REVISTA CIENTÍFICA TRAJETÓRIA MULTICURSOS
E-ISSN 2178 - 4485

Segurança em redes sem fio: um estudo sobre o nível de conhecimento dos usuários domésticos e as vulnerabilidades que estão expostos

Renan Scheffer Zeferino[1]
Bruno Casagrande Porcher[2]

Resumo: Com o passar dos anos, as redes sem fio vêm sendo cada vez mais utilizadas em todo o planeta, por esse motivo é normal que surjam preocupações com relação à segurança. A partir deste contexto foi desenvolvido um estudo, em primeiro momento composto por pesquisa bibliográfica, abordando as principais tecnologias e ferramentas utilizadas para segurança de rede sem fio, assim como as técnicas de invasão. Em um segundo momento, foi realizada uma pesquisa qualitativa descritiva, por meio de questionário fechado, aplicado a um total de 106 respondentes, com o objetivo de identificar os níveis de conhecimento destes com relação ao tema proposto. A análise dos resultados constatou níveis elevados de conhecimento dos participantes e foi satisfatória em apontar que apesar de cerca de 60% das pessoas ainda não realizarem estudo/mapeamento de suas redes sem fio, mais de 90 % delas reconhecem a importância de investir em segurança.

Palavras-chave: Segurança, redes sem fio, invasão, criptografia.

Abstract: *Over the years, as unprecedented networks have become more widely used around the globe, it is normal for security concerns to surface. From this context, a first study was developed in search of the bibliography, addressing the most important technologies for wireless network security, as well as invasion techniques. Secondly, a descriptive qualitative research was carried out, with a research medium, applied to a total of 106 respondents, in order to identify the levels of knowledge corresponding to the proposed theme. The analysis of the results resulted in a large number of participants and was satisfactory in relation to the previous year.*

Keywords: *Security, wireless networks, invasion, encryption.*

[1] Graduado em Licenciatura em Informática - UNICNEC
[2] Professor Orientador

Introdução

As comunicações por meio de redes sem fio são utilizadas, atualmente, pela maioria das pessoas, objetivando estabelecer conexão por meio de aparelhos domésticos (televisões inteligentes, aparelhos de som, telefones celulares, notebooks e etc.) para navegar pela internet. (FERREIRA, 2013).

Poucos usuários possuem conhecimento quanto ao funcionamento de um Access Point. O AP é um aparelho de rede sem fio, o mais utilizado é o roteador WIFI. Normalmente, funciona desta maneira: colocam-se, dentro das residências, um ou mais APs, dependendo da necessidade, no qual é realizada a configuração de acesso WIFI com uma chave, que pode ser chamada de senha, esta fornece uma determinada segurança para a rede sem fio. (MENDES, 2013.)

As criptografias WIFI são as formas mais comuns de proteção de rede sem fio, dentre elas as mais conhecidas são: WEP, WPA, WPA2, TKIP e AES, que estão disponíveis em vários dispositivos AP, tendo em vista que modelos mais antigos não possuem todas estas criptografias. No entanto, para grandes empresas, que precisam de mais segurança, não é indicada a utilização destas criptografias para a configuração da rede sem fio. Nestes casos são utilizados firewalls, colocados entre o AP e a internet. Cada firewall tem uma configuração própria, normalmente é um servidor no qual é possível fazer diversas restrições de acesso a rede, bloqueando sites e IPs, porém mesmo os firewalls estão suscetíveis a falhas. (CAMPOS, 2006.)

As redes WIFI precisam ser bem gerenciadas e seguras, um AP que teve sua configuração realizada de forma incorreta poderá facilmente ser acessado por outros usuários, sem autorização do proprietário do ponto de acesso. (CAMPOS, 2006.)

O processo de configuração de firewalls apresenta um grau de dificuldade maior do que as criptografias, pois eles precisam ser instalados em um servidor, no qual funcionarão como uma espécie de barreira de segurança. Esses níveis de complexidade que envolvem configurações de proteção as

redes WIFI e as prováveis falhas as quais elas estão expostas são os fatores que levaram a abordagem deste tema para o presente projeto. (SILVA, 2003.)
O objetivo geral deste trabalho foi realizar uma pesquisa sobre segurança de redes sem fio a fim de identificar e exemplificar as falhas mais comuns que podem ocorrer com os usuários de redes WIFI domésticas, pesquisar sobre os níveis de conhecimento dos usuários e compreender a importância que eles atribuem a este tema.
De forma mais específica foi realizada uma pesquisa bibliográfica sobre as principais criptografias WIFI existentes, quais as mais utilizadas, como elas funcionam e o nível de confiabilidade e segurança de cada uma delas. Pesquisou-se também sobre firewalls, quais os mais comuns, como é a relação dele com o AP, como funcionam e o quão seguro eles são. Foram demonstradas as vulnerabilidades das redes sem fio, através da quebra da criptografia de senhas de acesso. Buscou-se também identificar o nível de conhecimento de usuários de redes sem fio domésticas, por meio de questionário, sobre todas as alternativas de segurança citadas anteriormente, a fim de verificar a opinião deles quanto à importância deste tema.

