FACULDADE E ESCOLA TÉCNICA ALCIDES MAYA
CURSO TECNOLÓGICO EM REDES DE COMPUTADORES

ALESSANDRO ARANHA DELFINO JUNIOR

Vulnerabilidade do Protocolo WPA:
Com Senhas padrões em Ambiente Doméstico.

Porto Alegre
2020

Alessandro Aranha Delfino Junior[1]

Vulnerabilidade do Protocolo WPA:
Com Senhas padrões em Ambiente Doméstico.

Projeto de Pesquisa apresentado como requisito parcial para obtenção do título de Tecnólogo em Redes de Computadores, pelo Curso de Redes da Faculdade e Escola Técnica Alcides Maya.

Orientador: Prof. Me. Fagner Coin Pereira

coorientador Prof. Me. João Padilha Moreira

Porto Alegre

2020

[1] Acadêmico do Curso Superior de Redes de Computadores – email: a.aranhajunior@gmail.com

RESUMO

A utilização da tecnologia wireless é parte do cotidiano tanto de empresas quanto em residências. Arquivos sigilosos e pessoais trafegam nestas redes o tempo todo. Existem protocolos extremamente vulneráveis a ataques, estes ainda são usados, e protocolos mais seguros, por vezes, são utilizados de forma errada deixando margem a ataques conhecidos como no caso de ataques com força bruta usando dicionário de palavras. Esse projeto tem como objetivo o aprendizado sobre redes sem fio, bem como conhecer suas principais fragilidades e formas de se prevenir a um ataque. Neste trabalho demonstraremos fragilidade do protocolo wpa (*wi-fi protected access*) em redes domésticas, vulnerabilidades das senhas padrões dos roteadores, ferramentas em software livre usadas nos ataques, demonstrando técnica de ataque de força bruta em roteadores, dicas de como se prevenir a esses ataques, identificar se apenas a segurança pré-definida nos roteadores são suficientes e quais são suas vulnerabilidades, gerando assim um relatório com o objetivo de trazer uma noção dos riscos que os usuários de uma rede doméstica estão correndo e o que ele pode fazer para prevenir-se, com resultados dos testes de ataque e considerações finais em relação a introdução e as conclusões dos testes.

Palavras-chave: Tecnologia. Wireless. Residências. Protocolos. Vulneráveis. Seguros. Fragilidade. Roteadores. Prevenir. Ataques. Monitoramento

Foi realizado um método de pesquisa misto e exploratório, onde é apresentado os conceitos do Wi-Fi e sua segurança, um software livre que contém ferramentas de intrusão à redes sem fio, é visto de forma prática a utilização dos conceitos realizando a invasão e quebra de senha de um roteador com a técnica de força bruta, após a pratica é demostrado como evitar a invasão e um procedimento de acessar a rede de forma mais segura, ao final é exibido o resultado de um questionário de uma pesquisa realizada ao decorrer desse projeto sobre alteração da senha de autenticação do acesso ao Wi-Fi e do roteador onde podemos verificar que existem redes configuradas de forma padrão. 33

- Conceituar Wi-Fi e suas ferramentas de segurança; 33
- Entender a ferramenta utilizada e as formas de invasão; 33
- Implantação da ferramenta Kali linux; 33

ABSTRACT

The use of wireless technology is part of the daily life of both companies and homes. Confidential and personal files travel on these networks or at all times. There are protocols that are extremely vulnerable to attacks, these are still used, and safer protocols are sometimes used in the wrong way, leaving room for attacks related to force attacks using the word dictionary. This project aims to learn about wireless networks, as well as to know their main weaknesses and ways to prevent an attack. In this work, a fragment of the WPA protocol is demonstrated in home networks, vulnerabilities in router standards, software tools used freely in attacks, technical demonstration of brute force attack on rotators, tips on how to prevent these attacks, and monitor the network, identify yourself only as pre-activated security on routers that are vulnerable and what their vulnerabilities are, generating a report with the objective of generating a sense of the risks that the user of a home network is running and what he can do to prevent, with results of the attack tests and final considerations regarding the introduction and conclusions of the tests.

Key words: Technology. Wireless. Residences. Protocols. Vulnerable. Insurance. Fragility. Routers. To prevent. Attacks. Monitoring.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AES - *Advanced Encryption Standard*
AES - *Advanced Encryptation Sytem*
BSSID - *Identify Access Points and Their Clients*
Ddos - *Distributed Denial of Service*
DHCP - *Dynamic Host Configuration Protocol*
EAP - *Extensible Authentication Protocol*
ESSID - *Extended Service Set Identifier*
FMS - *Fluhrer, Mantin and Shamir attack*
FSF - *Free Software Foundation*
GHz - *Gigahertz*
GNU - *GNU's Not Unix*
IEEE - *Instituto de Engenheiros Eletricistas e Eletrônicos*
KB/s - *Kilo Bytes*
LDAP - *Lightweight Directory Access*
MAC - *Media Access Control*
MB - *Megabyte*
Mbps - *Megabits*
MIC - *Message Integrity Check*
PTW - *Pyshkin, Tews, Weinmann*
RADIUS - *Remote Authenticantion Dial-in User Service*
RFID - *Radio-Frequency IDentification*
RFMON - *Radio Frequency MONitor*
RSN - *Robust Security Network*
TKIP - *Temporal Key Integrity Protocol*
WEP - *Wired Equivalent Privacy*
Wi-Fi - *wireless fidelity*
WiMax - *Worldwide Interoperability for Microwave Access*
WPA - *Wi-Fi Protected Access*
WLAN - *wireless local área network*
WPA-PSK - *Wi-Fi Protected Access - Pre-Shared Key*
WWiSE - *World Wide Spectrum Efficiency*
ZigBee - *ZigBee Alliance*

SUMÁRIO

1. INTRODUÇÃO

Quando se fala em segurança da informação, é sempre importante lembrar que essa abrange um conjunto de medidas que envolve, entre outros fatores, os procedimentos técnicos. Temos algumas dessas medidas cautelares a de classificação de material, descarte de documentos, cópias de segurança, educação do usuário, princípios éticos dos administradores, segurança física, políticas de segurança, entre outros itens. Os temas que serão aqui tratados correspondem apenas a uma pequena parte da segurança da informação, que, por consequência, procura analisar e resolver apenas a parte técnica da questão.

Rede sem fio ainda é algo novo na vida de algumas pessoas, e diferentemente das redes cabeadas, sobre as quais era necessário conhecimento técnico um pouco mais específico, a montagem e a instalação de redes Wi-Fi é absolutamente factível por um usuário iniciante. Por tanto, toda essa simplicidade de instalação tem feito com que muitas redes sem fio (caseira ou não) sejam montadas com padrões de fábrica, ou seja, completamente vulneráveis a inúmeros tipos de ataque.

O objetivo principal deste projeto é proporcionar ao leitor uma visão abrangente das características e peculiaridades de redes sem fio (notadamente tecnologia Wi-fi), mas também permitir entendimentos das vulnerabilidades comuns associadas à tecnologia, de seus riscos e das possibilidades de uso com mais segurança.

O projeto também é composto por tópicos, nos quais são apresentados conceitos de rede sem fio, seguidos de riscos inerentes à modalidade e propostas de soluções. Tais informações permitem entender o universo das redes sem fio, consolidando a parte teórica e conceitual antes de abordar aspectos técnicos, em que a base conceitual será requerida.

Inúmeras tecnologias estão incluídas na categoria de redes sem fio. Nas quais essas categorias estão relacionadas desde redes simples como infravermelho, em que normalmente podem fazer parte apenas dois dispositivos, e esses, em geral devem estar um em frente ao outro, passando por tecnologias mais recentes, como Bluetooth, WiMax, 4G, RFID e ZigBee. Entretanto a ênfase desse

projeto recairá sempre nas relacionadas com o padrão 802.11 (conhecido genericamente como Wi-Fi).

1.2 Problema

Roteadores são por padrões, configurados de forma para ter o desempenho satisfatório para o usuário final contratante do serviço, o que se torna um problema devido ao padrão pré-configurado, com senhas fracas e configurações que permitem o fácil acesso, onde esses estão disponíveis na internet.

1.3 Delimitações do Trabalho

Este projeto delimitou-se em demonstrar a falha de segurança de um roteador configurado por padrão pela operadora sem nunca ter feito quaisquer alterações no nome de rede e senha de acesso, para demonstrar a falha é utilizado o Kali Linux uma distribuição GNU/Linux baseada no Debian, o mesmo dispõe de numerosos softwares pré-instalados porem é utilizado apenas os softwares necessários para um ataque de força bruta, após a teoria e a prática poderemos ver métodos para evitar uma possível invasão, ao final está disponível uma pesquisa realizada com 344 pessoas que aponta um resultado positivo sobre a alteração das configurações do roteador onde podemos ver que a grande maioria troca a senha do seu Wi-Fi.

1.4 Objetivo Geral

O projeto consiste em identificar a vulnerabilidade em redes wireless com a utilização de ferramentas que quebram a segurança de um equipamento sem ter autorização para acessá-lo, o que acaba tornando a rede não cabeada vulnerável a um ataque, e ter suas informações contidas nelas facilmente capturadas.

1.4.1 Objetivos Específicos

- Conceituar redes Wi-Fi.
- Determinar os mecanismos de segurança presentes em roteadores
- Apresentar ferramentas e a forma de um ataque a rede sem fio.
- Analisar falhas na segurança da rede.
- Definir procedimentos para proteger a rede e os dispositivos conectados a ela.

1.5 Justificativa

Nos tempos modernos, não é apenas a conexão da internet nas mãos do invasor, são seus dados particulares, senhas de bancos, fotos pessoais etc.

