Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

Curso Superior de Tecnologia em Segurança da Informação

Gabriel Silva Lopes

VULNERABILIDADE DO PADRÃO DE SEGURANÇA WPS

Americana, SP

2019

Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

Curso Superior de Tecnologia em Segurança da Informação

Gabriel Silva Lopes

VULNERABILIDADE DO PADRÃO DE SEGURANÇA WPS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Marcus Vinícius Lahr Giraldi

Área de concentração: Segurança da Informação

Americana, SP

2019

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

L852v LOPES, Gabriel Silva

Vulnerabilidade do padrão de segurança WPS. / Gabriel Silva Lopes. – Americana, 2019.

24f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. Marcus Vinícius Lahr Giraldi

1 Segurança em sistemas de informação I. GIRALDI, Marcus Vinicius Lahr II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: *681.518.5*

Fatec Americana
Ministro Ralph Biasi

Centro Paula Souza

SÃO PAULO
GOVERNO DO ESTADO

Faculdade de Tecnologia de Americana

Gabriel Silva Lopes

VULNERABILIDADE DO PADRÃO DE SEGURANÇA WPS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana.
Área de concentração: Segurança da Informação

Americana, 07 de Dezembro de 2019.

Banca Examinadora:

Marcus Vinícius Lahr Giraldi
Prof. Esp.
Fatec Americana

Alberto Martins Júnior
Prof. Ms.
Fatec Americana

Estevão da Silva Barros
Prof. Esp.
Fatec Americana

RESUMO

O uso das redes de comunicações vem se modificando pelos avanços tecnológicos e pela necessidade da sociedade em integrar os equipamentos na vida corriqueira. O Wi-Fi, ferramenta essencial para a sociedade contemporânea, possui padrões de segurança para manter a confidencialidade da rede sem fio, e dentre esses padrões está o WPS (*Wi-Fi Protected Setup*). Esse projeto busca analisar a vulnerabilidade desse modo de segurança, demonstrando sua falha através de um teste de invasão em uma rede sem fio, verificando se o mesmo é viável para garantir a confidencialidade de redes domésticas ou empresariais. Para isso, foram realizadas pesquisas bibliográficas através de artigos científicos de autores especialistas da área em questão, apresentando uma breve história da tecnologia e da internet até o surgimento dos padrões de segurança para redes sem fio, focando no padrão WPS e seu funcionamento, e, por fim, realizando um estudo de caso para comprovar sua vulnerabilidade, deixando recomendações para que os leitores evitem possíveis invasões em suas redes.

Palavras Chave: Segurança da Informação; Redes Sem Fio; WPS.

ABSTRACT

The use of communications networks has been changing due to technological advances and the need of society to integrate the equipment into everyday life. Wi-Fi, an essential tool for contemporary society, has security standards to maintain the confidentiality of the wireless network, and one of those standards is Wi-Fi Protected Setup (WPS). This project seeks to address the vulnerability of this security mode by demonstrating its flaw through a wireless network penetration test, verifying if it is viable to ensure the confidentiality of home or business networks. To this end, bibliographic researches were conducted through scientific articles by experts in the field, presenting a brief history of technology and the Internet until the emergence of security standards for wireless networks, focusing on the WPS standard and its operation, and, finally, by conducting the case study to prove its vulnerability, leaving recommendations for readers to prevent potential intrusions into their networks.

Keywords: *Information Security; Wireless Networks; WPS.*

SUMÁRIO

LISTA DE FIGURAS

1 INTRODUÇÃO

A inevitável evolução tecnológica facilitou inúmeras tarefas do cotidiano de pessoas e empresas. Novos sistemas computacionais surgem, o que faz com que o ambiente empresarial se integre cada vez mais na Internet.

Alguns anos atrás, essa integração das empresas na rede global de computadores só era possível através de cabos de redes físicos e dispositivos computacionais de médio porte, hoje, a conexão com a Internet pode ser realizada de modos mais fáceis, rápidos e simples, como, por exemplo, através de redes sem fio. Foi nesse contexto que surgiu o WPS (*Wi-Fi Protected Setup*), a fim de estabelecer uma conexão via Wi-Fi rápida e fácil, porém, junto a essa praticidade, abriram-se novos meios de ataques a rede.

Esse projeto busca analisar e demonstrar a vulnerabilidade e problemas ocasionados pelo WPS, verificando a viabilidade de mantê-lo ativo de modo seguro, buscando a confidencialidade, integridade e disponibilidade dessas redes sem fio, para que se possa trabalhar em um ambiente empresarial ou doméstico de forma segura. Mais especificamente, este trabalho buscou analisar e discutir o funcionamento do WPS e realizar um teste de invasão a fim de demonstrar as vulnerabilidades desse padrão de segurança. Para isso, foi feito um levantamento bibliográfico através de artigos científicos de especialistas da área e estudo de campo realizado pelo autor.

O trabalho se estruturou em cinco capítulos, sendo que o primeiro tratada da origem e evolução da tecnologia e, consequentemente, da história da internet até a chegada das redes sem fio e criação dos padrões de segurança para as mesmas, focando no funcionamento do WPS. No segundo capítulo foi apresentado como ocorre o ataque ao sistema WPS, abordando a sua falha estrutural quando submetido a um ataque de força bruta. No terceiro capítulo foi realizado um estudo de caso, a fim de comprovar e explorar a vulnerabilidade através de um ataque a uma rede sem fio doméstica do próprio autor. No quarto capítulo, recomendações foram sugeridas para os leitores com o intuito de evitar possíveis ataques às suas redes sem fio. Por fim, o último capítulo se reserva às considerações finais.

2 EVOLUÇÃO DA TECNOLOGIA / WPS

As pessoas costumam pensar na tecnologia como algo muito mais recente e restrito do que ela realmente é, isto porque ela está mais integrada na nossa vida do que podemos imaginar, como dito pelo pai da computação ubíqua - aquela que faz parte do cotidiano de modo imperceptível: “As mais profundas tecnologias são aquelas que desaparecem. Elas se misturam no tecido da vida cotidiana até o momento em que não se pode mais distingui-las.” (Weiser, 1991). Afinal, o que é tecnologia?

