SEGURANÇA EM REDES SEM FIO: principais formas de ataques, testes de invasão e modelos de segurança

WIRELESS NETWORK SECURITY: main forms of attacks, intrusion tests and security models

Aline Francine Rodrigues
Graduando em Redes de Computadores pela Fatec Bauru
E-mail: aline.rodrigues31@fatec.sp.gov.br

Josiane Pereira Gonçalves
Graduando em Redes de Computadores pela Fatec Bauru
E-mail: josiane.goncalves2@fatec.sp.gov.br

Marta Valeria Castilho
Graduando em Redes de Computadores pela Fatec Bauru
E-mail: marta.castilho@fatec.sp.gov.br

Henrique Pachioni Martins
Docente na Fatec Bauru
E-mail: henmartins@gmail.com

RESUMO:

O crescimento das redes sem fio ocasionou grande aumento de acesso à internet através de dispositivos com placa wireless. Com isso, as ameaças através de ataques às redes aumentaram sensivelmente. O presente artigo objetiva discorrer sobre os principais padrões de redes wireless e seus protocolos de criptografia, expondo assim, possíveis vulnerabilidades através de uma ilustrativa de ataque de quebra de criptografia à função WAP2. Com a análise desse estudo de caso das vulnerabilidades descobertas, foram constatadas algumas barreiras de segurança que dificultaram esse tipo de invasão. Concluindo a abordagem serão apresentados o protocolo WPA3 e suas novas tecnologias que visam a proteção de dados nas redes domésticas e/ou corporativas buscando o aumento da segurança nas redes sem fio atuais.

Palavras-chave: Redes wireless. Vulnerabilidades. Criptografia. Protocolos. Segurança.

ABSTRACT:

The growth of the wireless network has caused a massive increase in internet access through wireless card devices. Because of this, threats made by network attacks have increased considerably. This paper aims to discuss the main wireless network standards and their encryption protocols, thus exposing possible vulnerabilities through an illustration of a cryptographic break attack to the WAP2 function. Analyzing the case study of these discovered vulnerabilities, it was found some security barriers that made this type of invasion difficult. Concluding the approach, the WPA3 protocol and its new technologies that aim to protect data on home and/or corporative networks are seeking enhancement in current wireless networks.

Keywords*: Wireless networks. Vulnerabilities. Cryptography. Protocols. Safety*

INTRODUÇÃO

No decorrer da história, as redes de computadores foram criadas para facilitar a comunicação nos quartéis militares e centros de pesquisa de instituições universitárias, mas acabaram sendo direcionadas também para outras finalidades já que estudos tornaram possível o surgimento de protocolos de comunicação possibilitando que redes diferentes trocassem dados independente dos fabricantes.

Com a popularização da internet percebeu-se a necessidade de uma rede não limitada ao espaço, surgindo a comunicação sem fio ou *wireless.* Atualmente a rede mais usada para acesso à internet, quando falamos em redes sem fio, é a *Wireless Fidelity* (Wi-Fi) e com sua popularidade em alta, surgiram os problemas de segurança. A WI-FI é conhecida por sua versatilidade no uso da internet, pois torna possível o sinal trafegar fazendo diversas atividades com facilidade, normalizando a convivência com roteadores ligados vinte e quatro horas por dia.

Todavia, com esse avanço ocorrem problemas que afetam a segurança das informações e riscos de invasões e ataques cibernéticos. As diversas formas de ataques às redes sem fio têm o propósito de interceptar os dados que estão trafegando por ondas eletromagnéticas a fim de capturar os pacotes de dados dando acesso às informações contidas.

Com o aumento exponencial dessa rede, os riscos aumentaram e evoluíram na mesma velocidade e proporção. Muitas vezes a segurança nas redes wireless é negligenciada, pois não se tem o conhecimento das técnicas certas de aprimoramento de seguridade da rede tais como padrões e protocolos. As regras que os protocolos propõem tornar uma rede wireless mais segura, funcionam através de informações criptografadas que precisam de chaves específicas, as senhas do usuário, para liberação do acesso. Ao elevar as exigências de transmissão de sinal através desses protocolos faz-se real a segurança deste tipo de rede garantindo desta forma segurança, confidencialidade e integridade dos dados, deixando de ser um alvo fácil.

Este trabalho descreverá o conceito e o funcionamento de uma rede sem fio, citando os principais protocolos de segurança, estudando suas vulnerabilidades, testando ataques e aprimorando a segurança das conexões para verificar a possibilidade de uma rede sem fio ser realmente segura.

1 FUNDAMENTAÇÃO TEÓRICA

1.1.1 Conceito de Redes sem Fio

A evolução da rede sem fio se tornou notória e ganhou popularidade de forma globalizada devido ao crescimento exponencial de tecnologias que a empregam. O surgimento de protocolos de comunicação viabilizou o surgimento de diferentes tipos de redes, sendo as mais conhecidas: *Local Area Network* (LAN), *Metropolitan Area Network* (MAN) e *Wide Area Network* (WAN).

Para Oliveira (2015, p. 12), “A evolução das redes de computadores fez com que aumentasse a necessidade de comunicação entre mais distintos dispositivos, não somente entres os dispositivos fixos, mas também entre os dispositivos móveis.”

Subtende-se que a revolução tecnológica proporcionou o surgimento de diversos tipos de dispositivos que usam a comunicação sem fio tais como: celulares, notebooks, tablets e, com sua ampliação essas e outras tecnologias começaram a surgir, como a *Internet of Things* (IOT), que objetiva conectar os itens domésticos usados em nosso cotidiano à uma rede *wirelles*. Seu uso será extremamente imprescindível no futuro sem falar da sua maior vantagem quando comparada a uma rede cabeada, seja pelos seus custos, facilidade de instalação, mobilidade dos equipamentos e facilidade de expansão.

Moraes (2010, p. 17), analisa da seguinte forma. “As redes wireless ou redes sem fio são um sistema de comunicação de dados extremamente flexível, que pode ser usado como uma extensão ou uma alternativa a redes locais (LANs cabeadas).” Essa alternativa fica evidente principalmente por sua versatilidade no uso da internet, pois torna possível o ter acesso a rede em diversas atividades do dia a dia em qualquer lugar, tudo isso porque seu sinal trafega pelo ar.

Basicamente a radio frequência utiliza microondas para transmitir seu sinal através do ar, usando por padrão bandas reservadas, sendo as principais as de 900 MHz, 2.4 GHz e 5 GHz e, justamente por utilizar o ar para transmitir, os dados tornaram-se suscetíveis a ataques.

1.1.2 Padrão IEEE 802.11

Moraes (2010, p. 41), " Na verdade, o padrão 802.11 é um conjunto de normas e padrões de transmissão em redes sem fio, sendo os principais padrões utilizados 802.11a, 802.11b, 802.11g e 802.11n."

