TÉCNICAS DE INVASÃO DE REDE WI-FI 802.11

Lucas Honorato da Cruz; Prof. Me. José Aparecido de Aguiar Viana; Prof. Me. Walter Gomes Pedroso Júnior

e-mail:

honoratolucas15@gmail.com, jose.viana@fatec.sp.gov.br, walter.pedroso@fatec.sp.gov.br

Resumo: O uso da tecnologia sem fio faz parte do cotidiano das empresas e residências. Arquivos confidenciais e pessoais circulam constantemente nessas redes. Embora alguns protocolos sejam conhecidos por serem extremamente vulneráveis, eles ainda estão em uso, e protocolos mais seguros às vezes são usados incorretamente, deixando espaço para ataques conhecidos, como aqueles que usam um dicionário de palavras em um dicionário. Nesta pesquisa irá ser estudado as vulnerabilidades da rede sem fio e ataques, vai ser usado as ferramentas de distribuição Linux.

Palavras-chave: Técnicas de invasão. Padrão 802.11. Vulnerabilidades do Wi-Fi. Protocolos de Segurança WEP, WPA e WPA2.

Abstract: The use of wireless technology is a part of everyday life in businesses and homes. Confidential and personal files are constantly circulating over these networks. Although some protocols are known to be extremely vulnerable, they are still in use, and more secure protocols are sometimes used incorrectly, leaving room for known attacks, such as those that use a dictionary of words in a dictionary. In this research we will make wireless network vulnerabilities and attacks we will use, test, and use Linux distribution tools.

Keywords: Intrusion techniques, 802.11 Standard, vulnerabilities, Wireless Networking, Security Protocols.

1. Introdução

A popularização da rede sem fio tornou-se uma tendência na atualidade, sendo utilizada em residências, empresas e universidades devido à portabilidade, flexibilidade e baixo custo de instalação, além de oferecer ampla área de cobertura. Entretanto, como essa tecnologia utiliza ondas de rádio para transmitir dados, a segurança acaba sendo comprometida, expondo seus usuários a diversos riscos.

Com o intuito de evitar vulnerabilidades, foi criado o padrão de segurança 802.11i para redes sem fio, que garante confidencialidade e integridade dos dados por meio de protocolos de criptografia. O cliente que se conecta ao ponto de acesso é configurado com uma chave autenticadora, armazenada e transmitida quando necessário. Segundo Tanenbaum e Wetherall (2011), “as chaves usadas para codificar o tráfego são calculadas como parte de um handshake de autenticação”.

No entanto, ao longo do tempo, diversas ferramentas foram desenvolvidas para violar os protocolos de segurança, utilizando técnicas de força bruta, ataques baseados em dicionários e exploração de vulnerabilidades conhecidas. Algumas chaves são facilmente quebráveis, independentemente da eficiência da ferramenta utilizada. Além disso, as vulnerabilidades presentes no ponto de acesso expõem usuários despreocupados ou com pouco conhecimento a ataques sofisticados que podem ter consequências irreversíveis.

Além das falhas de protocolos que vem acontecendo, as vulnerabilidades em ponto de acesso a rede sem fio acabam deixando o usuário despreocupado ou com pouco conhecimento para configurar uma chave mais complexa para a rede ou protocolos de segurança mais seguro. Existe ataques mais sofisticados que são muitos difíceis de serem reconhecidos. A admissão em um ponto de acesso é uma porta de entrada para outros riscos de segurança. Muitas vezes esses danos são causados pelo próprio usuário ou por empresas que são devastadoras. Segundo Tanenbaum e Wetherall (2011), “a rede sem fio é um sonho que se tornou realidade para espião: dados gratuitos sem nenhum trabalho”.

2. Justificativa

Os fabricantes de redes sem fio continuam disponibilizando configurações em seus dispositivos de protocolos de redes, tais como o Wired Equivalent Privacy (WEP) e o Wi-Fi Protected Setup (WPS). Esses protocolos apresentam falhas de segurança consideradas críticas

que já foram estudadas e divulgadas (Teixeira, 2017). O protocolo Wi-Fi Protected Access (WPA2) é considerado mais seguro, mas também apresenta algumas vulnerabilidades a serem exploradas, dependendo da complexidade da senha utilizada em um ponto de acesso, é facilmente descoberta com a utilização de dicionários. (Tanenbaum, 2011)

Constantemente, os usuários por despreocupação ou por não ter um conhecimento específico, acabam utilizando ou deixando determinados serviços vulneráveis em execução nos seus dispositivos. As senhas usadas são um grande problema, pois muitas vezes acabam configurando como data de nascimento, número de telefone, palavras triviais como "senha", "123456", etc. As redes Wireless Fidelity (Wi-Fi) no Brasil estão sob risco de ataques cibernéticos. Mais da metade dos roteadores são mal configurados e protegidos por fazerem configurações simples e que os consumidores acabam usando nome, endereço, nome de rua etc. Com isso acaba se tornando mais fácil de serem invadidos por ser senhas simples. (Teixeira, 2017)

A rede tornou-se um alvo fácil para os atacantes porque, além de comprometer a rede atacada, o agente pode ter acesso às redes interconectadas à rede sem fio. Esta pesquisa vai analisar, explicar e diferenciar tipos de ataques que podem ser feitos à rede e mostrar as vulnerabilidades que ocorrem na invasão. (Teixeira, 2017)

3. Objetivo(s)

O objetivo principal é aplicar técnicas de invasão em redes sem fio usando ferramentas de invasão e descobrindo as vulnerabilidades. Assim, serão feitas as descritas as vulnerabilidades da rede sem fio, os tipos de ataques a rede sem fio, demonstrando os ataques à rede sem fio, apresentando a ferramenta Kali Linux.

4. Fundamentação Teórica

Este trabalho apresenta uma revisão teórica abrangente dos principais conceitos relacionados a roteadores, padrões de redes sem fio e autenticação de segurança. O objetivo desta pesquisa é fornecer uma compreensão sólida desses tópicos, a fim de analisar os desafios enfrentados e explorar as soluções existentes no campo das redes sem fio. A revisão abrange aspectos fundamentais, como o papel dos roteadores na interconexão de dispositivos e transmissão de dados em redes sem fio. Além disso, são discutidos os padrões de redes sem fio, como os padrões 802.11, que definem parâmetros cruciais, incluindo frequência de operação, taxas de transmissão e técnicas de acesso ao meio.

No contexto da segurança, são abordados os protocolos WEP, WPA e WPA2, destacando suas características, vulnerabilidades e melhorias em relação à proteção de redes sem fio. Além disso, é explorado o funcionamento da EAP (*Extensible Authentication Protocol*), um *framework* versátil para autenticação em redes sem fio. Por meio desta revisão teórica, espera-se contribuir para o aprimoramento do conhecimento sobre as bases teóricas das redes sem fio e seus desafios de segurança, fornecendo uma base sólida para futuras pesquisas e desenvolvimento de soluções avançadas nessa área.

4.1. Roteador

Um roteador sem fio (ou *wireless*) é um dispositivo de rede que permite a conexão de dispositivos de forma sem fio, através de ondas de rádio, eliminando a necessidade de cabos. O roteador sem fio é capaz de transmitir e receber dados através da tecnologia Wi-Fi (*Wireless Fidelity*), que é um padrão de comunicação sem fio para redes locais. (Teixeira, 2017)

O roteador sem fio é responsável por gerenciar o tráfego de dados entre dispositivos, além de atuar como ponto de acesso para a conexão com a internet. Ele também permite a criação de redes locais sem fio, possibilitando a conexão entre dispositivos de uma mesma rede, como computadores, *smartphones, tablets* e impressoras, por exemplo. Alguns modelos de roteador sem fio também possuem funcionalidades adicionais, como firewall, controle parental, QoS (*Quality of Service*), entre outras.

As funcionalidades de um roteador sem fio são basicamente as mesmas de um roteador comum, acrescidas de recursos específicos para a rede sem fio. As principais funcionalidades do roteador sem fio são:

- Roteamento de pacotes: o roteador sem fio é responsável por encaminhar os pacotes de dados entre diferentes redes, seja por conexão sem fio ou por cabo de rede.
- Conexão com a internet: o roteador sem fio pode ser conectado a uma fonte de internet, como um modem de banda larga, para compartilhar a conexão com os dispositivos conectados à rede sem fio.
- Gerenciamento de endereços IP: o roteador sem fio atribui endereços IP aos dispositivos conectados à rede sem fio, permitindo a comunicação entre eles.

- Configuração de rede sem fio: o roteador sem fio permite a configuração de parâmetros da rede sem fio, como o nome da rede (SSID), o tipo de criptografia, a senha de acesso, entre outros.
- Controle de acesso: o roteador sem fio permite a criação de regras de acesso à rede, como restrição de acesso por horário, bloqueio de dispositivos específicos, entre outros.
- Qualidade de serviço (QoS): o roteador sem fio permite a priorização de tráfego de dados na rede, garantindo uma melhor qualidade de serviço para aplicativos que demandam maior largura de banda, como streaming de vídeo ou jogos online.
- Ampliação de sinal: alguns modelos de roteador sem fio permitem a expansão do sinal da rede sem fio através do uso de repetidores de sinal, ampliando a área de cobertura da rede sem fio. (Cisco Systems, 2022),

4.2. Padrões 802.11

Desde 1990, a *Institute of Electrical and Electronics Engineers* (IEEE) aprovou vários padrões de Wireless. Esses são os padrões mais comuns que definam o tipo de WLAN: 802.11, 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11i.