> Podemos dizer que a tecnologia é o uso de técnicas e do conhecimento adquirido para aperfeiçoar e/ou facilitar o trabalho com a arte, a resolução de um problema ou a execução de uma tarefa específica. (KARASINSKI, 2013)

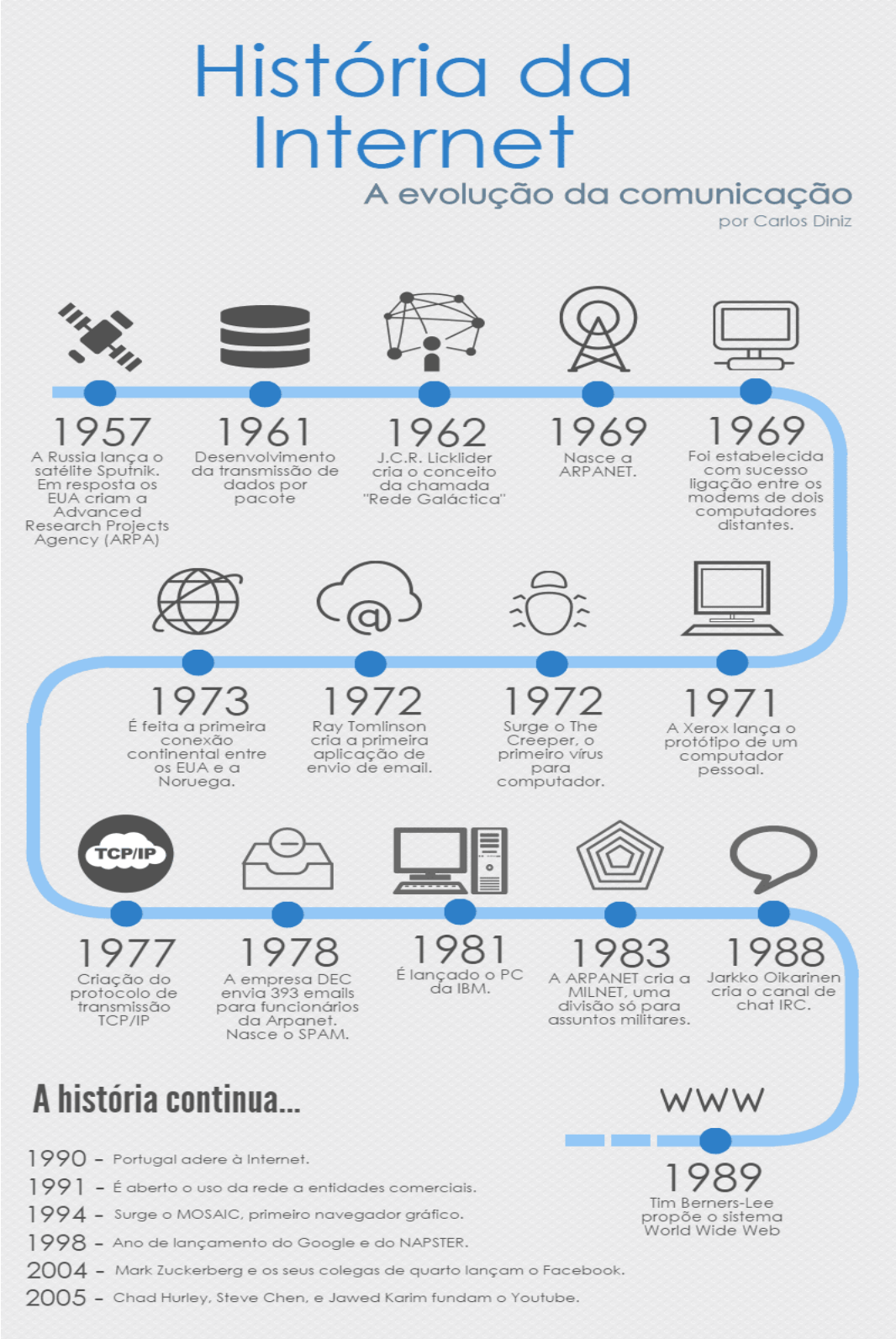
Partindo dessa definição, o surgimento da tecnologia pode ser reconhecido há mais tempo do que se imagina, mesmo que não haja uma data precisa de sua origem, existem registros (como a descoberta do fogo ou a criação de ferramentas de pedra) datados há mais de milhões de anos. Portanto, a tecnologia abrange os avanços das diversas áreas do conhecimento humano, como uma forma de lidar com os inúmeros obstáculos encontrados no cotidiano.

Uma dessas ferramentas tecnológicas mais utilizadas hoje em dia, a internet, surgiu em 1969, inicialmente era denominada de ARPANET (*Advanced Research Projects Agency Network*), que levou esse nome por ter nascido na Agência para Projetos de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos da América. Sua finalidade era ser um sistema de telecomunicações descentralizado de alta disponibilidade, sem que pudesse ser interrompido ou desmantelado por um ataque localizado. Tal preocupação era justificada pelo fato dos EUA estarem em meio a Guerra Fria, que estava em seu auge.

Logo após alguns anos, a ARPANET foi crescendo, cada vez mais computadores e dispositivos iam se conectando, formando assim a internet - que é basicamente a rede internacional de computadores e dispositivos informáticos conectados e dispersos por todo o planeta que se comunicam através de uma linguagem (protocolo) em comum.

Na figura 1, abaixo, estão as datas da origem e evolução da internet, desde o lançamento do Sputnik pela Rússia, durante a Guerra Fria, até a concepção da *World Wide Web* (www), que permitiu o acesso a internet como temos hoje.

Figura 1 - História da Internet



Fonte: Carlos Diniz (2015)

O padrão internacional para redes sem fio (IEE 802.11) foi criado em 1997 pelo Instituto de Engenheiros Eletricistas e Eletrônicos, ele definiu diversas normas que estabeleciam a transmissão e codificação para as redes sem fio através de ondas de rádio. De acordo com o site da WiFi Alliance, o grupo criador do padrão Wi-Fi surgiu em 1999, e desde então, o mercado começou a adotar esse padrão de conectividade e diversas novas tecnologias foram surgindo, até chegar no ponto em que estamos hoje.

O Wi-Fi funciona, de acordo com Juliane Pixinine:

> As redes Wi-Fi fazem uso de ondas de rádio comuns para transmitir as informações de Internet, assim como acontece com a televisão, rádio e celular, por exemplo. Essas redes funcionam através de ondas de rádios transmitidas por meio de um adaptador, o roteador, que recebe os sinais, decodifica e os emite a partir de uma antena, sendo a parte principal do Wi-Fi. A troca de informações acontece em uma das duas frequências disponíveis pelos governos, a de 2.4 GHz ou a de 5GHz. Quanto mais alta a frequência, maior também a capacidade do sinal carregar um alto número de informações. (PIXININE, 2015)

Os roteadores modernos facilitam a configuração de redes sem fio domésticas, sendo capazes de cobrir toda ou boa parte da casa do usuário. Tal cobertura da rede sem fio, na maioria dos casos, estende-se para mais longe do que a área planejada de seu uso, tornando possível o acesso a essa rede e aos dados trafegados nela por terceiros não autorizados. Isto levanta uma importantíssima questão de segurança da informação, o que fez necessário a criação de padrões de segurança nas redes Wi-Fi para garantir a confidencialidade, integridade e disponibilidade dos dados.

O primeiro padrão que surgiu para tentar contornar esta situação foi o *Wired Equivalent Privacy*, que se provou ineficiente para lidar com esse problema (devido a um algoritmo criptográfico fraco). O padrão, mais seguro, que surgiu para substituir o WEP foi o Wi-Fi *Protected Protocol* (WPA), e após ele o WPA2 - que possui um forte modo de criptografia e melhor segurança. Como dito pelos autores Petiz *et al* (2013), protocolos mais seguros requerem configurações mais complexas, o que é um problema para os usuários, podendo fazer com que eles desabilitem a segurança sem fio para evitar tais configurações difíceis.