O autor também explica nesse trecho o que é de fato o padrão 802.11 e cita os principais utilizados. Desta forma podemos analisar que são versões diferentes, ou seja, uma atualização da anterior que visa aumentar a taxa de transmissão de dados, minimizar interferências no sinal e melhorar os protocolos de criptografia para transmissão segura dos dados. Um exemplo disso é o padrão 802.1x que usa o protocolo *Extensible Authentication Protocol* (EAP) que utiliza o endereço MAC para autenticação do usuário tornando possível usá-lo junto com servidor RADIUS de autenticação que tem o mesmo conceito para dar acesso ao usuário. No Brasil os principais padrões IEEE 802.11 são: 802.11a, 802.11b, 802.11g e 802.11n e 802.11ac.

O algoritmo *Wired Equivalent Privacy* (WEP) é definido pelo padrão 802.1, como será aprofundado no tópico 1.1.4. O protocolo foi projetado para garantir a segurança da rede, porém persistiam a existência de falhas e para essa correção de erros, surgiu então o protocolo de criptografia *Wireless Application Protocol* (WAP) com um conjunto de capacidades para tratar das questões de segurança das redes.

1.1.3 Criptografia

Conforme mencionado anteriormente, as redes sem fio usam frequências de rádio para trocar dados, portanto, são mais fáceis de serem expostas, já que não precisam de um meio físico para serem invadidas ou descobertas. Com o avanço dos estudos tecnológicos surgiram padrões com o objetivo de tornar a rede mais segura como o padrão 802.11 que criou especificações para redes locais *Wireless Local Area Network* (WLAN) e consequentemente técnicas para manter a rede segura como os protocolos de transmissão WEP, WAP e WAP2 que usam criptografia para manter os dados que trafegam pela rede livre de invasões.

De acordo com Moraes (2010, p.123), "Criptografia é a ciência que utiliza algoritmos matemáticos para criptografar/encriptar (cripto = esconder) dados (texto claro) numa forma aparentemente não legível (texto cifrado) e recuperá-los (descriptografá- los)." Sendo assim a criptografia nada mais é que um conjunto de regras com objetivo de codificar as informações usando de várias técnicas através de algoritmos para gerar chaves criptografadas. Devido às inúmeras técnicas de invasão existentes atualmente sua utilização tornou-se imprescindível para a segurança principalmente nas redes wireless.

Seu processo de encriptação por ser computacional deixa as informações contidas mais seguras e como resultado mais difícil de "quebrar".

Existem três tipos de sistemas de criptografia: a de chave secreta, também conhecida como privada, chave pública e a baseada em *hashing*. A comunicação baseada na chave secreta conta com a troca de informações, onde ambos têm o conhecimento da chave e pode-se dizer que a segurança está em manter a chave em segredo. A chave pública tem um sistema de duas chaves, onde uma é pública e a outra é secreta, sendo essa última responsável por encriptar os dados e os dois lados devem gerar essas duas chaves. No sistema baseado em *hashing* resumidamente, a criptografia é aplicada diretamente na informação sem a preocupação com o tamanho e por causa disso, seu resultado tem um tamanho fixo.

1.1.4 Mecanismos de Criptografia

Nas redes *wireless* o processo de autenticação sempre vai exigir uma chave ou senha quando o usuário requisitar essa conexão. Esse sistema é embasado no *Service Set Identifier* (SSID) que é o nome que vai identificar a rede sem fio, sendo necessário que todos os computadores e componentes tenham o mesmo SSID, podemos dizer que ele é como uma senha de entrada para rede sendo que cada fabricante vem um SSID que em algum momento será trocado durante as configurações.

À medida que mais pessoas vão tendo acesso, mais vulnerável ele se torna já que é incorporado em cada cabeçalho dos pacotes que pertencem a rede sem fio e se alguém mal-intencionado tiver acesso, essa informação poderá ser usada para encontrar brechas. Por isso foi necessário utilizar outras barreiras para proteção tais como os mecanismos de criptografia WEP não mais utilizado WAP e WAP2 que é o protocolo utilizado hoje.

O Protocolo *Wired Equivalent Privacy* (WEP) foi o primeiro protocolo de criptografia para redes sem fio adotado pelo padrão IEEE 802.11. Para Moraes (2010, p.153), "O WEP trabalha com o RC4 da RSA que é uma cifra baseada em stream ou fluxo (40 bits de chave + 24 bits de vetor de inicialização). É um algoritmo simétrico que usa a mesma chave para encriptar e decriptar a informação PDU (*Protocol Data Unit*)."

O principal objetivo dos idealizadores desse protocolo era fornecer mais segurança aos dados através de uma chave secreta utilizando a cifra RC4 para criptografar pacotes a serem transmitidos já que as chaves de acesso utilizam 64 ou 128 bits, mas não obteve o resultado esperado pois existiam muitas falhas. Uma delas era que, por usar um vetor de inicialização muito pequeno, seu processo de criptografia de chave se tornava suscetível a ataques que buscavam descobrir a chave. Outro ponto fraco é que todos os usuários da rede usam a mesma chave WEP além de ter uma vulnerabilidade na camada enlace e, por causa destas vulnerabilidades, foi necessário criar outro protocolo para melhorar a segurança da rede *wireless*.

1.1.5 Protocolo WAP

O *Wi-fi Protected Access* (WAP) foi o protocolo criado para melhorar as vulnerabilidades do protocolo WEP. Suas principais mudanças foram na criptografia, onde o funcionamento ocorre através de uma chave temporal a *Temporal Key Integrity Protocol* (TKIP).
De acordo com Moraes (2010, p. 155), “A TKIP combina a chave temporal com o endereço MAC da estação adicionando 16 octetos ao vetor de inicialização para produzir a chave que irá encriptar os dados. Cada chave temporal é trocada a cada 10.000 pacotes.” Ao utilizar a chave TKIP é criada uma chave de criptografia que é trocada periodicamente. Sua autenticação é feita através de trocas das chaves dinâmicas e seu vetor de inicialização passou a ser de 48 bits, o que previne ataques de retransmissão de pacotes. É possível dizer que sua principal mudança realmente foi no algoritmo de criptografia.

1.1.6 Protocolo WAP2

O protocolo WPA2 foi criado logo após o WPA apresentar instabilidades e significativa perda de desempenho. Ele teve grandes melhorias quanto a estabilidade e segurança, aperfeiçoando as técnicas de proteção dos dados e a autenticação dos usuários. Essa versão se destaca por manter a segurança no uso doméstico e nos níveis mais altos de proteção que uma empresa deve ter, isso porque apenas usuários autorizados tem acesso à rede, essa versão foi baseada nas especificações do padrão 802.11i e inclui a TKIP.

Segundo Moraes (2010, p.158), “O WPA2 utiliza como algoritmo criptográfico o CCMP, o mais seguro de todos, que se baseia na especificação final do AES (Advanced Encryption Standard).” Esse protocolo Counter *Mode CBC MAC Protocol*, CCMP foi criado especificamente para segurança de redes sem fio e utiliza um conjunto de métodos de encriptação de mensagem transmitidas.