A seguir, serão descritas as características de cada um desses padrões citados anteriormente. Então vamos começar com o "pai de todos" que é o 802.11. (Cisco Systems, 2022)

4.3. Organização IEEE 802.11

O padrão 802.11 também conhecido como Wi-Fi opera em 1 e 2 Mbps, trabalhando com a banda de 2,4GHz. Esse padrão é responsável pela transmissão de rede sem fio, podendo ser feita de duas formas, através de sinais de rádios ou infravermelhos. As técnicas de transmissão utilizadas podem ser o *Direct Sequence Spread Spectrum* (DSSS) e *Frenquence Hopping Spread Spectrum* (FHSS). O DSSS e o FHSS permitem que a transmissão utilize vários canais dentro de uma frequência. A diferencia entre eles é que o DSSS pode quebrar vários segmentos a informação a ser transmitida e os envios simultaneamente em vários canais, enquanto o FHSS utiliza métodos de "salto de frequência", onde as informações transmitidas utilizam determinadas frequências em certos períodos e, no outro, acaba utilizando outras

frequências, com isso o FHSS tem a velocidade de transmissão de dados um pouco menor, já que a frequência utilizada muda constantemente. Agora o DSSS é mais rápido, mas tem mais chances de sofrer interferências, porque acaba usando todos os canais ao mesmo tempo. (Cisco Systems, 2022)

Ao longo do tempo, várias revisões do padrão 802.11 foram lançadas para melhorar o desempenho, a segurança e a eficiência das redes sem fio. Algumas das revisões mais comuns são:

- 802.11b: Foi o primeiro padrão a ganhar popularidade e ofereceu taxas de transferência de até 11 Mbps na faixa de frequência de 2,4 GHz.
- 802.11a: Opera na faixa de frequência de 5 GHz e suporta taxas de transferência de até 54 Mbps. É menos suscetível a interferências e oferece maior capacidade devido à maior largura de banda disponível.
- 802.11g: É uma extensão do padrão 802.11b que opera na faixa de frequência de 2,4 GHz e oferece taxas de transferência de até 54 Mbps. É compatível com dispositivos 802.11b.
- 802.11n: Introduziu tecnologias como MIMO (*Multiple Input Multiple Output*) e canais de largura de banda dupla (40 MHz), permitindo taxas de transferência de até 600 Mbps.
- 802.11ac: Também conhecido como Wi-Fi 5, opera na faixa de frequência de 5 GHz e suporta taxas de transferência de até vários gigabits por segundo. Utiliza técnicas avançadas de modulação, *beamforming* e canais de largura de banda ampla (80 MHz ou 160 MHz).
- 802.11ax: Também conhecido como Wi-Fi 6, é projetado para fornecer melhor desempenho em ambientes com alta densidade de dispositivos. Oferece maior eficiência espectral, maior capacidade e taxas de transferência mais rápidas em comparação com padrões anteriores.

Cada revisão do padrão 802.11 introduz melhorias no desempenho, alcance, segurança e recursos das redes sem fio. Além disso, o 802.11 também especifica os protocolos de autenticação e criptografia que garantem a segurança das comunicações sem fio, como o WEP, WPA e WPA2. (Cisco Systems, 2022)

4.4. Protocolo de Seguranças

Nesta seção vão ser revistos os protocolos de segurança usados na rede 802.11.

4.4.1. Wired Equivalent Privacy (WEP)

O *Wired Equivalent Privacy* (WEP) foi o primeiro padrão de segurança para redes 802.11, ratificado em setembro de 1999. O objetivo geral era fornecer um nível de segurança como as redes cabeadas, mas não acabou tendo muito sucesso. (Cisco Systems, 2022)

O WEP é um cadeado que você pode quebrar dando um chute na porta, somente se for usado o WEP para a última opção possível mesmo ou para dispositivos antigos que não suportam o WPA ou WPA2, pois é melhor criptografar do que ficar sem nenhuma criptografia, mas entenda quais ricos pode proporcionar com o WEP:

- Sem autenticação mútua: somente os clientes podem autenticar, Access Point não, isso vai facilitar a proliferação dos Access Points não autorizados ou falsos APs;
- Sem autenticação em nível de usuário: As chaves do WEP estáticas ficam armazenados no dispositivo, isso é um problema, porque se o dispositivo for roubado ou acessado sem permissão;
- Reutilização de chave estática: A chave para autenticação e criptografia é a mesma.

WEP é uma chave secreta que é compartilhada entre computadores ligados a um ponto de acesso. Originalmente o tamanho da chave WEP é de 64 bits, mas existem dispositivos com suporte a chaves de 128 e 256 bits. As chaves, que podem ser apresentadas em caracteres hexadecimal ou ASII. (PAIM, 2015).

A chave WEP 64 bits, é formada por duas portas, são as próprias chaves secretas com o comprimento de 40 bits e uma aleatoriamente escolhida, chamada de *Initialization Vector* (IV), com um comprimento de 24 bits. À medida que as mensagens são geradas, o IV vai mudando seu valor. Então é aplicado o RC4 no IV e chave, formando a chamada *KeyStream.* Por meio de uma operação XOR com o conjunto dados e ICV, temos os dados com ICV codificados. Por fim, são adicionados o cabeçalho e o IV com a chave de número sem estarem cifrados. A de criptografia exige o IV do pacote recebido que é concatenado com a chave secreta, gerando a *keystream* com RC4 é realizado um XOR com os dados e o

ICV e a chave completa. Com o texto limpo, é calculado novamente o ICV dos dados e comparado com o original.

4.4.2. Wi-Fi Protected Access (WPA)

Em vista do que estava acontecendo com a segurança o WEP, o WPA criando em 2002 pela Wi-Fi *Alliance* (WFA) adiantou a parte de autenticação e cifração do trabalho que estava sendo feio para o fechamento do padrão 802.11 e liberou para poder ter mais segurança na rede. Muitas mudanças e avanços foram incorporados a esse protocolo, mas a maior parte deles exige a inclusão de outros elementos à infraestrutura e ainda deve trabalhar combinada com os outros protocolos. Durante a sua concepção, acabaram encontrando vulnerabilidades no protocolo, com isso, dentro das propostas de melhorias que fizeram, a mais utilizada foi o algoritmo RC4 para uma forma mais segura, dentro do protocolo TKIP. (Teixeira, 2017)

O *Temporal Key Integrity Protocol* (TKIP) é um protocolo de segurança desenvolvido em 2002 para substituir o WEP sem poder exigir a substituição dos hardwares. Responsável pelas gerencias de chaves temporárias usadas pelo equipamento de comunicação, para poder manter o segredo entre as trocas constante de chave, visto que foi uma das vulnerabilidades do WEP que mantém chaves estáticas e as partes que não o são atravessarem a rede em claro. Segundo RUFOS (2005) “outra vulnerabilidade do WEP, corrigida no WPA e usada no TKIP, é o aumento significativo do tamanho do vetor de indicação, que passou dos originais 24 para 48 bits, permitindo um substancial elevação na quantidade de combinações possíveis, tornando taques baseados na relativamente rápida repetição dos valores dos vetores praticamente inócuos, exigindo processamento, ainda, fora dos padrões atuais do mercado”.

O TKIP é baseado em chaves que se alteram a cada novo envio de pacotes. A frequência que muda as chaves é sua principal características. Por padrão a cada 10.000 pacotes enviados e recebidos pela placa de rede a senha é modificada hoje é um protocolo obsoleto e seu uso no padrão WPA2 é opcional.

4.4.3. Wi-Fi Protected Access2 (WPA2)

O *Wi-Fi Protected Access 2* (WPA2) é um padrão de segurança para rede sem fio atualmente disponibilizado pela Wi-Fi *Alliance* em 2006 correspondendo a todos os requisitos do padrão 802.11i. Esse padrão é considerado o mais seguro atualmente e deve ser utilizado sempre que possível, a despeito de uma teórica perda (baixa) de performance em equipamentos mais simples. Existem duas versões do WPA2: WPA2-*Personal* e WPA2- *Enterprise.*

4.4.4. Modo Personal (WPA-PSK e WPA2-PSK)

Operando no modo *Personal*, as chaves são pré-compartilhadas (PSK) obrigatoriamente. O conhecimento do PSK, faz com que as estações de rede wireless sejam autenticadas. O conhecimento vem através de um processo, em que ambas as partes usam o PSK para poder gerar chaves de criptografia. Com essas chaves geradas, os dois dispositivos serão capazes de criptografar e de descriptografar toda a comunicação entre eles. (Cisco Systems, 2022)

O objetivo dele é ser muito simples de usar, simultaneamente, permite um bom nível de segurança. A configuração tanto do lado do concentrador quanto do lado do cliente resume-se habilitar esse recurso para uma escolha da chave-mestra, porque a chave-mestra é muito difícil de ser descoberta.