Desta maneira, esperamos contribuir com o tema apontado, para conscientizar ao uso das redes e a configuração das mesmas adotando novas práticas de uso.

A principal motivação para o desenvolvimento desse trabalho, é a proteção dos dados contidos nas redes domésticas. Podemos afirmar que demonstrar a formas de ataque e apontar os pontos de vulnerabilidade a um ataque, é de fato importante para os usuários de uma determinada rede terem noção de como se proteger ou então de como age um invasor.

Uma pesquisa desenvolvida no ano de 2014 pela empresa Avast Software revela números alarmantes com relação à segurança de redes WLAN domésticas, como mostra a tabela 1, foram avaliados 18.000 domicílios que possuíam redes WLAN (Avast Software, 2014).

2. REVISÃO BIBLIOGRÁFICA

“Praticamente todos os equipamentos saem de fábrica com senhas de administração e endereço IP padrão. Caso estes não sejam trocados, poderão permitir a um atacante que se utilize delas em uma rede-alvo e tenha condições de identificar todas as configurações feitas, podendo até mesmo modificá-las. Essas informações constam em manuais e documentos públicos, portanto qualquer possível atacante pode acessá-las” (RUFINO, 2015).

2.1 Wi-Fi

É utilizada por produtos certificados que pertencem à classe de dispositivos de rede local sem fios baseados no padrão IEEE 802.11. Por causa do relacionamento íntimo com seu padrão de mesmo nome, o termo Wi-Fi é usado frequentemente como sinônimo para a tecnologia IEEE 802.11. O padrão Wi-Fi opera em faixas de frequências que não necessitam de licença para instalação e/ou operação. Para se ter acesso à internet através de rede Wi-Fi, deve-se estar no raio de ação ou área de abrangência de um ponto de acesso ou local público, onde opere rede sem fios e se usar dispositivo móvel, como computador portátil, tablet, PCs com capacidade de comunicação sem fio, deixando o usuário do Wi-Fi bem à vontade em usá-lo em qualquer lugar.

2.2 Fundamentos de rede Wi-Fi

Fatores externos causam muito mais interferências nas redes em fio do que nas redes convencionais. Isso acontece, obviamente, por não existir proteção em relação ao meio por onde as informações trafegam. Nas redes convencionais, os cabos podem se valer de diversos tipos de matérias para a proteção física, isolamento, tanto quanto for qualidade do material, o que ali trafega do resto do ambiente, mas, por outro lado, pode atingir, sem muito esforço, locais de difícil acesso para redes cabeadas. A seguir conceituaremos alguns dos principais elementos que compõem os protocolos das redes sem fio.

2.2.1 Frequências

A frequência 2,4 GHz é utilizada por uma vasta quantidade de equipamentos e serviços, por isso se diz que é poluída ou suja, por ser usada também por aparelhos de telefone sem fio, Bluetooth, forno de micro-ondas, babas eletrônicas e pelos equipamentos dispositivos que se conectam via wireless.

A principal diferença entre as frequências sem fio de 2,4 GHz e 5 GHz diz respeito ao número de dispositivos por frequência. O segundo motivo é que muitos outros aparelhos “roubam” a frequência 2,4 GHz, como os fornos micro-ondas e telefones sem fio. Esses dispositivos criam um ruído que diminui ainda mais a velocidade das redes sem fio. Apesar da frequência de 5 GHz ter alcance menor do que a de 2,4 GHz, ela é capaz de transmitir mais dados por segundo porque é virtualmente livre de interferências.

É possível, por exemplo, ter até 20 dispositivos de rede próximos operando na mesma frequência sem que haja perda de sinal ou velocidade de internet. Além disso, todos os roteadores que operam na frequência de 5 GHz são dual band, ou seja, também operam em 2,4 GHz simultaneamente, permitindo aos dispositivos que ainda não trabalham em 5 GHz também se conectarem. Em todos os aspectos, optar pela frequência de 5 GHz é a melhor opção, pois o usuário terá mais canais e poderá se isolar de outras redes, além de sofrer muito menos interferência.

2.2.2 Identificador do conjunto de serviço (SSID - Service set Identifier)

Esse conjunto de serviços é geralmente personalizável e mais conveniente porque, na maioria das vezes, ele usa a linguagem natural que é o Inglês. O SSID é considerado como um nome único para WLAN uma vez que existem várias WLANs que podem coexistir. Quando o conteúdo do SSID é arbitrário, o campo SSID também será definido como nulo. Este SSID nulo é chamado de SSID wildcard que é considerado como um SSID não broadcast ou SSID oculto. Uma vez que existem várias WLANs que podem coexistir. Se um ícone wireless for clicado, o SSID reconhecido pelo dispositivo será listado.

2.2.2.1 Identificadores do conjunto de serviços básicos (BSSID - Identify Access Points and Their Clients)

Um conjunto de serviços consiste num grupo de dispositivos de rede sem fios que funcionam com os mesmos parâmetros de rede. Os identificadores de conjunto de serviços básicos (BSSID) são usados para descrever seções de uma rede local sem fio ou WLAN. Ele reconhece o ponto de acesso ou roteador porque tem um endereço único que cria a rede sem fio. BSSID identifica os conjuntos de serviços básicos que são etiquetas de 48 bits e estão em conformidade com as convenções MAC-48. Na maioria das vezes ele é associado com o endereço MAC do AP. A informação será enviada no beacon AP mas não pode ser vista por nenhum outro usuário a menos que ele tenha um analisador ou ferramentas. Assim, BSSID é simplesmente o endereço MAC de um ponto de acesso wireless ou também conhecido como WAP.

2.2.2.2 Extended Service Set Identifier (ESSID)

Que também é conhecido como “nome da rede”, é a cadeia que deve ser conhecida tanto pelo concentrador, ou pelo grupo de concentradores que envia sinais com ESSID, é detectado pelos equipamentos na região de abrangência, fazendo com que estes enviem um pedido de conexão.

Quando o ESSID não está presente, ou seja, quando os concentradores enviam seu ESSID de forma gratuita, os clientes tem de conhecer de antemão os ESSIDs dos concentradores disponíveis no ambiente para, então requerer a conexão.

2.2.2.3 Beacon

Concentradores enviam sinais informando sobre sua existência, para que clientes que estejam procurando por uma rede percebam sua presença e estabeleçam corretamente conexão com um determinado concentrador.

A sua principal função é a de avisar todos os clientes de que a rede está ativa, e também sincronizar a transmissão dos dados trafegados no wireless.

2.2.3 Padrões Atuais

O Institute of Electrical and Electronics Enginners (IEEE) formou um grupo de trabalho com o objetivo de definir padrões de uso em redes sem fio. Um desses grupos de trabalho foi denominado 802.11, que une uma série de especificações que basicamente definem como deve ser a comunicação entre um dispositivo cliente e um concentrador ou a comunicação entre dois dispositivos clientes. Ao longo do tempo foram criadas várias extensões, nas quais foram incluídas novas características operacionais e técnicas. O padrão 802.11 original (também conhecido como Wi-Fi), em termos de velocidade de transmissão, prove, no máximo 2 Mbps, trabalhando com a banda de 2,4GHz.

2.2.3.1 Padrão 802.11b

Nas redes 802.11b, a velocidade teórica é de apenas 11 megabits. Como as redes wireless possuem um overhead muito grande, por causa da modulação do sinal, checagem e retransmissão dos dados, as taxas de transferências na prática ficam em torno de 750 KB/s, menos de dois terços do máximo. Conforme o cliente se distancia do ponto de acesso, a taxa de transmissão cai para 5 megabits, 2 megabits e 1 megabit, até que o sinal se perca definitivamente. No Windows você pode utilizar o utilitário que acompanha a placa de rede para verificar a qualidade do sinal em cada parte do ambiente onde a rede deverá estar disponível.

2.2.3.2 Padrão 802.11a

Definido após os padrões 802.11 e 802.11b e tentando resolver os problemas existentes nestes, o 802.11a tem como principal característica o significativo aumento da velocidade para um máximo de 54 Mbps, mas podendo operar em velocidades mais baixas. Outra vantagem deste padrão consiste na quantidade de canais não sobrepostos disponíveis, um total de 12, diferentemente dos três canais

livres disponíveis nos padrões 802.11 e 802.11g, o que permite cobrir uma área maior e mais densamente povoada, em melhores condições que outros padrões.

2.2.3.3 Padrão 802.11.g

Este padrão é mais recente que os comentados anteriormente e equaciona a principal desvantagem do 802.11a, que é utilizar a faixa de 5GHz e não permite interoperação com 802.11b. O fato de 802.11g operar na mesma faixa (2,4 GHz) permite que equipamentos de ambos os padrões (b e g) coexistam no mesmo ambiente, possibilitando assim evolução menos traumática do parque instalado.

2.2.3.4 Padrão 802.11i

Homologado em 2004, diz respeito a mecanismos de autenticação e privacidade e pode ser implementado em vários de seus aspectos aos protocolos existentes. Nele foi definido o padrão RSN (Robust Security Network), que permite meios de comunicações mais seguros que os difundidos atualmente. Está inserido neste padrão o protocolo WPA, que foi desenhado para prover soluções de segurança mais robustas, em relação ao padrão WEP, além do WPA2, que tem por principais características o uso do algoritmo criptográfico AES (Advanced Encryption Standard).

2.2.3.5 Padrão 802.11n

Também conhecido como WWiSE (World Wide Spectrum Efficiency), este padrão tem como foco principal o aumento da velocidade (cerca de 100 a 500 Mbps). Paralelamente, deseja-se aumento da área de cobertura. Em relação aos padrões atuais, há poucas mudanças.