Tecnologias Utilizadas na Segurança de Redes Sem Fio

As redes wireless ou sem fio (WLAN - Wireless Local Area Network), como quase todas as tecnologias disponíveis na atualidade, surgiram por necessidades militares. Eles precisavam de um meio fácil, rápido e seguro de levar informações durante a guerra, logicamente, nesta época, os dados a serem trafegados eram menores e a rede era restrita as forçar armadas. Com o fim da guerra, a internet sem fio foi ganhando espaço em empresas, faculdades e para usuários domésticos, hoje em dia podemos pensar em wireless como uma forma de evitar cabos e deixar o acesso à internet mais prático. (FARIAS, 2005).
WPAN (Wireless Personal Area Network) ou rede pessoal sem fio é utilizada em aparelhos que necessitam de conexão entre um dispositivo e outro sem a

utilização de cabos, como mouse e teclado sem fio, impressoras, telefones móveis, e outros dispositivos. Esses aparelhos citados já possuem a opção de conexão via Bluetooth, outra conexão muito utilizada atualmente é o infravermelho, aplicado em controles de televisão. (BUSCH, 2008).

A NBR ISSO/IEC 17799 (2005) define a Segurança da Informação (SI) como: política de proteção das informações dos usuários contra ameaças, para garantir que o usuário continue a utilizar as redes, de maneira a minimizar os riscos e maximizar o retorno de investimentos. É necessário estabelecer critérios quanto aos níveis de segurança, analisando periodicamente, verificando assim, avanços ou retrocessos no cenário de SI. Para garantir a Segurança da Informação não é suficiente proteger-se somente com antivírus ou barreiras de proteção (firewalls) conectada à rede. Faz-se necessário entender dos princípios de segurança em SI para poder distinguir quais as melhores políticas e soluções que possam atender as necessidades da organização. É importante entender os princípios de SI em um processo de implantação para verificar ferramentas que possam auxiliar os usuários contra possíveis falhas de segurança em sua rede. Este método é conhecido por processo de prevenção e contém duas categorias: prevenção e proteção do SI.

WI-FI consiste em uma tecnologia de rede sem fio embarcada (WLAN), originalmente lançada pela empresa (WI-FI Alliance) e usa como padrão IEEE (Institute of Electrical and Eletronic Enginners) 802.11, estes padrões operam em frequências que não necessitam de licença para instalação e/ou operação, deixando-as assim bem mais atrativas para o comércio. No entanto, segundo o autor, no Brasil é preciso passar por um licenciamento da Agência Nacional de Telecomunicações (Anatel). (MENDES, 2008).

Os principais padrões das redes sem fio são (Miranda, 2013):

a) 802.11a: alcança velocidades de 54 Mbps dentro dos padrões IEEE e de 72 a 108 Mbps quando não padronizados. A frequência utilizada nesta rede é de 5 GHz e inicialmente suporta 64 utilizadores por AP, a principal vantagem

é velocidade e usa frequência sem qualquer interferência. A maior desvantagem é a incompatibilidade com os padrões 802.11b e 802.11g em AP, ou seja, não fazem conexão AP com AP. Porém, aparelhos receptores (telefone móvel, Notebook etc.) com as frequências 802.11b e 802.11g conseguem se conectar a frequência 802.11a.

b) 802.11b: podem chegar a uma velocidade de 11 Mbps nos padrões IEEE, podendo chegar a 22 Mbps, por fabricantes que não utilizam esta padronização, sua frequência 2.4GHz, mais baixa comparada ao padrão 802.11a, suportando 32 utilizadores por AP. Este padrão possui um ponto negativo muito forte que é a alta interferência, tanto na transmissão quanto na recepção de sinais. Como funcionam em uma frequência de 2,4 GHz, existem outros dispositivos, telefones móveis ou sem fio, forno micro-ondas e dispositivos Bluetooth, que utilizam desta mesma frequência, ocasionando as interferências. Seu ponto positivo é o custo, neste tipo de padronização o preço dos dispositivos é baixo comparado ao padrão 802.11a, por este motivo são amplamente utilizados por provedores de internet sem fio.

c) 802.11g: fundado para fazer compatibilidade com os dispositivos 802.11b, com a mesma velocidade de 54 Mbps. Funciona dentro da frequência de 2.4GHz, possui os mesmos inconvenientes do padrão 802.11b (incompatibilidade com dispositivos de diferentes fabricantes). Usa autenticação WEP (Wired Equivalent Privacy) estática.

d) 802.11n: este padrão tem uma velocidade que chega aos 300 Mbps e alcança 70 metros, suas frequências são de 2.4GHz e 5GHz, ligadas em paralelo. É o padrão mais recente com uma nova tecnologia, MIMO (Mutiple Input, Multiple Output), múltiplas entradas e múltiplas saídas, utilizam várias antenas para transferência de dados. Os principais benefícios são o aumento significativo da banda e seu elevado alcance.

Estrutura de camadas no padrão 802.11.

A Figura 1 ilustra as camadas do padrão IEEE 802.11, comparando com o modelo RM-OSI da ISO (Reference Model - Open System Interconnecttion of the International Satandardization Organization). (PUC-RIO, 1998).

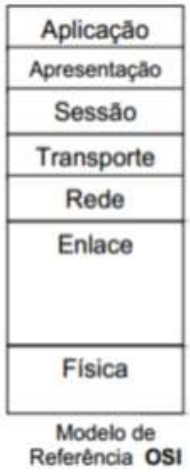

Figura 1- Estrutura de Camadas do padrão IEEE 802.11
Fonte: PUC-RIO, 1998.