A chave PSK é gerada com base em uma "senha" (*passphrase*) que pode variar entre 8 e 63 caracteres da tabela *American Standard Code for Information Exchange* (ASCII). Podemos usar números binários de 256 bits. Segue algumas dicas para poder criar a *passphrase*:

- Não usar palavras que possam de descobertas com um ataque de dicionário;
- Não usar nomes ou datas associadas a você, tipo: aniversário, telefone etc.
- Usar combinações de letras maiúsculas, minúsculas e números;
- Coloque pelo menos uns 20 caracteres;

Note que as observações que foram feitos acima, ainda é possível "quebrar" uma chave WPA/WPA2 ou descobrir a *passphrase* utilizando métodos nada comuns. O PSK não tem nada a ver como o modo *Shared Key* (SKA), que é usada no WEP.

Seja para qual protocolo de segurança, a chave ela tem que ser pré-configurada nos dispositivos que vão se comunicar entre si. O modo de operação (*Personal*) é recomentada só para as redes pequenas e deve manter o cuidado de não deixa o *passphrase* configurada por muito tempo, porque essas distribuições de chave que acontece, continua sendo um problema. Por isso indicamos que é a mesma coisa que fazemos na senha do e-mail ou em qualquer lugar que tenha senha, sempre está trocando de tempo em tempo.

4.4.5. Modulo Enterprise (IEEE 802.1X)

A utilização do modo *Enterprise*, o padrão 802.1X nos fornece uma interface para poder controlar os acessos baseados em portas além de outros recursos. O 802.1X é um protocolo da camada de enlace (modelo OSI), isso acaba prevenindo acessos não autorizados a serviços, como uma rede Wi-Fi. Dentro dessas características é a utilização de servidor RADIUS externo, porque ele tira toda a "responsabilidade" de autenticação das chaves PSK local do AP. (Teixeira, 2017)

O 802.1X são compostos por três componentes principais:

- Suplicante: Essa estação é a do cliente, onde o papel é adotado por um dispositivo que deseja acessar recursos providos pelo Autenticador.
- Autenticador: Aplica o Access Point, onde por um dispositivo que deseja restringir acesso aos recursos, liberando para as redes wireless que possam provar sua identidade.
- Servidor de Autenticação: Servidor da Radius é um dispositivo que realiza a função de autenticação para poder validar a identidade do Suplicante.

Na configuração em que o Suplicante e o Autenticador são alocados no mesmo dispositivo, é possível também posicionar o Autenticador e o Servidor de Autenticação no mesmo equipamento. Entretanto, é necessário ressaltar que essa disposição requer um roteador de maior capacidade para suportar tal configuração. Normalmente numa rede Wi-Fi, o Suplicante é tipicamente uma estação Wi-Fi tentando se conectar a uma infraestrutura, passando pelo Autenticador que vai repassando a comunicação de autenticação recebida pelo Suplicante para o Servidor de Autenticação.

Portando, o Servidor de Autenticação verificar as credenciais do Suplicante que chegaram até ele, em seguida vem o resultado da autenticação, seja com sucesso ou falha e é passado pelo Autenticador. Baseado nesses resultados o acesso é permitido ou negado. (Cisco Systems, 2022)

4.4.6. Acesso baseado em porta

O 802.1X usa o conceito de portas controladas e não controladas tanto para o suplicante quanto para o autenticador. As portas controladas são bloqueadas do tráfego de dados até que o processo de autenticação seja concluído com êxito na porta não controlada. É mais ou menos como uma ACL dinâmica em um roteador Cisco. Protocolo de autenticação *Extensible*

Authentication Protocol (EAP) é usado como base para 802.1X. Uma associação é estabelecida entre o cliente e o ponto de acesso, a autenticação EAP pode ser iniciada pelo suplicante ou pelo ponto de acesso validador. O solicitante pode enviar um pacote "inicial", que causará uma solicitação EAP no Autenticador, mas o Autenticador pode enviar pedidos aos clientes antes mesmo de receberem seus pacotes. Ou seja, qualquer um dos dois pode iniciar o processo. (Cisco Systems, 2022)

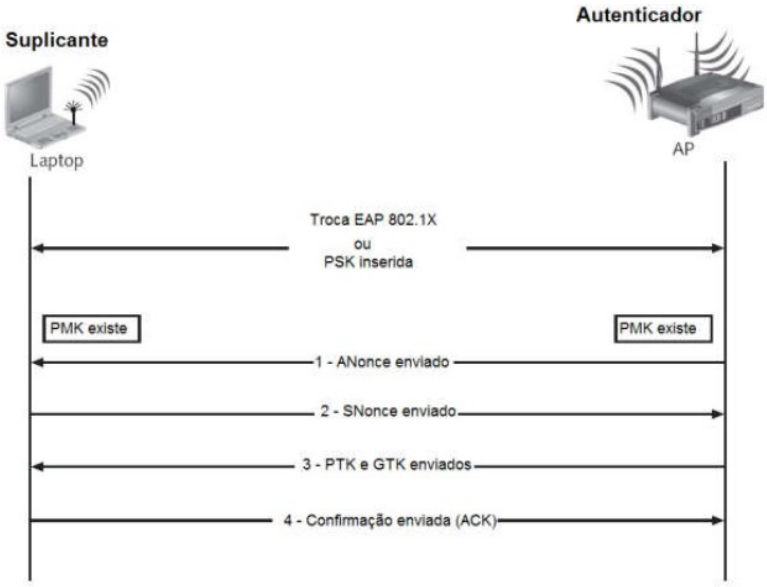
A porta controladora não está autorizada, quando acontece um “aperto de mão” em 4 vias (4-*way handshake*) é usado para poder enviar mensagens para o Suplicante e o Autenticador com os esses objetivos a seguir:

- Confirmar se a “chave mestra” (PMK – *Pairwise Master Key*) foi renovada;
- Auxiliar nas “chaves transientes” (PTKs) que são baseadas na PMK compartilhada;
- Gerar uma “chave temporal do grupo” (GTK – *Group Temporal Key*), caso se for necessário.

Note que no modelo PSK, a autenticação EAP é “pulada” e o processo vai direto para o *handshake*. Chegando no final da via, o Suplicante e o Autenticador já garante a suas identidades mais seguras. A controlado 802.1X entra no estado de autorização, onde os tráfegos de dados regular é permitido e tanto a estação do cliente quanto a AP acabam possuindo chaves simétricas transicionais que serão usadas para criptografar os dados. Na figura 1 mostra como é o funcionamento.

Figura 1 Acesso Baseado em Porta

Fonte: Livro – Wireless_Hacking_MFAA



Toda vez que acontecer a renovação das chaves transicionais que são utilizadas o *handshake* irá ocorrer todas vez quando o AP quer renovar.

4.4.7. Métodos EAP

A autenticação do EAP é conhecida como métodos, eles são as engrenagens da parte de segurança, porque eles fazem a autenticação e a derivação das chaves. Entre esses métodos são os tipos de credenciais que suportam, tipo: Certificados Digitais, Tokens, Usuário / Senha e o uso de chaves públicas e privadas.

O método EAP determinará se a autenticação é mútua ou ela não é suportada, mas, note que qualquer método que define a derivação de chaves deve ser obrigatoriamente suportado autenticação mútua. As comunicações utilizadas pela maioria dos métodos do EAP é o cliente e o servidor. (Cisco Systems, 2022).

4.4.8. Funcionamento do EAP

O EAP foi desenvolvido originalmente para trabalhar com o protocolo *Point-to-Point Protocol* (PPP). Portanto, sua função pode ser entendida como uma evolução desse modelo. Possui quatro tipos básicos de mensagens usados durante a conexão: solicitação, resposta, sucesso e falha.

A primeira etapa na conexão à rede sem fio usada pelo EAP é enviar uma mensagem de solicitação ao ponto de acesso. Isso, por sua vez, retorna uma solicitação para uma identidade de propriedade do solicitante. Após receber a resposta do suplicante, o *Access Point* a envia

diretamente ao servidor RADIUS. Ele então cria um desafio que o solicitante deve passar usando a senha que possui. Portanto, se responder corretamente, terá acesso à rede sem fio; caso contrário, você receberá uma mensagem de falha de conexão. (Cisco Systems, 2022),

Por fim, se o protocolo utilizado para criptografia for WPA ou WPA2, ocorre um acordo entre o solicitante e o ponto de acesso para determinar o valor da chave efêmera que será utilizada durante a comunicação.

4.4.9. EAP_TLS

A autenticação no modelo *Transport Layer Security* (TLS) é usado como Protocolo de Segurança em Nível de Transporte, ela acaba realizando troca inicial de certificados digitais entre cliente e servidor de autenticação da RADIUS, é considerado o método mais seguro disponível. A autenticação mútua é um único elemento adicional, ou seja, baseados na comprovação de autenticação. Quando a RADIUS aceita as credenciais, ele informa ao concentrador que está permitindo ao equipamento o acesso à rede, já que neste caso não há a autenticação do usuário. (Cisco System, 2022)

Veja algumas características de segurança do EAP-TLS:

- Autenticação mutual;
- Criptografia de chaves públicas;
- Negociação segura de cifras;
- Capacidade de gerenciamento de chaves.