2.2.3.6 Padrão 802.11ac

As principais características das redes 802.11ac são a maior velocidade (1,3Gb/s), utilizar somente a frequência de 5GHz (alguns concentradores permitem compatibilidade com 802.11n na frequência de 2.4 GHz) e melhor qualidade do sinal, o que torna as conexões mais estáveis.

2.2.3.7 Padrão 802.1x

Mesmo não sendo projetado para redes sem fio (por ser definido antes destes padrões), esse padrão tem características que são complementares a essas redes, pois permite autenticação baseada em métodos já consolidados, como o RADIUS (Remote Authenticantion Dial-in User Service), de forma escalável, expansível. Dessa forma é possível promover um único padrão de autenticação, independentemente da tecnologia (vários padrões de redes sem fio, usuários de redes cabeadas, discadas e etc.) manter a base de usuários em um repositório único, quer seja em banco de dados convencional, LDAP ou qualquer outro reconhecido pelo servidor de autenticação.

É importante notar que, para esta infraestrutura funcionar, devem estar interligados por meio de uma rede. A localização física de cada elemento tem pouca importância.

Este padrão pressupõe a presença de um elemento autenticador, geralmente um servidor RADIUS, e um requerente, ou seja, o elemento que requer autenticação, no caso, o equipamento cliente. Essa autenticação é feita antes de qualquer outro serviço de rede estar disponível ao usuário requerente. Este, primeiro solicita autenticação ao autenticador, que verifica em sua base de dados as credenciais apresentadas pelo cliente, e, conforme a validade ou não dessas credenciais (normalmente o binômio usuário/senha) permite ou não o acesso a essas. Uma autenticação bem-sucedida deflagrará todos os outros processos para permitir ao usuário acesso aos recursos da rede, o que pode incluir em receber um endereço cia DHCP.

2.3 Mecanismos de segurança

Os algoritmos de segurança de redes WiFi já passaram por muitas mudanças e melhorias desde a década de 1990 e se tornaram mais seguros e eficazes. Diferentes tipos de protocolos de segurança sem fio foram desenvolvidos para a segurança de redes sem fio domésticas.

Os protocolos de segurança sem fio são WEP, WPA e WPA2, e todos servem ao mesmo propósito, porém, são diferentes entre si.

2.3.1 WEP

Para que se possa ter uma comunicação em uma rede sem fio, basta apenas ter um meio para recepção do sinal, ou seja, uma recepção passiva, diferentemente de uma rede cabeada, que necessita obrigatoriamente de uma conexão física entre os dois componentes de rede. Por esta razão, o protocolo 802.11 oferece uma opção de cifragem de dados, onde o protocolo WEP é sugerido como solução para o problema, que está totalmente disseminado e presente nos produtos que estão dentro dos padrões definidos pela IEEE para redes Wi-Fi (RUFINO, 2005).

2.3.2 WPA (WI-FI PRETECTED ACCESS)

O protocolo WPA também conhecido como WEP2 ou TKIP (Temporal Key Integrity Protocol - protocolo de chave temporária) surgiu para corrigir os problemas de segurança encontrados no WEP, e implementou a autenticação e a cifragem do trabalho que estava sendo desenvolvido em outros padrões baseados no 802.11.

O WPA atua em duas áreas distintas: sua primeira atuação é a substituição total do WEP, ou seja, sua cifragem objetivando a integridade e a privacidade das informações que trafegam na rede. A segunda área de atuação foca diretamente a autenticação do usuário utilizando uma troca de chaves dinâmica, que não era feita pelo WEP e, também, a substituição do vetor de inicialização de 24 bits do WEP

para 48. Para isto o WPA utiliza as definições do padrão 802.1x e o EAP (Extensible Authentication Protocol - Protocolo de Autenticação Extensível).

(RUFINO, 2005, CANSIAN et al., 2004). 22 SILVA (2003) afirma que “O WPA padronizou o uso do Michael, também conhecido como MIC (Message Integrity Check), em substituição ao CRC-32, melhorando a garantia da integridade dos dados em trânsito”. Michael é uma função hash com criptografia chaveada, que produz uma saída de 64 bits. A segurança do Michael baseia-se no fato de que o valor do MIC é cifrado e desconhecido pelo atacante. O método do algoritmo de cifração do WPA é o mesmo utilizado pelo WEP, o RC4.

WPS (Wi-Fi Protected Setup): Existe um padrão de segurança que permite que você acesse a rede wireless sem precisar de uma senha: a tecnologia WPS.O recurso serve para que o usuário possa configurar o mecanismo de segurança WPA de forma mais fácil: apenas inserindo um nome e senha para a rede. Essa configuração é padrão e vem configurada automaticamente de fábrica e é ativada quando você liga o seu aparelho.

2.3.3 WPA/WPA2

Foi Ratificado em meados de 2004 corresponde a versão final do WPA, a diferença entre WPA e WPA2 e que o WPA utiliza o algoritmo RC4 o mesmo sistema de encriptação utilizado na WEB o TKIP (Temporal Key Integrity Protocol), enquanto o WPA2 baseia-se na criptografia AES (Advanced Encryption Standard) mais segura que a TKIP, mas exige mais processamento e algumas placas mais antigas não suportam o WPA2 nem mesmo atualizando a firmware (SILVA, 2012). WPA-PSK (Pre Shared Key) de maneira simples WPA-PSK é uma criptografia forte em que as chaves de criptografia (TKIP) e frequentemente mudada o que garante mais segurança protegendo de ataques hackers, muito utilizado por usuários domésticos. WPA2-PSK e ainda mais seguro que o WPA-PSK onde sua criptografia (AES) e extremamente forte e resistência a ataques, adotado como padrão de criptografia do governo americano.

2.3.4 TKIP (Temporal Key Integrity Protocol)

É um algoritmo de criptografia baseado em chaves que se alteram a cada novo envio de pacotes. Faz uso do algoritmo RC4, da mesma forma que o WEP, mas toma algumas precauções para evitar ataques, no qual a sua principal característica é a frequente mudanças de chaves que garante mais segurança.

2.3.5 AES (Advanced Encryptation Sytem)

É um protocolo de criptografia mais seguro introduzido com o WPA2, não é um padrão desenvolvido especificamente para redes Wi-Fi, é um sério padrão mundial de criptografia que até foi adotado pelo governo dos EUA. Considerado bastante seguro, os principais pontos fracos seriam ataques de força bruta e fraquezas de segurança em outros aspectos do WPA2.

2.4 HandShake

Handshake ou aperto de mão é o processo pelo qual duas ou mais máquinas afirmam que reconheceram umas às outras e estão prontas para iniciar a comunicação, o aperto de mão de 4 vias é o processo de troca de 4 mensagens entre um ponto de acesso (autenticador) e o dispositivo cliente (suplicante) para gerar algumas chaves de criptografia que podem ser usadas para criptografar dados reais enviados pela mídia sem fio

2.5 Modo monitor

Também chamado de Modo de Monitoramento ou modo RFMON, permite que um computador com uma placa com interface de rede wireless realize monitoramento de todo o tráfego recebido da rede wireless. Diferente do modo promíscuo, que também é utilizado para *sniffar* pacote, o modo monitor permite que pacotes sejam capturados sem precisar de associação com um Ponto de Acesso

ou rede Ad-hoc primeiro. Modo monitor cabe apenas às redes wireless, enquanto modo promíscuo pode ser usado em redes cabeadas.

2.6 Softwares Livres

De acordo com Costa e Paulino (2011), “software é a parte interna do computador, aquela que traz os programas e não envolve o equipamento técnico, como monitor e teclado”.

Softwares podem ser definidos como programas, ou uma sequência de instruções escritas para serem interpretadas com o objetivo de executar tarefas específicas, ou a parte lógica do computador. De acordo com Palmieri e Aceti (2014), “a definição de software livre foi criada pela FSF (Free Software Foundation), que diz que todo software livre pode ser usado, copiado, estudado, modificado e redistribuído sem restrição, de acordo com a necessidade de cada usuário”. Todas as ferramentas utilizadas nesse trabalho são softwares livres, começando pelo sistema operacional Debian GNU/Linux, e todos os pacotes e ferramentas que serão descritos a seguir. Um software de código fechado não oferece algumas ferramentas nem a possibilidade de se utilizar algumas técnicas necessárias nesse tipo de prática.

2.6.1 Debian GNU/Linux

Debian (pronúncia: débian) anteriormente chamado de Debian GNU/Linux e hoje apenas de Debian, é um sistema operacional composto inteiramente de software livre. É mantido oficialmente pelo Projeto Debian. O projeto recebe ainda apoio de outros indivíduos e organizações em todo mundo. O grupo distribui ainda núcleos Unix-like, como o Debian GNU/kFreeBSD e o Debian GNU/Hurd. O Debian é especialmente conhecido pelo seu sistema de gestão de pacotes, chamado APT, que permite: atualização relativamente fácil a partir de versões relativamente antigas; instalação quase sem esforço para novos pacotes e remoção limpa de pacotes antigos. Debian vem dos nomes dos seus fundadores, Ian Murdock e de sua esposa, Debra. O projeto Debian é mantido por meio de doações à organização sem fins lucrativos Software in The Public Interest (SPI).

2.6.1.1 Kali Linux

Kali Linux é uma distribuição GNU/Linux baseada no Debian. O projeto apresenta várias melhorias, além de mais aplicativos. É voltado principalmente para auditoria e segurança de computadores em geral. É desenvolvido e mantido pela Offensive Security Ltd. Desde 21 de janeiro de 2016, é uma distribuição "rolling-release".

