UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO SEMIPRESENCIAL EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

DOUGLAS AKIHIRO SATO

BOAS PRÁTICAS EM SEGURANÇA DE REDES SEM FIO DOMÉSTICAS

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2020

DOUGLAS AKIHIRO SATO

BOAS PRÁTICAS EM SEGURANÇA DE REDES SEM FIO DOMÉSTICAS

Monografia de Especialização, apresentada ao Curso de Especialização Semipresencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Dr. Kleber Kendy Horikawa Nabas

CURITIBA
2020

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba

Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrônica
Curso de Especialização Semipresencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes

TERMO DE APROVAÇÃO

BOAS PRÁTICAS EM SEGURANÇA DE REDES SEM FIO DOMÉSTICAS

por

DOUGLAS AKIHIRO SATO

Esta monografia foi apresentada em 16 de Outubro de 2020 como requisito parcial para a obtenção do título de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Orientador

_____
Prof. Dr. Edenilson José da Silva
Membro titular

_____
Prof. M. Sc. Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

AGRADECIMENTOS

Agradeço todos os familiares e amigos que me apoiaram e incentivaram a realização deste curso.

RESUMO

SATO, Douglas Akihiro. **Boas práticas em segurança de redes sem fio domésticas**. 2020. 33 p. Monografia de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2020.

As redes sem fio locais (wlan) são amplamente difundidas e utilizadas nas residências dos usuários de internet, é um recurso que facilita, dá mobilidade e torna mais prática nossa conexão com a rede mundial de computadores, contudo, traz consigo algumas preocupações relacionadas à segurança. O presente trabalho, buscou elencar riscos comuns no uso desta tecnologia através de pesquisa bibliográfica, em seguida teste de algumas das fragilidades encontradas e como eliminá-las ou diminuir a possibilidade de sua exploração. Durante o desenvolvimento do trabalho foram localizadas algumas redes que utilizam protocolos descontinuados há muito tempo, e nos testes de invasão controlados, os protocolos de criptografia e acesso mais modernos aliados a senhas mais complexas apresentaram resultados melhores. Por fim, elaborou-se um quadro com algumas fragilidades regulares e sua respectiva solução ou resposta para reduzir de seu risco, a fim de estabelecer um guia rápido de boas práticas na configuração de redes sem fio domésticas aumentando a sua respectiva segurança.

Palavras-chave: Redes de Computadores. Redes Sem Fio. Segurança. WiFi.

ABSTRACT

SATO, Douglas Akihiro. **Good practices in home wireless network security**. 2020. 33 p. Monografia de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2020.

Local wireless networks (wlan) are widespread and used in the homes of internet users, it is a resource that facilitates, gives mobility and makes our connection with the world wide web more practical, however, brings with it some security concerns . The present work, sought to list common risks in the use of this technology through bibliographic research, then testing some of the weaknesses found and how to eliminate them or reduce the possibility of their exploitation. During the development of the work, some networks were found using protocols that were discontinued for a long time, and in controlled invasion tests, the most modern encryption and access protocols combined with more complex passwords showed better results. Finally, a table was created with some regular weaknesses and their respective solution or response to reduce their risk, in order to establish a quick guide to good practices in the configuration of home wireless networks, increasing their respective security.

Keywords: Computer Networks. Wireless Networks. Security. WiFi.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AES	*Advanced Encryption Standard*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
IEEE	*Institute of Electrical and Electronics Engineers*
IP	*Internet Protocol*
LAN	*Local Area Network*
MAN	*Metropolitan Area Network*
PAN	*Personal Area Network*
PBC	*Push Button Configuration*
PIN	*Personal Identification Number*
TKIP	*Temporal Key Integrity Protocol*
WAN	*Wide Area Network*
WEP	*Wired Equivalent Privacy*
Wi-Fi	*Wireless Fidelity*
WPA	*Wi-Fi Protected Access'*
WPS	*Wi-Fi Protected Setup*

SUMÁRIO

1 INTRODUÇÃO

Todos os anos a quantidade de usuários conectados à internet aumenta, segundo a União Internacional de Telecomunicações (2019), que é a agência especializada em telecomunicações da Organização das Nações Unidas (ONU), em 2001, 495 milhões de pessoas eram usuárias de internet (8% da população mundial), já em 2019, estimou-se que 4,1 bilhões de indivíduos estejam conectados à rede mundial de computadores (53,6% da população mundial).

A popularização da internet se deve principalmente aos avanços tecnológicos que levaram ao barateamento dos aparelhos eletrônicos, pois tornaram a aquisição dos mesmos menos onerosa, aliado a expansão no uso de tecnologias sem fio para transmissão de dados, que permitiu aos usuários terem mobilidade durante o uso de seus equipamentos, gerando disponibilidade e comodidade (COMER, 2016).

Esta popularização e avanço foram assegurados pela padronização dos protocolos de comunicação, que garantiram interoperabilidade entre equipamentos de diferentes fabricantes (MORAES, 2020).

A facilidade com relação ao uso das redes sem fio, embora muito conveniente, traz consigo algumas preocupações, principalmente no aspecto de segurança, pois existem diversas vulnerabilidades nesta tecnologia (WRIGHTSON, 2014).

1.1 CONTEXTUALIZAÇÃO

Conforme Moraes (2020), as redes wireless apresentam diversos benefícios, entre eles mobilidade, escalabilidade, agilidade e redução de custo na instalação, além de aplicação em quase todos mercados.

As tecnologias sem fio evoluíram em uma velocidade altíssima tanto em sua aplicação quanto em sua disponibilidade. No início da década passada, uma rede sem fio era cara tanto para uso comercial quanto para uso doméstico, atualmente, a maioria dos comércios possuem uma rede sem fio para uso interno ou para disponibilizar para seus clientes, assim como quase todas as residências que possuem acesso à internet, possuem uma rede sem fio (WRIGHTSON, 2014).

Existem muitas tecnologias que utilizam ondas ou radiação eletromagnéticas para transmitir sinais, como exemplos temos as radiotransmissões, transmissões por

satélite, luz visível, luz infravermelha e raios X. O início da popularização destas tecnologias iniciou-se na década de 50 com o rádio e a televisão (WHITE, 2012).

Entre as redes sem fio locais, existem 3 tipos principais, as baseadas em infravermelho, baseadas em laser e baseadas em radiofrequência, esta última, predominantemente a mais popular nas residências (MORAES, 2020).