4.4.10. Autenticação Mútua e Criptografia de Chaves Públicas

As implementações de EAP-TLS devem suportar TLS v1.0, um protocolo de autenticação baseado em certificado digital. Neste método EAP, os certificados são usados para autenticação de cliente e servidor. Ele associa a identidade "confiável" com uma chave pública. Ele é então usado por outros para criptografar mensagens que serão enviadas ao proprietário da chave pública, que é a única pessoa que possui a chave privada para de criptografar a mensagem. (Cisco System, 2022)

4.4.11. CCMP (AES)

O *Counter Mode with CBC-MAC Protocol* (CCMP) é obrigatório para o WPA2. É o conjunto de iniciais mais bizarras e confusas que existe. O CCMP é totalmente independente

do funcionamento do WEP, diferentemente do WPA, por eles ser diferente é por causa do “Counter Mode”, ele é o modo de operação do AES, que as cifras são utilizadas ao invés da RC4. Ele é considerado atualmente um dos algoritmos de criptografia de bloco de confiança. O componente que provê integridade dos dados e autenticação é o Código de Autenticação de Mensagens de Bloco (CBC-MAC – *Cipher Block Chaining Message Authentication Code*).

A primeira grande diferença é encontrada no PTK: o WPA possui 512 bits, enquanto o WPA2 possui apenas 384 bits, pois utiliza TEK para criptografia e cálculos de MIC (ele "introduz" o algoritmo AES em todas as etapas), o que não inclui Use TMK. Além disso, o vetor de inicialização recebe uma nomenclatura: o número do pacote. Outro ponto importante é o uso de cabeçalhos de quadros nas duas partes principais do protocolo. Por fim, existe um vetor com determinados parâmetros, chamado *Nonce*, que é incrementado cada vez que o bloco AES é passado. (Teixeira, 2017)

Resumindo o contexto:

- Para criptografia: CCMP utiliza o AES;
- Para autenticação e integridade: CCMP usa CBC-MAC.

4.5. Ferramentas para teste

Neste módulo iremos apresentar as ferramentas que serão utilizadas para fazer os testes de invasão na rede sem fio.

4.5.1. Distribuição do Linux a ser utilizada

Os softwares que serão utilizados podem ser com qualquer distribuição do Linux, desde que sejam feitas as devidas adaptações. No entanto, existem distribuições especializadas em testes de invasão (*Penetration Test*). As sugestões que serão feitas para quem for fazer os testes de invasão, usar as ferramentas que serão utilizadas, porque os softwares que iremos precisar já estão pré-instalados. As duas distribuições mais conhecidas é o BackTrack e o Kali Linux.

4.5.2. Kali Linux

A história do Kali Linux começou em 2006 com o lançamento de uma distribuição Linux chamada BackTrack. O BackTrack é uma distribuição baseada no Ubuntu com o mesmo propósito do Kali Linux para ajudar os profissionais de segurança da informação.

Em 2013, a *Offensive Security*, empresa que mantém o Kali Linux, anunciou o fim do suporte ao BackTrack, apresentando o Kali Linux, que, ao contrário do BackTrack, é baseado no Debian. Assim nasceu a distribuição mais popular na área de segurança da informação. Kali é o "sucessor" espiritual do BackTrack. É desenvolvido e mantido pela equipe original da BT. Ele foi criado para ser mais geral, constantemente atualizado e fornecer apenas ferramentas totalmente gratuitas. Tem quase todas as ferramentas BackTrack e algumas outras ferramentas de diferenciação.

Por ser um sistema super avançado, não é qualquer pessoa que está apta a utilizá-lo profissionais especializados se saem muito bem com a interface e os recursos, mas nem sempre os iniciantes terão o mesmo sucesso.

Mas, isso não quer dizer que, após se familiarizar com a ferramenta, não seja possível utilizá-la como aliada em estratégias de segurança em Linux e TI e confiabilidade de dados. Na verdade, é interessante que você se interesse pela área e, caso já goste de desenvolver ou programar e tenha interesse em seguir carreira como hacker ético, você encontrou no Kali Linux o que precisava para começar.

Um dos maiores pontos positivos nessa ferramenta é a possibilidade de obtê-la gratuitamente, ou seja, desfrutar de todos esses recursos sem precisar pagar nada. (Kali Linux, 2022).

5. Trabalhos Similares

A contribuição dos trabalhos para poder realizar essa pesquisa, foi de grande ajuda para obter as informações e poder analisar para poder escrever esse trabalho. Portando citaremos os trabalhos e explicar o que cada um deles proporcionou:

- Ruldofo Kunde Ludtke (Teste de Invasão em Redes Sem Fio 802.11): O trabalho proporcionou para a pesquisa teoria sobre a rede sem fio, ferramentas utilizadas para poder fazer as invasões. As ferramentas utilizadas são o KALI LINUX, configuração de roteador e antenas USB para poder fazer as invasões. Esse teste que o Ruldofo fez foi para invadir as vulnerabilidades da rede sem fio usando *wordlist* e outras configurações de comando que já vem no Kali Linux

- Catharina Daher Teixeira, Mariana de Lacerda Clarim (Estudos de Casos de Tecnologias Sem Fio Utilizadas em Ambientes IOT): O estudo de caso veio de

grande ajuda na parte de fundamentação teórica, onde ele explica sobre a rede sem fio 802.11, as vulnerabilidades que ela tem WEP, WPA, WPA2.

- Marcos Flavio Araújo Assunção (*Wireless Hacking* Ataques e segurança de redes sem fio Wi-Fi): Esse curso ajudou na parte de fundamentação teórica, onde ele explica sobre a rede sem fio 802.11, suas vulnerabilidades dos protocolos de segurança e a ferramentas utilizadas para poder fazer as invasões. As ferramentas que ele utilizou foi o KALI LINUX, configuração de roteador e antenas USB para poder fazer as invasões. Marcos usou ferramentas para poder mostrar que os protocolos de segurança têm vulnerabilidades, usando comando internos e criando *wordlist* para poder fazer os testes de invasão.
- Jeferson Luiz Miranda Ferreira (Segurança de Rede Sem Fio): Esse artigo proporcionou teste de invasão usando a máquina virtual BACKTRACK para poder fazer teste de invasão. Usando o programa "*Gerix wifi cracker*" para poder fazer as buscas de alcance dos Access Point dos vizinhos e conectá-los para poder invadir a rede deles.

6. Metodologia

Foram realizadas pesquisas de vulnerabilidades nos protocolos de segurança, visando demonstrar as falhas existentes nesses protocolos, que permitem a descoberta de senhas e o acesso não autorizado ao Access Point. Foi montada uma máquina virtual com 2gb de memória-ram, com 2 núcleos do processor i7-10700F, 256 GB de HD utilizando o sistema operacional Kali Linux, juntamente com uma antena USB atacante TP-Link TL-WN722N e um roteador D-Link modelo DIR-610 para realizar as configurações e apresentar as invasões realizadas.

Dentre os vários tipos de invasões possíveis, foram escolhidas as mais simples e menos complexas, porém ainda demandando um tempo considerável. Essas invasões foram realizadas utilizando *wordlists*, ataques de criptografia e ataques de autenticação.

Para embasar essa abordagem, foram realizadas pesquisas focadas nas vulnerabilidades, utilizando artigos, trabalhos de graduação (TG) e vídeos como referência para auxiliar nas invasões. Além disso, foram utilizados recursos disponíveis em sites direcionados à marca Kali Linux e invasões de redes sem fio.

Essa abordagem foi embasada em pesquisas para a obtenção de comandos para testes de invasão, configurações do Kali Linux e utilização de sites para a geração de *wordlists* para

criação de senhas. As amostras coletadas consistem nos comandos de invasão mais aprofundados, utilizados nos testes, e em sites e vídeos utilizados como recursos auxiliares.

A análise será realizada após a conclusão dos testes de invasão, com o intuito de identificar os pontos vulneráveis desses protocolos de segurança, conforme mencionado anteriormente. Foram realizadas pesquisas para obter os comandos necessários para descobrir as vulnerabilidades dos protocolos de segurança.

Com base nos testes realizados e na exposição das vulnerabilidades presentes nos protocolos de segurança, empresas e fabricantes poderão reavaliar suas medidas de segurança e implementar métodos para solucionar esses problemas. Foram utilizadas máquinas virtuais para instalar o sistema operacional Kali Linux, antenas especializadas para realizar as invasões e um Access Point para realizar as configurações e demonstrar as falhas de segurança nos protocolos.

7. Desenvolvimentos

7.1. Ferramentas utilizadas para teste de invasão

Nesta etapa foi usada a máquina virtual para poder fazer as invasões com o sistema operacional KALI LINUX, utilização da antena para poder ter acessos aos dados que vão ser configurado no Access Point.

7.2. Vulnerabilidades do WEP

Nessa etapa, serão descritas as vulnerabilidades e os mais frequentes métodos de ataque utilizados contra a WEP (*Wired Equivalent Privacy*). Abordamos alguns problemas no capítulo 4, mas agora vamos demostrar na prática alguns métodos de exploração de cada um deles.

Primeiro, vamos dividir os ataques a WEP em dois tipos:

- Ataque à criptografia WEP;
- Ataque à autenticação WEP.

O primeiro ataque visa obter a *passphrase* (“senha”) utilizada para gerar chaves criptográfica WEP. Já o segundo ataque utiliza-se técnicas para conseguir se autenticar ao Access Point, mesmo que a *passphrase* não seja conhecida.

