demonstrada na Figura 5:

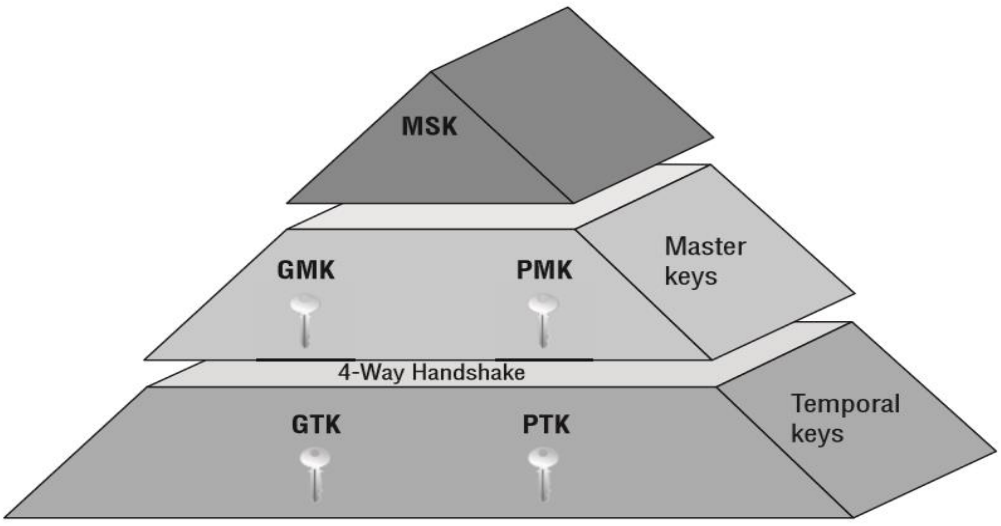

Figura 5: Hierarquia de chaves para a autenticação no protocolo WPA2. [4-way handshake 2019]

2.5 Kali Linux

A distribuição Kali Linux é desenvolvida com o foco em realização de ataques de penetração, lançada em 2012, é a distribuição recomendada pelo grupo "OffSec Services Limited" para realização de diversas certificações no ramo da segurança da informação. É voltada, principalmente, para testes de invasão, auditoria e segurança de computadores. Essa distribuição dispõe de diversos softwares e scripts para auxiliar no trabalho de testes de penetração. Atualmente, o projeto *Kali* Linux, através da iniciativa "Kali Everywhere", "Kali ARM", "Kali NetHunter" e "Win-KeX", é capaz de se instalar *Kali* Linux em muitos dispositivos, como por exemplo, no android, no Windows, em circuitos integrado com chips diversos, Docker, em máquinas virtuais, entre outros. Para ataques relacionados às redes sem fio, essa distribuição contém ao menos 10 ferramentas desenvolvidas com esse propósito.

No presente trabalho, para a realização dos ataques no Kali Linux, utilizou-se dispositivo controlador de interface de redes sem fio, através da conexão USB TP Link (TL-WN722N v1). Foi assim utilizado porque esse usa o chipset "*Atheros AR9271*", que permite que o dispositivo entre no modo monitor, utilizando esse modo de operação. Nesse modo é possível capturar pacotes (sniff/farejar) de redes cuja autenticação não foi completada.

3. Metodologia

Neste trabalho, para a realização dos testes de invasão, foi utilizada uma máquina virtual Oracle Virtual Box, com uma imagem do *Kali* Linux instalada, com o USB TP Link (TL-WN722N v1). Utilizou-se um computador de placa única RaspberryPi Zero, dois circuitos integrados ESP-8266, dois pontos de acesso diferentes como vítimas, um D-Link DAP-2360 v1 e um TP Link AC750 v5.

Geralmente, o dispositivo Raspberry Pi Zero pode ser integrado a uma tela de papel eletrônico (e-ink). No entanto, em decorrência do custo, neste trabalho, foi instalado uma imagem do projeto Pwnagotchi no RaspberryPi Zero. Esse projeto tem a intensão de ser um farejador "*sniffer*" de todo tráfego que ocorre ao seu redor. O projeto Pwnagotchi foi lançado através da plataforma GitHub em outubro de 2019, sendo desenvolvido para discernir entre pacotes de autenticação de 4 fatores completos, parciais e PMKID, os quais são pacotes de autenticação do PA, formado através do PMK (como dispostos nas figuras 4 e 5). Fazendo analogia com o Tamagotchi, o Pwnagotchi se alimenta de chaves de autenticação de 4 fatores.