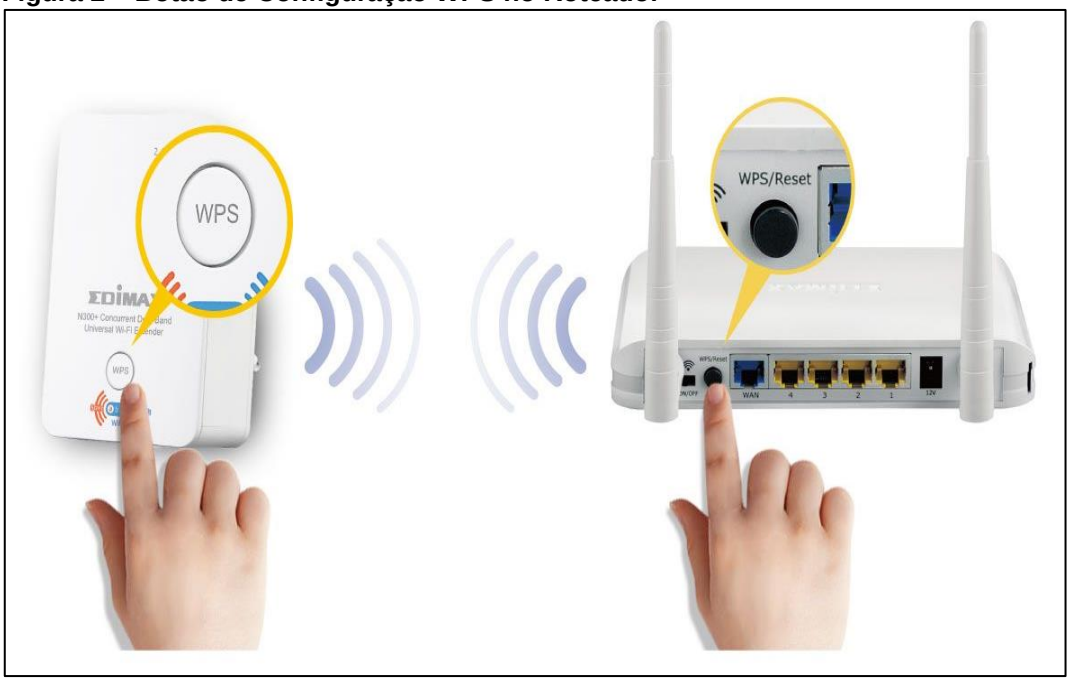
O WPS foi criado justamente para tentar resolver este problema, sendo um padrão de fácil configuração por usuários leigos, unindo a praticidade e segurança ao mesmo tempo.

2.1 FUNCIONAMENTO DO WPS

O WPS foi criado com a finalidade de simplificar e unir praticidade e segurança na conexão de dispositivos com a rede Wi-Fi. A criptografia utilizada pela rede e seu SSID (nome identificador) são definidos automaticamente, o que faz com que seja possível a conexão com a rede de duas formas diferentes, de acordo com os autores Zisiadis *et al* (2012):

- PBC (*Push Button Configuration*): para estabelecer conexão dessa forma é necessário inicializar o procedimento de configuração automática, que é realizado ao apertar o botão do WPS no dispositivo que você quer conectar e no ponto de acesso ou roteador, ao qual será conectado o dispositivo, conforme exemplificado na figura 2. Este botão pode ser físico, localizado no aparelho, ou virtual, mostrado na tela durante a configuração.

Figura 2 – Botão de Configuração WPS no Roteador



Fonte: Edimax Technology

- PIN (*Personal Identification Number*): neste método, os dispositivos que possuem o WPS habilitado recebem um PIN instalado de fábrica (no próprio dispositivo ou gerado dinamicamente e exibido na tela). O PIN do dispositivo a ser conectado na rede deve ser lido e inserido na interface web do AP ou roteador que realizará a configuração, se o PIN for validado com sucesso. A caminho inverso também pode ser realizado, ler o PIN do

AP (localizado normalmente em um adesivo na base do roteador, conforme figura 3) e inserir o mesmo na interface da tela do dispositivo a ser conectado.

Figura 3 – Número do PIN Localizado no Roteador

Fonte: The Sh3llc0d3r's Blog (2016)

3 COMO O ATAQUE OCORRE

O grande problema do WPS é que em muitos roteadores domésticos dos principais fornecedores não há segurança necessária para manter o recurso ativo. De acordo com o Instituto de Engenharia de Software da Universidade Carnegie Mellon, os roteadores que possuem o método PIN do WPS estão suscetíveis a ataques de força bruta (tipo de ataque baseado em testar todas possibilidades de senhas até obter acesso ao sistema), como constatado pelos autores Petiz *et al* (2013), se inserirmos o PIN do roteador sem fio no dispositivo do usuário (por meio do método PIN), é possível, em roteadores domésticos de marcas mais presentes no mercado, realizar várias tentativas antes do endereço MAC (*Media Access Control* – endereço físico que identifica o equipamento) do dispositivo atacante ser bloqueado. Além disso, alguns roteadores nem sequer bloqueiam esses dispositivos, permitindo a execução de um ataque por força bruta contínuo sem quaisquer restrições. A maioria dos roteadores que usam o WPS tem o recurso PIN habilitado por padrão e são incapazes de desabilitá-lo. A importância dessa falha é que, se olharmos para a estrutura do PIN, conforme figura 2 abaixo, vemos que o mesmo consiste em 8 dígitos, onde o oitavo dígito é um *checksum* (soma de verificação dos outros dígitos), então, o número de tentativas necessárias para descobrir o PIN é igual a, no máximo, 10^8 (cem milhões).

Figura 4 - Estrutura do PIN

1	2	3	4	5	6	7	8
1ª Parte				2ª Parte			CS

Fonte: Carlos Diniz (2015)

O *checksum* é o oitavo dígito, que é calculado da seguinte forma, de acordo com o site WiFi Libre (2015): o primeiro, terceiro, quinto e sétimo dígitos são multiplicados por 3, enquanto o segundo, quarto e sexto dígito são multiplicados por 1. O resultado de cada multiplicação é somado, obtendo-se um número novo. É guardado o último dígito desse número da soma, o qual será reservado para o próximo cálculo. Nesse próximo cálculo, o número reservado é o subtraendo de uma subtração que possui o minuendo com o valor de 7. O resultado dessa última subtração é o número do *checksum*. Por exemplo, se quisermos calcular o último dígito (*checksum*) do PIN 9999999, deve ser feito da seguinte forma:

- **1º Passo: Multiplicação**

(9x3) + (9x1) + (9x3) + (9x1) + (9x3) + (9x1) + (9x3)

- **2º Passo: A soma**

27 + 9 + 27 + 9 + 27 + 9 + 27 = **135**

- **3º Passo: Dígito de verificação**

Reservamos o último dígito da soma acima = **5**

- **4º Passo: Subtração**

10 – 5 (dígito de verificação) = **5 (*checksum*)**

Portanto, o PIN WPS válido é **99999995**.