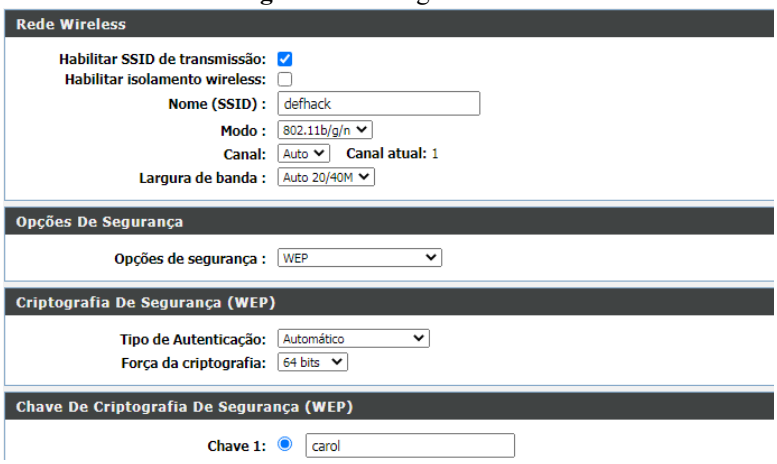
Agora vai ser iniciado a criptografia do WEP, mas antes disso vão ser feito a configuração do Access Point para o teste que será realizado.

7.2.1. Preparando o Access Point para os testes WEP

Serão configurado o Access Point colocando o tipo de criptografia como WEP.

Veja na figura 2 abaixo:

Figura 2 - Configurando Access Point



Será criado uma rede SSID como defhack. A criptografia utilizada pode ser tanto de 64 quando 128 bits. O exemplo que estou fazendo, estou configurando a passphrase “carol” utilizando uma chave de 64 bits.

7.2.2. Ataques à Criptografia WEP

As chaves que são utilizadas pelo WEP não são trocadas com o tempo, isso acontece apenas no Dynamic WEP, mas não é um método realmente eficiente. Isso acaba permitindo que os atacantes farejam uma rede com WEP, e se ele obtiver o número máximo de IVs (Vetores de Inicialização) capturados, a passphrase pode ser deduzida pelo aircrack-ng através do processo de criptoanálise.

7.2.3. Monitorando as Redes WEP com o Airodump-ng

Vamos começar inicializando o airodump-ng para verificar todas as redes WEP que podemos visualizar. A opção -c define o canal para 6, mas você pode omiti-la caso queira visualizar todos os canais.

Veja na figura 3 abaixo:

Figura 3 Airodump-ng

```
root@bt:~# airodump-ng mon0 -c 6 --encrypt WEP
```

Digitando o comando e percebemos que podemos visualizar uma rede com o SSID defhack, que foi a rede configurada no Access Point. Além disso, ela traz informações bem úteis sobre esta rede. O BSSID do AP, o número de beacons e frames enviados/recebidos e olhando para a parte inferior a figura 4, vamos observar que uma estação cliente MAC C4:85:08:3A:0D:D6 está tentando se associar à rede defhack (probing), mas ainda não conseguiu realizar essa associação *(not associateed)*.

Figura 4 Visualizar a Rede defhack

```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F0:7D:68:E3:AD:58  -59 100      246      461   11   6  54e. WEP  WEP         defhack

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   C4:85:08:3A:0D:D6  -43    0 -12      0       14  defhack
```

O próximo passo que vamos fazer é configurando o adaptador mon0 para o canal 6 porque, primeiramente não é possível injetar pacotes em nenhuma rede a menos que o adaptador mon0 esteja configurado para o mesmo canal, então iremos usar o comando **iwconfig mon0 channel 6:**

Veja na figura 5 abaixo:

Figura 5 Configurando adaptador

```
root@bt:~# iwconfig mon0 channel 6
root@bt:~# iwconfig mon0
mon0      IEEE 802.11bgn  Mode:Monitor  Frequency:2.437 GHz  Tx-Power=20 dBm
          Retry  long limit:7   RTS thr=2347 B   Fragment thr:off
          Power Management:on
```

Agora que foi configurado o nosso adaptador, podemos injetar pacotes na rede defhack. Em uma janela, será aberto o comando airodump-ng e será usado a opção **– bssid** (esse comando vamos filtrar o MAC do Access Point) e **– write** (esse comando é para salvar os IVs capturados para o arquivo **WEPquebra** – que pode ter qualquer nome). Então o comando para o airodump utilizando a sintaxe é:

airodump-ng – bssid <MAC do AP> - channel <canal> -- write <arquivo> mon0.

Veja na figura 6 abaixo como ficou o comando:

Figura 6 Executando Airodump

```
root@bt:~# airodump-ng --bssid F0:7D:68:E3:AD:58 --channel 6 --write WEPquebra  mon0
```

Quando foi digitado esse comando, devemos aguardar até que sejam capturados os diversos IVs junto com os frames na coluna #Data. Em torne de 5000 a 10000 IVs são suficientes para quebrar uma chave de 40 bits, e de 20000 a 30000 IVs para uma chave de 104 bits. A figura 7 abaixo mostra que temos 539 frames capturados até agora.

Figura 7 Frames capturados

```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F0:7D:68:E3:AD:58  -73 100      219        539  150   6  54e. WEP  WEP         defhack

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   C4:85:08:3A:0D:D6  -127    0 - 0      0       15  defhack,nerd-cave
```

7.2.4. Injetando Requisições ARP com o Aireplay-ng

Agora precisará aumentar muito o número de frames capturados em #Data para que seja possível a criptoanálise do WEP. O comando aireplay vai ajudar nesse processo por meio da opção – **aireplay (-3).**

Como será inserido o comando, embaixo corresponde a seguintes informações:

- **- aireplay:** que é o tipo de ataque;
- **-b:** que indica qual a bssid do Access Point;
- **-h:** que indica uma estação cliente válida que deve estar associada ao AP (pode ser vista no airodump-ng).

Observação: O airodump-ng deve continuar rodando em outra janela.

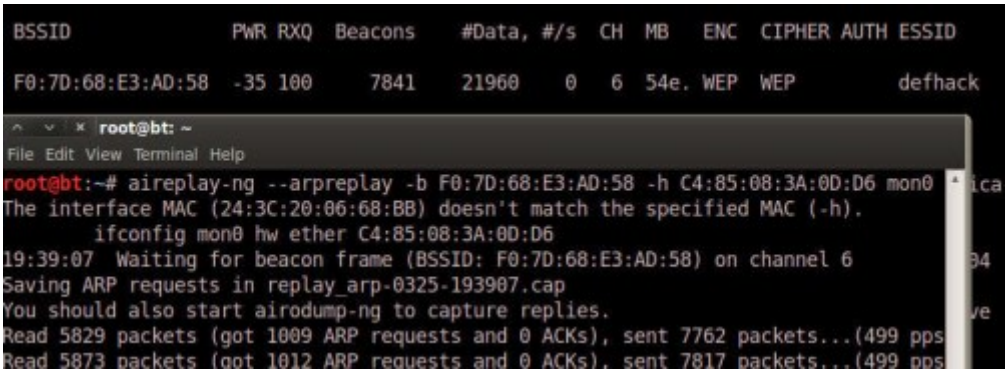
Veja na figura 8 abaixo:

Figura 8 Aumentando os frames

```
root@bt:~# aireplay-ng --arpreplay -b F0:7D:68:E3:AD:58 -h C4:85:08:3A:0D:D6 mon0
```

O que vai acontecer agora quando será executado esse comando é que o aireplay-ng enviará requisições ARP para o AP, que responderá ao cliente, que acaba respondendo de volta, gerando milhares de requisições. Quando o AP acaba gerando uma nova requisição, um novo IV será capturado. Então teremos as seguintes respostas na figura 9:

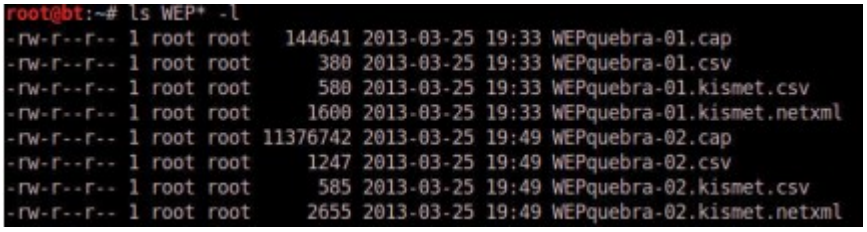
Figura 9 Resultado dos frames



Agora podemos visualizar que o número de frames capturados pelo airodump-ng em #Data já passa dos 20000, isso é mais do que suficiente para decodificarmos a chave. Agora será digitado o comado (ls) para listar os arquivos que foram gerados no teste em que fizemos.

Veja na figura 10 abaixo a listagem dos arquivos:

Figura 10 Listando os arquivos



Como mostrado na figura 10, foram gerados vários arquivos WEPquebra. Os que estão com o número “01” foram gerados na primeira vez que executou o airodump-ng, mas não acabamos aguardando o tempo suficiente para poder capturar muitos IVs. Os arquivos com número “02” são o que fizemos nas últimas execução, na qual conseguimos 20000 IVs.

Esses arquivos WEPquebra-02.cap contêm armazenados os IVs, mas nesses arquivos não tem só os IVs, ele contém os frames de dados que foram capturados e estão contido nesse arquivo. Os outros arquivos que aparece são formatos para serem trabalhados junto ao kismet.

7.2.5. Utilizando Aircrack-ng para Decodificar a Chave WEP

O arquivo WEPquebra-02.cap com o número bem generoso de IVs, vamos utilizar o software aircrack-ng e indicar este arquivo (lembrando que não é necessária nenhuma opção):

aircrack-ng WEPquebra-02.cap

O comando aircrack vai iniciar o processo de criptoanálise dos IVs de 24 bits, e os resultados que vão ser exibidos quando a for concluído.