Foi utilizado um circuito integrado ESP-8266, gravado com a imagem "esp8266_deauther", para a realização de ataques de desautenticação, ataques de "probe" e ataques de "beacon".

Para realizar este trabalho, foram selecionadas duas redes WPA com (TFG_TPLink) ou sem (TFG_DLink) PSK a serem invadidas (Figura 6).

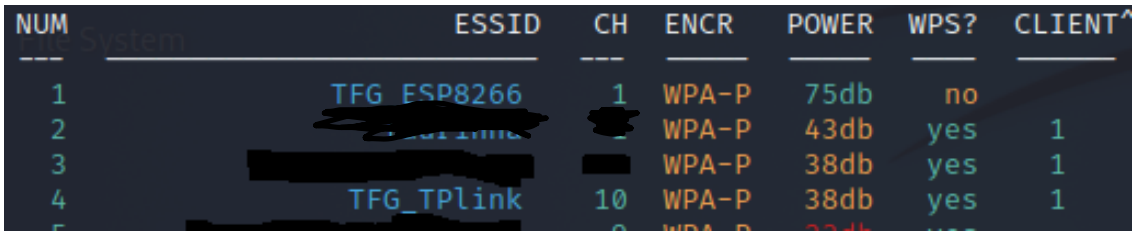

Figura 6: Script Wifite identificando vítimas e se elas possuem chaves WPS. [Dos Autores 2021]

4. Resultados

Utilizando o script "Wifite", que é um script utilizado para testar a penetração de redes móveis, através de ferramentas disponíveis no *Kali Linux*. Obteve-se automaticamente acesso ao modo monitor do dispositivo USB Wireless. Como pode ser observado na figura 7, foi permitido a utilização do modo monitor (enabling monitor mode on wlan0, mudando o nome para wlan0mon).

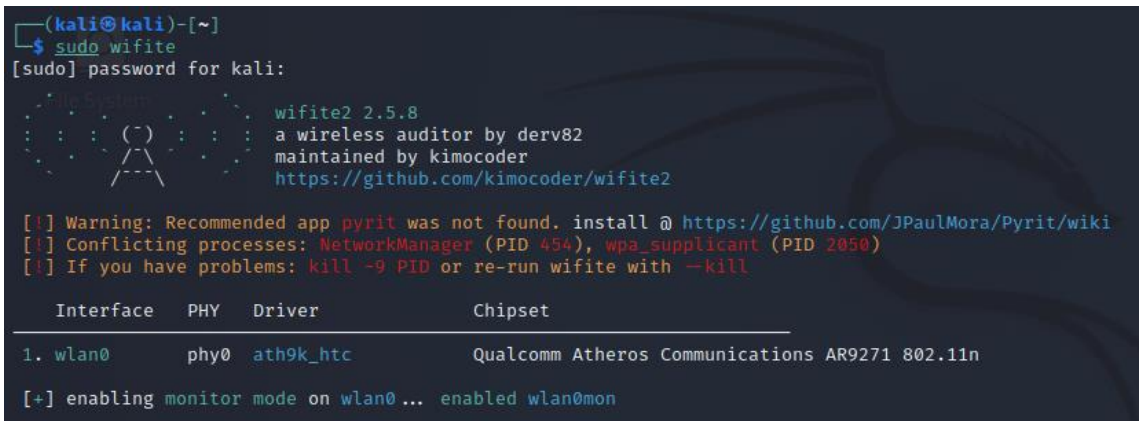

Figura 7: Script Wifite colocando o dispositivo USB em modo monitor. [Dos Autores 2021]

O script Wifite tenta executar três testes de invasão, começando pelo "WPS Pixie-Dust" cuja funcionalidade é enviar pacotes de pareamento WPS para o PA. Esse ataque foi efetivo no TP Link AC750 v5 e tentou creakear, automaticamente, com o método "Bully" para descobrir a senha PSK por método de força bruta, ou seja, testando todas as formas possíveis. Pois, a PSK é formada por apenas 8 números o que facilita a invasão (Figura 8).

Figura 8: Script Wifite identificou a chave WPS, utilizando o método "bully". [Dos Autores 2021]

Tendo em vista que a senha PSK foi adquirida através do "WPS Pixie-Dust", essa tentativa de força bruta se torna viável e é automaticamente realizada pelo script "Wifite" (Figura 8). Já com o Pwnagotchi, foram detectados tanto os PMKID dos dois PA quanto a autenticação de 4 fatores.