O WAP2 tem dois métodos de autenticação o *personal mode* que oferece segurança simples para uso doméstico e de pequenos escritórios e o *enterprise mode* usado quando se necessita de um grau maior de segurança pois neste método é usada a autenticação 802.1x com RADIUS. O protocolo WAP2 é o principal modelo usado já que sua utilização varia de acordo com o grau de segurança necessária.

2 Vulnerabilidades da Rede sem Fio

Examinar e entender como implementar soluções de segurança na rede para reduzir significativamente as vulnerabilidades das informações será sempre uma das formas de minimizar a falta de infraestrutura. Para identificar ataques contra redes sem fio e tomar contra-medidas eficazes, é necessário analisar as vulnerabilidades inerentes às redes. Por isso, é necessário um estudo detalhado dos protocolos que os suportam, o que foi analisado na etapa anterior do artigo e será posto em prática no capítulo de materiais e métodos.

As deficiências serão apontadas e as mudanças apropriadas poderão ser introduzidas. Como referenciado anteriormente, as redes wireless usam o ar como meio de transmissão das informações e por este motivo é mais suscetível aos ataques que visam interceptar dados pessoais como senhas de cartões de crédito e de contas bancárias ou de dados privados de empresas.

Segundo Moraes (2010, p.177), “É preciso garantir a implementação de um ambiente seguro com criptografia de chave forte, porém antes disso deve-se entender as reais ameaças que nos afetam.” É de nosso entendimento a existência de várias técnicas para realizar uma invasão em uma rede wireless, tais como: *WLAN Scanners, Man in the Middle Attack, Ataque de Inundação UDP, Ponto de Acesso Falso, Ataques Sniffers, Denial of Service (DoS) e Port Scanning* porém contando com a presença dos mecanismos corretos de implementação de segurança, será mais difícil a realização de quaisquers ataques e deste modo, poderão ser reconhecidas as vulnerabilidades e pontos fracos das redes sem fio, para promover o melhor método de segurança.

3 MATERIAIS E MÉTODOS

Para a realização deste trabalho, o mesmo foi divido em duas etapas: a primeira com o intuito de identificar os principais temas teóricos e a segunda, uma parte prática onde será realizado a implementação prática e a análise dos resultados obtidos.

Na primeira etapa foi realizado um levantamento bibliográfico, sendo que estes conteúdos estavam presentes em livros, artigos científicos e outras fontes disponíveis na internet, contendo referências sobre redes de computadores, redes sem fio, roteadores e invasão de redes.

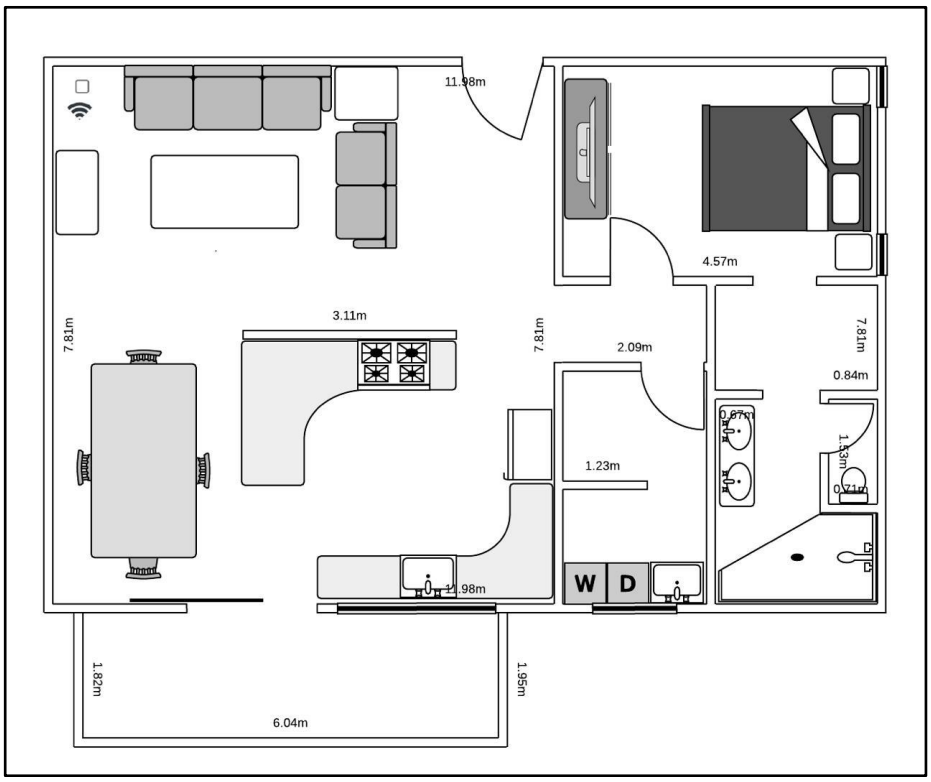
Para a segunda etapa o principal objetivo é manter a eficiência da rede *wireless* e verificar se, com o uso das ferramentas certas, essa rede se tornará segura.

Este estudo foi realizado em dois ambientes distintos, uma residência e um escritório de prestação de serviços. Ambos utilizam rede sem fio padrão 802.11n e protocolo WAP2 Personal sendo o residencial AES e o do escritório PSK, e cada um tem um provedor de internet diferente.

Visando melhorar a segurança foi realizada uma invasão em cada um dos roteadores, para descobrir a senha de acesso à rede wireless, termo técnico: quebra de criptografia. Para a conclusão desta ação foi necessária a utilização do sistema operacional Kali Linux versão 2021.1, com a instalação das ferramentas *Aircrack-ng* e *Wifite* que, em conjunto, promoveram a quebra da senha da rede de apenas um dos roteadores acessados. Através de um pendrive bootável e alteração na ordem de inicialização do sistema operacional na BIOS do computador e do notebook realizamos os ataques.