Veja na figura 11 abaixo:

Figura 11 Arquivo aircrack-ng

A figura 11 contém a chave “carol” que foi descoberta. Mostrando que foi um processo bem simples para poder descobrir a chave.

7.3. Vulnerabilidades do WPA

Neste capítulo, serão abordadas as vulnerabilidades e a realização de ataques contra *Wireless Protected Access (*WPA) na versão 1 e 2.

O teste que será realizado não é tão simples para obter a chave WPA como foi feito no WEP, é isso ocorre por diversos motivos:

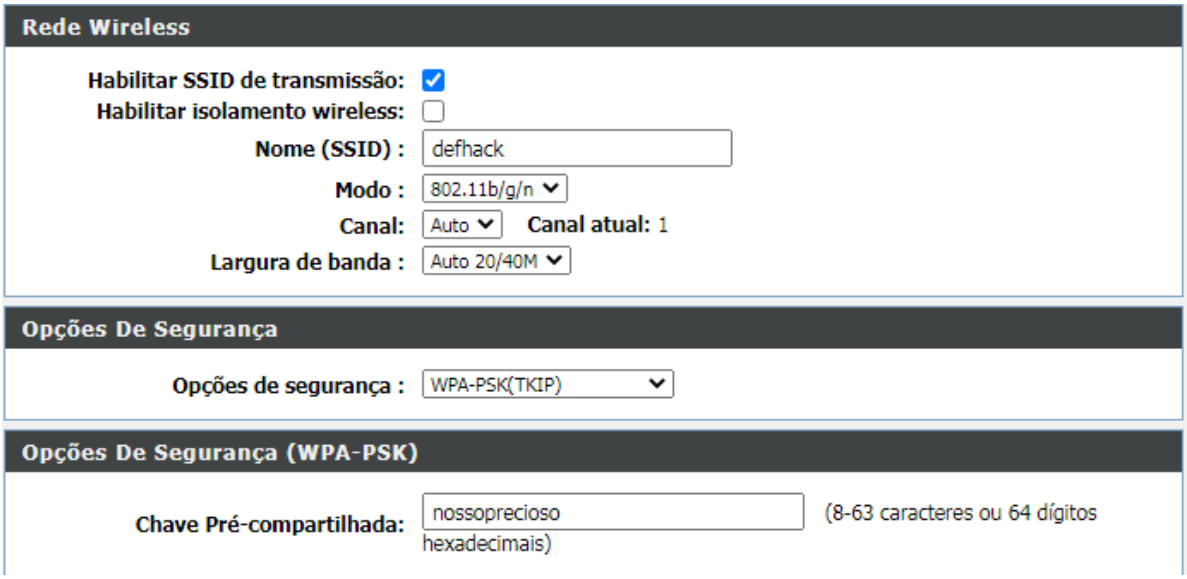
- Algoritmos mais robustos;
- Renovação das chaves;
- Tamanho maior das chaves;
- Chave mestra;
- Handshake em 4 vias.

7.3.1. Configurando ao AP para Teste do WPA

Será configurado o Access Point colocando WPA-PSK ou WPA2-PSK (modo personal). Qualquer uma dessas configurações servirá nos nossos testes (mesmo WPA2 sendo mais difícil para se obter resultados). É irrelevante neste cenário o uso do TKIP ou AES.

Então será feito a configuração, colocando uma Pre-shared key (passphrase) de 13 caracteres como **“nossoprecioso”.** Veja na figura 12 abaixo:

Figura 12 Configuração do AP para WPA



O processo ocorrido anteriormente, é a mesma coisa que será realizado agora, conseguindo visualizar a rede de teste “’defhack” utilizando o airodump-ng. A diferença que foi usado o –encrypt WEP, será utilizado como filtro –encrypt WPA.

Veja logo abaixo o comando que irá digitar e como ficou na figura 13:

airodump-ng -c 6 –encrypt WPA mon0

Figura 13 Airodump WPA

```
root@bt:~# airodump-ng -c 6 --encrypt WPA mon0
```

Digitando o comando, podemos visualizar que encontramos quatro redes no canal 6 com WPA1 ou WPA2. Os clientes não foram mostrados porque eles ainda não são de relevância neste momento, podem perceber na figura 14 logo abaixo.

Figura 14 Encontrando defhack

```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:11:88:BF:1A:70  -38   0        1        1    0   6  54e  WPA  TKIP   PSK  AP-EDUC1
00:11:88:BF:11:B0  -38   0        5       14    0   6  54e  WPA  TKIP   PSK  AP-EDUC2
78:44:76:2C:55:18  -55  58       99        5    0   6  54e  WPA  CCMP   PSK  ADEN
F0:7D:68:E3:AD:58  -38 100      135        0    0   6  54e. WPA  TKIP   PSK  defhack
```

Este processo que vamos fazer, é quase parecido com o ataque de autenticação do WEP. Precisamos monitorar aquela rede WPA específica (defhack) e aguardar que capturemos

o handshake completo em 4 vias. Se conseguimos obter, podemos tentar usar o aircrack-ng e uma worlist (lista de palavras) para descobrir as chaves. Com isso, será feito por partes e fazendo os testes com calma.

Fechando o comando airodump-ng (será aberto para poder visualizarmos todas as redes com WPA) e o será aberto novamente, mas desta vez diferente, filtrando pelo bssid do AP responsável pelo SSID defhack. Salvando o resultado da sessão (-w) para chave WPA.

Veja o comando abaixo e na figura 15:

airodump-ng -c <canal> --bssid <Mac do AP> -w <arrquivo da chabe WPa> mon0

Figura 15 Filtrando pelo BSSID

```
root@bt:~# airodump-ng -c 6 --bssid F0:7D:68:E3:AD:58 -w chaveWPA mon0
```

Neste momento, o uso do Aireplay-ng é necessário para poder realizar os ataques de desautenticação nas estações clientes. Isso é necessário, porque é muito comum capturarmos apenas parte do handshake de 4 vias (o que torna o arquivo de chave praticamente inútil).

7.3.2. Desautenticando Estações com Aireplay-ng

Este processo de desautenticação é bem simples, apesar de ele ser muito usado para simples ataques de Denial of Service (Recusa de Serviço), é extremamente útil para ajudar a capturar o *handshake*. Para poder realizar a desautenticação, observe na figura 16 logo abaixo o comando airodump-ng e veja que foi mostrado duas estações clientes associadas.

Figura 16 Desautenticação

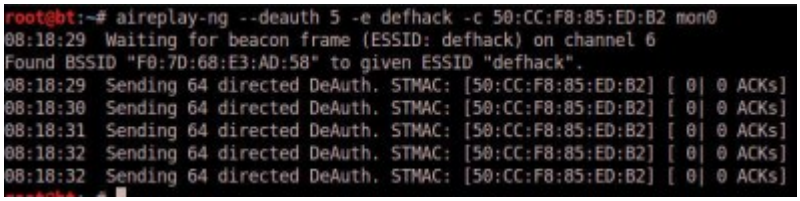
```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F0:7D:68:E3:AD:58  -65   0     5029     1973   25   6  54e. WPA  TKIP   PSK  defhack

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

F0:7D:68:E3:AD:58  50:CC:F8:85:ED:B2  -55    0 - 1   2242      118
F0:7D:68:E3:AD:58  C4:85:08:3A:0D:D6  -127    0 - 0e     3      302
```

Agora será utilizado o endereço MAC da primeira estação (50:CC:F8:85:ED:B2) junto ao aireplay para desautentica-lá. A operação para isso é -deauth juntamente com o argumento do número de tentativas de desautenticação.

Então, será enviado cinco tentativas para o cliente. Portanto, você pode ver abaixo como ficou o comando e mostrado na figura 17:

aireplay-ng –deauth 5 -e <nome da rede> -c <MAC do cliente> mon0

Figura 17 Tentativas para o cliente



No final da linha, prestem atenção na imagem anterior

[0 | 0 ACKs].

Vocês podem perceber que nenhum ACK foi capturado do AP que é o primeiro número e nem na estação do cliente que fica no segundo número. Isso é muito importante, porque para o handshake WPA completo ser capturado, você precisa receber essas ACKs.

Esses problemas podem ocorrer por alguns motivos:

- A estação cliente ou AP está fora de alcance;
- O chipset da placa não permite realizar injeção adequadamente;
- Alguma fonte externa está “matando” o sinal;
- Existe a atuação de um wIPS inteligente.

Por outro lado, pode ser que você consiga obter os ACKs de outra estação do cliente, além daquela que tentamos. Então será repetido o comando e enviado o –deauth para todas as estações conectadas usando a opção -a com o bssid de argumento ao invés de -c e o MAC do cliente. Outra alteração seria que ao invés de 5 tentativas, colocaríamos 0 (zero) para tentativas limitadas.