Kurose (2010) explica, de maneira mais detalhada, as camadas do modelo OSI:

a) camada física: é responsável por transportar fluxos de bits através de um meio físico. Consiste nas especificações mecânicas e elétricas da interface e do meio de transmissão. Nesta camada que são definidos os procedimentos e funções que cada dispositivo deve executar na transmissão.

- características físicas da interface: define o tipo do meio de transmissão.
- representação em bits: para serem transmitidos, a camada física cria um fluxo de bits (sequência de 0s ou 1s) e codifica em sinais – elétricos ou ópticos.
- taxa de dados: número de bits enviados a cada segundo.
- sincronização de bits: emissor e receptor precisam estar em sincronismo total para a transmissão correta dos bits.

- configuração da linha: é definido o modo de transmissão, seja ele ponto a ponto (conexão direta entre o emissor e o receptor) ou multiponto (conexão compartilhada entre emissor e receptor).
- modo de transmissão: define o sentido da transmissão, sendo eles simplex, half-duplex ou full-duplex. No modo simplex somente um dispositivo pode enviar dados, o outro pode apenas receber, controles de televisões, por exemplo, aperta-se o botão e o televisor recebe. Modo half-duplex, dois dispositivos podem enviar e receber, porém em quanto um dispositivo for o emissor o outro é exclusivamente o receptor, por exemplo, rádio amador, quando alguém fala o outro lado somente recebe e não consegue transmitir. Modo full-duplex neste modo os dois podem receber e enviar ao mesmo tempo, pode-se usar como exemplo, telefones celulares e internet, a grande maioria dos dispositivos usam full-duplex.

b) camada de rede: é responsável por entregar os dados desde sua origem até o seu destino, normalmente por meio de redes (links). Em geral é necessário utilizar conexões entre redes para realizar comunicações.

- endereçamento lógico: nesta camada vai o endereço lógico de cada emissor e do receptor.
- roteamento: trata-se de redes independentes conectadas para criar internetwork (rede de redes) ou uma grande rede. Dispositivos de conexão (chamados de roteadores) encaminham pacotes para o destino.

c) camada de transporte: é responsável pela entrega da mensagem enviada de um host (usuário) por um aplicativo, a camada de transporte garante que a mensagem chegue intacta e na sequência correta. Ela supervisiona, controla erros e faz controle de fluxo no nível origem-ao-destino.

- endereçamento do ponto de acesso ao serviço (service-point addressing): computadores podem executar vários programas ao mesmo tempo, por esta razão a entrega origem-ao-destino não é somente entrega de um computador para outro, e sim 2a entrega de um aplicativo em execução de um computador para um aplicativo em outro. O cabeçalho define onde

iremos mandar está mensagem ou arquivo, neste cabeçalho deve conter o endereço do ponto de acesso ao serviço (também denominado como endereço de porta). Dessa forma, cada pacote é encaminhado corretamente para cada computador.

- segmentação e remontagem: uma mensagem é dividida em vários segmentos para ser transmitida, cada segmento contém um número de sequência, permitindo assim que a camada de transporte remonte a mensagem de forma correta.
- controle de erros: a camada de transporte possui esse sistema de controle de erros, ele é feito processo-a-processo e não em um único link.

d) camada de sessão: é responsável por controlar o diálogo entre as redes, estabelece, sincroniza e mantém a interação entre os sistemas que se comunicam entre si.

- controle de diálogo: estabelece um diálogo entre dois processos, existe o diálogo em modo half-duplex (um sentido por vez), por exemplo um radio amador, quando um usuário fala o outro escuta, não se pode falar ao mesmo tempo. Há também o modo full-duplex (a comunicação é feita simultaneamente) alguns exemplos conhecidos são chats de mensagens como Whtasapp, Facebook, Hangout.
- sincronização: é responsável por verificar se o arquivo está sendo enviado de forma correta, adicionando um ponto de verificação, fazendo uma sincronização do arquivo mesmo antes dele ser completamente enviado, um exemplo é o envio de um livro com muitas páginas, caso não seja realizada a sincronização não é possível saber se o livro chegou completo ao outro lado.

e) camada de apresentação: é responsável por fazer a tradução, criptografia e compressão dos dados.

- tradução: consiste em uma troca de informações entre dois ou mais sistemas em forma de Strings (texto), números etc., estas informações precisam ser convertidas para bits para que possam ser transmitidas. Como computadores utilizam sistemas diferentes de codificação, essa camada é

responsável por trocar informações entre esses sistemas. O emissor traduz as informações para um formato comum e a máquina receptora traduz o formato comum para um formato específico.

- criptografia: serve para transmitir informações com segurança e garantir a privacidade. Criptografar é o ato de converter informações em um formato diferente para enviá-las pela rede, quando chega ao receptor a mensagem é descriptografada, reverte-se o processo deixando o documento como original.
- compressão: serve para diminuir o arquivo, ou seja, diminuir a quantidade de bits enviados, dessa forma um vídeo ou um áudio podem ser enviados de forma mais rápida e com menos consumo de banda de internet.

f) camada de aplicação: habilita o usuário para acessar a rede, possibilita o acesso a interfaces e suporte a serviços como e-mail, transferência de arquivos, gerenciamento de banco de dados e outros tipos de serviços.

Mecanismos de criptografia.