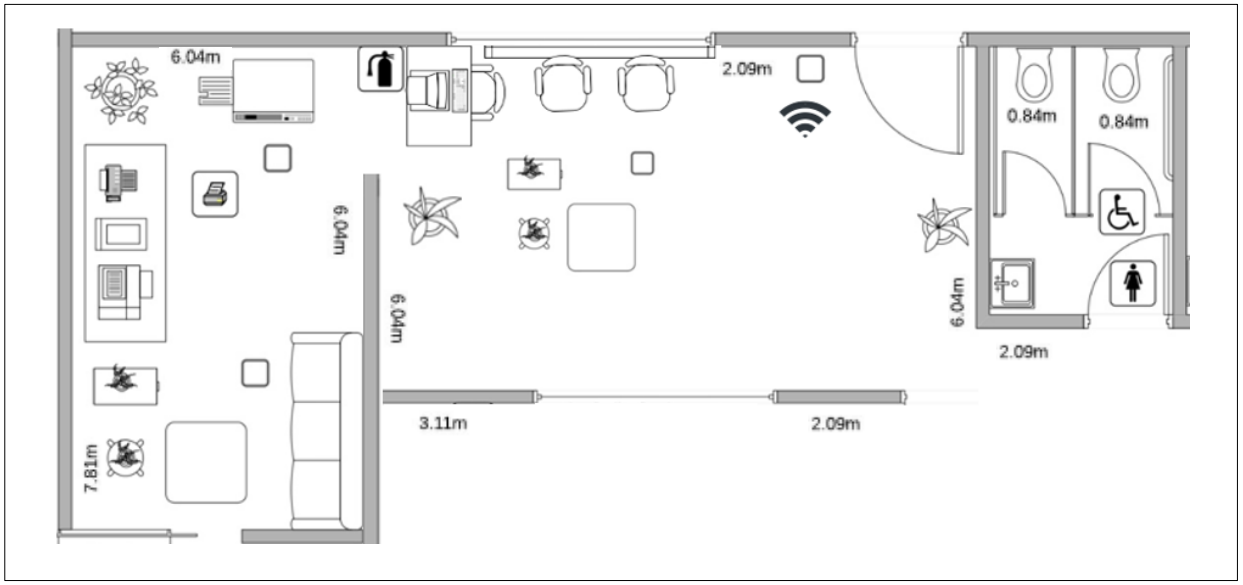
A partir da execução dessa técnica de ataque, surgiram alguns pontos fracos em um dos roteadores, o que possibilitou a descoberta da senha. As figuras 1 e 2 apresentam um layout de cada ambiente de teste.

FIGURA 1: PLANTA DA RESIDÊNCIA



Fonte: Os autores (2021)

FIGURA 2: PLANTA DO ESCRITÓRIO



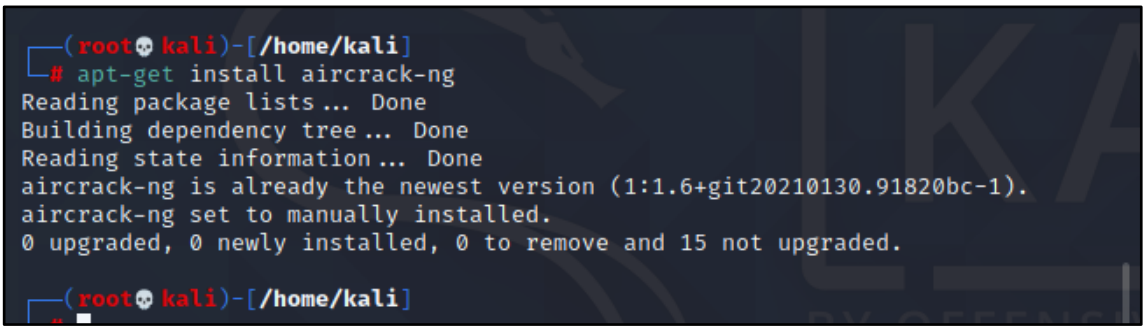
Fonte: Os autores (2021)

3.1.1 Quebra de Criptografia do Modem da Residência

Como citado anteriormente, criptografia é a ciência que utiliza algoritmos matemáticos para camuflar os dados de rede e seus usuários, através de técnicas que geram chaves criptografadas. Subentende-se que as redes sem fio transmitem os dados através de radiofrequência e por este motivo ficam suscetíveis a diversos tipos de ataques. Para torná-las seguras é necessário usar padrões e protocolos de criptografia, por exemplo: WAP2.

A quebra de criptografia consiste em identificar o nome da rede sem fio SSID, canal CH, a encriptação ENCR, o sinal POWER e o WPS. Para conseguir essas informações foi utilizado o *Aircrack-ng*, uma ferramenta de quebra de senhas de redes wireless que possui a autenticação WEP/ *WAP,* em conjunto com a ferramenta *Wifite,* um incremento do *Reaver* que realiza invasões de várias redes sem fio criptografadas através da captura de *Handshakes WPA* fazendo a autenticação dos clientes e corrompendo o endereço MAC.

FIGURA 3: INSTALAÇÃO DA FERRAMENTA AIRCRACK-NG



Fonte: Os autores (2021)

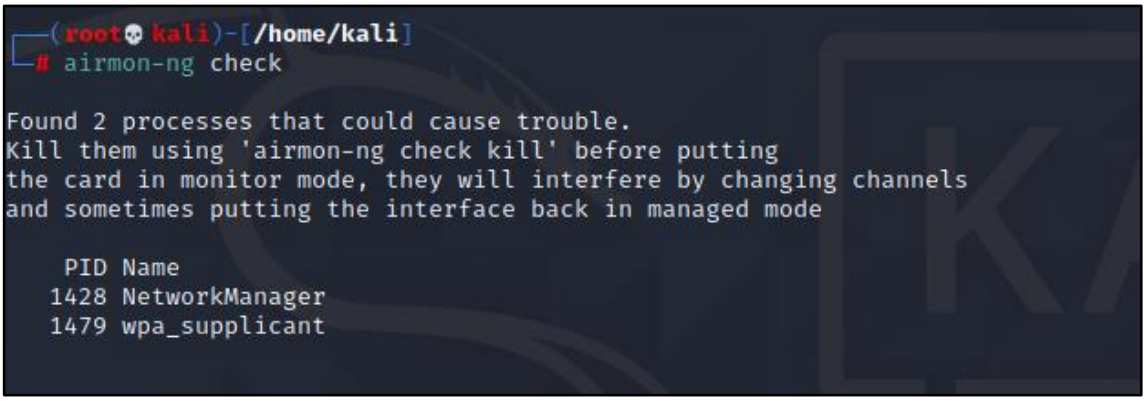
A instalação do *Aircrack-ng* permitiu o acesso às suas ferramentas, como a *Airmon-ng*, que serve para criar ou finalizar interfaces em modo monitor e checar a finalização de processos. Inserindo o comando *Airmon-ng start wlan0,* a placa wireless passou-se a operar em modo monitor, exemplificado na figura 4.

FIGURA 4: PLACA WIRELESS EM MODO MONITOR

Fonte: Os autores (2021)

Para que a invasão seja bem-sucedida, é necessário checar a existência de processos que possam atrapalhar a suíte, com o comando A*irmon-ng check*, conforme apresentado na figura 5.