1.2 PROBLEMA

Dentre os problemas relacionado ao uso das redes sem fio, podemos destacar o acesso não autorizado, a captura dos dados trafegados, vazamento de dados e uso indevido de recursos, que podem causar enormes transtornos para indivíduos e empresas.

Redes cabeadas possuem a característica que só quem possui acesso físico aos cabos pode acessá-las, sendo uma camada adicional de segurança, contudo, nas redes sem fio os sinais são irradiados em todas as direções, podendo ser captadas por qualquer um com uma antena dentro do alcance da rede (MORIMOTO, 2011).

Segundo Wrightson (2014), inconveniências adicionais são intrínsecas à segurança, como exemplo, podemos botar documentos em um cofre para protegê-los, porém, agora precisamos memorizar uma senha para poder acessá-los. Contudo, existe um ponto de inflexão, onde mecanismos de segurança que teoricamente deveriam ser mais robustos são fragilizados por negligência dos usuários, devido ao grau elevado de inconveniência.

1.3 OBJETIVOS

Nesta seção são apresentados os objetivos geral e específicos do trabalho, relativos ao problema anteriormente apresentado.

1.3.1 Objetivo Geral

Catalogar riscos e fragilidades conhecidas de uma rede local sem fio, suas potenciais consequências e como mitigá-los e, auxiliando no planejamento e implementação de mecanismos de segurança adequados.

1.3.2 Objetivos Específicos

Para atender ao objetivo geral neste trabalho de conclusão de curso de especialização os seguintes objetivos específicos serão abordados:

- Elencar alguns tipos de riscos conhecidos e potencialmente perigosos envolvidos nas redes locais sem fio.
- Possibilitar a identificação de vulnerabilidades em redes sem fio e como evitá-las ou reduzi-las.
- Testar algumas fragilidades conhecidas e suas respectivas soluções utilizando Kali Linux.

1.4 JUSTIFICATIVA

O presente trabalho tem como objetivo auxiliar na mitigação de riscos inerentes ao uso de redes sem fio, através da proposta de configurações que otimizem a proteção, buscando a operação mais segura desta tecnologia.

1.5 ESTRUTURA DO TRABALHO

O presente trabalho está dividido em 5 (cinco) seções. Nesta primeira seção foi introduzido o assunto tema do trabalho e também foram abordados a motivação e os objetivos da pesquisa, a justificativa e a estrutura geral do trabalho.

A segunda seção traz os fundamentos teóricos, da literatura e documentação que embasam o desenvolvimento da pesquisa.

Na terceira seção está o desenvolvimento prático do trabalho, quais foram os testes, desenvolvidos acerca da segurança das redes sem fio.

A quarta seção reserva-se para apresentação dos resultados obtidos nos testes da seção anterior.

Na quinta e última seção, estão as considerações finais sobre a proposta, como os objetivos foram atingidos bem como a pesquisa poderia ser complementada.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo é dedicado a apresentação das bases utilizadas para fundamentar cientificamente os conceitos, teorias e assuntos abordados neste trabalho e suas respectivas fontes.

2.1 SEGURANÇA DA INFORMAÇÃO

Moraes (2010) ensina que “não existe rede ou mesmo informação 100% segura. Todas as vezes que estamos fazendo uso da Internet para buscar e disponibilizar informações estamos sujeitos a riscos , uma vez que a Internet e´ uma enorme rede pública, fora de controle, e sujeita a ataques”.

Dadas as potenciais vulnerabilidades das redes TCP/IP bem como técnicas para eliminá-las, percebemos que apenas uma infraestrutura de segurança geral e de múltiplas camadas pode lidar com possíveis ataques aos sistemas de redes de computadores (ALENCAR, 2015).

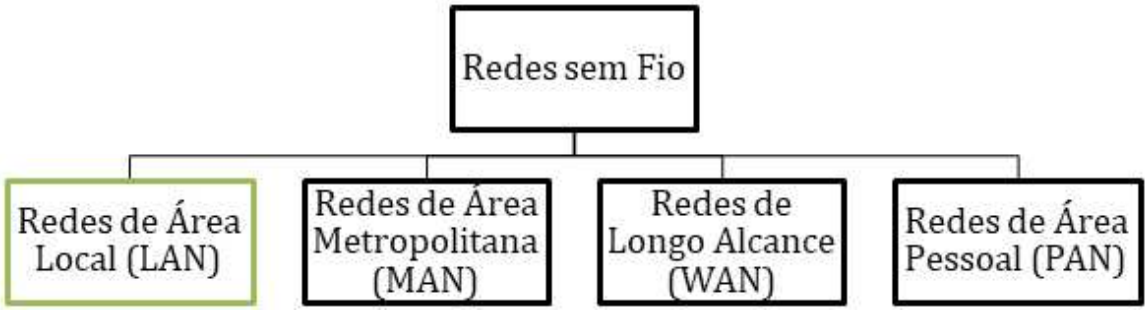
Alencar (2015) enumera os princípios de segurança da informação:

- Integridade
- Confidencialidade
- Autenticidade
- Disponibilidade
- Não Repudiação
- Responsabilidade
- Controle de Acesso

2.2 REDES SEM FIO

As redes sem fio podem ser classificadas em Pessoais (*Personal Area Network* - PAN), Locais (*Local Area Network* - LAN), de Longo Alcance (*Wide Area Network* - WAN) ou Metropolitanas (*Metropolitan Area Network* - MAN). As redes locais são o foco deste trabalho e utilizam as faixas de frequência do espectro eletromagnético conhecida como ISM, que não são licenciadas para operadoras específicas (COMER, 2016).

Figura 1 - Taxonomia de redes sem fio



Fonte: Adaptado de Comer (2016).

Machado (2014), ainda lembra que as redes por redes Wi-Fi operarem em frequências públicas, teoricamente todos próximos do sinal podem captá-lo, por isso o uso de soluções criptográficas se faz tão necessário.

2.3 PADRÃO IEEE 802.11

É o padrão que norteia os princípios de conectividade sem fio tomando como escopo uma rede local, direcionando quais os requisitos e características que os dispositivos que aderentes a este padrão devem apresentar.

> "Este padrão também oferece aos órgãos reguladores um meio de padronizar o acesso a um ou mais bandas de frequência para fins de comunicação de área local [...] Descreve as funções e serviços exigidos por um dispositivo para operar de forma independente, pessoal e infraestrutura de redes bem como os aspectos da mobilidade do dispositivo (transição) dentro dessas redes [...] Descreve as funções e serviços que permitem que um dispositivo se comunique diretamente com outro dispositivo fora de uma rede independente ou de infraestrutura" (IEEE, 2016, p. 122)

Os fabricantes que produzem equipamentos de rede que seguem este padrão garantem ao usuário final compatibilidade entre os equipamentos de diferentes fabricantes.