Veja a sintaxe abaixo e como ficou na figura 18:

aireplay-ng –deauth 0 -a <bssid> mon0

Figura 18 Tentativas para o cliente 2

```
root@bt:~# aireplay-ng --deauth 0 -a F0:7D:68:E3:AD:58 mon0
08:15:39  Waiting for beacon frame (BSSID: F0:7D:68:E3:AD:58) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
08:15:40  Sending DeAuth to broadcast -- BSSID: [F0:7D:68:E3:AD:58]
08:15:40  Sending DeAuth to broadcast -- BSSID: [F0:7D:68:E3:AD:58]
08:15:41  Sending DeAuth to broadcast -- BSSID: [F0:7D:68:E3:AD:58]
08:15:42  Sending DeAuth to broadcast -- BSSID: [F0:7D:68:E3:AD:58]
08:15:42  Sending DeAuth to broadcast -- BSSID: [F0:7D:68:E3:AD:58]
08:15:43  Sending DeAuth to broadcast -- BSSID: [F0:7D:68:E3:AD:58]
08:15:44  Sending DeAuth to broadcast -- BSSID: [F0:7D:68:E3:AD:58]
```

Durante todo esse tempo, a janela com o airdump-ng permaneceu aberta (sempre o aireplay e o airodump em janelas separadas). Após esse tempo, o airodump irá capturar o *handshake* do WPA. Lembrado que aguarda um pouco para que esse *handshake* seja capturado com todas as suas 4 vias para não gerar um arquivo corrompido.

Observe a figura 19 abaixo o handshake:

Figura 19 Handshake

```
                                                ][ WPA handshake: F0:7D:68:E3:AD:58

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F0:7D:68:E3:AD:58   -7  21    31007      327    6   6  54   WPA  TKIP   PSK  defhack

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

F0:7D:68:E3:AD:58  C4:B5:08:3A:0D:D6  -127    1 - 0     67      537
F0:7D:68:E3:AD:58  50:CC:F8:85:ED:B2  -36     1 - 1      0       40
```

Agora que o *handshake* foi capturado, podemos fechar o airodump-ng e se preocuparmos em como descobrir a chave criptografada armazenada no arquivo **chaveWPA.**

7.3.3. Utilizando Aircrack-ng e Wordlists para Descobrir a Chave WPA

Quando estávamos executando os comandos, salva o *handshake* WPA em um arquivo PCAP no disco. A figura 20 logo abaixo vai visualizar o nome do arquivo.

Figura 20 Listando o PCAP

```
root@bt:~# ls -l chave*
-rw-r--r-- 1 root root 792798 2013-03-26 13:13 chaveWPA-01.cap
-rw-r--r-- 1 root root    573 2013-03-26 13:13 chaveWPA-01.csv
-rw-r--r-- 1 root root    586 2013-03-26 13:13 chaveWPA-01.kismet.csv
-rw-r--r-- 1 root root   3690 2013-03-26 13:13 chaveWPA-01.kismet.netxml
```

Utilizando o comando aircrack junto com o WEP, o processo foi bem simples, fazendo a criptoanálise dos vetores de inicialização (IVs) levando à dedução da chave. Agora no WPA, isso não é possível, então iremos contar com um pouco da sorte. Iremos descobrir a chave WPA, fazendo ataques de força bruta com o uso de uma wordlist (dicionário).

A wordlist é uma lista de palavras que serão testadas e comparadas uma a uma para ver se a passphrase é descoberta.

7.3.4. Criando e Preparando a Wordlist

Existem várias possibilidades para você criar sua *wordlist*. Existem vários programas que podem ser utilizados para esse fim, cada vez que sua lista for maior, aumentam as chances de se descobrir a chave WPA. Outra maneira é que você pode utilizar a lista de palavras que em com as distribuições Kali Linux (/pentest/passwords/wordlist).

Outra sugestão interessante pode fazer é acessar o site <pastebin.com>. Senhas de facebook, twitter ou gmail que são vazadas acabam indo para esse site. Recolher esses arquivos com essas senhas misturada com lista do tipo" as 500 senhas utilizadas" ajudam a formar uma boa *worlist*.

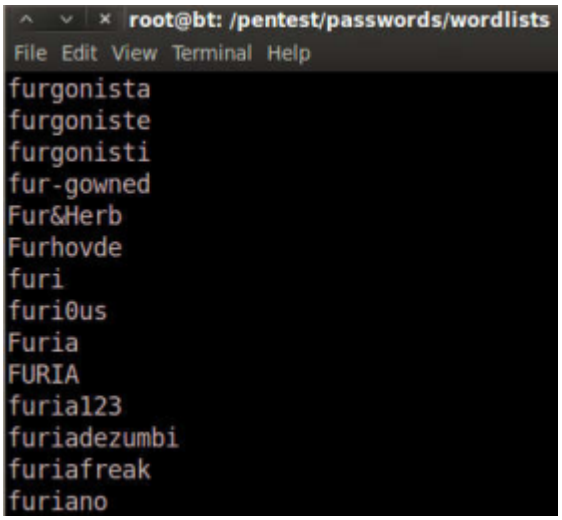
Mas, temos um, porém. Ao juntarmos muitos arquivos de texto, haverá muitas palavras repetidas e a sequência alfabética estará toda bagunçada. Para evitar que isso aconteça, podemos usar os comandos do Linux, por exemplo, **sort** (para ordenar as palavras) e **uniq -u** (para remover as palavras duplicadas). Veja a figura 21 logo abaixo.

Figura 21 Wordlist

Incluindo o comando **"> final.text"**, enviei o conteúdo filtrado para um arquivo.

Como vocês viram a worlist com mais de 260 MB que será criado, só "juntando pedaços" no pastebim, acabei sendo chamado de "wordlist-definitiva.txt". A seguir na figura 22, um trecho da wordlist abaixo:

Figura 22 Trecho da Wordlist



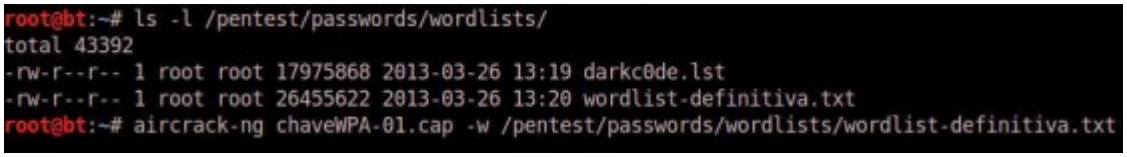
7.3.5. Usando a Wordlist Personalizada

Então será utilizado a *wordlist* para tentar descobrir a passphrase por trás da chave WPA que foi capturada. A sintaxe do aircrack-ng é ligeiramente diferente do que usando com o WEP:

aircrack-ng <chaveWPA> -w <wordlist>

Veja a figura 23 logo abaixo:

Figura 23 Usando a wordlist para achar passphrase



Para este teste, será incluído a pre-shred key da minha rede defhack no meio dos dois arquivos de wordlist que estão na figura anterior. Primeiramente, será utilizada a worlist-definitiva.txt e em seguida, vamos trabalhar com o darkc0de.lst junto com a compatty.

Esse processo do aircrack-ng, quando ele é realizado puro, leva muito tempo para testar todas as palavras da *wordlist*. Isso se deve ao fato de que ele precisa constantemente realizar o cálculo das chaves mestras (PMK) e transiente (PTK) antes de testar a *passphrase*. Essa demora leva aproximadamente uns 20 minutos para testar metade da *wordlist* e encontrar a chave.

Veja na figura 24 logo abaixo:

Figura 24 Chave encontrada

Pronto, a chave foi encontrada, mas nem sempre vai ser assim tão fácil, especialmente quando a wordlist ou a chave forem muito grandes.

7.3.6. Pré-computando Worlists com o Genpmk

O Utilitário genpmk permite pré-computar todos os cálculos necessários para as chaves PMK e PTL, gerando arquivos que podem ser necessários pelo cowpatty ou pelo piryt para realizar a força bruta do keystream.

Sintaxe: genpmk <opções> <arfquivo(s)>

Opções:

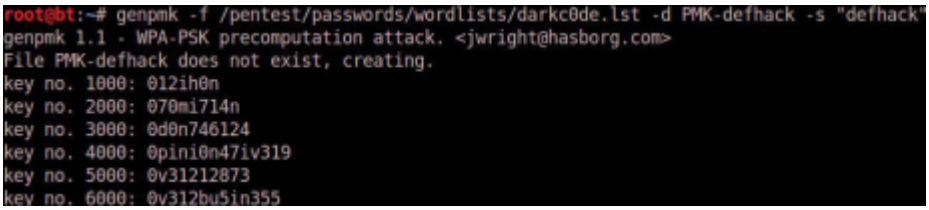
- **-h:** Ajuda;
- **-f:** Arquivo de dicionário;
- **-d:** Arquivo de saída;
- **-s:** SSID da Rede;
- **-v:** Mostrar mais informações (Verbose).

Para utilizar o comando básico é bem simples:

genpmk -f <wordlist> -d <arquivo PMK de saída> -s <nome da rede>

Veja na figura 25 logo abaixo que utilizei a wordlist **darkc0de.lst** para gerar o arquivo **PMK-defhack**.

Figura 25 Wordlist pré-computada



O genpmk leva um tempo para pré-computar todas as palavras da wordlist, mais vale a pena porque ela ajuda muito.

7.3.7. Usando wordlists Pré-computada ou Rainbow Tables com Cowpatty

O cowpatty é um aplicativo de implementação muito útil força bruta. Ele oferece suporte a vários formatos e métodos de força bruta, como o uso de tabelas arco-íris (bem, as tabelas arco-íris parecem melhores) e Listas de palavras pré-computadas geradas por genpmk. Tudo isso é para acelerar o processo de descoberta de chaves. Uma mesa arco-íris é uma "mesa" gigante que contém milhões de senhas e seus equivalentes "criptografados". Eles só funcionam com WPA1.