FIGURA 5: VERIFICANDO PROCESSOS QUE ATRAPALHAM A INVASÃO

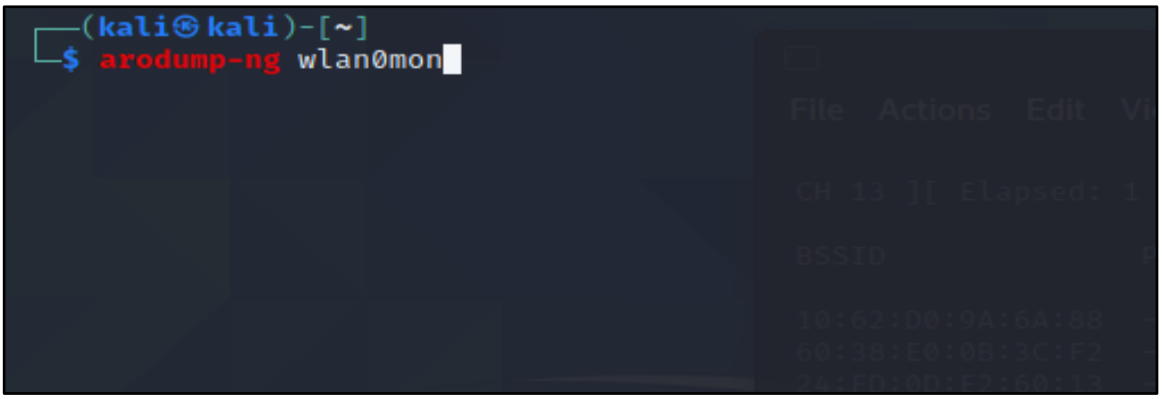


Fonte: Os autores (2021)

O comando A*irmon-ng check kill*, utilizado para encerrar os processos que entravam o *Aircrack-ng.*

O comando *airodump-ng wlan0mon*, torna possível visualizar as redes próximas, conforme apresentado na figura 6.

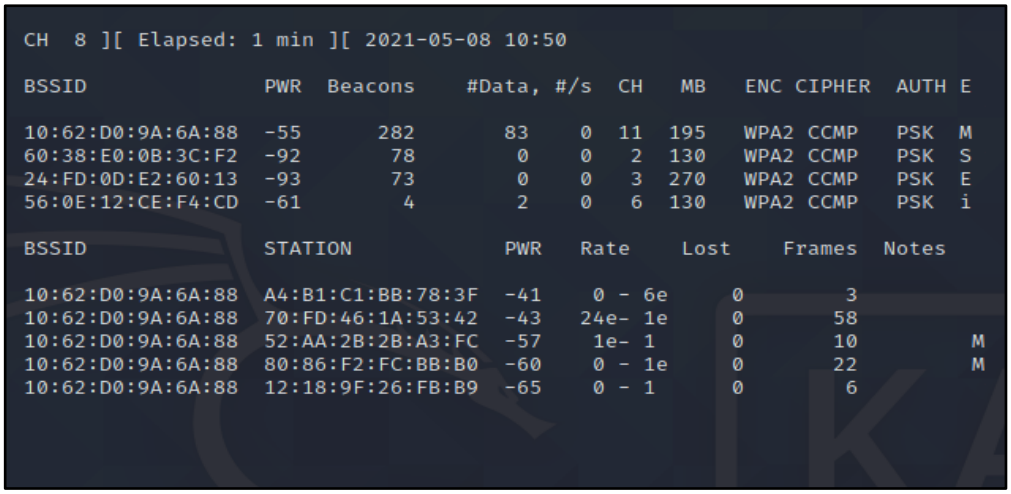
FIGURA 6: VISUALIZANDO AS REDES SEM FIO



Fonte: Os autores (2021)

De acordo com a figura 7, é possível visualizar as redes dentro perímetro.

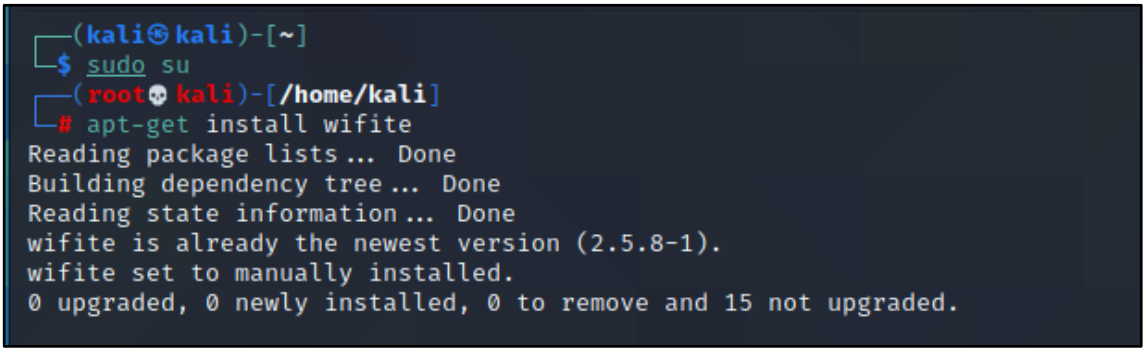
FIGURA 7: REDES WIRELESS DISPONÍVEIS



Fonte: Os autores (2021)

É necessário que a rede continue visível com o processo de instalação do *Wifite* a partir do comando apt-get install *wifite:*

FIGURA 8: INSTALAÇÃO WIFITE



Fonte: Os autores (2021)

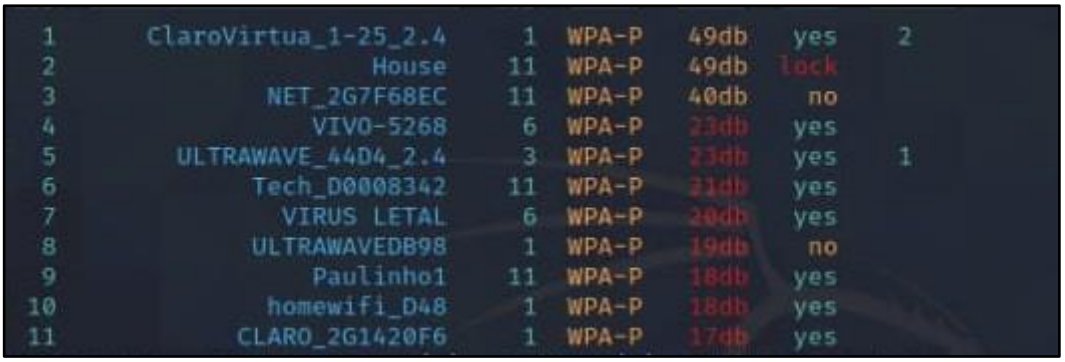
Após a instalação foram utilizados o comando *sudo wifite,* que tem como finalidade inserir a rede wi-fi em *modo assistir* e começar o processo de procura das redes *wireless* por perto, de acordo com a figura 9.

FIGURA 9: COLOCANDO A REDE WI-FI NO MODO ASSISTIR

Fonte: Os autores (2021)

Encontradas várias redes disponíveis a partir do comando de inicialização do *Wifite* como é possivel observar na figura 10 com os seguintes dados disponíveis: SSID (nome da rede), canal CH, encriptação ENCR, o sinal POWER e o WPS. Ao ser encontrada a rede que sofrerá o ataque, foram digitadas as teclas CTRL+C. Por motivo de segurança, não será demonstrado o número da rede em que realizamos a invasão .