2.4 PROTOCOLOS DE AUTENTICAÇÃO E CRIPTOGRAFIA

WEP, WPA e WPA2, nesta ordem, foram criados para prover segurança em redes sem fio, melhorando a criptografia a cada evolução, todos estão sujeitos a ataques via WPS, força bruta, ataques de dicionário entre outros, porém quanto mais recente o método, maior proteção ele oferece (MORAES, 2010).

2.4.1 WEP

O *Wired Equivalency Privacy* (WEP) surgiu baseado no padrão IEEE 802.11b, buscando oferecer confidencialidade no mesmo nível que a rede cabeada para redes sem fio do padrão IEEE 802.11, através de algoritmos criptográficos de chave secreta e processamento rápido (MORAES, 2010).

Segundo Moraes (2010, p.204) “O WEP possui algumas vulnerabilidades . A primeira delas e´ que ele trabalha com um vetor de inicialização muito pequeno, o que o torna ainda mais vulnerável a ataques que buscam descobrir a chave criptográfica” além disso, a chave criptográfica de um ponto de acesso é compartilhada por todos usuários conectados a ele.

Atualmente, a criptografia utilizada pelo WEP pode ser quebrada com facilidade graças a grande evolução do poder computacional desde que ele foi lançado e é considerado um protocolo defasado e existe recomendação para interrupção de seu uso há anos. Foi considerado protocolo legado e sucedido pelo WPA (IEEE, 2016).

2.4.2 WPA

O *Wireless Protected Access* (WPA) foi inicialmente chamado de WEP2, e conforme White (2012), mantinha inicialmente mantinha a chave de criptografia de 40 bits do WEP, contudo, havia uma melhoria bastante significativa, a inclusão do protocolo de integridade de chave temporal (TKIP), que passou a promover criptografia dinâmica de chave e autenticação para clientes sem fio.

Também é considerado um protocolo defasado, sendo sucedido pelo WPA2.

2.4.3 WPA2

O WPA2 foi lançado oficialmente em 2004, pelo consórcio Wi-Fi para oferecer alto nível de segurança para redes domésticas e corporativas, é baseado na especificação final do padrão IEEE 802.11i, garantindo que apenas usuários autorizados tenham acesso à rede (MORAES, 2010).

2.5 WPS

O *Wi-Fi Protected Setup* (WPS) foi projetado para tornar o mais fácil possível para que dispositivos entrassem em uma rede segura. Possui, três métodos de entrada *Push Button Configuration* (PBC), *Personal Identification Number* (PIN) e *Near Field Communication* (NFC). NFC possui certo nível de segurança para uso doméstico, mas o PBC permite que qualquer dispositivo no alcance da rede (WI-FI ALLIANCE, 2020).

2.6 KALI LINUX

O Kali Linux é uma distribuição opensource de Linux baseada em Debian mantida e fundada pela Offensive Security. Este sistema é considerado o sucessor do Back Track e possui centenas de ferramentas inclusas para testes de segurança e auditoria de computadores e redes (KALI, 2019).

3 DESENVOLVIMENTO

Para os testes de invasão, foram utilizados um roteador Huawei HG8245H, um roteador TP-Link TD-W8961ND e um roteador Askey RTF3505VW-N2, todos próprios do autor. Não houve invasão de nenhuma rede de terceiros.

3.1 QUEBRA DE AUTENTICAÇÃO

Ingressar na rede não permite apenas que o invasor possa capturar os dados ou causar indisponibilidade. Uma vez dentro da rede, ele pode mapeá-la e potencialmente alterar configurações de equipamentos, identificar os recursos, dispositivos mais importantes e inspecionar o tráfego sensível.

3.1.1 WEP

Foi configurada uma rede sem fio, chamada Teste WEP, com as seguintes configurações no roteador da Huawei:

- SSID: Teste WEP
- SSID: Habilitada
- SSID: Divulgada
- Método de Autenticação: Shared
- Comprimento da chave criptográfica: 128 bits
- Senha: aaaaaaaaaaaaa

Para realizar o ataque, utilizou-se o programa Fern WiFi Cracker, que é um dos softwares de ataques a redes sem fio que vem embutido na distribuição Kali Linux 2020. Possui interface amigável e exige um nível muito baixo de conhecimento para operá-lo.

Inicia-se o ataque realizando o procedimento de reconhecimento das redes ao redor (scan). O programa separará as redes em WEP, WPA (onde também agrupará as redes WPA2), as chaves de redes já conhecidas

Figura 2 - Interface inicial - Fern WIFI Cracker

Fonte: Autoria própria.

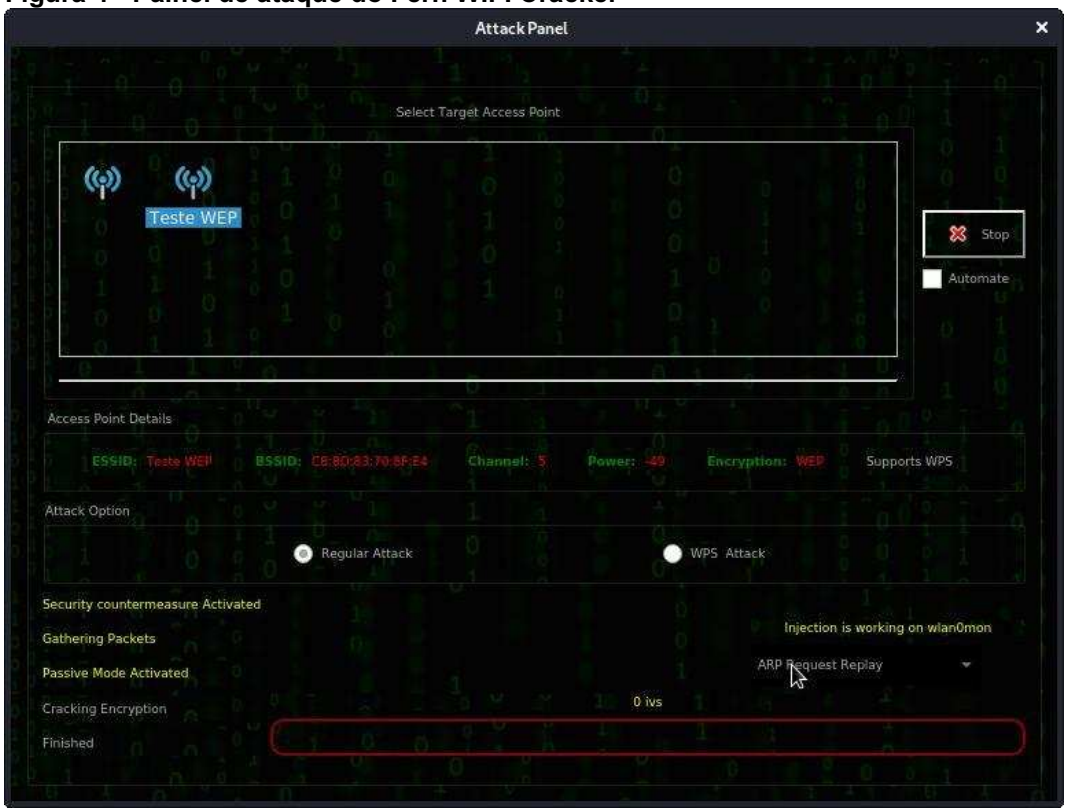
O programa indicará quantas redes foram encontradas tipo, e qual o protocolo de autenticação elas utilizam.