Com o Circuito integrado (CI) ESP-8266, foi possível realizar os 3 ataques diferentes (Figura 9), através da interface gráfica, uma vez que se acessa o PA criado pelo CI, nomeado TFG_ESP8266. Ao clicar no botão Probe, o CI cria 60 usuários diferentes,

tentado associá-los ao PA vítima (Figura 10). Dessa forma, uma reinicialização do PA é forçada. Isso desativa a proteção do PA 802.11W. A descrição de cada ataque pode ser observada na figura 11.

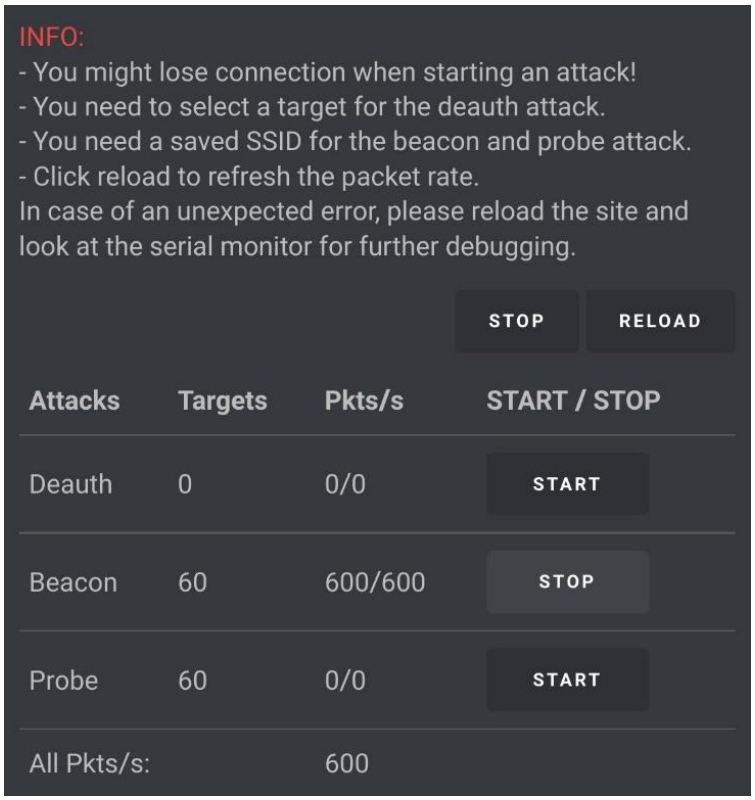

Figura 9: Interface do ESP-8266, ataques Beacon. [Dos Autores 2021]

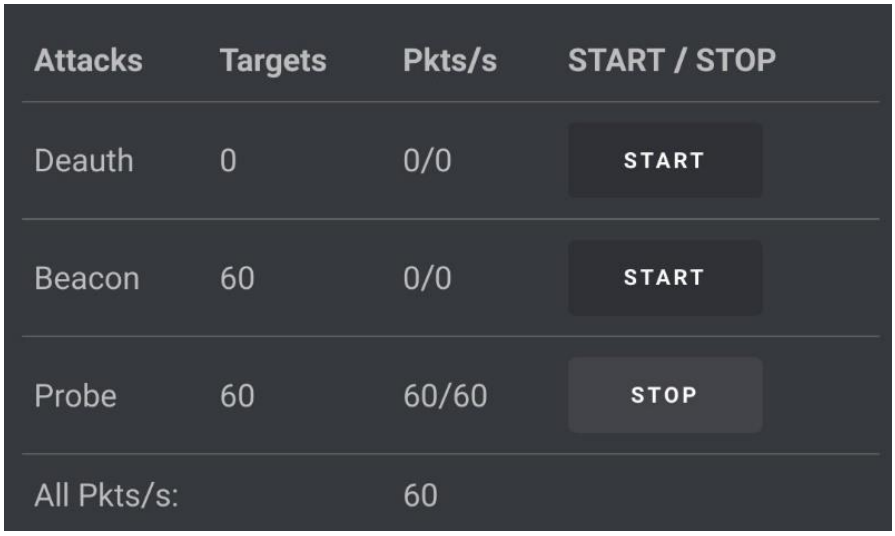

Figura 10: Interface do ESP-8266, ataque probe em andamento. [Dos Autores 2021]