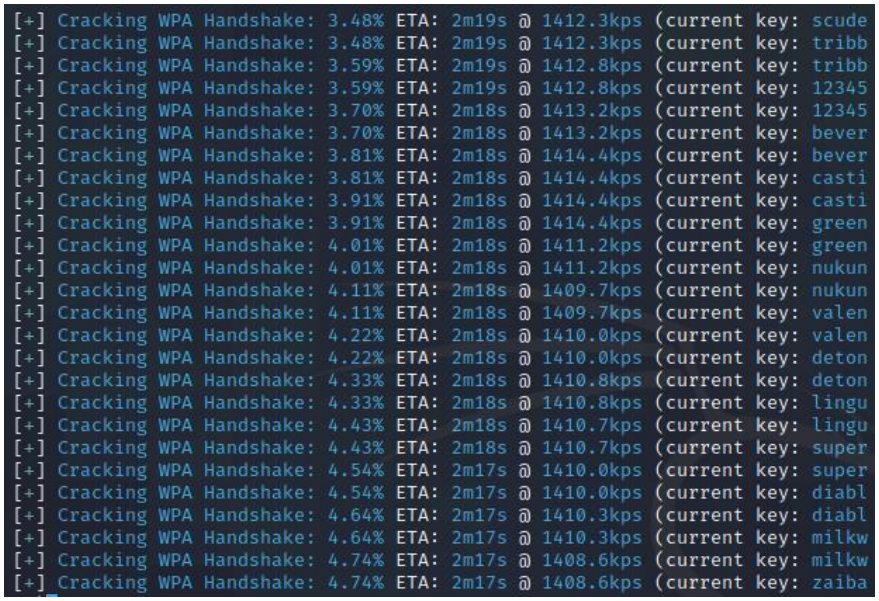
FIGURA 10: REDES SEM FIO DISPONÍVEIS NO MOMENTO DA INVASÃO



Fonte: Os autores (2021)

Com a rede selecionada deve-se aguardar cerca de 5 minutos para que o processo de scanner termine, conforme apresentado na figura 11.

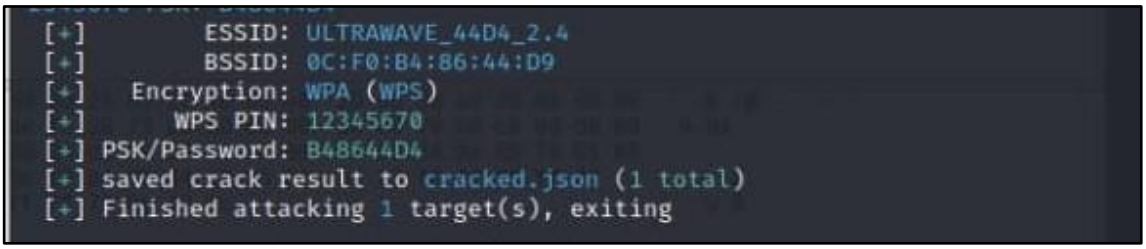
FIGURA 11: PROCESSO DE CRACKING DO WAP2



Fonte: Os autores (2021)

Após o termino, é possivel visualizar a senha, conforme figura 12 e para encerrar o modo monitor digitamos o comando *airmon-ng stop wlan0mon*.

FIGURA 12: QUEBRA DA CRIPTOGRAFIA

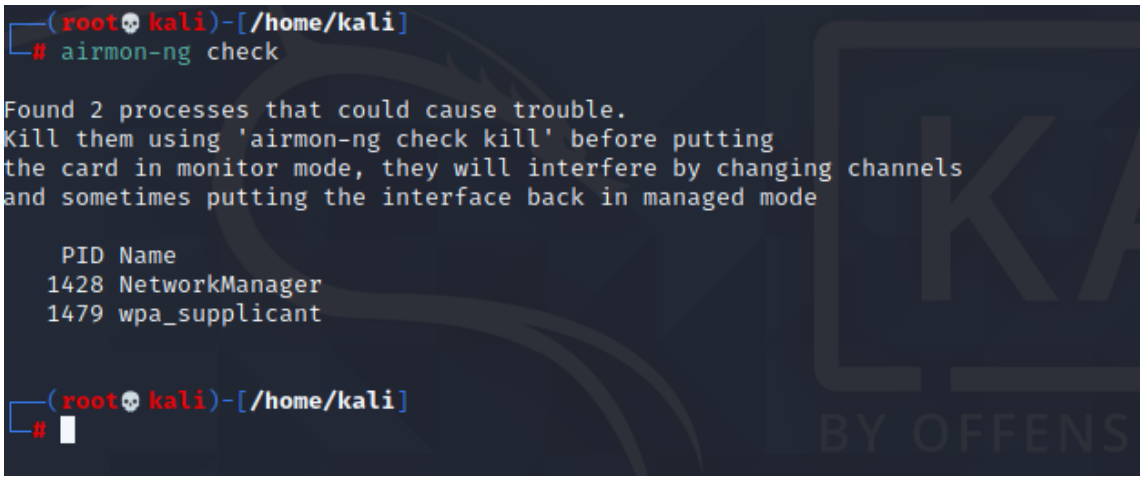


Fonte: Os autores (2021)

3.1.2 Quebra de Criptografia do Modem do Escritório

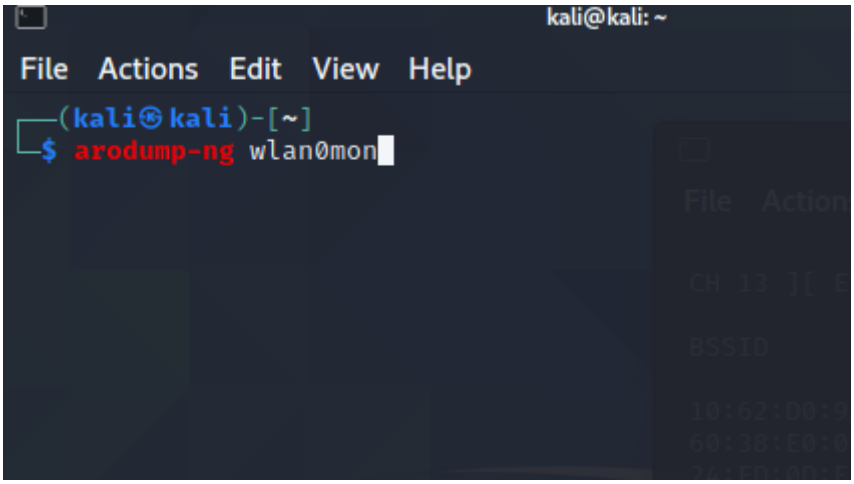
Foram utilizadas as mesmas ferramentas: *Aircrack-ng* e o *Wifite,* para a tentativa de quebra a senha do roteador do escritório, conforme detalhou-se o passo a passo anteriormente. Para que a quebra de criptografia tenha êxito é necessário localizar a existência de processos que possam entravar a invasão**,** colocar a placa *wireless* em *modo monitor* e, com o auxílio da ferramenta *Wifite* encontrar redes disponíveis para realizar o processo de *cracking* do WAP2 como é possível verificar nas figuras 13, 14, 15 e 16.