O processo de autenticação do WPS entre os dispositivos, segundo Goncharov et al (2018), é realizado em oito etapas, da seguinte forma, conforme figura 3 abaixo:

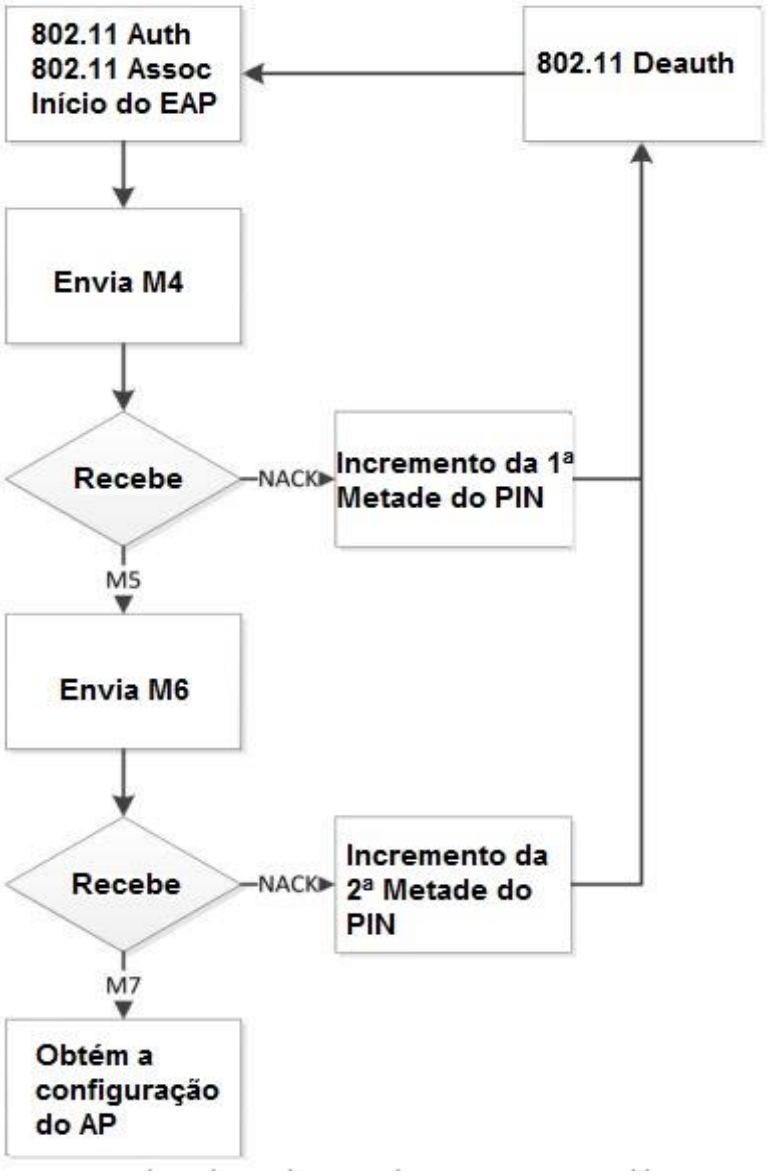
Figura 5 – Processo de Autenticação do WPS

Nº MSG	*Tipo*	*Ação*
M1	AP→client	Cálculo das chaves públicas pelo algoritmo Diffie-Hellman para a primeira e segunda parte do código PIN
M2	AP←client	
M3	AP→client	Envio das chaves públicas para a primeira e segunda parte do código PIN
M4	AP←client	Confirmação da primeira metade do PIN
M5	AP→client	Confirmação da segunda metade do PIN
M6	AP←client	Confirmação e reconhecimento da segunda metade do código PIN
M7	AP→client	Confirmação e reconhecimento da segunda metade do PIN, envio da configuração do AP
M8	AP←client	Configuração do *Access Point*

Fonte: Autor (2019)

AP (*access point*) é o roteador que está realizando a comunicação com o *client*, que é o dispositivo requisitor da conexão. Cada mensagem trocada entre eles (numeradas de M1 até M8) é responsável por uma etapa na comunicação entre os dispositivos. Um ataque *brute force* otimizado, de acordo com Stefan (2011), funciona da seguinte maneira, como explícito na figura 4:

Figura 6 – Ataque Brute Force Otimizado



Fonte: Autor (2019)

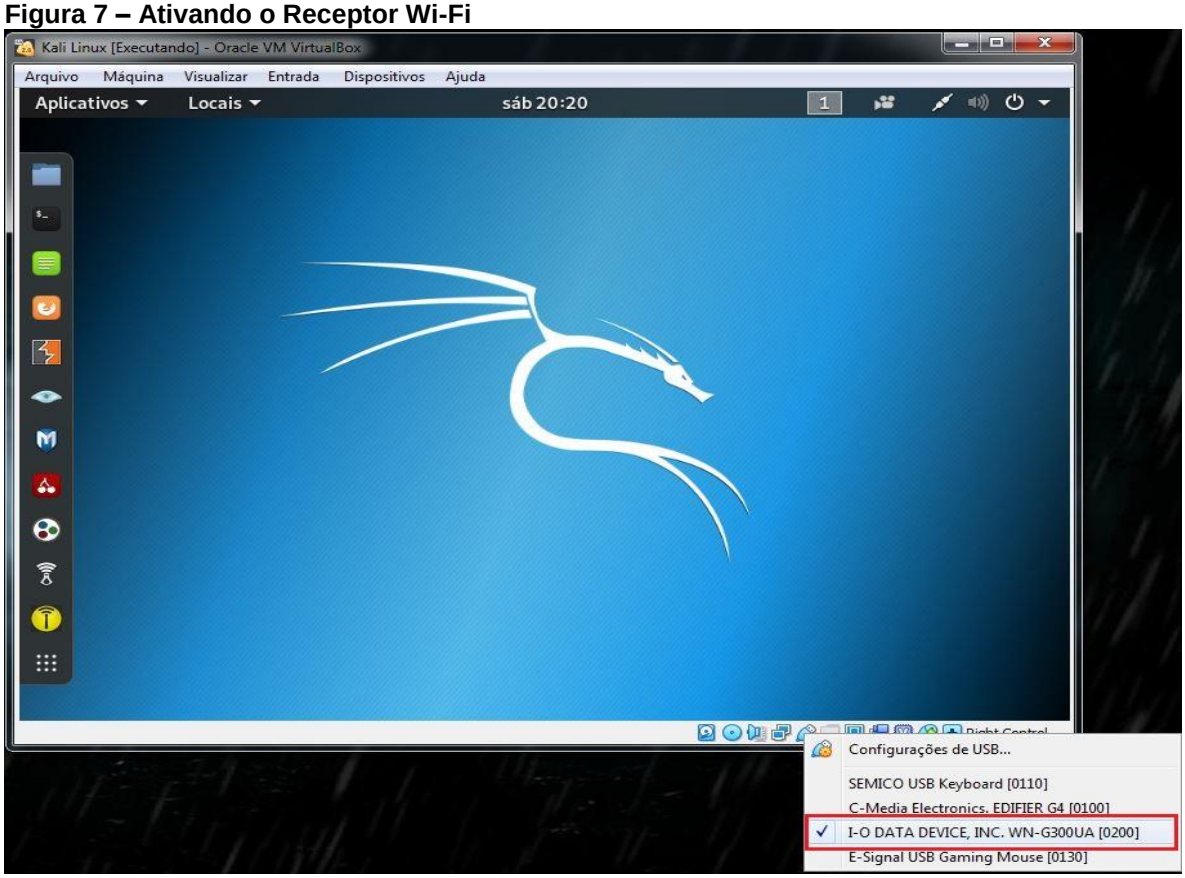
O ataque por força bruta, dessa forma, verifica os 4 primeiros dígitos e em seguida, se esses 4 primeiros dígitos estiverem corretos, iniciam-se as tentativas para descobrir os últimos 4 últimos dígitos. Sendo assim, no pior caso, seria necessário tentar 10^4 (dez mil) combinações numéricas para descobrir a primeira parte, e então, outras 10^3 (mil) tentativas para encontrar a última parte: como o último número é o *checksum* e pode ser calculado pelo atacante, são necessárias apenas 11.000 tentativas, no máximo, para descobrir o PIN correto do roteador sem fio e descobrir a senha do WPA/WPA2, sendo que, na maioria das vezes, é necessário testar apenas metade das combinações possíveis.