O Kali Linux dispõe de numerosos softwares pré-instalados, incluindo o Nmap (port scanner), Wireshark (um sniffer), John the Ripper (crackeador de password) e Aircrack-ng (software para testes de segurança em redes sem fios). O sistema pode ser utilizado a partir de um Live CD ou live-usb, além de poder ser instalado como sistema operacional principal. É distribuído em imagens ISO compilados para as arquiteturas x86, x64 e ARM, seguem algumas ferramentas que o acompanham.

2.6.1.3 Airmon-ng

Airmon-ng, este script pode ser usado para ativar o modo de monitor em interfaces sem fio. Também pode ser usado para voltar do modo monitor para o modo gerenciado. Inserir o comando airmon-ng sem parâmetros mostrará o status das interfaces. Ele também pode listar / matar programas que podem interferir na operação da placa sem fio.

2.6.1.4 Airodump-ng

O airodump-ng é usado para captura de pacotes de quadros 802.11 brutos com a intenção de usá-los com o aircrack-ng. Se você tiver um receptor GPS conectado ao computador, o airodump-ng poderá registrar as coordenadas dos pontos de acesso encontrados. Além disso, o airodump-ng grava um arquivo de texto contendo os detalhes de todos os pontos de acesso e clientes vistos.

2.6.1.5 Aircrack-ng

Aircrack-ng é um programa de quebra de chave 802.11 WEP, 802.11i WPA / WPA2 e 802.11w WPA2.

Ele pode recuperar a chave WEP depois que pacotes criptografados suficientes foram capturados com airodump-ng. Esta parte do pacote aircrack-ng determina a chave WEP usando dois métodos fundamentais. O primeiro método é através da abordagem PTW (Pyshkin, Tews, Weinmann). A principal vantagem da abordagem PTW é que são necessários muito poucos pacotes de dados para quebrar a chave WEP. O segundo método é o método FMS / KoreK. O método FMS / KoreK incorpora vários ataques estatísticos para descobrir a chave WEP e utiliza-os em combinação com a força bruta.

Além disso, o programa oferece um método de dicionário para determinar a chave WEP. Para quebrar as chaves pré-compartilhadas WPA / WPA2, para isso uma lista de palavras deve ser usada.

2.6.1.6 Crunch

Crunch é um gerador de lista de palavras onde você pode especificar um conjunto de caracteres padrão ou um conjunto de caracteres que você especificar. A trituração pode gerar todas as combinações e permutações possíveis.

2.6.1.7 Aireplay-ng

A principal função é gerar tráfego para uso posterior no aircrack-ng para quebrar as chaves WEP e WPA-PSK. Existem ataques diferentes que podem causar desautentificações com o objetivo de capturar dados de Handshake WPA, autenticações falsas, repetição de pacotes interativos, injeção de solicitação ARP criada manualmente e reinjeção de solicitação ARP.

3 METODOLOGIA

Foi realizado um método de pesquisa misto e exploratório, onde é apresentado os conceitos do Wi-Fi e sua segurança, um software livre que contém ferramentas de intrusão à redes sem fio, é visto de forma prática a utilização dos conceitos realizando a invasão e quebra de senha de um roteador com a técnica de força bruta, após a pratica é demostrado como evitar a invasão e um procedimento de acessar a rede de forma mais segura, ao final é exibido o resultado de um questionário de uma pesquisa realizada ao decorrer desse projeto sobre alteração da senha de autenticação do acesso ao Wi-Fi e do roteador onde podemos verificar que existem redes configuradas de forma padrão.

- Conceituar Wi-Fi e suas ferramentas de segurança;
- Entender a ferramenta utilizada e as formas de invasão;
- Implantação da ferramenta Kali linux;
- Conectar em redes sem saber a criptografia, apenas utilizando softwares livres;
- Aplicar métodos de defesa;
- Comprovar que após fazer algumas configurações a invasão não ocorrerá facilmente;
- Apresentar relatório de alteração de senhas em roteadores domésticos.

4 IMPLEMENTAÇÃO

A implementação é baseada em capturas de telas feitas no Sistema operacional Kali Linux, na utilização das ferramentas que o software disponibiliza, e

em pesquisas na internet sobre senhas padrões de acordo com o modelo do roteador.

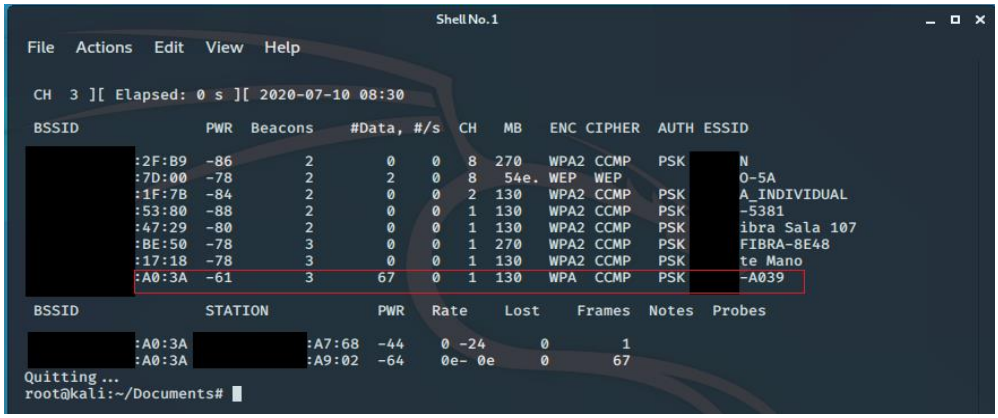
4.1 Monitorar a rede do ataque

No modo monitoramento é possível visualizar as redes ativas dentro da área do alcance da antena, diferente do método promiscuo de conexão Wi-Fi onde vemos apenas o ESSID, em modo monitoramento demonstrado na Figura 1, é possível capturar informações primordiais para uma invasão do dispositivo, além de mostrar o MAC de rede de usuários conectados nos pontos de acesso.

O comando utilizado no terminal do Kali Linux para alterar o modo da placa para modo de monitoramento é “airmon-ng start wlan0”, com a placa em modo monitor é possível gerar uma lista em tempo real para analisar os dispositivos ativos na área de alcance da antena aplicando o comando airodump-ng wlan0mon, com esse comando é gerada duas tabelas, na primeira é possível ver os pontos de acessos e suas informações, na segunda é possível ver os dispositivos conectados (STATION).

Após a seleção do alvo, como vemos na Figura 1 foi selecionado o alvo com final BSSID “A0:3A” e com o ESSID “-A039”, vamos fazer o monitoramento isolado daquela rede para capturar o handshake.

Figura 1 - Figura 1 – Monitoramento do Wi-Fi.



Fonte: Elaborada pelo autor

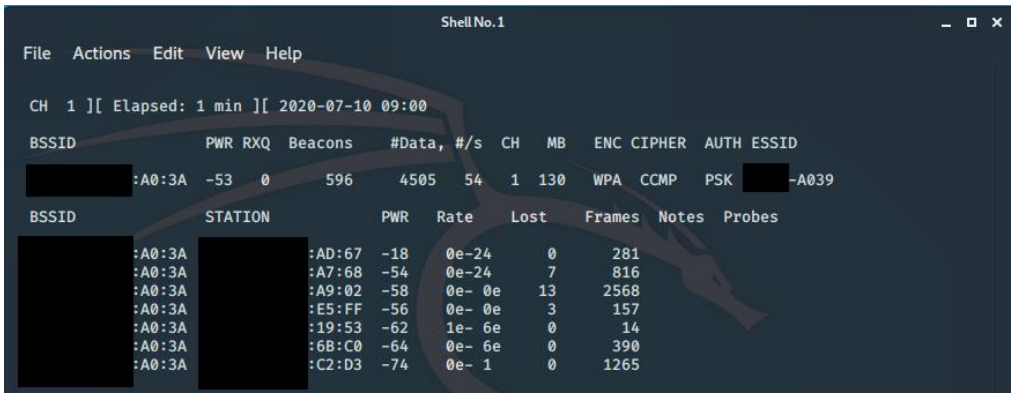
4.2 Capturando HandShake.

A captura do handshake pode ser feita quando um dispositivo for conectado ao ponto de acesso, isso pode demorar alguns minutos, horas ou dias, para agilizar esse processo o atacante pode fazer um ataque DdoS em algum dispositivo da rede como mostra a Figura 2, obrigando o dispositivo a se desconectar e conectar novamente.

Após escolher um alvo do ataque, usando o comando “airodump-ng --bssid (MAC do dispositivo) --channel 1 (canal) --write (nomedoarquivo) wlan0mon” é possível monitorar apenas um ativo de rede e gravar as informações capturadas como vemos na Figura 2, foi escolhida a rede X-A039.

Na linha “STATION” é possível ver os MACs de rede dos dispositivos conectados, possibilitando um ataque de DDoS a um único dispositivo, e podendo assim capturar o HandShake.