FIGURA 13: CHECANDO PROCESSOS



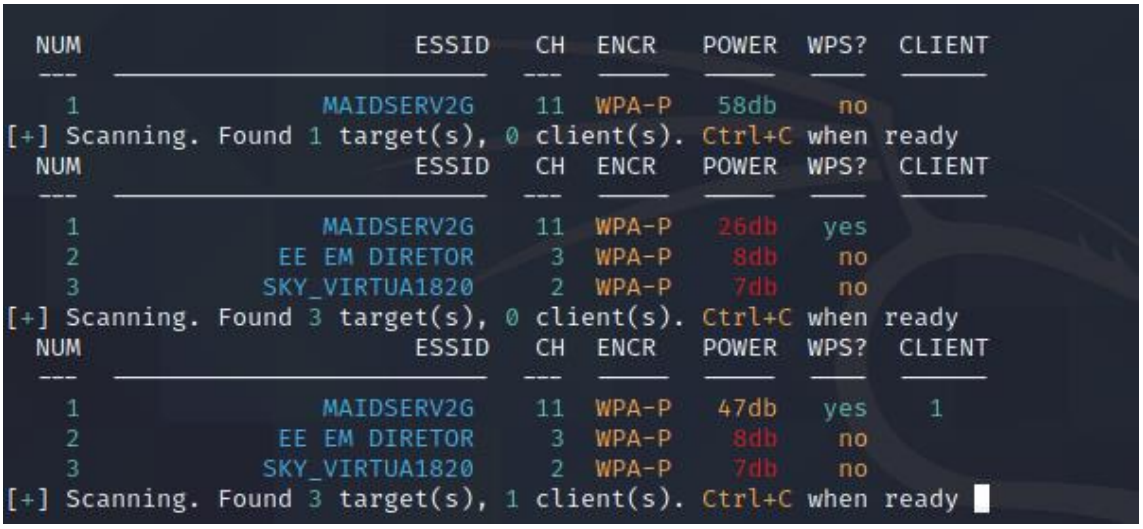
Fonte: Os autores (2021)

FIGURA 14: PLACA WIRELESS EM MODO MONITOR



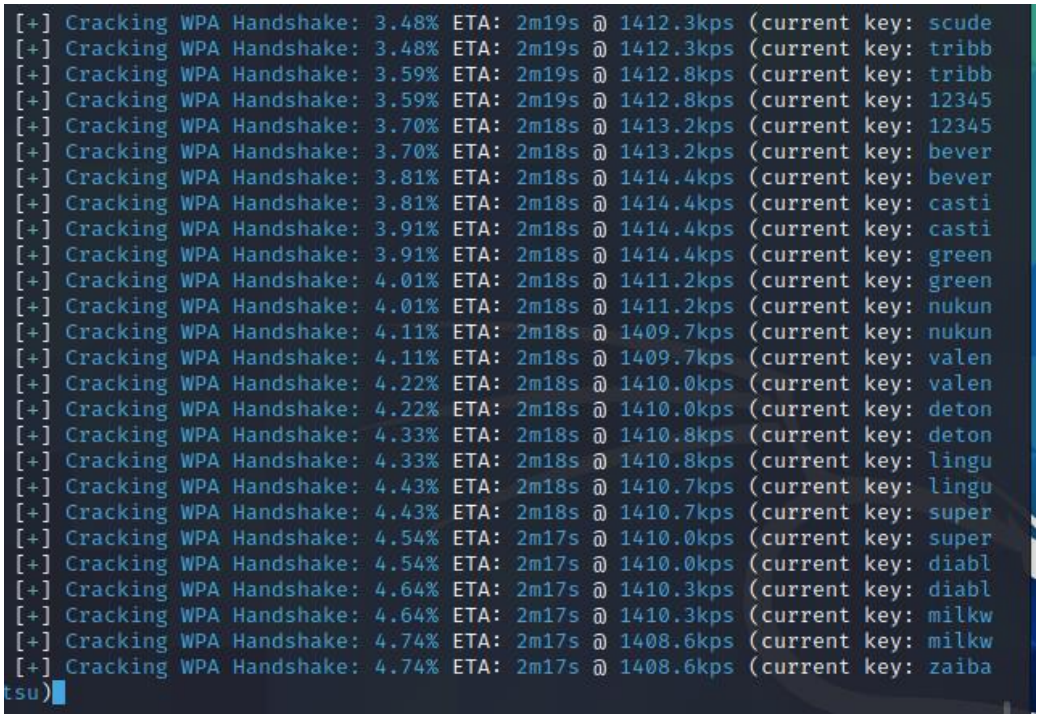
Fonte: Os autores (2021)

FIGURA 15: REDES WIRELESS DISPONÍVIES



Fonte: Os autores (2021)

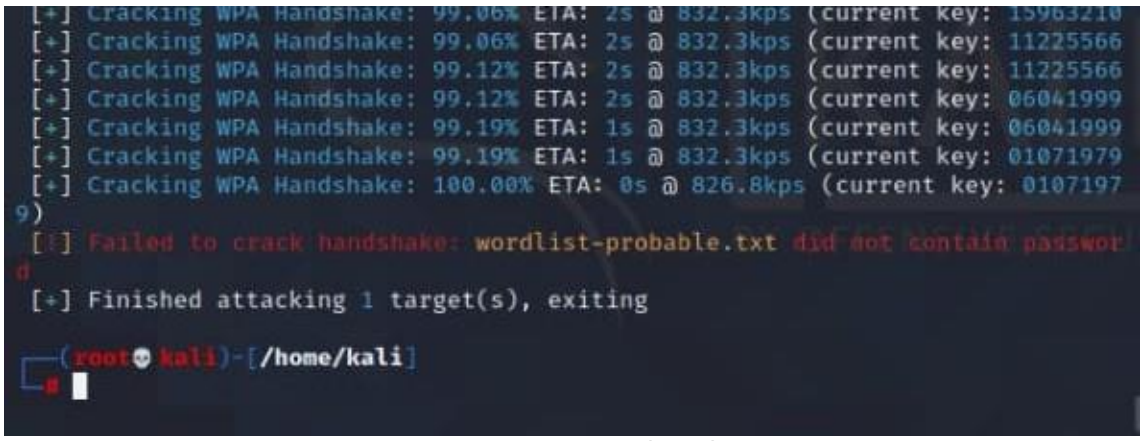
FIGURA 16: PROCESSO DE CRACKING DO WAP2



Fonte: Os autores (2021)

Neste ambiente comercial não foi possível quebrar a senha. Foi gerado um arquivo extensão txt: wordlist-probable contendo as possíveis senhas, conforme apresentado na figura 17.