O protocolo WEP age na camada de enlace de dados e tem como base a criptografia RC4 da empresa RSA Data Security, utilizando um vetor de inicialização de 24 bits, tem uma chave secreta compartilhada com mais 104 bits que acabam por se somar criando uma criptografia de 128 bits. Para checar a integridade dos dados criptografados, o protocolo WEP utiliza um CRC-32 para calcular o checksum da mensagem, este processo ocorre nos dois lados da conexão tanto no transmissor quanto no receptor. Existe ainda o protocolo WEP de 64 bits onde a chave pode ser de 40 ou 24 bits, assim a criptografia é diferente do padrão de 128 bits, garantindo duas opções diferentes para tentar obter um nível mínimo de segurança na rede. (CANSIAN et al., 2004 e AMARAL; MAESTRELLI, 2004).

O protocolo WPA também conhecido como WEP2 ou TKIP (Temporal Key Integrity Protocol – protocolo de chave temporária) foi desenvolvido para corrigir problemas relacionados a criptografia WEP, funciona de maneira a

implementar criptografias já utilizadas em outros padrões de segurança como os padrões 802.11. O WPA atua em duas áreas distintas: primeiramente em uma substituição total da criptografia WEP, tendo como objetivo garantir a integridade e a privacidade das informações que trafegam na rede. A segunda forma de atuação é para a autenticação do usuário, nesse caso utiliza-se uma troca dinâmica, que não era feita pelo WEP, troca-se o vetor de inicialização para 48 bits. Para isto o WPA utiliza definições do padrão 802.1x e o EAP (Extensible Authentication Protocol – Protocolo de Autenticação Extensível). (RUFINO, 2005, CANSIAN et al., 2004).

WPA2, foi validado em meados de 2004 e corresponde a versão final do WPA, única diferença entre este e o WPA é a criptografia que mudou de WEB o TKIP (Temporal Key Integrity Protocol) para AES (Asvanced Encryption Standard), mais segura que a TKIP, porém exige mais processamento e algumas placas mais antigas não suportam o WPA2, nem mesmo atualizando o firmware. (SILVA, 2012).

MAC (Media Access Control) - para o funcionamento correto e eficaz na rede, seja ela Ethernet ou Wi-Fi, cada dispositivo (Placas de redes) possuem uma identificação, isto faz com que todos os equipamentos conectados a rede fiquem em uma mesma organização, isto é, tem um número que os identifica para não serem utilizados por outra pessoa, cita-se como exemplo as placas de um carro, cada um tem a sua placa e nenhum outro carro pode ter a mesma. Essa identificação foi definida pelo IEEE, como sendo um número único para cada dispositivo fabricado mundialmente para evitar qualquer conflito ou colisão entre eles. (RUFINO, 2005).

Segurança em Redes sem fio - Dispositivos de redes com tecnologia Wi-Fi tornaram-se uma realidade de acesso a internet para muitas empresas, instituições, hotéis, restaurantes e residências domésticas, no entanto, redes sem fio apresentam muitas vulnerabilidades que tem como origem os padrões adotados.

Redes sem fio são transmitidas em um meio comum acessível a todos que estão dentro do raio de ação da antena de rádio. Assim, caso a rede sem fio não possua uma configuração mínima de segurança, basta o usuário ter um receptor compatível com a tecnologia utilizada, que poderá acessá-la livremente.

Existem vários tipos de ataques a redes sem fio, os mais comuns referem-se à obtenção de informações sem autorização, acesso indevido à rede e ataques de negação de serviço. O nível de dificuldade para realização desses ataques depende da forma de implantação da rede, isto é, para que uma rede sem fio possua as mesmas características de segurança de rede com fio, é necessário à inclusão de mecanismos de autenticação de dispositivos e confidencialidade de dados.

Segurança física - A mesma segurança que uma rede física possui deve ser considerada em uma implementação de rede sem fio. Em uma rede cabeada a segurança é feita por trás de uma porta de entrada (Firewall ou um servidor de autenticação) com a necessidade de um ponto de acesso físico (cabeado) a um equipamento (notebook, computador pessoal ou outros), quando se trata de abrangência de sinal em que o seu alcance será captado a dezenas e centenas de metros, esta preocupação muda. (RUFINO, 2005). Os pontos de acesso Wi-Fi precisam ser posicionados em local que não venha a colidir com possíveis sinais ou barreiras (paredes muito grossas, sinais de outros rádios com a mesma frequência, vidros etc.) para que suas necessidades essenciais possam ser utilizadas: velocidade e desempenho corretos. Para encontrar o posicionamento correto são desenvolvidos vários estudos no ambiente, pois o posicionamento do AP pode evitar ou diminuir a chance de invasão ao sinal. Quando o AP é disposto em um direcionamento correto pode gerar sinal somente para o ambiente onde ele se encontra não dispersando o sinal para seus arredores. (RUFINO, 2005).

Configuração de fábrica - Toda empresa que fábrica um produto procura deixá-lo o mais compatível possível com os dispositivos atuais, para

simplificar sua instalação, para isto deixam muitos recursos de segurança desativados, colocando em risco muitas redes montadas por administradores inexperientes. (RUFINO, 2005). Um grande exemplo citado é o nome do usuário e a senha de acesso padrão em APs e seus endereços IP (Internet Protocol – Protocolo de Internet). Dessa forma, as informações podem ser facilmente encontradas na internet estando assim suscetíveis a sofrer ataques, facilmente, caso estas informações não forem alteradas. (RUFINO, 2005).