4 ESTUDOS DE CASO

Para realizar o teste de intrusão, a fim de comprovar a vulnerabilidade do padrão WPS, foram utilizados os seguintes recursos: o sistema operacional Kali Linux virtualizado através do Virtual Box, um receptor Wi-Fi USB e um roteador Tp-Link com o WPS ativo. O passo a passo para a execução se deu da seguinte forma:

1. O primeiro passo, como exibido na figura 5, foi ativar o receptor Wi-Fi no sistema operacional Kali Linux virtualizado.

Figura 7 – Ativando o Receptor Wi-Fi

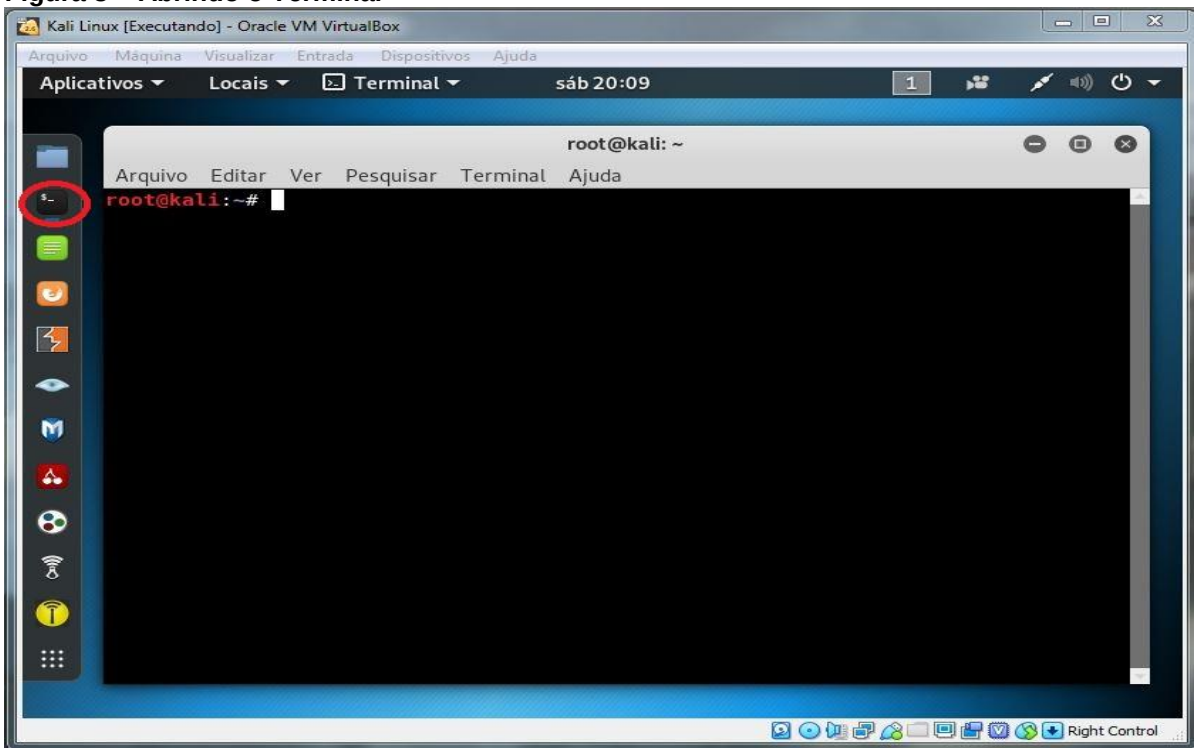


Fonte: Autor (2019)

2. O segundo passo, mostrado na figura 6, foi abrir o terminal e executar o comando *iwconfig* (conforme figura 7) para descobrir o nome da interface de rede do adaptador wireless USB, percebemos que a mesma está no modo *managed,* isto é, o modo padrão, utilizado para realizar conexões sem fio na forma comum, escolhendo uma rede e inserindo a senha da mesma. Em seguida, como podemos ver na figura 8, foi executado o programa *Aircrack-ng* (instalado por padrão no Kali Linux), inserindo o comando *airmon-ng start wlan0mon*.

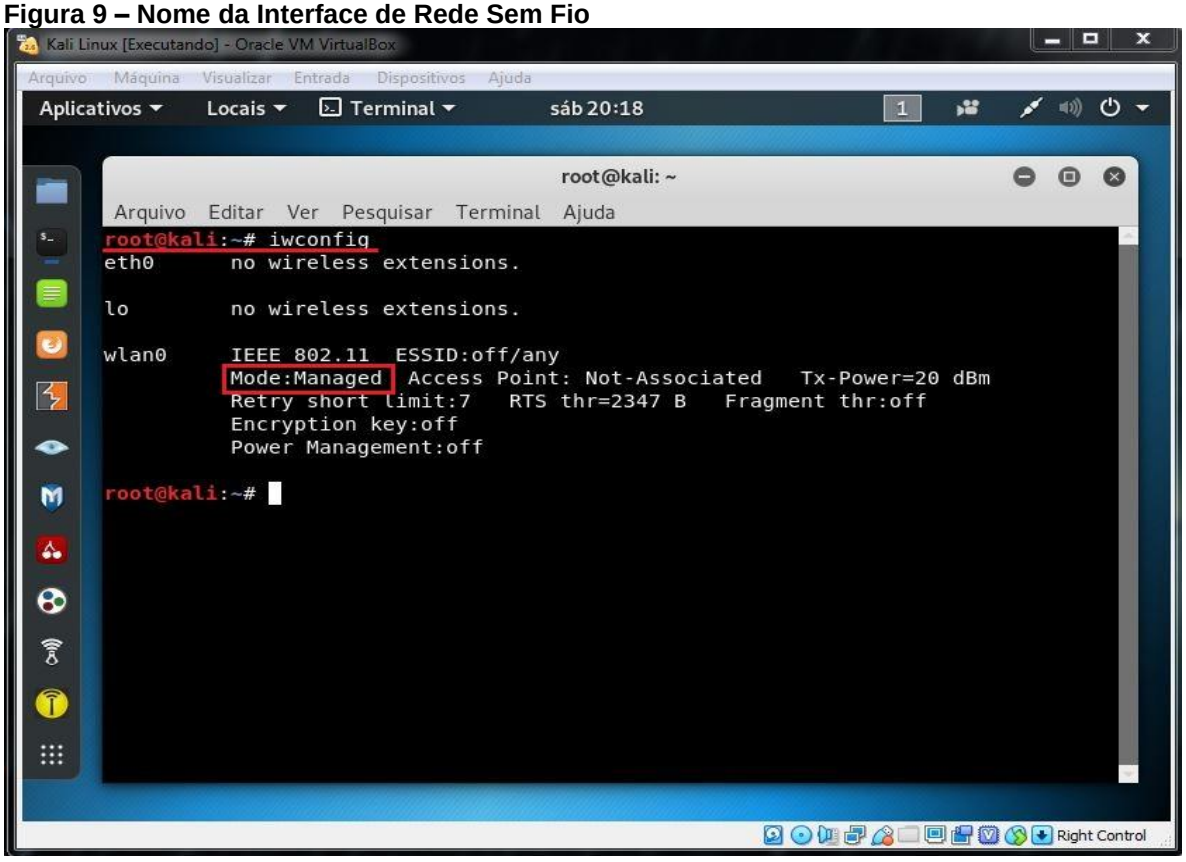
Este comando configura a placa de rede Wi-Fi para o modo monitor, ou modo de escuta. Neste modo a antena capta as Redes Wi-Fi que estão em seu alcance.