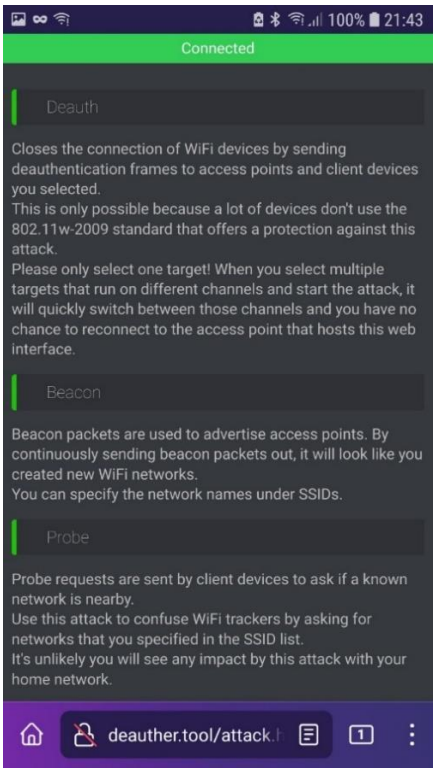

Figura 11: Interface do ESP-8266, possibilidade de ataques. [Dos Autores, 2021]

Por meio desse CI foi possível criar 60 redes Wi-Fi diferentes, com nomes e proteção aleatórios (Figura 12).

Figura 12: Ataque Beacon em andamento. [Dos Autores 2021]

5. Prevenções

Atualmente, a prevenção está na dependência da qualidade da máquina atacante para fazer um ataque de força bruta. Com máquinas potentes, as proteções atuais são vulneráveis. Chaves de autenticação de 4 fatores são encriptografadas, mas caso ela for adquirida por uma pessoa com a intenção de invasão, a vítima estará segura somente até a chave ser descriptografada. Nos dias de hoje, a quebra da criptografia se dá por meio de softwares que se utilizam do processador central do computador, assim como da placa gráfica, para acelerar o teste de diferentes senhas contra as chaves de autenticação.

Se possível, a chave de pareamento WPS não deve ser utilizada no PA, tendo em vista que essa chave é vulnerável, permitindo que com um script e um USB no modo monitor sejam capazes de se descobrir a senha do PA. O usuário deverá utilizar sempre a melhor forma de proteção que o PA disponibiliza. Caso a melhor forma de proteção seja WEP, considerar a substituição do PA.

Atualmente, uma nova forma de proteção de redes Wi-Fi foi lançada, denominada WPA3. Essa proteção foi lançada por meio do protocolo 802.11ax, também chamada de Wi-Fi 6. Essa tecnologia não faz mais uso de uma senha compartilhada entre dois dispositivos para fazer o aperto de mão, mas implementa a tecnologia RADIUS (Remote Authentication Dail In User Service), a qual distingue, particularmente, cada usuário da rede, gerando novos hashes para cada novo usuário.

Outra proteção introduzida pelo protocolo WPA3 é a proteção dos quadros de autenticação (Beacon protection), a qual passa a exigir um período mínimo para a realização da autenticação. Dessa forma, o PA se protege de todas as formas de coleção de pacotes de autenticação (Sniffing attacks; Figura 13).

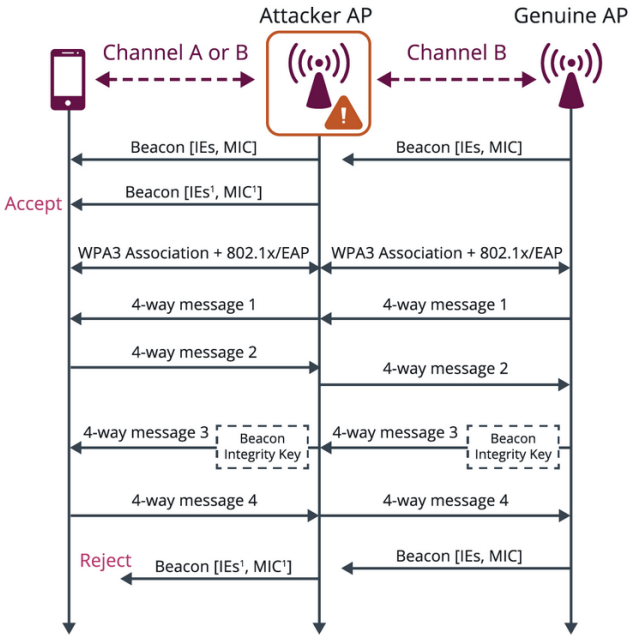

Figura 13: Proteção de Beacon (Derham & Bhandaru (2021)