Mapeamento - O mapeamento é a primeira ação feita pelos invasores. O invasor precisa conseguir o maior número de informações possíveis da rede que está tentando invadir, assim seu ataque se torna mais preciso e que sua presença demore a ser detectada. Vejamos os dois tipos possíveis de mapeamento:

a) Mapeamento Ativo - usando este tipo de mapeamento é possível identificar equipamentos que estão conectados na rede assim como seu endereço de MAC, assim com estas informações caso haja algum tipo de vulnerabilidade conhecida possa ser usada pelo invasor para invadir a rede. (RUFINO, 2005). Um programa que pode ser usado para realizar o mapeamento ativo é o TCH-rut, que permite identificar os endereços MAC que estão sendo utilizado pelos dispositivos, assim como seu fabricante. Assim para que o ataque seja efetivo o atacante deverá estar participando da rede. Escolhendo um alvo na rede o atacante parte para o ataque direto, utilizando outras ferramentas combinadas, ou isoladas, como por exemplo, o NMAP (Network Mapper – Mapeador de Rede), verifica quais dispositivos estão ativos no momento e efetua uma varredora nas portas abertas no alvo a ser atacado. (RUFINO, 2005).

b) Mapeamento Passivo - método que permite ao atacante mapear as atividades da rede que se está tentando atacar, com a vantagem de não ser percebido. Uma ferramenta utilizada para fazer este mapeamento é o p0f, que necessita apenas que o atacante esteja dentro da área sinal do ponto de

acesso do atacado. Esta ferramenta fornece informações para que o invasor possa selecionar um dos dispositivos conectados à rede possivelmente esteja mais vulnerável, sem ser visto, melhorando as chances de conseguir êxito na invasão. (RUFINO, 2005).

Ferramentas para Redes Sem Fio

Serão descritas, a seguir, de forma simplificada, algumas ferramentas de redes que foram utilizadas nos testes de segurança e intrusão, para demonstrar algumas das vulnerabilidades mencionadas no presente trabalho.
Netstumbler - ferramenta utilizada para scanner de redes sem fio. Incluem-se neste software muitas características como potência do sinal, SSID da rede, além de suporte a GPS. Este programa pode ser utilizado por gerentes de rede para monitorar a qualidade de sinal e quantos dispositivos estão instalados no seu ambiente de rede, porém também podem ser utilizados por usuários maliciosos para atacá-la. Estes fazem uso do método de sondagem ativa da rede, analisando o tráfego dela. (MILNER, 2004).
Kismet - criado em código aberto este aplicativo inclui muitas ferramentas e opções. Projetado como cliente e servidor, monitora uma gama enorme de origens diferentes e armazena pacotes de formatos diferentes. Este software gera dados relacionados à localização aproximada do dispositivo monitorado. Um ponto positivo deste programa é salvar automaticamente todas as redes encontradas, ele disponibiliza quase todas as informações necessárias para um usuário não autorizado desenvolver um ataque. Algumas informações que o KISMET consegue obter são: número de WLANs detectadas, número total de pacotes capturados por WLAN, existência ou não de criptografia WEP, número de pacotes irreconhecíveis, número de pacotes descartados e tempo decorrido durante a execução do programa. (KERSHAW, 2016).
Kali - criado em código aberto este sistema operacional possui diversas ferramentas avançadas para penetração e auditoria de segurança de rede. Kali Linux foi lançado em 13 de março de 2013 e é uma reconstrução completa

do BackTrack Linux, possui mais de 600 ferramentas de testes de penetração. (AHARONI; KEARNS; HERTZOG, 2010). Está ferramenta foi utilizada para simular uma invasão em uma rede criptografada em modo WEP.

Técnicas de Invasão

A facilidade de acesso que os dispositivos sem fio proporcionam para usuários e empresas é enorme, logo segurança de rede deveria ser prioridade, porém nem sempre isto acontece, acabam por dar prioridade somente ao desempenho, não adotando uma configuração adequada de segurança e criptografia para obter confiabilidade de transmissão de dados em redes sem fio. Devido à falta de preocupação com a segurança nas redes sem fio, muitos usuários e empresas utilizam equipamentos com configuração de fábrica (Default), isso se dá pela má informação que algumas vezes são passadas para o consumidor final. (RUFINO, 2005).

Segundo Rufino (2005), as principais técnicas de invasão são:

a) interrupção: nesse procedimento o invasor influi interrompendo as passagens de dados de um ponto para outro.

b) interseção: nesse procedimento o invasor realiza coleta de informações para saber o que se passa dentro da rede e ter acesso a ela futuramente.

c) modificação: nesse procedimento o invasor não apenas escuta o tráfego de rede, mas também modifica e compromete os dados para depois enviá-los para o dispositivo que está sendo atacado. O objetivo é que este se torne um dispositivo zumbi e o invasor tenha total controle.

d) fabricação: nesse caso, o invasor desenvolve os dados a serem enviados para um determinado destino com o intuito de se obter acesso a rede sem fio.

Quando um invasor descobre uma rede sem fio mal configurada, ele pode utilizar softwares maliciosos (Scanners) que capturam os pacotes de dados com o intuito de obter o SSID e a chave de acesso. O atacante pode

se passar por um membro da rede sem fio e assim ter permissão para executar tarefas como se fosse um usuário normal. (RUFINO, 2005).

Inicializando o Kali Linux

Para a utilização do Kali Linux basta baixá-lo e colocá-lo em um DVD ou um pendrive com sistema de inicialização ativa, logo após iniciar o computador por um destes dois instrumentos. Para download do Kali Linux, acessar o link: https://www.kali.org/downloads/.