Figura 8 – Abrindo o Terminal



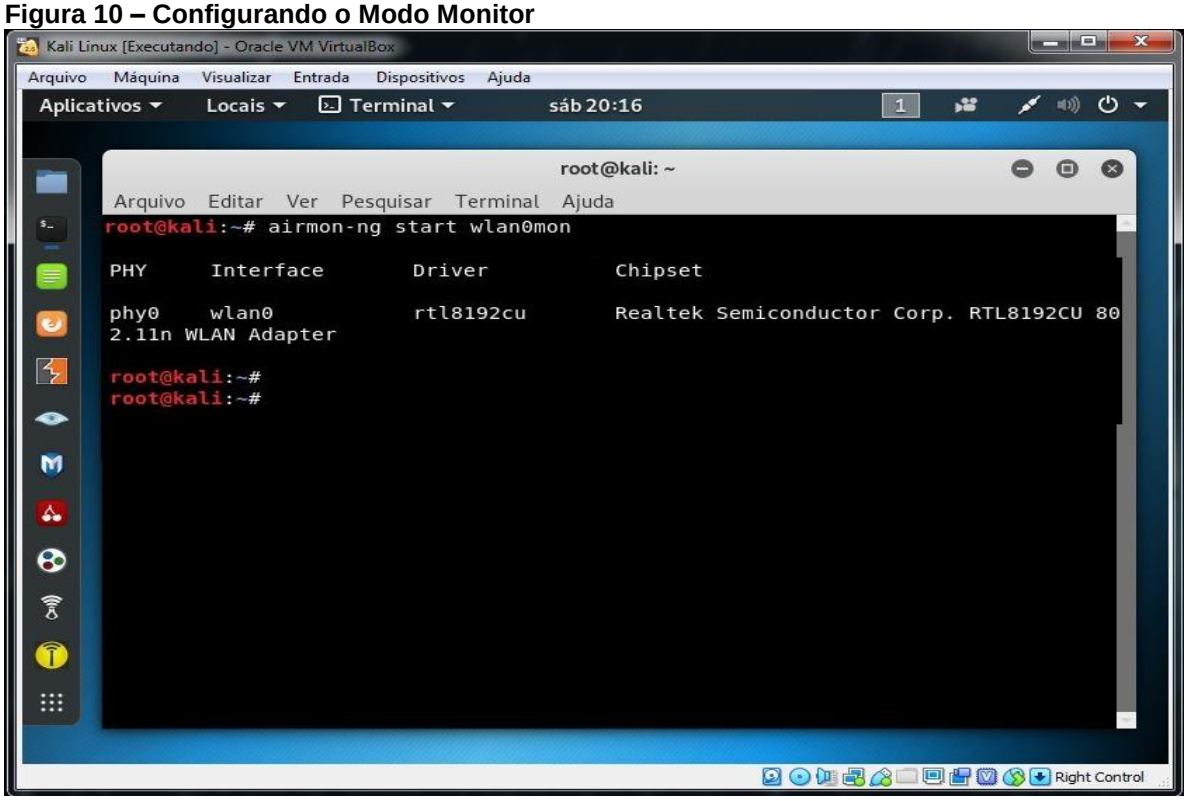
Fonte: Autor (2019)

Figura 9 – Nome da Interface de Rede Sem Fio



Fonte: Autor (2019)

Figura 10 – Configurando o Modo Monitor



Fonte: Autor (2019)

3. O terceiro passo, de acordo com a figura 9, foi executar o programa *Wash* (instalado por padrão no Kali Linux), inserindo o comando *wash -i wlan0mon*, este comando lista as redes Wi-Fi captadas pelo modo monitor e exibe informações como o nome identificador, endereço MAC, potência de conexão e fabricante das redes sem fio.

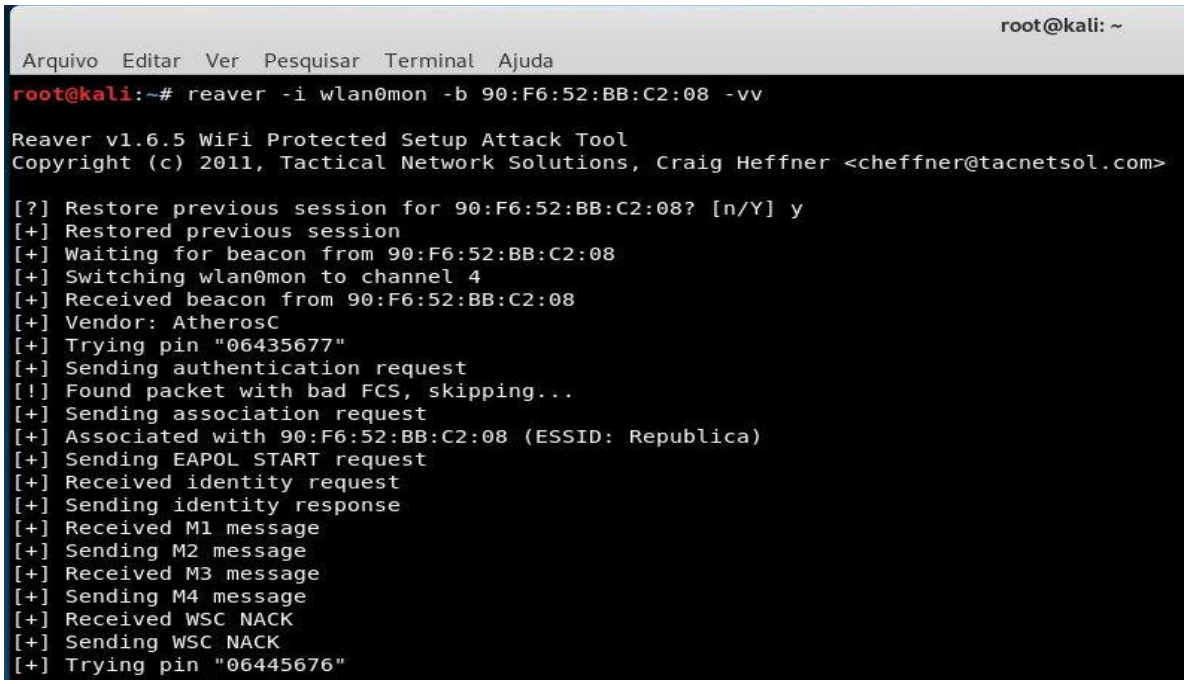
Figura 11 – Descobrindo as Redes Próximas

```
root@kali:~# wash -i wlan0mon
BSSID               Ch  dBm  WPS  Lck  Vendor    ESSID
--------------------------------------------------------------------------------
98:97:D1:F9:F0:40    1  -74  2.0  No   RalinkTe  VIVO-F040
70:54:D2:DC:2D:E7    1  -40  2.0  No   Broadcom  Wifi Teste
90:F6:52:BB:C2:08    4  -44  1.0  No   AtherosC  Republica
4C:D0:8A:D0:D8:6E    6  -72  2.0  No   Broadcom  STYLLO_VEST
8C:04:FF:13:97:3D   11  -74  2.0  No   Broadcom  Adilson
^C
```