Ideias de mesa arco-íris está mudando a quantidade de tempo que você gasta tentando uma lista de palavras comuns Através da memória HD. Quanto mais HD você ocupa em sua área de trabalho, levará menos tempo.

Outro problema com as Rainbow Tables é que, como elas são “pré-preparadas por padrão, eles se aplicam apenas a SSIDs específicos. Por exemplo, uma tabela Rainbow de 10 GB feita para SSID linksys não funcionará em um switch de rede com SSID dlink. muitos sites fornecem 100 sementes de tabelas de arco-íris com a maioria dos SSIDs usados.

Agora confere a sintaxe do cowpatty:

cowpatty <opções> <arquivo(s)>

Opções:

- **-f:** arquivo de dicionário;
- **-d:** Arquivo hash do genpmk;
- **-r:** Arquivo com pacotes capturados;

- **-s:** SSID da rede;
- **-2:** Usa frames 1 e 2 ou 2 e 3 para ataque às chaves;
- **-c:** Checa se o 4-way hanshake do frame está pk. Não realiza quebra;
- **-v:** Modo verbose (ostra mais informações);
- **-h:** Mostra a ajuda.

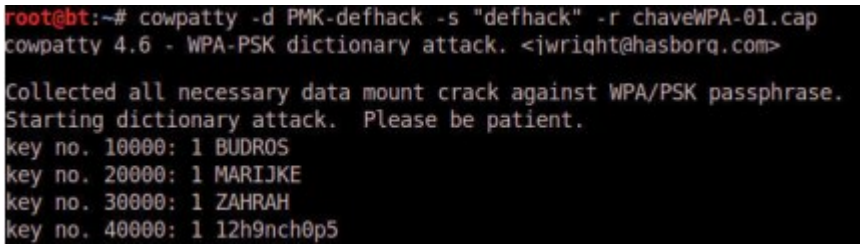
Veja o exemplo abaixo da sintaxe:

Coypatty -d <arquivo PMK> -s <SSID> -r <arquivo PCAP>

Agora podemos focar em usar o arquivo pré-computado gerado pelo genpmk, no exemplo abaixo é o "PMK-defhack".

Observe a execução abaixo do cowpatty:

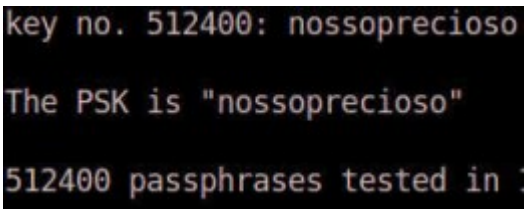
Figura 26 Cowpatty



Podemos visualizar que o arquivo PMK-defhack foi realmente gerado com sucesso, pois todas as passphrases mostradas na figura 26 anterior vieram do arquivo darkc0de.lst.

Veja na figura 27 abaixo:

Figura 27 Resultado Final



Também, além de usar o cowpatty poderíamos ter utilizado o pyrit. A maior vantagem do pyrit sobre o cowpatty é possuir um modo de funcionamento interessante, permitindo atuar como um "cluster" usando processamento de diferentes computadores em rede para auxiliar no processo de "quebra". Os softwares estão disponíveis no Kali Linux.

8. Resultados e Discussões

O presente trabalho proporcionou resultado as vulnerabilidades dos protocolos de segurança da rede sem fio, usando comandos para poder fazer as quebras das senhas, descobrindo as passphrase, usando wordlist para poder fazer comparações se realmente encontra a passphrase. Algumas vulnerabilidades não foram possíveis demostrar por causa que não conseguimos atingir os objetivos, por conta de ser mais complexos do que foi mostrando anteriormente.

Em situações em que se evidenciam vulnerabilidades, é preocupante constatar que algumas distribuidoras continuam disponibilizando protocolos de segurança mais frágeis, sem efetuar melhorias nos métodos de proteção associados a esses protocolos. As demonstrações apresentadas neste trabalho podem contribuir para fortalecer as marcas ou distribuidoras que fornecem esses dispositivos, a fim de reforçar a segurança. Além disso, é importante considerar não apenas a ênfase na segurança do dispositivo em si, mas também informar os profissionais responsáveis pela configuração dos equipamentos, para que possam aprimorar os métodos de segurança disponíveis.

9. Conclusão

O presente estudo teve como objetivo apresentar conceitos de tecnologias em redes sem fio, bem como explorar alguns dos padrões atualmente adotados, com ênfase nos protocolos de segurança. Foi destacado que, mesmo em padrões mais recentes, ainda persistem diversas vulnerabilidades que podem comprometer a segurança dessas redes.

Foi evidenciado que o uso de protocolos de segurança robustos não é suficiente se não forem empregadas práticas corretas, como a escolha de senhas fortes. Dispositivos que não adotam as devidas medidas de segurança podem se tornar alvos fáceis para invasores. Nesse contexto, o protocolo WEP foi mencionado como exemplo de uma opção insegura que ainda é disponibilizada por alguns fabricantes, apesar das suas conhecidas falhas de segurança. Por outro lado, o protocolo WPA foi considerado mais robusto, porém também apresenta vulnerabilidades.

O trabalho demonstrou que os ataques às redes sem fio podem ocorrer de várias formas, incluindo ataques de dicionário e a utilização de programas específicos, como aqueles disponíveis na distribuição Kali Linux. Além disso, ressaltou-se que a eficácia desses ataques está diretamente relacionada ao poder computacional da máquina utilizada. Portanto, é recomendado utilizar dispositivos mais potentes para realizar invasões com maior eficiência.

Conclui-se, portanto, que a segurança das redes sem fio é um desafio contínuo, mesmo com a adoção de protocolos mais avançados. É essencial que os usuários estejam cientes das vulnerabilidades existentes e adotem práticas adequadas para proteger suas redes, como o uso de senhas complexas, atualizações regulares de firmware e a configuração correta dos dispositivos. Além disso, é fundamental que os fabricantes ofereçam suporte e atualizações de segurança contínuas para garantir a proteção dos usuários.

Agradecimentos

Quero agradecer primeiramente a Deus, agradecimento a todos os professores que tiraram seu tempo para poder me ajudar e tirar dúvidas, agradecimento para o meu orientador professor Viana e meu coorientador Walter por seus ensinamentos e dedicar todo o seu tempo ao projeto, agradecer a minha família por ter me apoiado em minhas decisões e me apoiando para que eu tenha um futuro melhor.

Referências

ASSUNÇÃO, Marcos flavio araujo. Tecnicas de Invasão Rede sem fio: Wi Fi Hacking. *In*: **Wireless Hacking:** Ataques e segurança de redes sem fio Wi-Fi. Udemy: André Henrique do Santos, 10 out. 2021. Disponível em: https://www.udemy.com/course/tecnicas-de-invasao-em-redes-sem-fios-wi-fi-hacking/. Acesso em: 20 maio 2022.

Cisco Systems. Site da Cisco. Disponível em: https://www.cisco.com. Acesso em: 15 set. 2022.

FERREIRA, Jeferson Luiz Miranda Segurança em Redes sem Fio. 2013. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

IEEE Advancing Tchnology for Humanity. Disponível em:< https://www.ieee.org.br/organizacao/> Acesso em: 14. novembro.2022.

KALI LINUX. What is Kali Linux? Disponível em: https://www.kali.org/docs/introduction/what-is-kali-linux/. Acesso em: 23 ago. 2022.

LERNER, Sandy. **Introdução às Redes**. San José, Calofórnia, 22 jun. 2016. Disponível em: www.netacad.com. Acesso em: 9 ago. 2022.

LUDTKE, Rudolfo Kunde. **Teste de Invasão em Redes Sem Fio 802.11**. Orientador: Prof. Dr. Murilo Cervi. 2015. Tecnologia em Redes de Computadores (Ensino Superior) - Universidade Federal de Santa Maria, Santa Maria, 2015.

O Modelo OSI. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_modelo_osi.php>. Acesso em 09/10/2022.

Pacote de Dados RADIUS. Disponível em:<http://www.gta.ufrj.br/grad/08_1/radius/PacotededadosRADIUS.html>. Acesso em: 21/04/2023.

PAIM, R. R. WEP, WPA e EAP, 2015. Disponível em: <http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/wep.html>. Acesso em: 16 de outubro. 2022.

Práticas de Segurança para Administradores de Redes Internet. Disponível em: <http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html>. Acesso em: 02/04/2023.

Roteamento IP. Disponível em:<http://technet.microsoft.com/ptbr/library/cc785246(WS.10).aspx>. Acesso em:18/10/2022.

RUFINO, Nelson Murilo de Oliveira. Segurança em Redes sem Fio. 4ª Ed. Editora

TANENBAUM, A. S; WETHERALL, D: Redes de Computadores. 5ª Ed., Editora Pearson Education Inc, São Paulo, 2011.

TEXEIRA, CLARIM, Cathatina, Mariana. **Estudos das vulnerabilidades de tecnologia sem fio utilizadas em ambientes IOT**. 2017. Trabalho de Graduação (Ensino Superior) - Faculdade de Tecnologia, Universidade de Brasilia, Brasília, 2017.