Demonstração de quebra de senha com Kali Linux:

Primeiramente deve-se identificar a placa de rede sem fio abrindo o terminal e digitando o comando “iwconfig”, esta ferramenta é a responsável por listar os dispositivos de redes disponíveis no computador.

Logo após, alterar a placa de rede sem fio de modo receptor (recebendo algum sinal) para modo monitor (monitorar os dados trafegados na rede), para isto é necessário abrir o terminal e digitar o comando “airmon-ng start wlan0”. Verifica-se que a rede wlan0 foi alterada para monitoramento ficando com o nome de wlan0mon. Próximo passo será buscar por redes sem fio que estão ao alcance do receptor em modo monitor usando o comando “airodump-ng wlan0mon”.

Pode-se verificar que se encontram várias informações como BSSID, PWR, CH, ENC e ESSID, onde BSSID refere-se ao nome físico de cada aparelho de rede sem fio, PWR é a intensidade do sinal, CH é o canal que ele se encontra, ENC é a criptografia utilizada pela rede e o ESSID é o nome criado pelo usuário para a rede sem fio. Neste caso, serão utilizadas as informações referentes ao ESSID “Seila”, para isto será utilizado um comando onde serão salvas as informações do que acontece nesta rede sem fio.

O comando “airodump-ng –bssid” (refere-se à rede) -w (nome com o qual o documento será salvo) -c (canal da rede sem fio)”. Por fim, a rede de monitoramento, o comando ficará da seguinte forma, “airodump-ng --bssid F8:D1:11:24:C2:AE –w senha –c 8 wlan0mon”.

Após executar o comando citado acima serão encontradas algumas informações referentes aos aparelhos conectados no roteador que se quer invadir, próximo passo será derrubar um usuário que já está conectado para, logo após, quando este reconectar-se ao aparelho será possível captar o pacote onde se encontra a senha criptografada. O comando a ser utilizado é o seguinte: aireplay-ng -3 –b (BSSID da rede atacada) –h (BSSID do usuário a ser derrubado) e a rede de monitoramento. O comando ficará assim:
aireplay-ng -3 –b F8:D1:11:24:C2:AE –h F4:EC:38:ED:11:A9 wlan0mon.
Após a execução do comando, serão capturados vários pacotes que virão da rede que está sendo invadida. O próximo passo é pegar estes pacotes que estão sendo salvos no arquivo e usar outro comando para encontrar a senha, como no exemplo: aircrack-ng (nome do arquivo -01.cap). O comando final ficará assim: aircrack-ng senha-01.cap.
A senha estará no campo “KEY FOUND!”, é necessário apenas retirar os dois pontos entre os números e a senha ficará 9988669988.
Conforme a demonstração realizada pôde-se comprovar que senhas com criptografia WEP são facilmente descobertas. Nesta simulação, a senha de um roteador configurado em WEP foi desvendada em aproximadamente 5 minutos. Sendo assim, é possível afirmar que a utilização desta rede não é aconselhável, recomenda-se a configuração de roteadores com a criptografia mais atualizada, a WPA2.

Caminhos metodológicos

Para o presente trabalho utilizou-se como método, a pesquisa bibliográfica exploratória. A pesquisa bibliográfica, de acordo com Macedo (1994), consiste na busca de informações, seleção de documentos que se relacionam com o problema de pesquisa, como livros, enciclopédias, artigos de revistas, trabalhos de congressos, teses etc., e o respectivo fichamento das referências para que sejam posteriormente utilizadas (na identificação de material referenciado ou na bibliografia final). Segundo o autor, a revisão bibliográfica

é uma espécie de “varredura” do que existe sobre um assunto e o conhecimento dos autores que tratam desse assunto, a fim de que o pesquisador não reinvente os conceitos.

Complementarmente, a pesquisa exploratória é realizada quando há pouco conhecimento sobre o tema, neste tipo de pesquisa não é necessário formular hipóteses a serem testadas, o seu objetivo é apenas buscar informações sobre determinado assunto. (CERVO; BERVIAN; DA SILVA, 2007).

A pesquisa, em um primeiro momento, no projeto de pesquisa, TC I, realizada no segundo semestre de 2017, foi inteiramente bibliográfica, com o intuito de pesquisar sobre o tema segurança de redes Wi-Fi. Em um segundo momento, para o Trabalho de Conclusão de Curso fase II, elaborado no primeiro semestre de 2018, foi realizada uma pesquisa qualitativa sobre o mesmo tema. Nesta pesquisa foram coletados os dados por meio de questionário qualitativo fechado disponibilizado via GoogleDocs.

Objetivou-se que a pesquisa fosse respondida pelo maior número de pessoas possível, desde que elas fossem usuárias de redes sem fio. Dessa forma, o link de acesso ao questionário foi divulgado nas mais diversas redes sociais, Facebook, Youtube, Twitch e whatsApp.

Para este projeto foi utilizado, como método de coleta de dados, questionário criado em GoogleForms. Este formulário é composto por perguntas relacionadas à segurança de rede sem fio, com base nas respostas obtidas foi realizada uma análise descritiva dos resultados. Segundo Afonso (2002) o principal objetivo de uma análise descritiva é resumir, sumarizar e explorar o comportamento dos dados.