5. Considerações Finais

A tecnologia Wi-Fi está crescentemente sendo utilizada no Brasil [IBGE 2018]. No entanto, as formas de proteção dessa tecnologia mudaram pouco nos últimos 11 anos. Portanto, é muito importante ter conhecimento das diferentes formas de ataques de invasão que podem ocorrer a essas redes sem fio.

Salienta-se que métodos de prevenção já vêm sendo discutidos e implementados há algum tempo. No entanto, a última inovação no protocolo 802.11 ocorreu no ano de 2009 e só limitou ataques de desautenticação e negação de serviço [Cordeiro 2020]. Isso não é uma solução efetiva, pois não protege contra-ataques de forma passiva (Sniffing Attaks). É necessário saber as vulnerabilidades que essas redes apresentam, para então criar estratégias de proteção, como por exemplo a criação de uma senha segura, ou seja, uma senha com mais de 12 caracteres que misture letras maiúsculas e minúsculas e caracteres especiais, desabilitando a opção de utilizar WPS e, se possível, utilizar WPA2 ou, em uma situação possível, o WPA3.

Como fabricantes de dispositivos dependem do estabelecimento de protocolos de segurança pelo instituto de engenheiros e eletricistas eletrônicos para poder implementar inovações em novos equipamentos, é de grande importância que estes protocolos sejam atualizados regularmente, ou seja, na hora que a inovação foi descoberta ou na hora que uma vulnerabilidade seja concertada, para que o consumidor esteja sempre protegido. Infelizmente o protocolo 802.11 ficou 9 anos sem atualizações, o que possibilitou todas as vulnerabilidades discutidas neste trabalho.

Finalmente, esse conhecimento poderá ser utilizado na prática em trabalhos futuros que exploram a segurança do protocolo WPA3, assim que forem descobertas. Essas informações são importantes e devem ser ampliadas para um sistema de segurança em empresas.

6. Referências Biliográficas

4-way handshake. https://www.wifi-professionals.com/2019/01/ Acesso em: outubro de 2020.

Ahmad, M. S. e Tadakamadla, S. (2011): “security evaluation of IEEE 802.11w specification”, Proceedings of the fourth ACM conference on Wireless network security. p. 53 - 58.

Broad, J. and Bindner, A. (2014) Hacking com Kali Linux. Técnicas práticas para testes de invasão. Novatec editora Ltda. 1a Edição.

Cordeiro, F. A. et al. (2020). Aplicação de técnicas de ethical hacking-demonstração do uso de ferramentas e ambiente de estudo para acadêmicos ou iniciantes em segurança web.

Derham, T.; Bhandaru, N. (2021). Wi-Fi CERTIFIED WPA3™ December 2020 update brings new protections against active attacks: Operating Channel Validation and Beacon Protection.

https://www.wi-fi.org/ko/beacon/thomas-derham-nehru-bhandaru/wi-fi-certified-wpa3-december-2020-update-brings-new-protections

de Souza, E. F. and da Silva Gonçalves, P. A. (2010). Segurança em redes ieee 802.11: Integridade de dados, autenticaçao e confidência.

IBGE. (2018) Acesso a Internet e a Televisão e Posse de Telefone Móvel Celular para Uso Pessoal. Rio de Janeiro: Fundação Intituto Brasileiro de Geografia e Estatística.

IPEA. (2020) Pesquisa analisa desafios para o avanço da medicina de precisão no país.

Linhares, A. G. and Gonçalves, P. d. S. (2009). Uma análise dos mecanismos de segurança de redes ieee 802.11: Wep, wpa, wpa2 e ieee 802.11 w. Universidade Federal de Pernambuco (UFPE)-Centro de Informática (CIn).

Medeiros, R. C. d. (2017). Implementação de um modelo de segurança para rede sem fio wpa2-eap.

Rosseto, C. K. (2018). Criptografia como recurso didático: uma proposta metodológica aos professores de matemática.

Weidman, G. (2014). Testes de Invasão. Uma introdução prática ao hacking. Novatec Editora Ltda. 1a impressão.