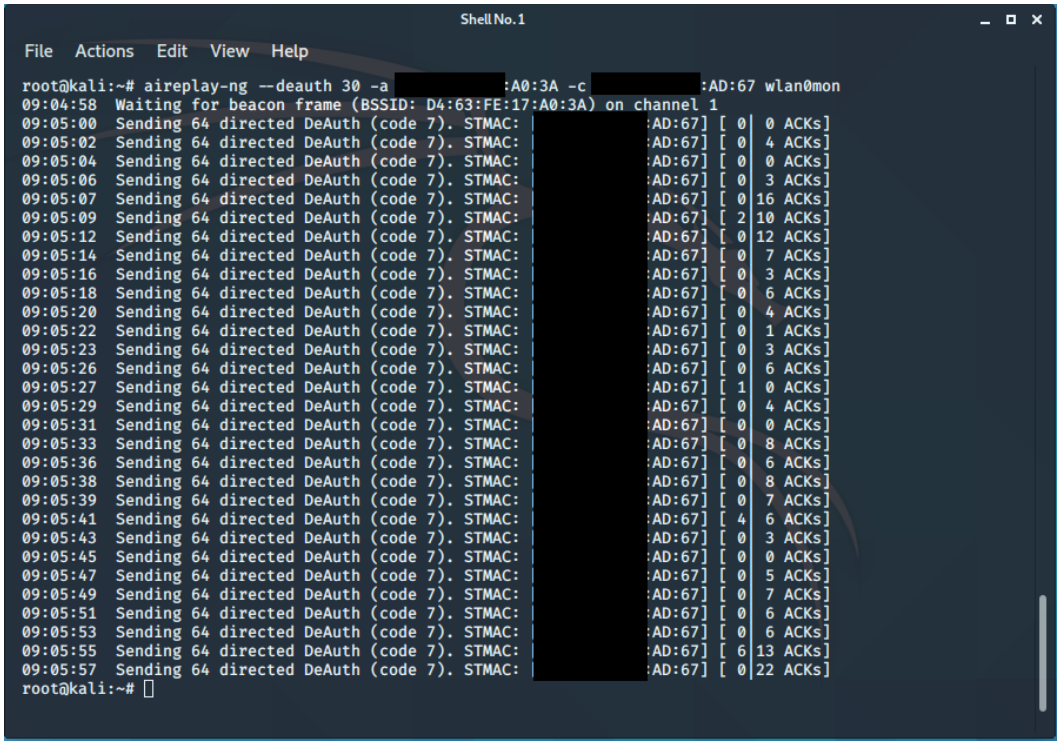
Figura 2 - Monitoramento do alvo.



Fonte: Elaborada pelo autor

Para fazer o ataque DDoS foi utilizado o comando “aireplay-ng --deauth 30 –a (MAC do roteador) –c (MAC do alvo) wlan0mon forçando o dispositivo a se desconectar e conectar novamente como mostra na FIGURA 3.

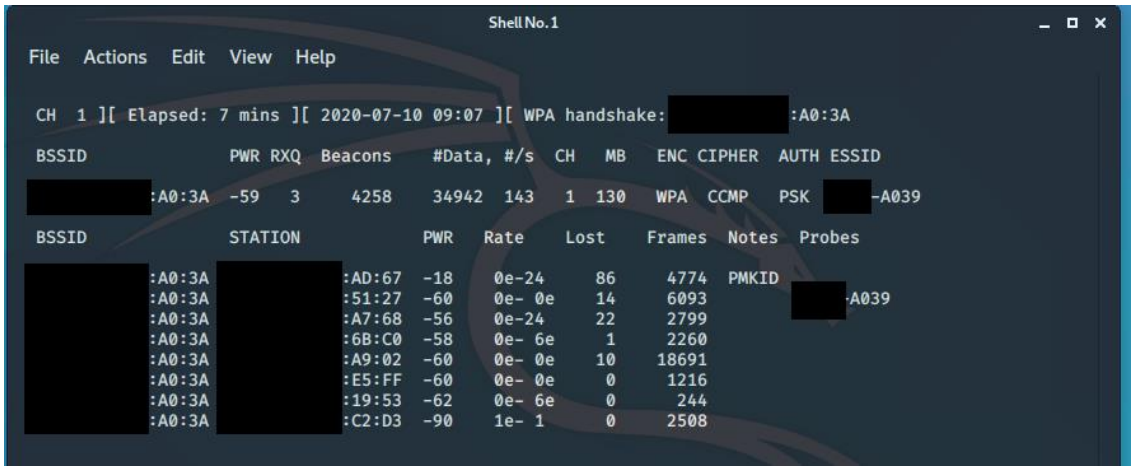
Figura 3 - Ataque DdoS.



Fonte: Elaborada pelo autor

Na FIGURA 4 é possível ver o handshake que foi capturado após alguns minutos depois do ataque DDoS ao dispositivo, onde o dispositivo se conectou novamente ao ponto de acesso.

Figura 4 - Captura do HandShake.



Fonte: Elaborada pelo autor

4.3 Pesquisa de senha padrão

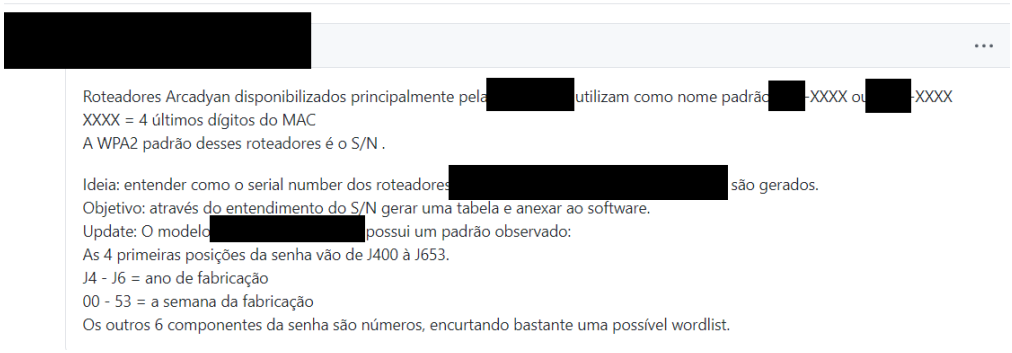
Feito isso, agora basta criar uma wordlist para efetuar o ataque, é essencial para o atacante ter essas informações do dispositivo, ESSID, BSSID, pode-se ver que é notavelmente um roteador que está com as configurações padrões, dito isso o atacante irá fazer pesquisar em manuais com a própria operadora que fornece o serviço ou com uma simples pesquisa no Google como mostra na FIGURA 5.

Figura 5 - Captura do HandShake.

Fonte: Elaborada pelo autor

Com essa busca foi encontrado na primeira página de pesquisa um artigo sobre as senhas padrões do modelo de ataque mencionado até então, no site, como mostra na FIGURA 6, temos padrões estabelecidos pelo modelo trazido para este projeto, visto que existe na internet diversos padrões dependendo do modelo e ou operadora.

Figura 6 - Consulta de senha padrão.



Fonte: Elaborada pelo autor

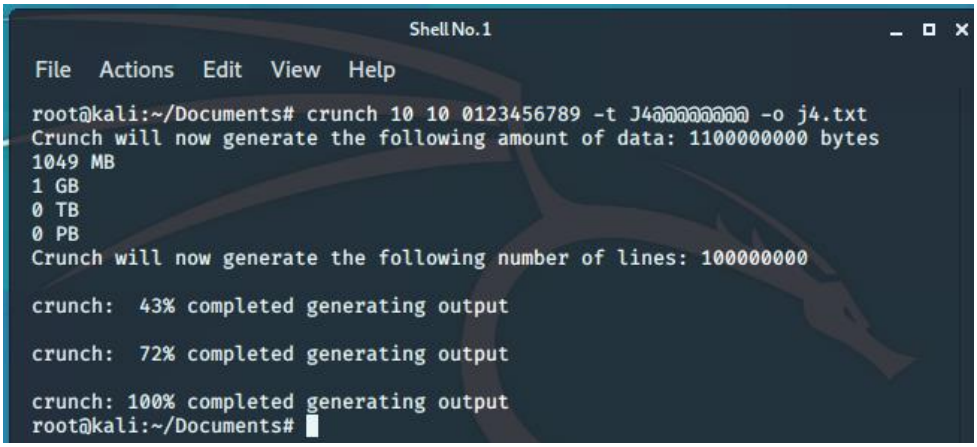
4.4 Criando WordList

Com as informações obtidas foram criadas 3 listas (figuras 7, 8 e 9) para descriptografar a senha de acesso a rede sem fio, com os seguintes parâmetros mínimo e máximo 10, com os números de 0 a 9 começando com J4, J5, J6:

Lista 1:

```
root@kali:~# aircrack-ng –w j4.txt chavecapturada1.cap
```

Figura 7 - Word List 1.

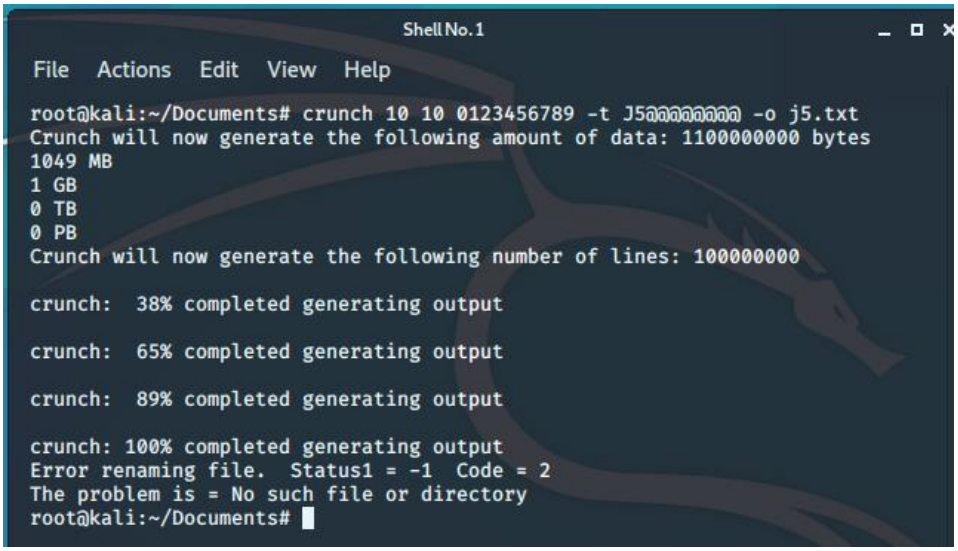


Fonte: Elaborada pelo autor

Lista 2:

```
root@kali:~# aircrack-ng –w j5.txt chavecapturada3.cap
```

Figura 8 - Word List 2.