Figura 3 - Resultado do scan das redes sem fio

Fonte: Autoria própria.

A interface carregará algumas informações sobre as redes, como o ESSID, BSSID, canal, potência do sinal, método de criptografia e se o ponto de acesso suporta WPS ou não. Após selecionar a rede alvo, basta selecionar o método de ataque

Figura 4 - Painel de ataque do Fern WIFI Cracker



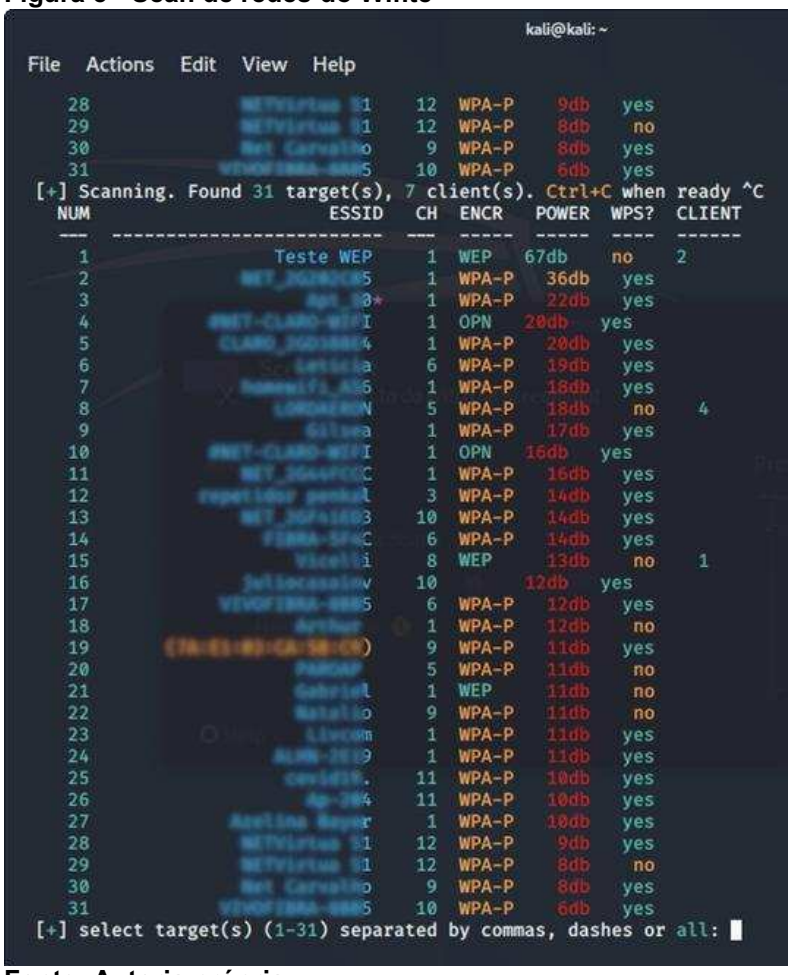
Fonte: Autoria própria.

Após algumas horas o programa finalizou a quebra, exibindo o texto “WEP KEY: aaaaaaaaaaaaa” em seu rodapé.

Outro programa utilizado para quebrar a autenticação com WEP é o Wifite, que como o Fern Wifi Cracker, possui interface gráfica e é relativamente simples de utilizar, basta iniciá-lo como super usuário.

Desta vez o alvo foi o roteador da Askey, com as configurações similares da rede gerada inicialmente para o teste anterior. O procedimento também é similar, abre-se o programa, executa-se o scan, selecionam-se os alvos e métodos de ataque, e aguardamos o processamento do programa.