Fonte: Autor (2019)

4. O quarto passo, conforme figura 10, foi executar o programa *Reaver* (instalado por padrão no Kali Linux), inserindo o comando *reaver –i wlan0mon –b 90:F6:52:BB:C2:08 –vv,* este é o comando que executará o ataque de força bruta, nele está definida a interface de rede do receptor Wi-Fi, o endereço MAC do roteador e o modo *verbose*, que permite acompanhar tudo o que está sendo feito em tempo real.

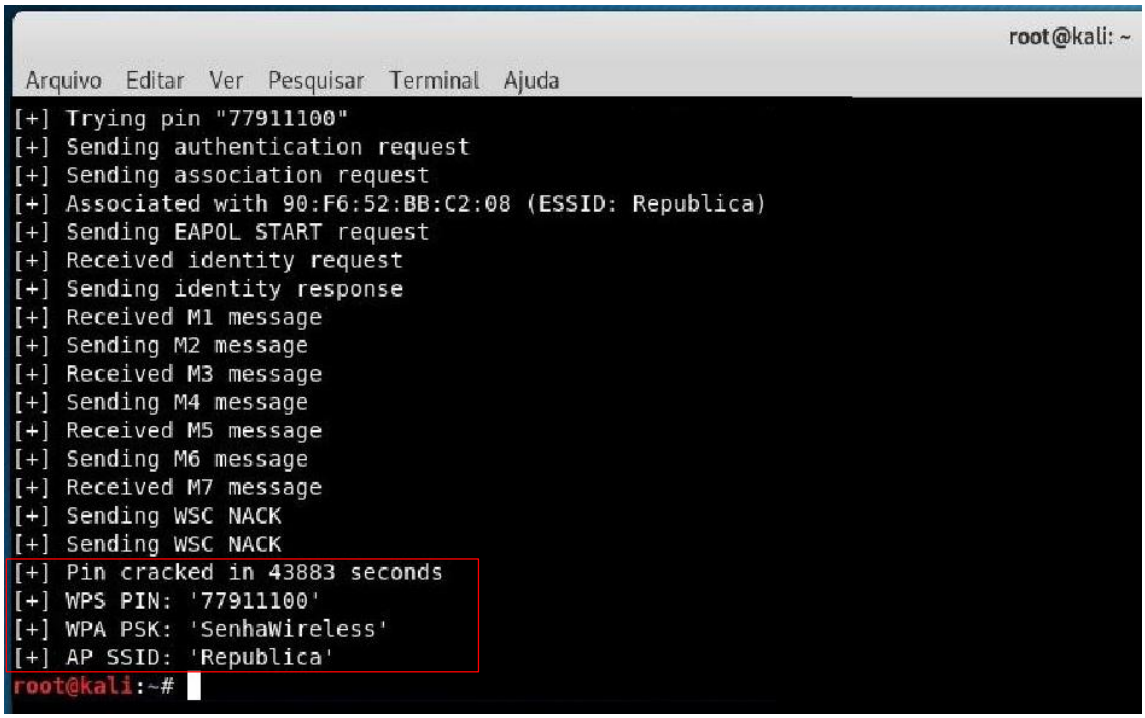
Figura 12 – Executando o Ataque Brute Force



Fonte: Autor (2019)

5. Após mais de 10 horas, o ataque foi bem-sucedido e exibiu no terminal (figura 11) o PIN e a chave de acesso WEP da rede Wi-Fi.