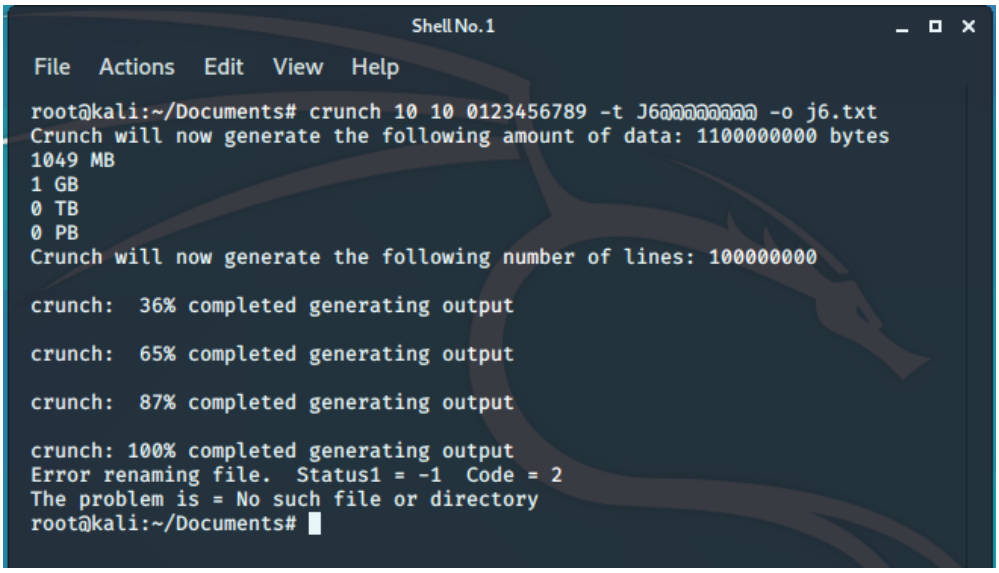


Fonte: Elaborada pelo autor

Lista 3:

```
root@kali:~# aircrack-ng –w j6.txt chavecapturada3.cap
```

Figura 9 - Word List 3.



Fonte: Elaborada pelo autor

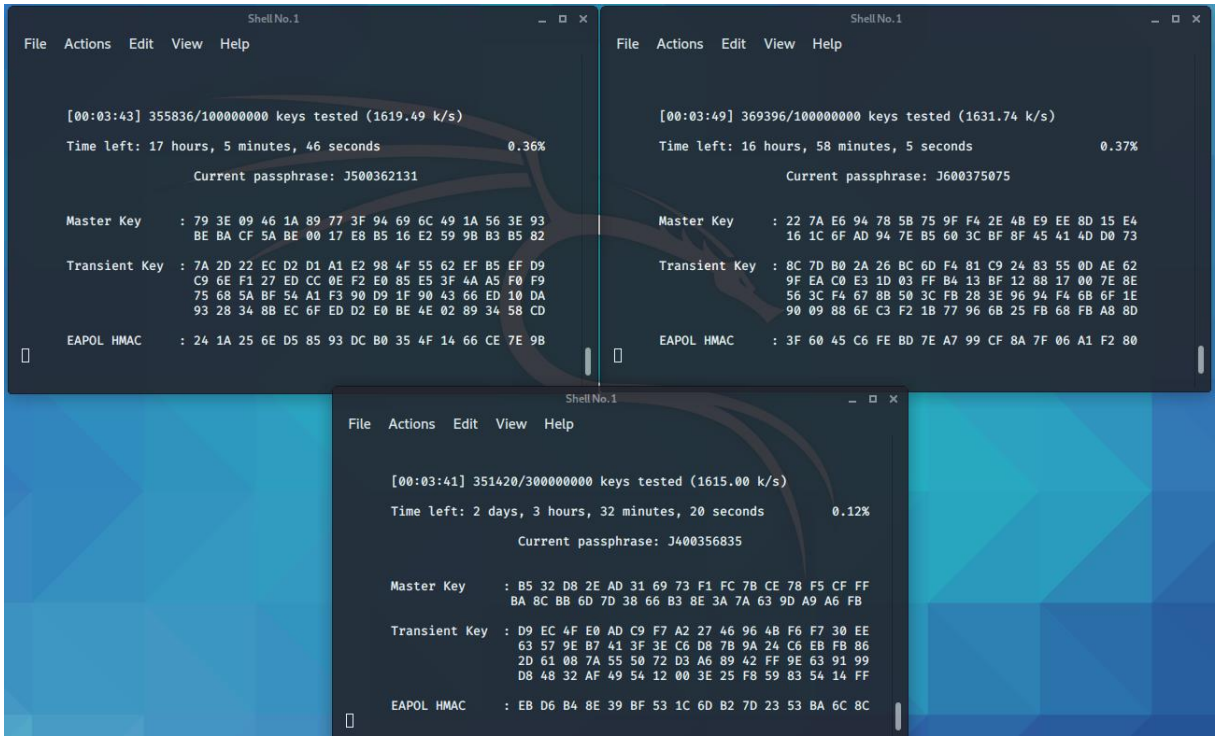
4.5 Descriptografando com Brutal Force (Força Bruta).

Com o aircrack-ng é possível usar as wordlists criadas para descodificar o handshake capturado no airodump-ng, para isso basta usar o comando aircrack-ng -w (wordlist) (arquivo do handshake), para acelerar o processo foi replicada o arquivo handshake capturado para ser usado ao mesmo tempo com as 3 wordlists geradas.

Neste caso em específico, como mostra a figura 10, executamos o comando em 3 janelas do terminal do Linux, mudando apenas a wordlist desejada e a chave capturada.

```
root@kali:~# aircrack-ng -w j5.txt chavecapturadalimpa2.cap
```

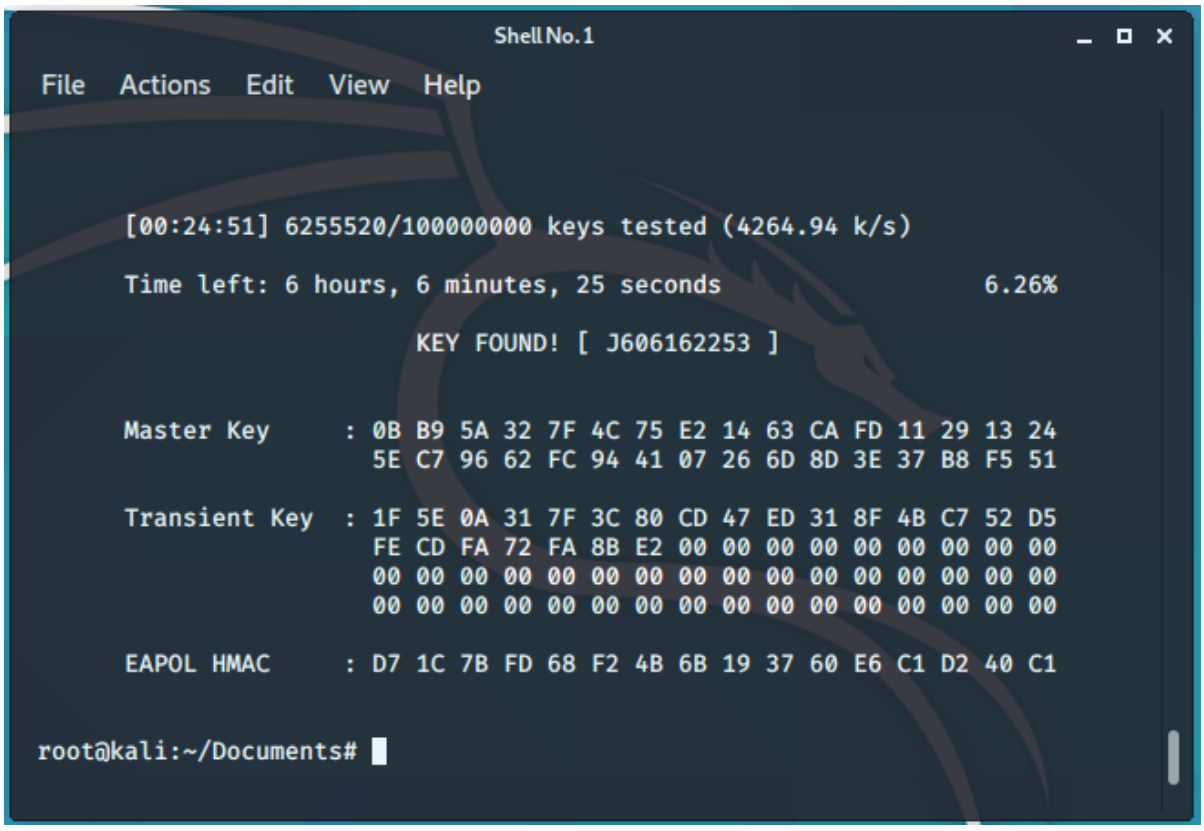
Figura SEQ Figura * ARABIC10 - Descriptografando.



Fonte: Elaborada pelo autor

Como mostra na FIGURA 11 abaixo, vemos a mensagem “KEY FOUND” e entre “[ ]” a senha, notamos também que a senha foi decodificada em 6.25% do processo, demorou por volta de 24 minutos, poderia demorar horas ou dias, mas com as informações encontradas na internet foi possível quebrar a senha padrão com três wordlists.

Figura 11 - Descriptografia.