Figura 5 - Scan de redes do Wifite

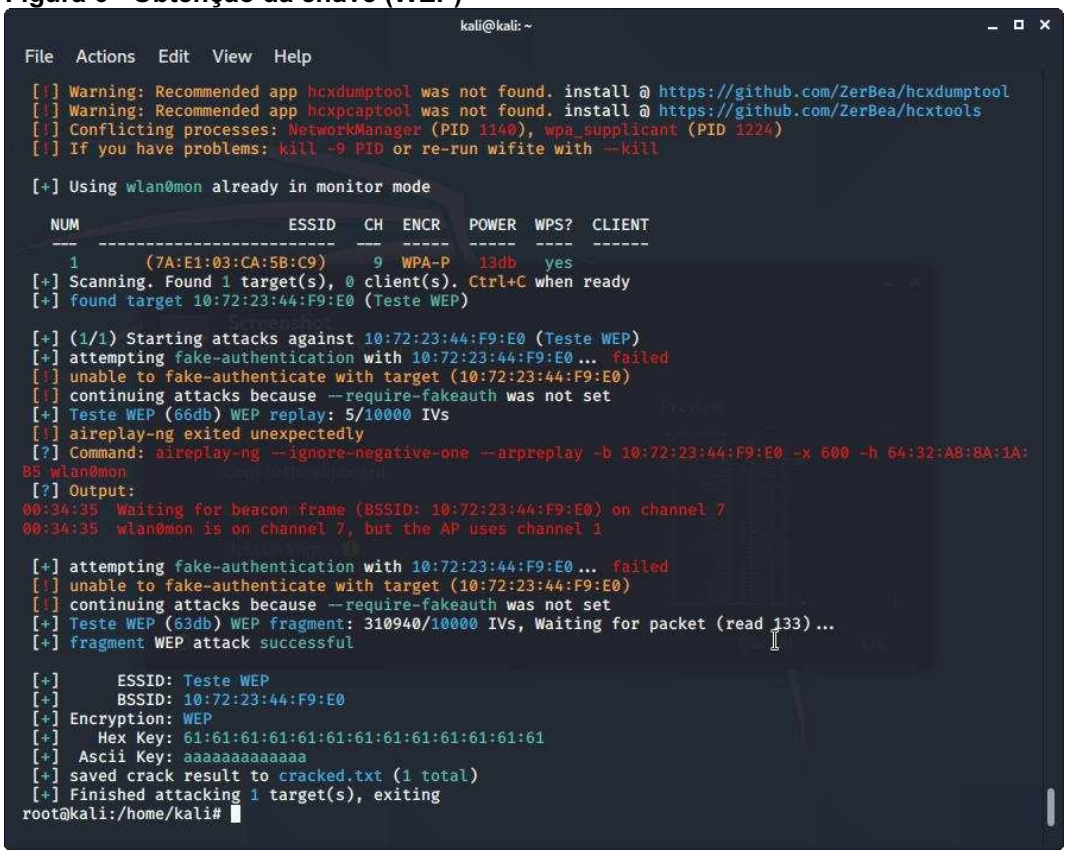


Fonte: Autoria própria.

Ao elecionar a rede a partir de um scan, pode-se atacar de 1 até n redes encontradas.

Existe um modo onde direcionamos o ataque da rede através do ESSID, ou seja, com um alvo específico, a partir desta seleção, o próprio programa tenta executar o ataque variando os métodos disponíveis de acordo com o tipo de rede que está sendo invadido.

Figura 6 - Obtenção da chave (WEP)



Fonte: Autoria própria.

Estes foram apenas alguns dos programas utilizados para acessar redes protegidas com o protocolo WEP, há relatos de soluções que quebram o WEP de 104 bits em menos de dois minutos.

3.1.2 WPA

Foi configurada uma rede sem fio, chamada Teste WPA, com as seguintes configurações no roteador da TP-Link:

- SSID: Teste WPA
- SSID: Habilitada
- SSID: Divulgada
- Método de Autenticação: WPA-PSK
- Encriptação: TKIP
- Senha: bbbbbbbb

Repetiu-se o processo utilizando o Wifite e novamente obtivemos a senha sem maiores problemas:

Figura 7 - Obtenção da chave (WPA)

Fonte: Autoria própria.

Por padrão o ataque do Wifite a redes WPA inicia tentando se aproveitar da configuração WPS ativa, caso não tenha sucesso, após o tempo estabelecido se esgotar ele vai para o próximo método, por padrão segue a seguinte ordem, Pixie Dust, Null Pin, Pin Attack, PMKID Attack e Handshake Capture + Brute Force.

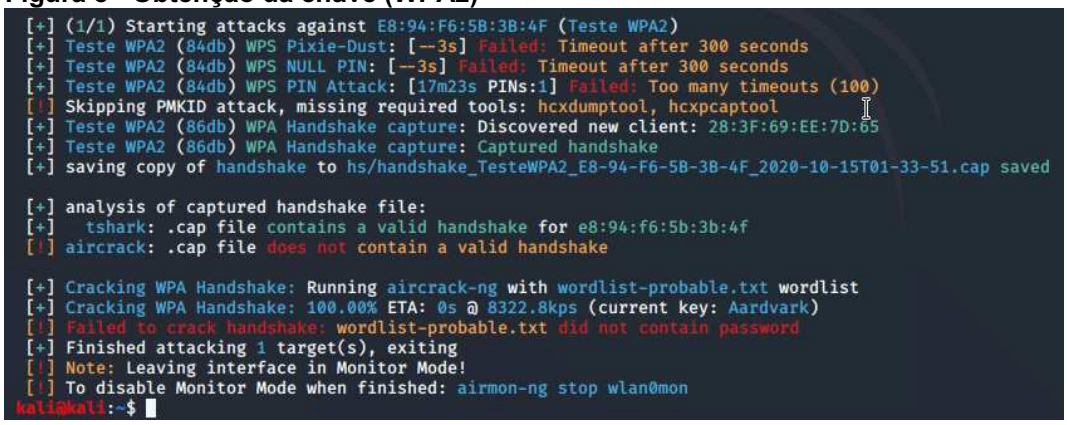
O método de ataque de força bruta pode basear-se numa lista de senhas para realizar tentativas de acesso, inclusive o próprio programa já vem com uma lista de senhas comuns para executar algumas tentativas, mas também, o invasor pode montar a sua própria lista de senhas.

3.1.3 WPA2 COM SENHA COMPLEXA

Foi refeito o teste anterior alterando apenas os seguintes parâmetros:

- SSID: Teste WPA2
- Método de Autenticação: WPA2-PSK
- Encriptação: TKIP/AES
- Senha: -#geser@UTF PR2020+

Figura 8 - Obtenção da chave (WPA2)



Fonte: Autoria própria.

Desta vez, o Wifite não conseguiu realizar o ataque via WPS, e apesar de ter capturado o handshake entre o dispositivo final e o roteador, não conseguiu realizar o ataque de dicionário para obter a chave da rede.

3.2 WPS

O WPS (*Wi-Fi Protected Setup*), possui a sua maior fragilidade no modo de configuração via PBC devido a sua janela de 2 minutos para aceitar conexões, onde qualquer dispositivo ao alcance do roteador possa se conectar, mesmo que indevidamente.

A conexão via PIN também apresenta problemas de segurança, um deles é a redução de combinações possíveis, pois o último algarismo é a soma dos anteriores, isso faz com que programas que realizam ataques de força bruta sobre os 8 algarismos do PIN consigam quebrá-lo em questão de horas, não importando o tamanho da senha configurada via WEP, WPA ou WPA2.

3.3 ACESSO A ROTEADORES DOMÉSTICOS

Quando lidamos com redes pequenas, é comum que exista apenas um equipamento entre os dispositivos finais e a conexão com o provedor de internet. Diversas configurações sensíveis podem ser acessadas diretamente no mesmo dispositivo de rede.