FIGURA 17: LISTA DE POSSÍVEIS SENHAS



Fonte: Os autores (2021)

Segundo Moreno (2016, p.16):

> "O pentest é uma bateria de testes metodológicos que tem como objetivo descobrir, mapear e expor todas as possíveis vulnerabilidades de uma rede. Há diversos tipos de teste que podem ser realizados: rede cabeada, redes sem fio (wireless), web, revisão do código-fonte, desenvolvimento de programas que exploram vulnerabilidades em outros softwares".

Seguindo essa lógica, foi realizado um comparativo para sanar as dúvidas acerca dos roteadores, de que forma cada um deles eram configurados, que se permitiu a quebra de criptografia em um e no outro não.

FIGURA 18: TABELA DE COMPARAÇÃO DOS ROTEADORES POR PRESTADOR DE SERVIÇO

ROTEADOR ULTRAWAVE	ROTEADOR NET
Marca: MKTECH	Marca: PACE
Modelo: MP-G421R Wi-Fi Standard IEEE 802.11 b/g/n, 802.11 a/ac	Modelo: TC7337NET – eMTA DOCSIS 3.0 WI-Fi IEEE 802.11 n/b/g
Speed 1166 Mbps 2.4 GHz 2 T2R+5.8 GHz 2T2R	Speed 2.4 GHz 2T2R+5.8GHz 2T2R – 400mW
Support Protocols ITU-T G.948/G.988, IEEE 802.1D - Spanning Tree, IEEE 802.1Q – VLAN, IEEE 802.1W – RSTP, IGMP v1/v2/v3, ITU-T Y.1291, VoIP SIP	Support Protocols MAC filtering, LSB-WAN, PORT filtering, IEEE 802.1Q-VLAN, Spanning Tree, IGMP Proxy, MLd Proxy, SSDP, VoIP
Access Mode PPPoE,Bridge, IPoe	Access Mode Bridge, IPoe
Management OMCI, TR-069	Management
Algorithm SP/WRR/SP+WRR	Algorithm
Networking IPv4 & IPv6 Dual Stack	Networking IPv4 & IPv6 Dual Stack WAN
Encryption WPA-AES 128	Encryption WPA-PSK 128 TKIP
Authentication CHAP, EAP, Loopback	Authentication Loopback,

Fonte: Os autores (2021)

FIGURA 29: TABELA DE COMPARAÇÃO DOS ROTEADORES POR CONFIGURAÇÕES

ROTEADOR DA RESIDÊNCIA	ROTEADOR DO ESCRITÓRIO
O SSID não foi alterado	Teve o SSID alterado
Protocolo de Criptografia WAP2-AES	Protocolo de Criptografia WAP2-PSK
Senha sem combinação de caracteres	Senha com combinação de caracteres
Nenhum mecanismo de segurança	Teve outros mecanismos de segurança

Fonte: Os autores (2021)

No primeiro ambiente, onde a invasão foi bem-sucedida é possível associar a primeira falha encontrada no próprio SSID que não foi alterado e, quando falamos em segurança é extremamente importante, pois é inserido no cabeçalho de cada pacote que trafega pela rede, seguido de sua senha que era muito fácil e mesmo o protocolo WAP2-AES não se caracterizou como barreira para proteger a rede, sem nenhum outro mecanismo de segurança.

No segundo ambiente, o escritório, o SSID foi alterado para o próprio nome da empresa, o protocolo de criptografia é WAP2-PSK, versão que associa os pontos de acesso utilizando o método de encriptação TKIP essa versão de protocolo usa PSK (*Pre-Shared Key*) que possui oito ou mais caracteres de extensão, até um máximo de 63 caracteres. Em sua página de configurações verificamos ainda outras barreiras de proteção como o *IP Sec Passthrough* (Passagem Ipsec), conjunto de protocolos usados para implementar a troca segura de pacotes na rede como um *VPN* (Rede Virtual Privada), o *Firewall* ativado*,* habilitado nas opções no IPv4 modo baixo e IPv6 somente ligado, e a senha que tinha uma composição mais complexa combinada com caracteres. Essas opções deixaram de ser configuradas no primeiro roteador, conseguem retratar que com essas barreiras associadas ao protocolo de criptografia tornaram o ataque ineficaz.

Sendo assim é possível entender que apenas o protocolo WAP2 não mantém a rede sem fio segura, tornando necessário utilizar outros métodos de segurança. Outra opção para correção destas falhas é o protocolo WAP3 que tem como característica a utilização do protocolo *Simultaneous Authentication of Equals* (SAE) que melhora a segurança do *handshake,* sendo uma solução capaz de combater problemas de privacidade. Contudo, o protocolo WAP3 ainda não foi implementado no Brasil e se trata de uma excelente aposta para melhorar a segurança de redes sem fio.

4 Conclusão

Obter o SSID e o endereço MAC de redes sem fio que apresentam como característica de segurança, apenas o protocolo WAP2 torna a rede extremamente susceptível a invasões. A partir da implementação de outros métodos de proteção, como a própria alteração do nome da rede, a ativação de Firewall, a encriptação TKIP e uma senha combinatória de caracteres alfanuméricos e especiais, a probabilidade de acesso reduz sensivelmente.

A partir da realização do estudo Pentest, concluímos que não existem redes com criptografia indecifrável, já que com apenas duas ferramentas instaladas no sistema operacional Linux, em menos de 5 minutos declaramos a senha de um dos roteadores. Com esse estudo fica comprovada a ineficiência da segurança baseada apenas no protocolo WAP2.Todavia, o objetivo do presente estudo foi atingido, uma vez que pretendeu-se demonstrar que se associarmos o protocolo de criptografia com métodos de segurança conseguimos ter uma rede sem fio mais segura.

Portanto podemos concluir que o protocolo WPA2 torna a rede sem fio segura quando associada a outros mecanismos de segurança, assim tornando-a mais resistente a ataques em análise das criptografias utilizadas nas redes wireless, as mais antigas como WEP tornaram-se obsoletas, substituídas por o protocolo WPA2 e em breve, o WPA3, que poderá servir de base de estudos para compor novas pesquisas futuras.

5 REFERÊNCIAS

IEEE, **IEEE Standards Association:** Conjuntos de normas segundo o padrão IEEE 802.2020. Disponível em: https://standards.ieee.org/standard/index.html Acesso em: 28 set. 2020.

MORAES, Alexandre Fernandes. **Redes Sem Fio Instalação Configuração e Segurança e Fundamento.** São Paulo**:** Saraiva. 2010.

MORENO, Daniel. **Pentest em redes sem fio.** São Paulo: Novatec. 2016.

OLIVEIRA, Alan Teixeira de. **Análise das Vulnerabilidades das Redes Sem Fio na Cidade de Vitória da Conquista**. Vitória da Conquista, 2010. Monografia (Ciência da Computação) - Universidade Estadual do Sudoeste da Bahia, Vitória da Conquista. 2010.

Segurança, **Segurança Informática:** WPA3 o novo protocolo para redes WiFi. Disponível em: https://seguranca-informatica.pt/2507-2/#.YLY3QahKhPZ Acesso em: 25 maio. 2021.