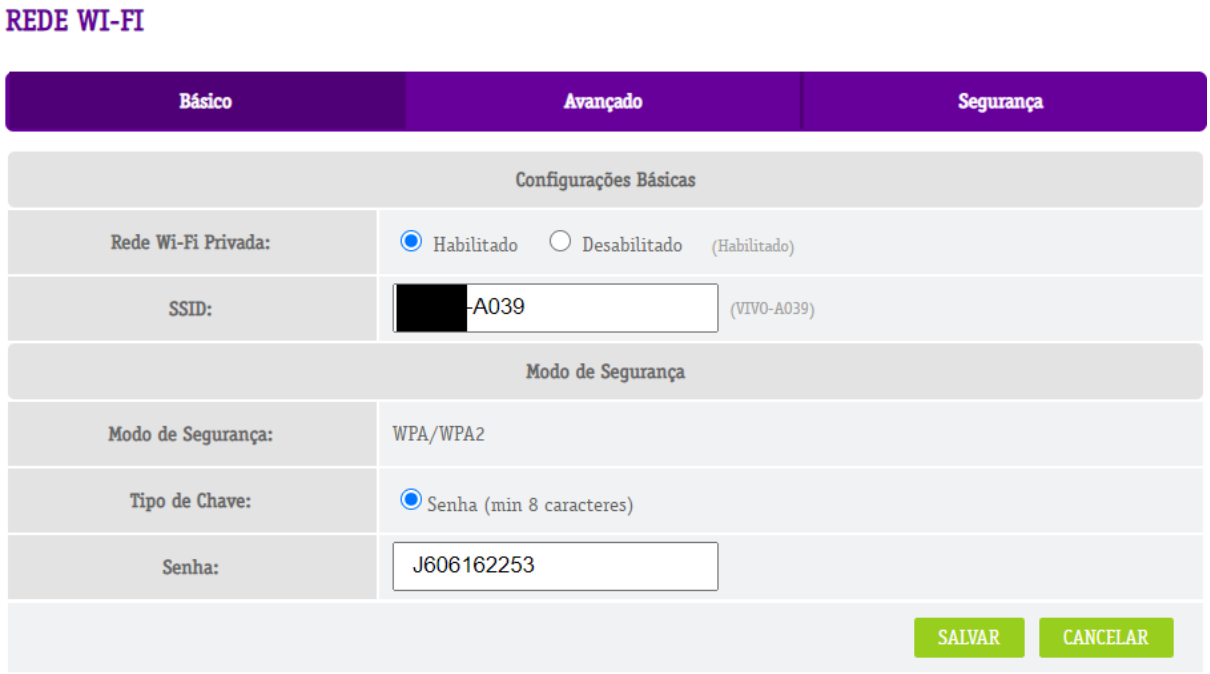
Fonte: Elaborada pelo autor

5 VALIDAÇÃO

5.1 Padrões

Caso a senha não fosse a padrão poderia demorar dias e dependeria muito de uma engenharia social para ter sucesso na captura de senha, no caso desse projeto, como mostrado na figura 12, o alvo foi um roteador com as configurações padrões aonde nunca foi alterada a senha.

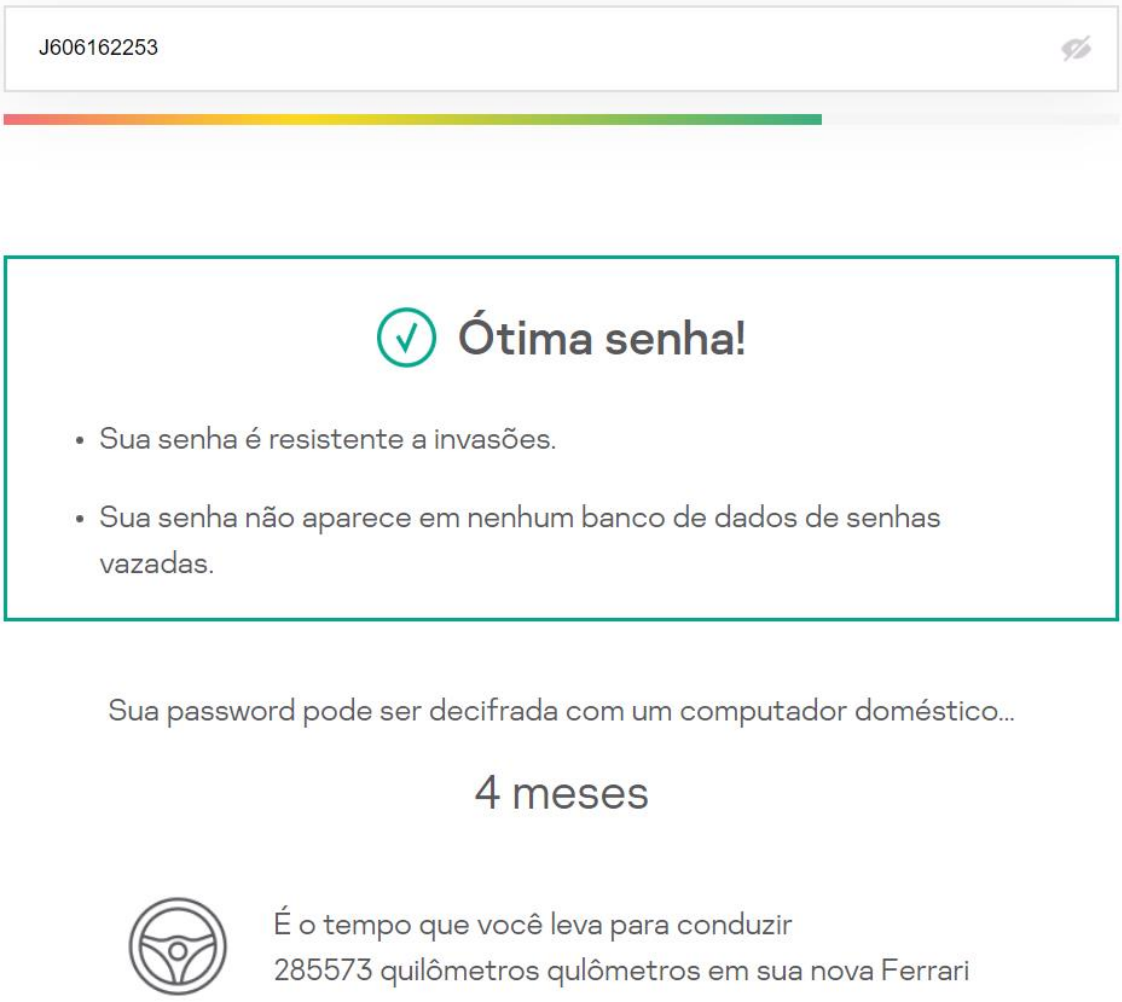
Figura 12 - Senha Padrão.



Fonte: Elaborada pelo autor

Se for alterado o SSID e a senha que vem pré-configurada pela operadora é possível dificultar a vida de um invasor se não até impedir uma invasão, nesse caso o padrão é designado pela operadora aonde a senha é o número de série do aparelho.

Figura 13 - Teste de Senha Padrão



Fonte: Elaborada pelo autor

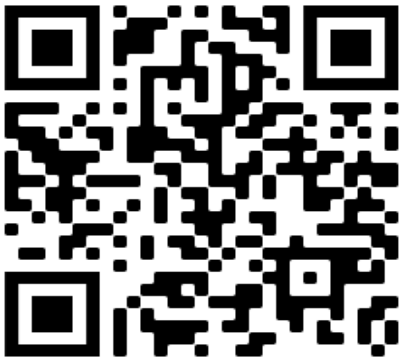
Foi feito um teste como mostra na FIGURA 13 com a senha padrão no site oficial da Kaspersky, aponta que a senha é ótima, e que demoraria 4 meses para ser decifrada por um computador doméstico, mas o que quebra essa teoria é o fato dela ser uma das senhas padrões em roteadores domésticos.

5.2 MÉTODO DE SEGURANÇA

Vale mencionar aqui que existem configurações onde podemos ocultar o SSID do roteador, porem isso dificultaria o acesso, visto que teria que pôr o nome da rede e a senha de acesso.

Existe um método onde podemos gerar um código QR da rede Wi-Fi, que torna possível autenticar na rede Wi-Fi apenas lendo o código com a câmera do celular.

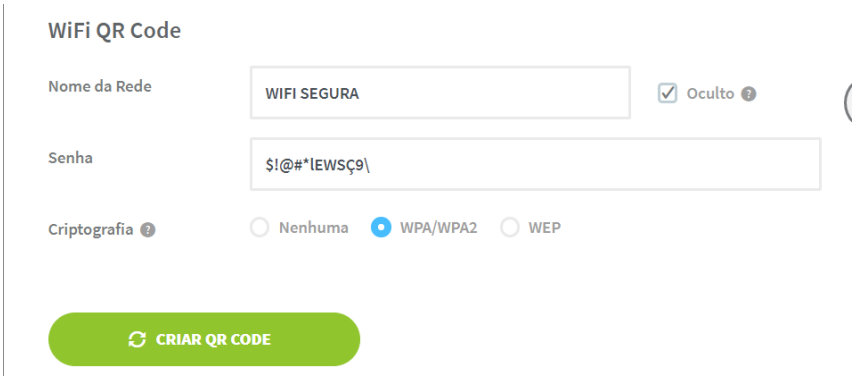
Figura 14 - QR CODE



Fonte: Elaborada pelo autor

Para fazer isso basta entrar em um site gerador de QR-Code e preencher com as informações necessárias para acesso, como o nome e a senha configurada no roteador, como mostra a FIGURA 15.