Caso seja interesse do invasor, ele procurará acessar o dispositivo normalmente buscando o gateway padrão, e em seguida, tentará utilizar o administrador padrão e a senha padrão do equipamento, estes, geralmente são encontrados facilmente no site dos fabricantes ou em fóruns pela internet.

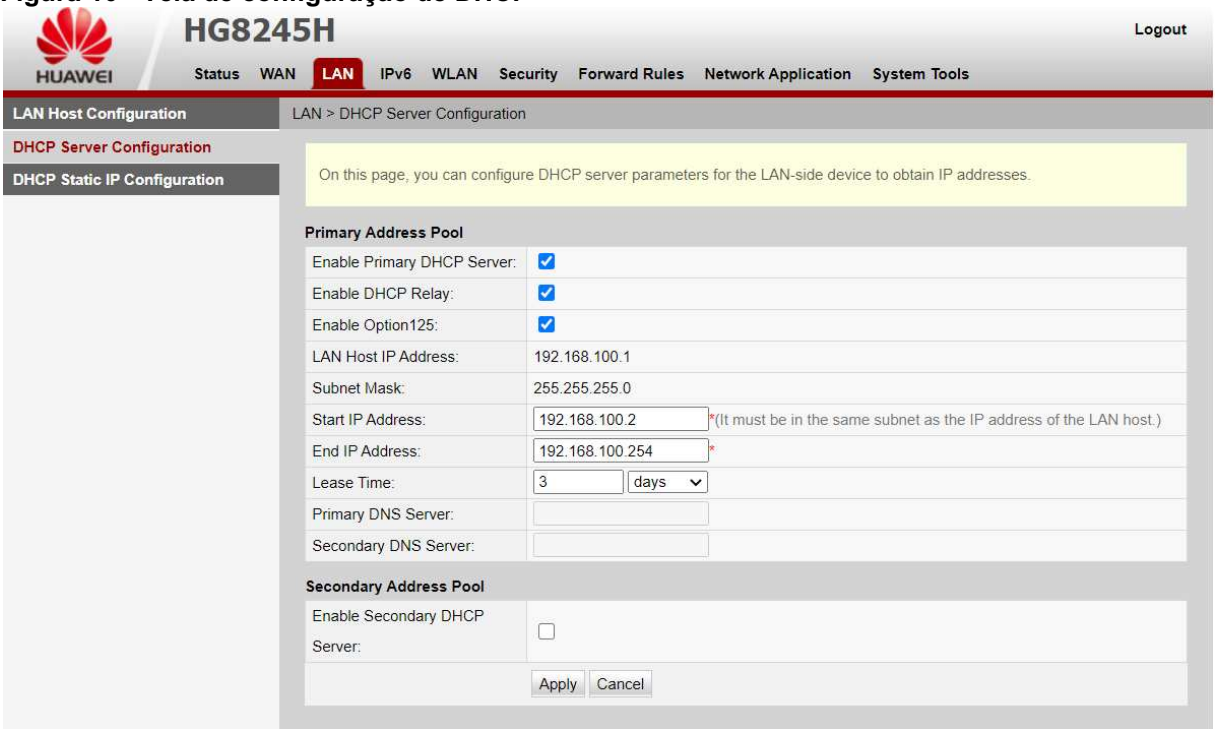
Dentre os pontos sensíveis, tanto para captura de dados, quanto para depredação da acessibilidade ou disponibilidade da rede o invasor pode fazer uso das configurações, as quais destacamos nos parágrafos abaixo.

Figura 9 - Tela de login do roteador

Fonte: Autoria própria.

O *Dynamic Host Configuration Protocol* (DHCP) é o protocolo que distribui números de IPs automaticamente. Se o invasor tiver acesso às configurações do servidor DHCP, ele pode restringir ou negar a distribuição de endereços ou faixas de IP, ainda incluir outro servidor DHCP e desativar o atual.

Figura 10 - Tela de configuração de DHCP

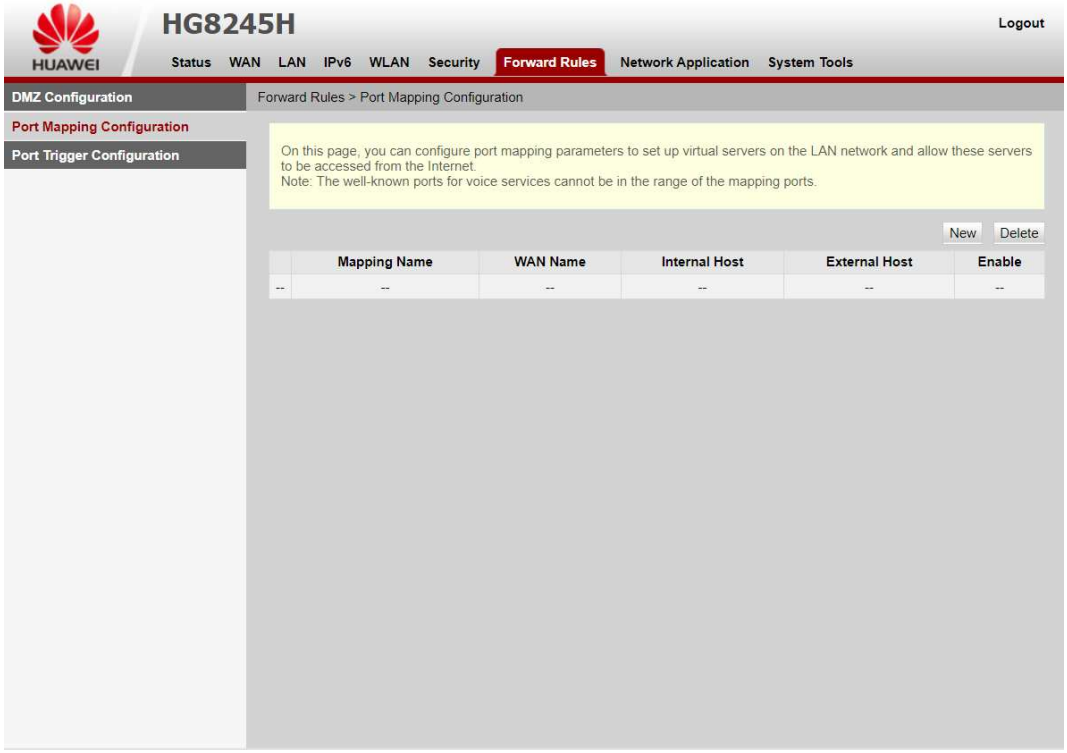


Fonte: Autoria própria.