Com base nas informações que surgiram a partir dos formulários preenchidos, foi possível demonstrar quais os níveis de conhecimento dos usuários em relação à segurança de rede sem fio, e, em contrapartida, quais são as maiores preocupações dos mesmos em relação a este tema.

Análise dos Resultados

Esta análise pretende apontar os resultados obtidos por meio do questionário qualitativo aplicado em uma amostra aberta disponível via internet, onde foram obtidas 106 respostas.

Quanto à idade dos participantes constatou-se que 13,2 % deles têm menos de 20 anos, 63,2% têm de 20 a 30 anos, 13,2% têm de 30 a 40 anos, 4,7% têm de 40 a 50 anos e 5,7 % têm de 40 a 50 anos. Quando questionados sobre o uso de redes sem fio como forma de acesso à internet, 70,8% dos respondentes afirmaram utilizar redes móveis “3g” e WIFI, 27,4 % declararam utilizar somente WIFI, 0,9% afirmaram usar apenas redes móveis “3g” enquanto 0,9% declararam não fazer uso. Quando questionados sobre possuir redes sem fio em casa, 95,3% dos usuários afirmaram que possuem e 4,7% não possuem. Na questão que tratava sobre seus conhecimentos quanto às configurações básicas de segurança da sua rede (Criptografias, Configurações de IP estático e dinâmico, criação de um novo nome de rede), 40,6 % dos usuários afirmaram conhecer, enquanto 39,6% responderam desconhecer totalmente e 19,8% acreditam conhecer totalmente.

Na pergunta: “o seu roteador WIFI possui senha? Qual o número de caracteres?” 7,5% dos participantes não responderam, 37,7 % deles afirmaram utilizar de 0 a 8 caracteres, 51,9 % responderam utilizar de 8 a 16 caracteres e 2,8 % mais de 16 caracteres. Ao serem questionados se uma senha pequena com caracteres especiais pode ser mais forte que uma senha com mais dígitos alfanuméricos, 23,6% dos usuários afirmaram não acreditar, 43,4% acreditam e 33% acreditam totalmente.

Diante da informação de que muitos aparelhos de rede sem fio têm suas configurações padrão de fábrica, com um nome de rede padrão e totalmente sem senha, 20,8% dos participantes afirmaram não ter conhecimento desta informação, 39,6% têm conhecimento e 39,6% têm total conhecimento. Quando questionados se tinham conhecimento de que sua rede sem fio pode ser vista ou até mesmo utilizada por outros usuários sem sua autorização, 12,3% responderam não ter conhecimento, 51,9% afirmaram ter

conhecimento, enquanto 35,8% acreditam ter total conhecimento. Quando questionados se realizaram um estudo/mapeamento antes de colocar sua rede sem fio em funcionamento, 66% afirmaram não ter realizado, 29,2% realizaram um estudo básico e 4,7% realizaram total mapeamento.

Quando questionados sobre a importância de mapear a rede para não ter sinal maior que o necessário, 28,3% dos usuários afirmaram não considerar importante, 51,9% deles consideram importante e 19,8% consideram muito importante. Ao serem questionados sobre a importância de investir em segurança de rede sem fio 9,4% dos participantes afirmaram não considerar importante, 56,6% deles consideram importante e 34% consideram muito importante.

Ao relacionar as respostas é possível chegar as seguintes considerações:

a) Tendo em vista que 63,2% dos respondentes possuem entre 20 e 30 anos, 13,2% possuem menos de 20 anos, 13,2 % de 30 a 40 anos, 4,7% entre 40 e 50 anos e 5,7% mais de 50 anos, faz-se possível acreditar que pelo fato da maioria deles (cerca de 90%) ter 40 anos ou menos, explica-se o fato de apenas 1,8% não utilizarem redes sem fio como meio de acesso a internet e 4,7% não possuírem redes sem fio em suas casas.

b) Aproximadamente 60% dos participantes responderam conhecer as configurações básicas de segurança da sua rede sem fio, esses são os mesmos 60% dos usuários que afirmam possuir uma senha de mais de 8 caracteres em seu roteador. O índice de usuários que têm conhecimento de que uma senha menor com caracteres especiais pode ser mais forte do que uma senha maior composta apenas por caracteres alfanuméricos é também muito semelhante aos anteriores, cerca de 70%. No entanto, obteve-se um percentual de 39,6% que não conhecem as configurações básicas da sua rede e 23,6% também não conhecem a informação sobre a maior “força” da senha de caracteres especiais em relação à de dígitos alfanuméricos, esses resultados podem estar relacionados com a idade, pois 25% dos respondentes têm menos de 20 ou mais de 40 anos.

c) Aproximadamente 60% dos respondentes têm conhecimento de que seu aparelho vem de fábrica com uma configuração padrão totalmente sem senha e quase 90% têm conhecimento de que sua rede pode ser vista ou até mesmo acessada por outros usuários sem seu consentimento. Além de cerca de 70% considerarem importante realizar mapeamento de rede para que ela não tenha um alcance maior do que o necessário e mais de 90% julgarem importante investir em segurança de rede, ainda assim 66% dos usuários nunca realizaram um estudo ou mapeamento de sua rede sem fio, fato muito contraditório, pois demonstra que mesmo havendo conhecimento ainda não há a devida preocupação.

Considerações finais

Este estudo teve como objetivo investigar o nível de conhecimento dos usuários com relação e redes sem fio. Buscou-se identificar as preocupações dos usuários com relação à segurança e, mais do que isso, obter dados sobre seus conhecimentos a respeito do tema.