Figura SEQ Figura * ARABIC15 - Gerador de QR Code

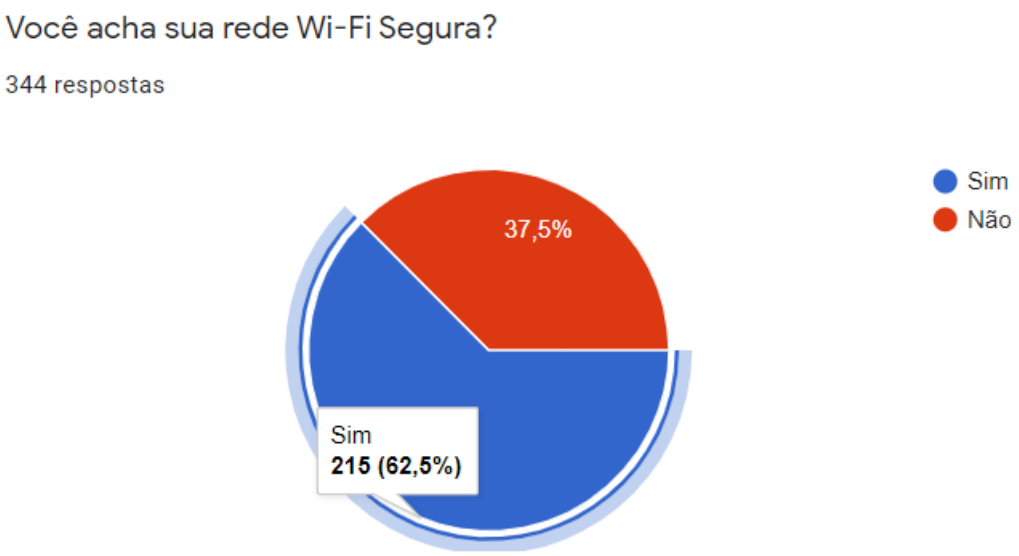


Fonte: Elaborada pelo autor

5.2 Pesquisa de senhas padrões.

Foi realizada uma pesquisa via Google Forms com as pessoas que tem acesso Wi-Fi em casa, foi questionado se elas acham a rede Wi-Fi segura e sobre as senhas de autenticação e senhas dos roteadores.

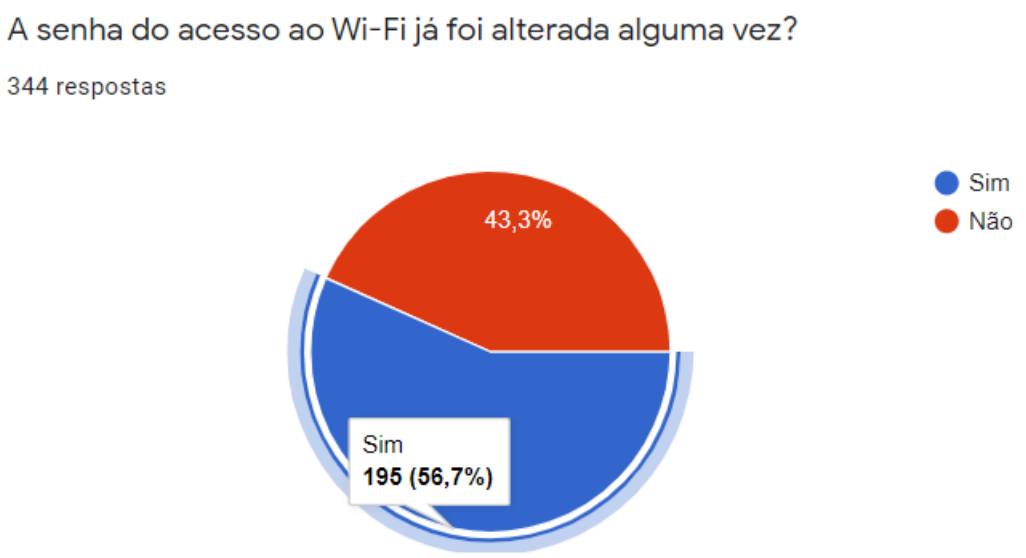
Figura 16 - Pesquisa Wi-Fi Segura



Fonte: Elaborada pelo autor

Na FIGURA 16 é possível ver que a grande parte das pessoas confiam na segurança do seu Wi-Fi.

Figura 17 - Pesquisa Alteração de Senha Wi-Fi



Fonte: Elaborada pelo autor

Na FIGURA 17 é possível verificar que boa parte já fez a alteração de senha de acesso do Wi-Fi tornando ela mais segura e resistente aos ataques visto nesse projeto.

Figura 18 - Pesquisa Alteração de Senha Roteador

Fonte: Elaborada pelo autor

E boa parte respondeu que não troca a senha do roteador, vale ressaltar aqui que existem outros modos de ataque ao acesso de um ponto de Wi-Fi, e o modo mais seguro de se proteger de eventuais problemas é trocando a senha padrão do roteador.

6 CONCLUSÃO

Esse trabalho teve como finalidade conceituar o que é Wi-Fi, ferramentas utilizadas no método de força bruta, analisar a forma de quebra de senha usando procedimentos de certa forma simples e que pode ser executado por qualquer pessoa, com as informações que obtivemos na internet e artigos e livros é o suficiente para uma invasão, nela temos desde o método de ataque até a forma de proteger sua conexão, o intuído foi trazer com mais clareza a fragilidade das senhas padrões.

É possível analisar com a tabela abaixo que grande parte dos pesquisados acredita que sua rede Wi-Fi é segura, porém alguns não alteraram se quer alguma vez a senha do roteador e de acesso ao Wi-Fi, deixando assim a rede vulnerável a um ataque.

Tabela 2 - Pesquisa com formulário

Perguntas	Sim	Não
Você acha rede Wi-Fi segura?	215	129
A senha do acesso ao Wi-Fi já foi alterada alguma vez?	195	149
Você já alterou a senha do roteador?	131	213

Fonte: Elaborado pelo autor

Existe algumas precauções a serem tomadas que dificultam a invasão a uma rede Wi-Fi. A realização deste trabalho propõe em aumentar a segurança de uma rede que contem conexão wireless, demonstrando a forma de como age um invasor, alertando sobre a importância da troca de senha e da alteração de configuração de fábrica dos roteadores domésticos.

Com esse projeto é possível concluir que um roteador sem a alteração da senha é mais vulnerável a um ataque de força bruta do que um roteador com a senha alterada, o projeto delimitou-se a apenas o teste de um roteador, podendo no futuro haver testes com outros roteadores, modelos e operadoras, utilizando o mesmo método apenas alterando as wordlists geradas a partir da pesquisa do modelo do roteador.

7 REFERÊNCIAS

Aircrack-ng. Disponível em: https://www.aircrack-ng.org/doku.php?id=pt-br:cracking_wpa Ace <último acesso em 16 jun. 2020>

ARAUJO, Assunção Marcos Flávio. Wireless Hacking - Ataque e Segurança de Redes Sem Fio Wi-Fi. Editora Visual Books, 1ª ed., 2013, 180p.

GitHub. Disponível em: https://github.com/caioluders/DPWO/issues/4. <último acesso em 11 set. 2019>.

Kali Linux. Kali Docs Official Documentation. Disponível em: <https://www.kali.org/docs/> Acesso em 23 nov. 2020

Kaspersky. Disponivel em: <https://password.kaspersky.com/pt/> >. Disponível em: 1 de jun. 2020.

MACEDO, Diego. 2016. Atacando redes wifi com Aircrack-ng protegidas com criptografia WEP. Disponível em <https://www.diegomacedo.com.br/atacando-redes-wifi-com-aircrack-ng-protegidas-com-criptografia-wep/>. Acesso em 16 fev. 2020.

MORIMOTO, Carlos E. 2008. Redes wireless, parte 2: Padrões. Disponível em: <http://www.hardware.com.br/tutoriais/padroes-wireless/pagina6.html>. Acesso em 10 jan. 2020.

NetSpot. Disponível em: https://www.netspotapp.com/pt/wifi-encryption-and-security.html <último acesso em 08 out. 2020>

PANTAS, Willians. Portal Understech. 2017. Segurança Wi-Fi: Você deve usar WPA2-AES, WPA2-TKIP ou ambos? Disponível em

<http://understech.com.br/deve-usar-wpa2-aes-wpa2-tkip/>. Acesso em 10 jan. 2020.

Ranjith. Aircrack-NG: WiFi Security Auditing Tools Suite. Disponível em: <https://kalilinuxtutorials.com/aircrack-ng-wifi-security/>. Acesso 14 abr. 2020

RICCE, Gabriel. 2015. As diferenças entre 2.4GHz e 5GHz. Disponível em <https://medium.com/@gabrielricce/bem-vindos-amigos-ao-segundo-post-deste-blog-e-o-primeiro-com-um-conte%C3%BAdo-tecnico-pra-variar-29e42372cfc4>. Acesso em 02 mai. 2020.

RUFINO, Nelson de O. Rufino. Segurança em Redes sem Fio: Aprenda a proteger suas informações em ambiente Wi-Fi e Bluetooth. 4ª Edição. São Paulo: Novatec, Janeiro/2015.

Tanenbaum, Andrews S. REDES DE COMPUTADORES. 5ª Edição. São Paulo: Person Pearson Prentice Hall, 2011. 582p..

Sankar, Ravi. Reaver + PixieWPS – Tool to Bruteforce the WPS of a WiFi Router. disponível em: <https://kalilinuxtutorials.com/reaver-pixewps/> acesso em: 7 de abr. 2020

STALLINGS, William. Criptografia e Segurança de Redes: Princípios e Práticas. Editora Pearson, 6ª ed., 2014, 558 p..

WEIDMAN, Georgia. Testes de Invasão: Uma introdução prática ao hacking. Editora Novatec, 1ª ed., 2014, 576 p..