A principal preocupação com o redirecionamento de portas, é a permissão do tráfego de rede aplicações maliciosas com potencial de causar danos, transtornos e prejuízo aos usuários desta rede.

O conceito popular “abrir portas” do roteador para determinados hosts ou serviços é relativamente simples de ser implementado, mas exige certo conhecimento em redes para compreender os seus riscos potenciais, e é justamente neste ponto onde reside o perigo, pois, até mesmo o redirecionamento proposital criado por um usuário bem-intencionado visando alguma melhoria de performance é potencialmente perigosa, por permitir tráfego de dados que eventualmente seriam negados em condições normais.

Figura 11 - Tela de configuração de redirecionamento de porta

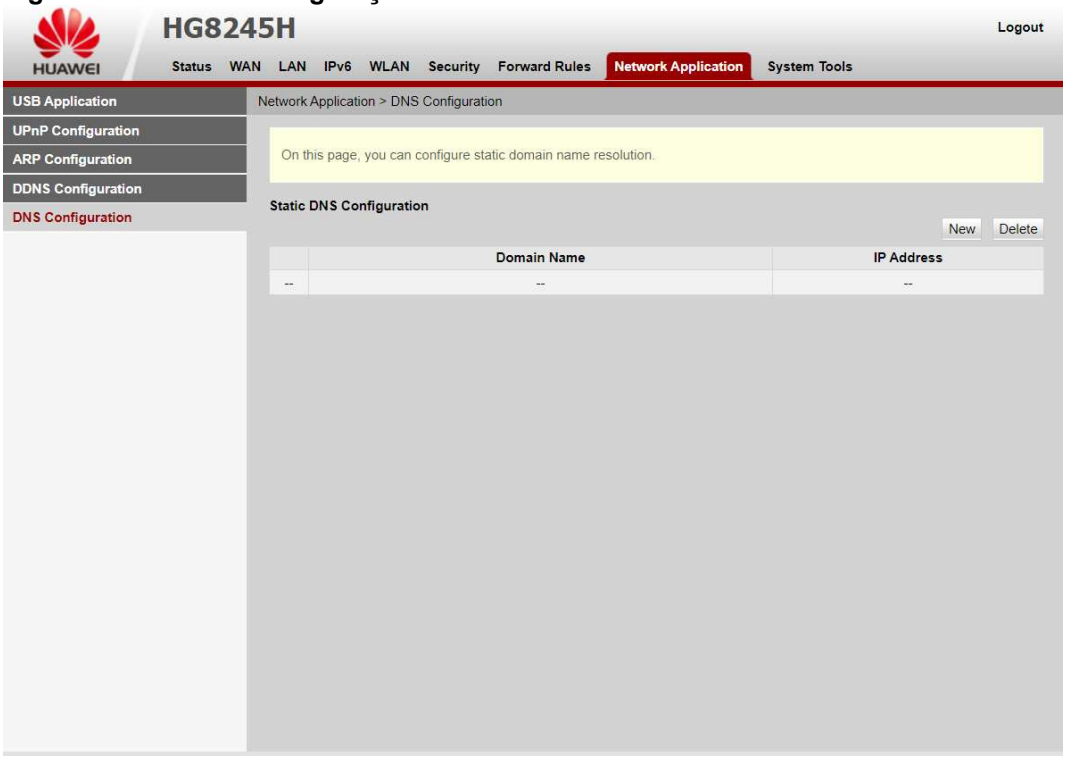


Fonte: Autoria própria.

Outro ponto que merece atenção é a configuração estática de DNS, que pode operar como um sequestro de DNS, fazendo com que o nome quando for resolvido, ao invés de encaminhar os dados para determinado servidor ou host, encaminhe os dados para outro servidor ou host que possivelmente tentará se passar pelo verdadeiro.

Este processo pode ser um recurso utilizado em um tipo de fraude chamado Phishing, que busca obter informações confidenciais, credenciais ou informações pessoais sensíveis, como exemplo, códigos de usuários, senhas ou número do cartão de crédito através de um disfarce que tenta se passar por um host ou entidade confiável, quando na verdade redireciona o usuário para um servidor ou domínio controlado pelos golpistas.

Figura 12 - Tela de configuração de DNS estático



Fonte: Autoria própria.

Por estes motivos, recomenda-se fortemente a trocar as senhas padrão que vem de fábrica. Atualmente, algum roteador já vem com usuários e senhas iniciais exclusivos para o aparelho, adicionando uma camada de segurança significativa, tendo em vista que o usuário médio não se preocupa ou não tem conhecimento suficiente para realizar esta configuração por conta.

3.4 FILTRO DE MAC ADDRESS

Um recurso que se demonstrou útil para redes domésticas, foi o filtro de MAC, disponível em todos os roteadores testados e operando de formas similares.

Basicamente há dois modos de operação, o de permissão (*white-list*) e o de bloqueio (*black-list*), ao cadastrar os endereços MAC na lista de permissão, será concedido o acesso à rede apenas a estes dispositivos, sendo negado a conexão de qualquer outro dispositivo. Já o modo de bloqueio funciona de maneira inversa, será permitida a conexão de todo dispositivo que não estiver na lista, e negada aos que constarem na mesma.

Uma vez que a rede doméstica possui um número praticamente estável de dispositivos, todos eles são conhecidos e a adição de novos dispositivos é

esporádica, pode-se utilizar o filtro de MAC no modo *white-list* para permitir apenas o acesso destes dispositivos à rede controlada pelo roteador, adicionando uma camada extra de segurança.

Esta solução consegue conter acessos indevidos de dispositivos onde os usuários de alguma forma obtiveram a senha da rede, mas infelizmente não consegue conter os ataques de MAC Spoofing caso a senha de acesso à rede seja quebrada por ser de fácil dedução ou muito curta.

4 APRESENTAÇÃO DOS RESULTADOS

Após pesquisa, testes e demonstrações de invasão, seguem os resultados deste trabalho.

4.1 TIPOS DE RISCOS

Apesar da comodidade e praticidade, existem diversos riscos envolvidos no uso de redes sem fio, alguns deles inerentes à esta tecnologia, outros compartilhados com as redes cabeadas convencionais. Entre os riscos, podemos destacar o acesso não autorizado à rede, a interceptação e modificação de dados, spoofing, roubo de dados e quebras de senhas.