Dessa forma foi realizada uma pesquisa qualitativa, descritiva, por meio de um questionário estruturado, aplicado no mês de junho de 2018, a uma amostra total de 106 respondentes.

Os resultados obtidos demonstram que a maior parte dos participantes da pesquisa tem até 40 anos (cerca de 90%), esse fator foi de grande relevância quanto às demais respostas, pois cerca de 90% deles faz uso de redes sem fio, seja por meio de WIFI ou “3g”, mais de 95% possui rede sem fio em casa e dentre eles aproximadamente 60% têm conhecimento das configurações básicas de segurança das suas redes. Além disso, mais de 50% dos respondentes utilizam senhas com mais de 8 caracteres e aproximadamente 80% têm conhecimento de que os aparelhos de rede sem fio vêm com configurações de fábrica padrão e sem senha.

Mais de 85% dos usuários sabem que sua rede pode ser vista ou até mesmo utilizada sem autorização, logo cerca de 70% deles acreditam ser importante

realizar mapeamento para reduzir o alcance da mesma somente ao espaço necessário, assim como mais de 90% deles afirmaram considerar importante investir em segurança de rede.

Chamou atenção a compreensão dos respondentes quanto à importância da segurança de rede sem fio, apenas 9,4% deles não acreditam ser necessário investir em segurança. No entanto um ponto negativo também foi notado, apesar de aproximadamente 70% dos participantes considerarem importante realizar mapeamento de rede, 66% deles não o fizeram antes da instalação em suas residências.

Diante disso, entende-se que o objetivo foi alcançado, pois foi possível obter, conhecer e descrever acerca da percepção dos questionados quanto ao tema proposto. Este trabalho além de instigar os usuários a refletirem sobre segurança de redes sem fio, foi importante no sentido de apontar os riscos aos quais estão expostos sempre que acessam esse tipo de rede.

Dentre as limitações deste trabalho destaca-se a dificuldade de encontrar autores com um conhecimento mais profundo sobre o tema. Dito isso, sugere-se para pesquisas futuras, aprofundar os assuntos abordados o referencial teórico a fim de ampliar ou acrescentar conceitos a respeito deste tema.

Referências bibliográficas

AHARONI, Mati .et al. Distribuição Kali Linux, Disponível em: https://www.kali.org/about-us/ - Acessado em 20/06/2018.

AFONSO, Edna, Análise Descritiva de Dados, Disponível em: http://www.est.ufmg.br/portal/arquivos/rts/rte0202.pdf acessado em 21/06/2018.

BUSCH, Jade, Wired ou Wirelles, 2008, Disponível em: http://jaderedes.blogspot.com.br/2008/11/wired-ou-wireless.html - Acessado em 11/09/2018.

CAMPOS, André. L. N. Sistema de Segurança da Informação: Controlando os Riscos. Florianópolis: Editora Visual books, 2006.

CERVO, Amado L.; BERVIAN, Pedro A.; DA SILVA, Roberto. Metodologia científica. 6 ed. São Paulo: Pearson, 2007.

FARIAS, Paulo César Bento, Rede Wireless, 2005, Disponível em: http://www.juliobattisti.com.br/tutoriais/paulocfarias/redeswireless001.asp - Acessado em 11/09/2018.

FERREIRA, Jeferson Luiz Miranda Segurança em Redes sem Fio. 2013. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

KERSHAW, Mike. Aplicação Kismet, Disponível em: https://www.kismetwireless.net/documentation.shtml - Acessado em 20/06/2018.

KUROSE, Ross, REDES DE COMPUTADORES E A INTERNET. Uma abordagem top-down. 5. ed. São Paulo: Addison Wesley, 2010.

MACEDO, Neusa Dias de. Iniciação à pesquisa bibliográfica: guia do estudante para a fundamentação do trabalho de pesquisa. 2 ed, São Paulo: Edições Loyola, 1994.

MENDES, Osvane, Wi-Fi, 2009, Disponível em: http://osvanewireless.blogspot.com.br/2009_08_01_archive.html - Acessado em 12/09/2018.

MENDES, Douglas R. Redes de Computadores: Teoria e prática. SP: Novatec Editora, 2007.

MIRANDA, Antônio, Redes Wi-Fi 802.11 o que é?, 2013, Disponível em: http://antoniomjf.wordpress.com/2013/08/24/redes-wi-fi-802-11-o-que-e-e-seuspadroes/- Acessado em 12/09/2018.

MILNER, Marius. Aplicação Kismet, Disponível em: http://netstumbler.com - Acessado em 20/06/2018.

PUC-RIO, 1998, Certificação Digital, Padrão IEEE 802.11, Disponível em: http://www2.dbd.puc-rio.br/pergamum/tesesabertas/0210420_05_cap_02.pdf - Acessado em 12/09/2018.

RUFINO, Nelson Murilo de O. Segurança em redes sem fio. 2. Ed. São Paulo: Novatec, 2005.

SILVA, Luiz Antonio F. da, DUARTE, Otto Carlos M. B. RADIUS em Redes sem Fio. Universidade Federal do Rio de Janeiro. RJ – 2003. Disponível em: http://www.gta.ufrj.br/seminarios/CPE825/tutoriais/lafs/RADIUS_em_Redes_sem_Fio.pdf - Acessado em 05/10/2018.