Figura 13 – PIN e senha WPA

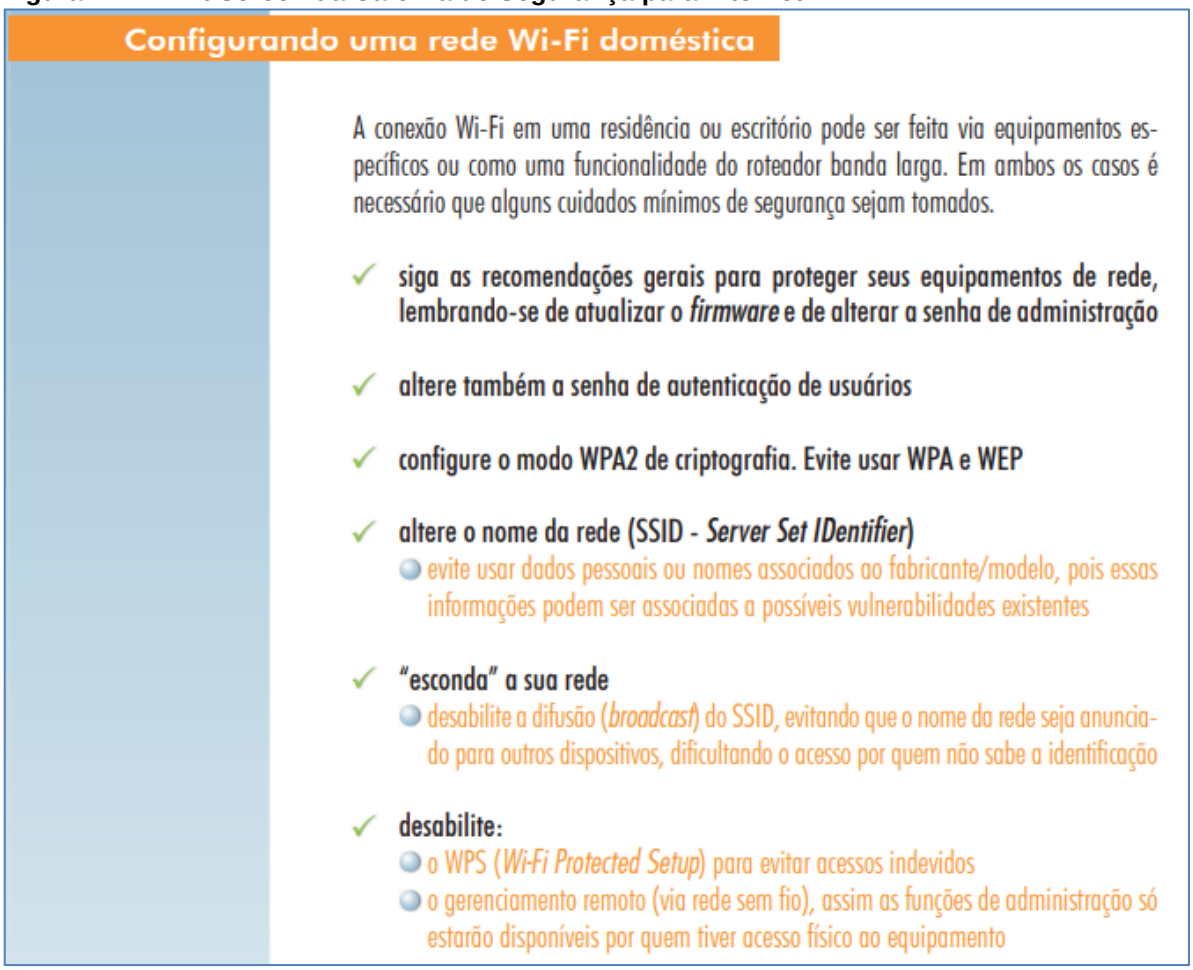


Fonte: Autor (2019)

5 RECOMENDAÇÕES

Tendo em vista a falha estrutural e de implementação do WPS, recomendo fortemente desativá-lo, principalmente nos casos de roteadores domésticos. Não é uma praticidade que vale a pena o risco. Nas situações em que os roteadores não permitem a desativação do recurso, é recomendável atualizar seu *firmware* (*software* programado diretamente no *hardware* do dispositivo), pois existem atualizações que corrigem a falha de tentativas de inserção do PIN ilimitadas. Caso a atualização de *firmware* não resolva o problema, deve-se considerar a aquisição de um novo roteador imune a este tipo de ataque. Na imagem abaixo, seguem algumas recomendações do CERT.BR para a segurança de redes Wi-Fi:

Figura 14 – Print Screen da Cartilha de Segurança para Internet



Fonte: CERT.BR (2017)

Outras recomendações de segurança são: desativar o acesso remoto ou outros serviços que não são utilizados e podem estar ativos no seu roteado; caso

seu roteador possuir *firewall* embutido, é uma boa prática ativá-lo; sempre utilize uma senha de acesso a rede forte de, no mínimo, 7 dígitos e misturando letras maiúsculas com minúsculas, junto de números e símbolos. Dessa forma você praticamente anula ataques de força bruta, pois o tempo necessário para descobrir uma senha formatada dessa forma é inviável para um possível atacante; evite realizar transações bancárias ou enviar informações pessoas se estiver conectado em uma rede pública; desabilite a funcionalidade de rede sem fio em seu roteador no caso de você usar apenas a rede local cabeada e não o Wi-Fi; Por fim, caso não esteja utilizando seu equipamento de rede, desligue-o. Ninguém invadirá seu roteador se o não estiver operando.

6 CONSIDERAÇÕES FINAIS

A internet é, atualmente, praticamente indispensável pela maior parte de seus usuários, e está cada vez mais se integrando no dia a dia da sociedade. As redes sem fio facilitaram muito o acesso a internet, trazendo mais conforto e flexibilidade. Grande parte dos dispositivos eletrônicos possuem comunicação sem fio, e a aquisição desses dispositivos está também, hoje, muito mais presente nas classes sociais mais baixas do que antigamente. Portanto, é essencial zelar pela segurança em dispositivos com conectividade sem fio, considerando que estamos em uma era que, às vezes, o seu bem mais valioso ou de uma empresa pode ser as informações.

A partir do desenvolvimento deste trabalho pela pesquisa teórica e de campo, conclui-se que apesar da falha do WPS não ser recente, ainda podem existir muitos roteadores sem fio com esta vulnerabilidade presente no equipamento, e no caso de ser explorada, pode resultar no comprometimento dos pilares da segurança da informação, sendo possível resultar no roubo de dados e informações, interrupção da disponibilidade do serviço ou adulteração dos dados armazenados.

Conforme recomendações do capítulo 5, como método mais efetivo e garantido deve-se desativar o recurso WPS, principalmente em roteadores domésticos.

Em trabalhos futuros é possível explorar as fraquezas do WEP, WPA, WPA2 e WPA3, a fim de se expandir e dar continuidade nas análises de vulnerabilidades dos padrões de segurança em redes Wi-Fi.

REFERÊNCIAS BIBLIOGRÁFICAS

CARNEGIE MELLON UNIVERSITY. **Wifi Protected Setup (Wps) Pin Brute Force Vulnerability**. Disponível em: <https://www.kb.cert.org/vuls/id/723755/>. Acesso em: 23 out. 2019.

CERT.BR. **Cartilha de Segurança Para Internet:** Fascículo Redes. 2017. Disponível em: <https://cartilha.cert.br/fasciculos/redes/fasciculo-redes.pdf>. Acesso em: 02 nov. 2019.

GONCHAROV, D. E. et al. **Vulnerability analysis of the Wifi spots using WPS by modified scanner vistumbler.** 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, 2018, pp. 48-51. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8317027&isnumber=8316851>. Acesso em: 16 out. 2019

KARASINSKI, L**. O Que é Tecnologia?.** 2013. Disponível em <https://www.tecmundo.com.br/tecnologia/42523-o-que-e-tecnologia-.htm>. Acesso em: 20 out. 2019.

PETIZ, I. et al. **Using multiscale traffic analysis to detect WPS attacks.** 2013. IEEE International Conference on Communications Workshops (ICC), Budapest, 2013, pp. 1020-1025. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6649386&isnumber=6649166>. Acesso em: 16 out. 2019.

PIXININE, J. **Como um Wi-Fi Funciona? Entenda a Tecnologia.** 2015. Disponível em: <https://www.techtudo.com.br/noticias/noticia/2015/02/como-um-wi-fi-funciona-entenda-tecnologia.html>. Acesso em: 23 out. 2019

VIEHBÖCK, S. **Brute forcing Wi-Fi Protected Setup.** 2011. Disponível em: < https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf>. Acesso em: 30 nov. 2019.

WHO WE ARE. WiFi Alliance. Disponível em: <https://www.wi-fi.org/who-we-are/history>. Acesso em: 23 out. 2019.

WI-FI LIBRE. **Calcular el Checksum WPS (La Ultima Cifra Del PIN).** 2015. Disponível em: < http://wifi-libre.com/topic-33-calcular-el-checksum-wps-la-ultima-cifra-del-pin.html>. Acesso em: 20 out. 2019.

ZISIADIS, D.et al. **Enhancing WPS security.** 2012. IFIP Wireless Days, Dublin, 2012, pp. 1-3. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6402836&isnumber=6402798>. Acesso em: 16 out. 2019.