4.2 IDENTIFICAÇÃO DE VULNERABILIDADES

Sempre existirão vulnerabilidades potenciais em qualquer tecnologia, no caso das redes sem fio já existem diversas catalogadas, seus riscos e como mitigá-las, e de tempos em tempos, a cada novo avanço, novas vulnerabilidades são encontradas e pesquisadores e outros profissionais buscam meios de eliminá-las ou reduzir as chances de explorá-las.

Quadro 1 - Vulnerabilidades de redes sem fio

(continua)

Vulnerabilidade	Risco	Resposta/Solução
Redes sem senha de acesso	Acesso não autorizado	Implementar o acesso com senha à rede
Uso de Protocolos de Autenticação Defasados	Invasão facilitada	Utilizar protocolos de autenticação mais atualizados
Uso de senhas simples, óbvias ou curtas	Maior facilidade na quebra de senha	Criar senhas mais complexas
Não alterar a senha de fábrica de acesso ao roteador	Em caso de invasão à rede, o intruso pode obter facilmente as senhas de fábrica do equipamento e alterar suas configurações, caso o fabricante não gere uma senha única por equipamento.	Alterar a senha de acesso ao roteador

Quadro 1 - Vulnerabilidades de redes sem fio

(conclusão)

Uso do WPS	Acesso não autorizado	Desativar o recurso WPS no roteador
Tráfego de informação em “texto simples”	Escuta, captura e alteração da informação trafegada	Implementação de solução de criptografia
Uso de criptografia antigo ou simples	Permite que a decriptação não autorizada seja realizada com maior facilidade	Utilizar protocolos de criptografia mais modernos e complexos

Fonte: Autoria própria.

Cabe lembrar que para determinadas situações, uma vulnerabilidade não pode ou é inviável de ser contornada, como exemplo podemos citar estabelecimentos comerciais que desejam oferecer conexão à internet a seus clientes através de redes sem fio e sem senha, mas exigem um check-in em uma rede social para tal.

4.3 TESTES DE FRAGILIDADES

Foi demonstrado a quebra de senha em invasões de redes e o uso de protocolos de autenticação mais modernos e senhas mais complexas demonstrou maior segurança.

WEP é considerado descontinuado a muitos anos, mas supreendentemente ainda foram localizadas algumas redes usando ele durante as práticas, contudo, deveria ter sua utilização interrompida o mais breve possível por quem ainda o utiliza.

O WPA que incorporou uma criptografia mais robusta que o WEP, também não é mais considerado seguro, já o WPA2, que adota o AES no lugar do TKIP, aliado a uma senha de maior complexidade e com o WPS desativado, resistiu às tentativas de invasão, sendo este o protocolo mais seguro testado neste trabalho. A desvantagem do WPA2+AES é que necessita mais poder computacional para processamento do que o WPA+TKIP.

5 CONSIDERAÇÕES FINAIS

As redes sem fio são recursos poderosos que auxiliaram muito no quesito praticidade de nossas vidas e a tendência é que permaneçam em nossas residências por vários anos, mas precisamos constantemente mantê-las atualizadas com as configurações mais adequadas para garantir a segurança.

Este trabalho apresentou uma breve abordagem sobre algumas das principais fragilidades e riscos, que podemos nos deparar ao configurar uma rede sem fio doméstica.

O problema foi resolvido em partes, pois os riscos são inerentes à tecnologia e as fragilidades são corrigidas à medida que são descobertas ou expostas, e sempre há novas fragilidades potenciais.

O objetivo geral foi atingido bem como os objetivos específicos. Foram catalogados riscos, vulnerabilidades e possíveis meios de evitá-los, reduzi-los ou diminuir a potencial exploração dos mesmos.

Os testes de invasão corresponderam à literatura, sendo as redes com maior resiliência aos ataques aquelas com o maior o nível de segurança e criptografia aplicado.

Dentre os objetivos específicos, a invasão das redes foi de longe o item mais complexo do trabalho, pois envolveu muita pesquisa e horas de tentativas para lograr êxito nas invasões simples, e muitas horas de processamento gastas tentando sem sucesso quebrar os protocolos mais seguros.

O esforço despendido na elaboração deste trabalho foi extremamente válido para o aprendizado e correta configuração do equipamento doméstico, espera-se que este trabalho consiga facilitar a obtenção das informações para os demais que tenham oportunidade de lê-lo.

Os resultados podem parecer triviais a usuários avançados, contudo a busca pelas informações e o conhecimento adquirido na construção deste trabalho promoveram o resultado esperado.

Cada risco e cada protocolo citado neste trabalho pode ter diversos estudos mais aprofundados em outros trabalhos, ou ainda, abordar e catalogar outros riscos e fragilidades não citados neste trabalho, tendo em vista que este buscava catalogar apenas alguns deles.

REFERÊNCIAS

ALENCAR, M. S. **Informação, codificação e segurança de redes**. 1. ed. Rio de Janeiro: Elsevier, 2015.

COMER, D. E. **Redes de computadores e internet**. 6. ed. Porto Alegre: Bookman, 2016.

IEEE. **IEEE Standard for information technology - Telecommunications and information exchange between systems Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications**. 2016. Disponível em: <https://ieeexplore.ieee.org/document/7786995>. Acesso em: 08 set. 2020.

KALI. Kali Docs. **Documentação.** 25 nov. 2019. Disponível em: <https://www.kali.org/docs/>. Acesso em: 08 jun. 2020.

MACHADO, F. N. R. **Segurança da informação**: Princípios e controle de ameaças. 1. ed. São Paulo: Saraiva, 2014.

MORAES, A. F. **Redes de computadores:** Fundamentos. 8. ed. São Paulo: Érica, 2010.

MORAES, A. F. **Segurança em redes:** Fundamentos. 1. ed. São Paulo: Érica, 2020.

MORIMOTO, C. E. **Redes:** Guia prático. 2. ed. Porto Alegre: Sulina, 2011.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES. **Estatísticas.** 2019. Disponível em: <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>. Acesso em: 10 jul. 2020.

WI-FI ALLIANCE. **Documentação.** Disponível em: <https://www.wi-fi.org/discover-wi-fi/wi-fi-protected-setup>. Acesso em: 13 set. 2020.

WHITE, C. **Redes de computadores e comunicação de dados**. São Paulo: Cengage Learning, 2012.

WRIGHTSON, T. **Segurança de redes sem fio**: Guia do iniciante. Porto Alegre: Bookman, 2014.